Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2 Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to support Completel UCM Service - Issue 1.0

Abstract

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

2. General Test Approach and Test Results

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

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 PSTN phones using the SIP Trunk provided by Completel, calls made to SIP and H.323 telephones at the enterprise
- Outgoing calls from the enterprise site completed via Completel to PSTN destinations, calls made from SIP and H.323 telephones
- Calls using the G.711A and G.729 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 Completel requiring Avaya response and sent by Avaya requiring Completel response

2.2. Test Results

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

- Calls to busy destinations were handled by the network using a backwards transmission path to play an announcement as opposed to sending “486 Busy Here” to the enterprise.
- Calls to unassigned numbers were handled by the network using a backwards transmission path to an announcement as opposed to sending “404 Not Found” to the enterprise.
- When there were no matching codecs on outgoing calls, the network sent an SDP answer with T.38 instead of rejecting the call with “488 Not Acceptable Here”. The SDP answer was rejected by the CM so the issue has limited impact.
- RFC 2833 was not used by the network to handle DTMF on test calls to international destinations. DTMF was successfully tested on calls between the enterprise and national destinations.
- Ringback was not heard on calls forwarded to international destinations. Call forwarding to national destinations was tested successfully.
- On incoming fax calls, the enterprise correctly sent a re-INVITE to change the codec to T.38. However the network also sent a re-INVITE which was rejected by the network with a “491 Request Pending - another fax request in progress”. The network cleared the call when it received this message. This was resolved by using the SBC to change the 491 response to a 200 OK.
- Test fax calls to international destinations failed. They were successfully tested to national destinations.
- EC500 Confirmed answer calls were not successful. Although broken dial tone was heard, the connection was not made when the digits were pressed on the mobile phone.
- When the trunk was busy and 500 Service Unavailable (Signaling Resources Unavailable) sent from the CM, the network re-attempted the call a number of times resulting in a delay before a tone was heard.
- When the signalling link was out of service and 500 Service Unavailable (Signaling Resources Unavailable) sent from the Enterprise, the network re-attempted the call a number of times resulting in a delay before a tone was heard.

2.3. Support

For technical support on Completel products please visit the website at www.completel.fr or contact an authorized Completel representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Completel UCM service. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Flare Experience (audio only), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone running on a laptop PC configured for SIP.

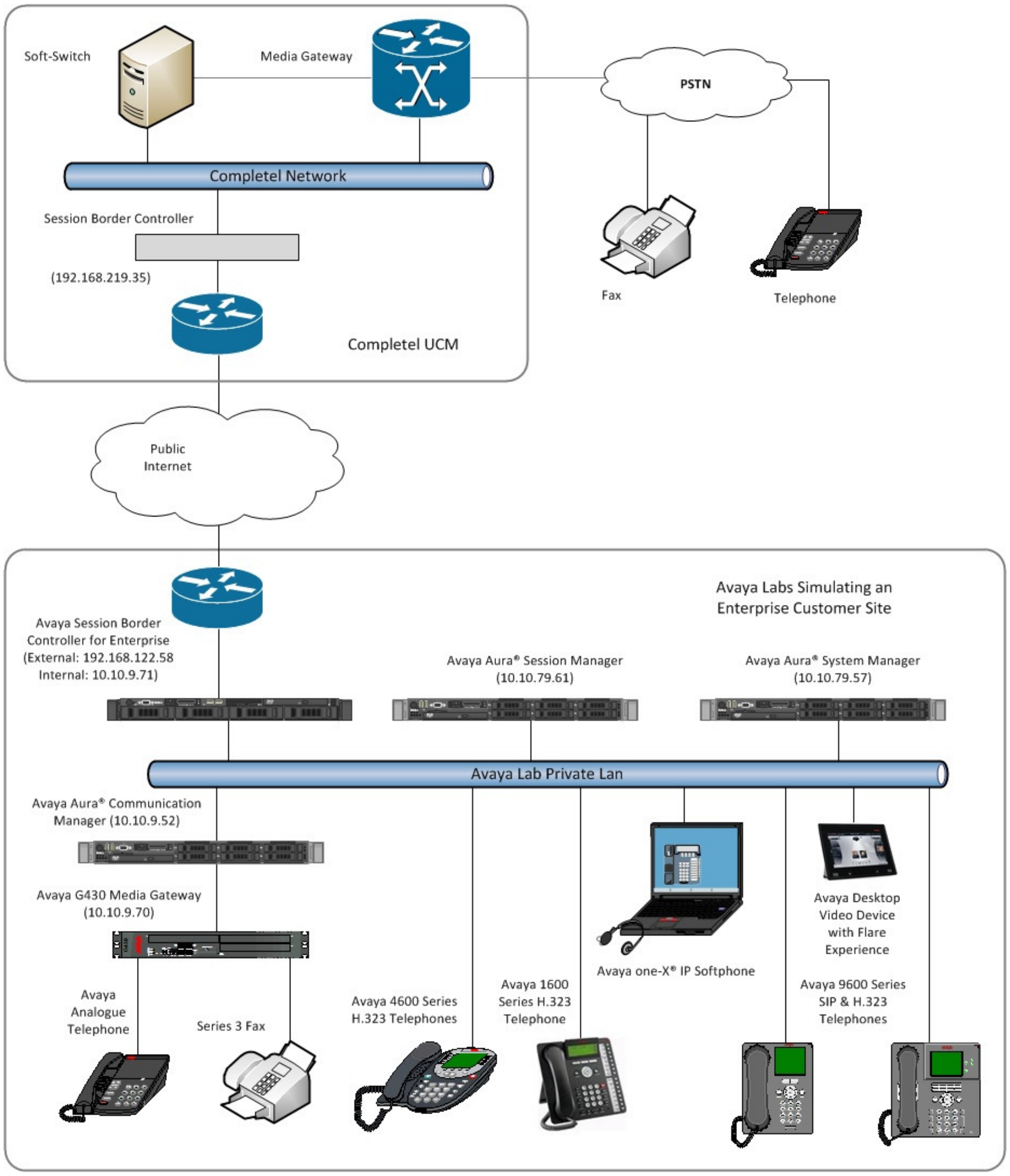

Soft-Switch
Media Gateway
PSTN
Completel Network
Session Border Controller
(192.168.219.35)
Fax
Telephone
Completel UCM
Public Internet
Avaya Labs Simulating an Enterprise Customer Site
Avaya Session Border Controller for Enterprise (External: 192.168.122.58 Internal: 10.10.9.71)
Avaya Aura® Session Manager (10.10.79.61)
Avaya Aura® System Manager (10.10.79.57)
Avaya Lab Private Lan
Avaya Aura® Communication Manager (10.10.9.52)
Avaya G430 Media Gateway (10.10.9.70)
Avaya Desktop Video Device with Flare Experience
Avaya one-X® IP Softphone
Avaya Analogue Telephone
Series 3 Fax
Avaya 4600 Series H.323 Telephones
Avaya 1600 Series H.323 Telephone
Avaya 9600 Series SIP & H.323 Telephones

Figure 1: Test Setup Completel UCM to Avaya Enterprise

4. Equipment and Software Validated

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

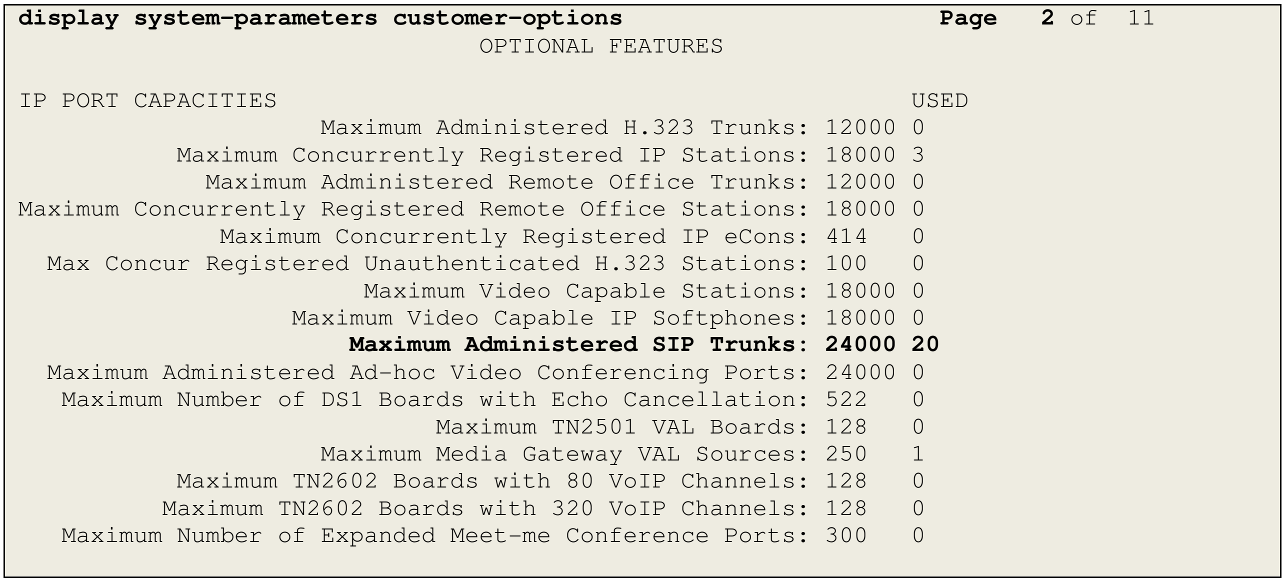
Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Session Manager on VM Version 8	SM-6.3.2.0.632023-e50-00
Dell PowerEdge R620 running System Manager on VM Version 8	SMGR-6.3.0.8.5682-e50-64 (Build 5682)
Avaya S8800 Server running Communication Manager	R016x. 02.0.823.0-20199 (R6.2 SP4)
Avaya Session Border Controller Advanced for Enterprise Server	6.2.0.Q48
Avaya 1616 Phone (H.323)	1.302
Avaya 4621 Phone (H.323)	2.902
Avaya 96x0 Phone (H.323)	3.200
Avaya A175 Desktop Video Device (SIP)	Flare Experience Release 1.1.2
Avaya 9630 Phone (SIP)	R2.6 SP9
Avaya 9608 Phone (SIP)	R6.2 SP1
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.8.06-SP8-40314
Analogue Handset	NA
Analogue Fax	NA
Completel	
ACME Net-Net 4500 SBC	SCX6.2.0 MR-5 GA (Build 777)
Cirpack Softswitch	v4.2J14

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 Completel UCM service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC 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 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 Completel 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.

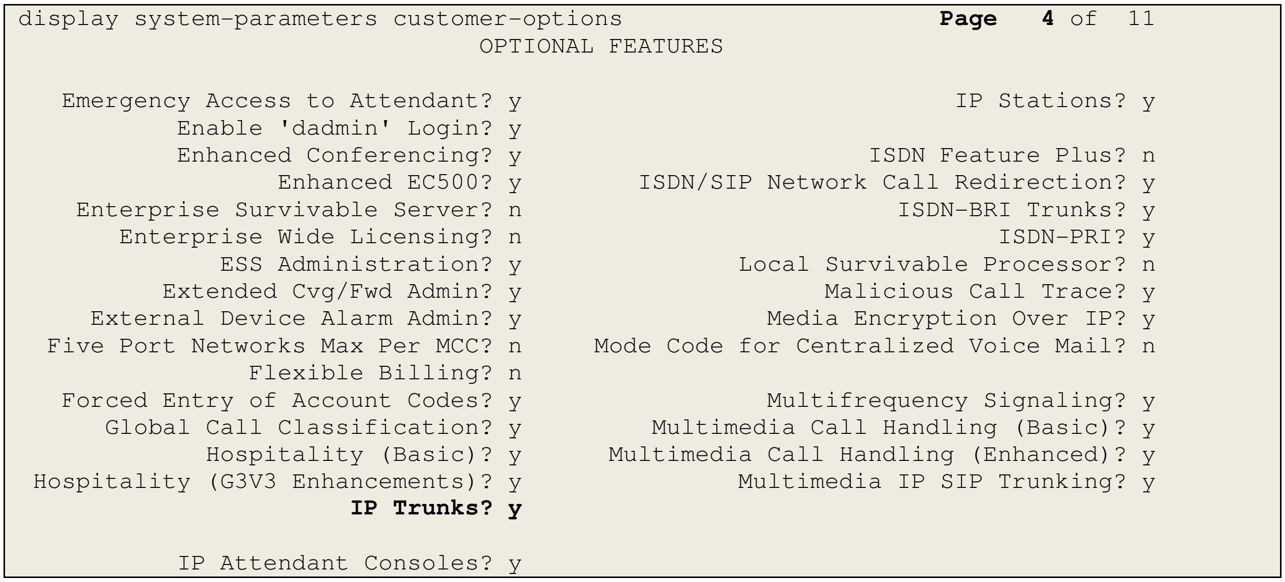
5.1. Confirm System Features

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 Completel network, and any other SIP trunks used.



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

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

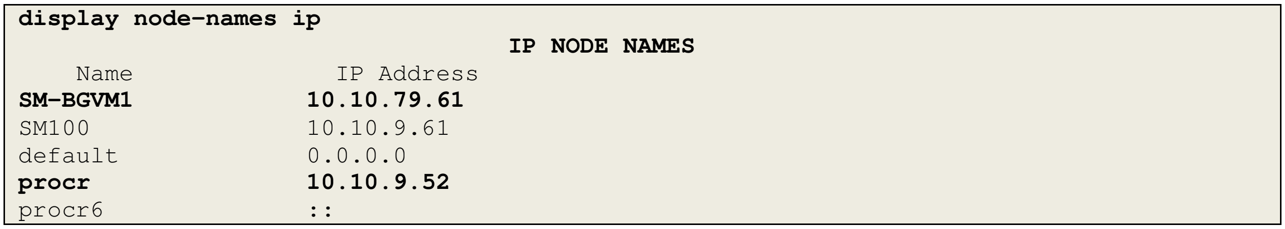
On **Page 4**, verify that **IP Trunks** field is set to **y.**



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

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? 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, **SM-BGVM1** and **10.10.79.61** 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
SM-BGVM1            10.10.79.61
SM100               10.10.9.61
default             0.0.0.0
procr               10.10.9.52
procr6              ::
```

5.3. Administer IP Network Region

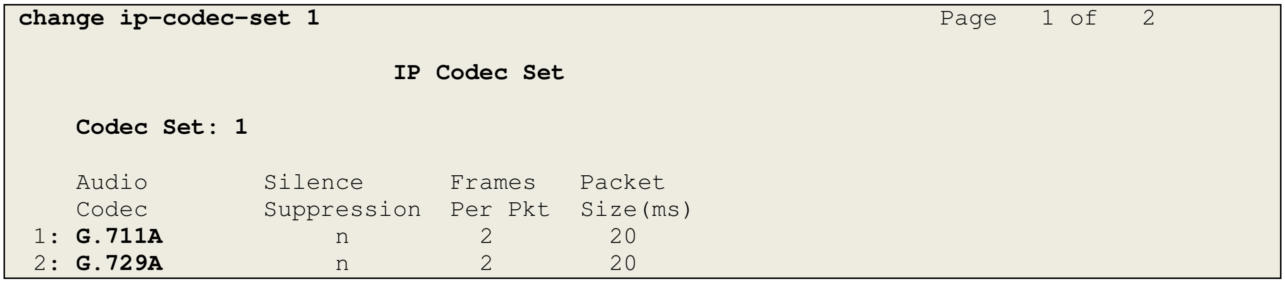
Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the SIP domain name configured on Session Manager. In this configuration, the SIP domain name is **trusted.voip.completel.fr**.
- 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.
- The UDP port values used for the RTP media stream are defined by **UDP Port Min** and **UDP Port Max**, during test these were set to values other than the default values, namely **10000** and **10201** respectively. Normally these can be left at default values.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: trusted.voip.completel.fr
    Name: default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 10000                     IP Audio Hairpinning? n
   UDP Port Max: 10201
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
```

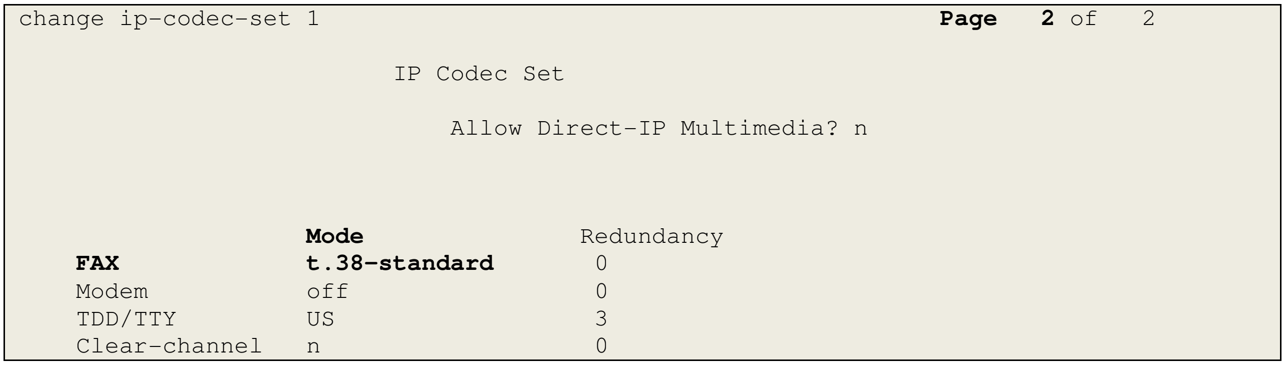
5.4. Administer IP Codec Set

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 Completel were configured, namely **G.711A** and **G.729A**.



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

                          IP Codec Set

    Codec Set: 1

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

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



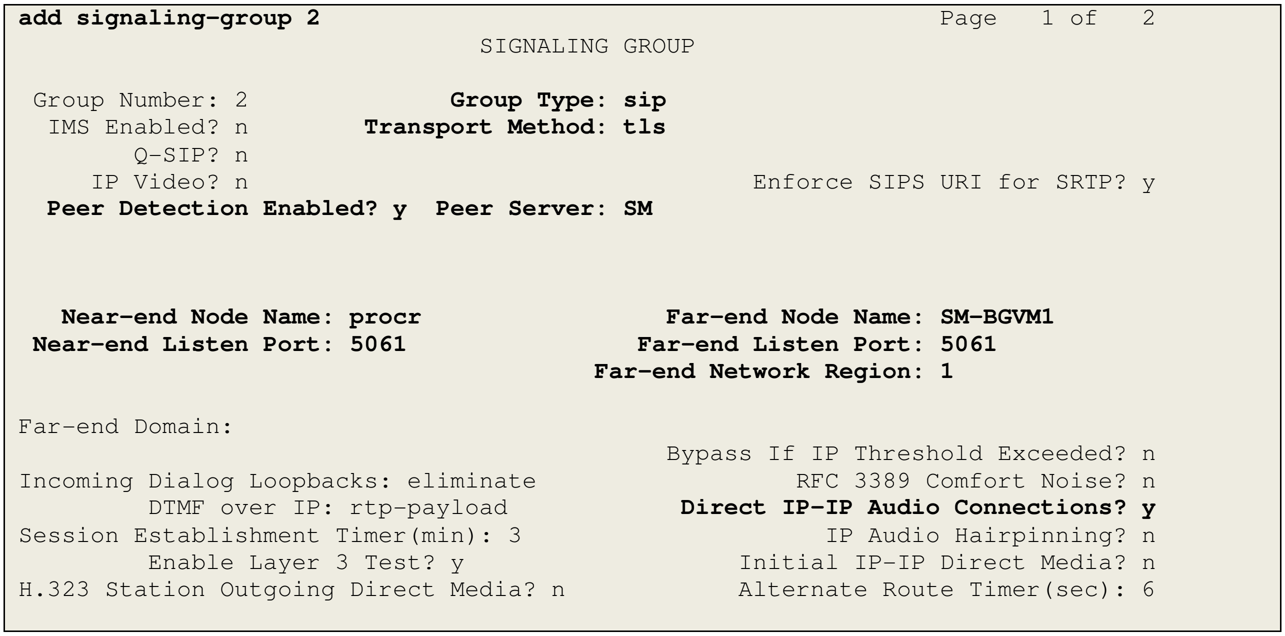
```
change ip-codec-set 1                                           Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



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

5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Completel UCM service. During test, this was configured to use TLS (Transport Layer Security) and the default TLS port of 5061 which is recommended for security.However, if tracing and fault analysis is required it may be more convenient to use TCP and port 5060. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tls**
- Set **Peer Detection Enabled** to **y** allowing 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 **SM-BGVM1** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5061** (commonly used TLS 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 Communication Manager 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 Communication Manager)

The default values for the other fields may be used.



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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tls
      Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM-BGVM1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

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

5.6. Administer SIP Trunk Group

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

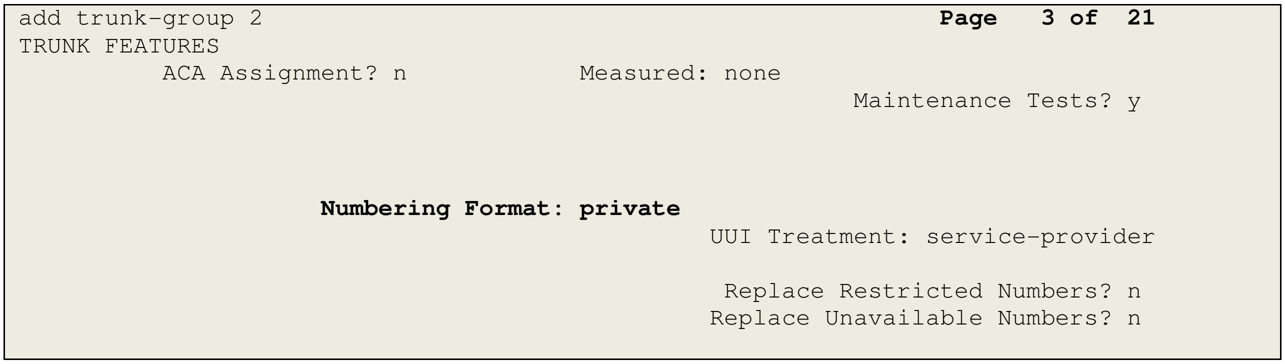
- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-netwrk**
- Specify the signalling 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 2                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip            CDR Reports: y
  Group Name: VM SM                       COR: 1        TN: 1        TAC: 102
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     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 Completel to prevent unnecessary SIP messages during call setup.

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

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

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

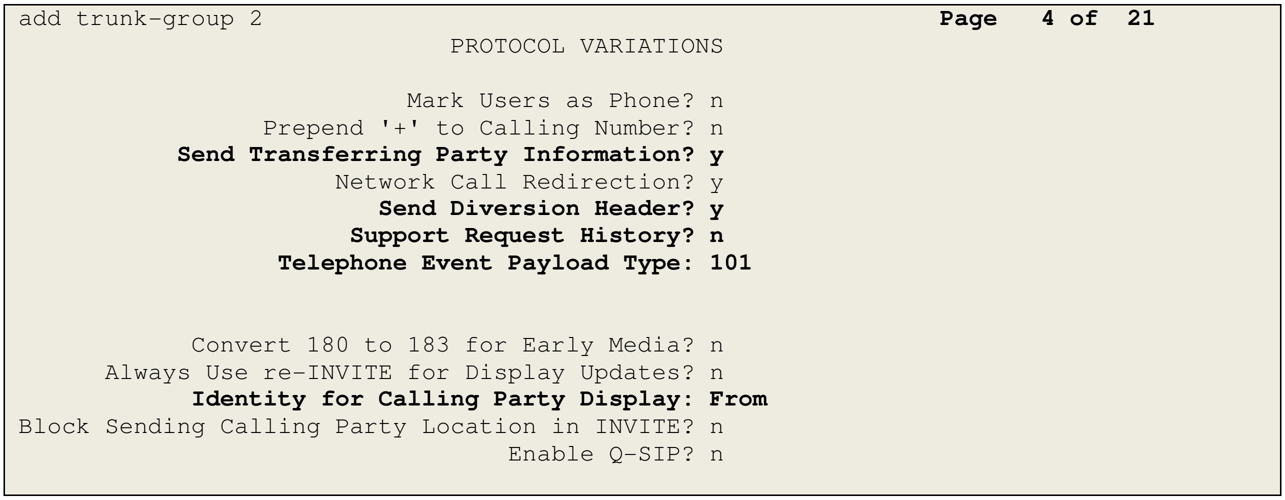
On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of Calling Line Identity (CLI) with leading zeros and without a “+” prefix.



```
add trunk-group 2                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

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

On **Page 4** of this form:

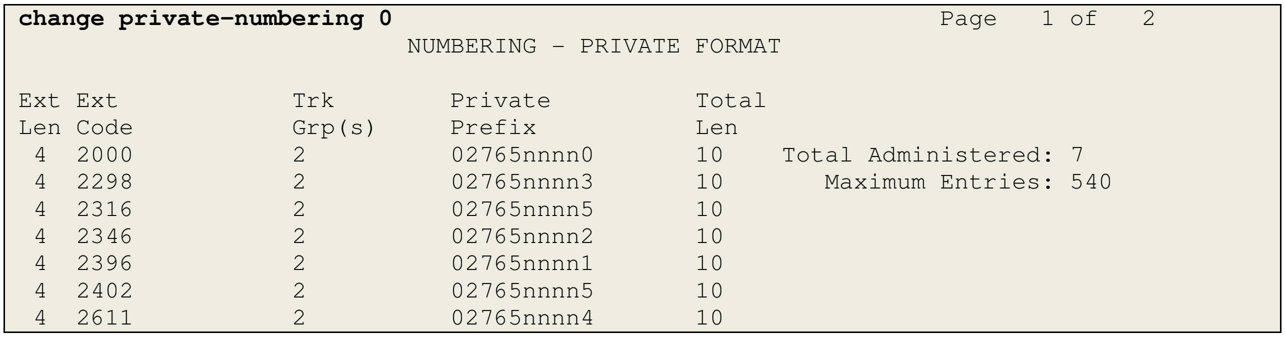
- Set **Send Transferring Party Information** to **y**
- Set **Send Diversion Header** to **y**
- Set **Support Request History** to **n** as this is not required by the Service Provider
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Completel (this Payload Type is not applied to calls from SIP end-points)
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension



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

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


            Convert 180 to 183 for Early Media? n
      Always Use re-INVITE for Display Updates? n
            Identity for Calling Party Display: From
Block Sending Calling Party Location in INVITE? n
                                  Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

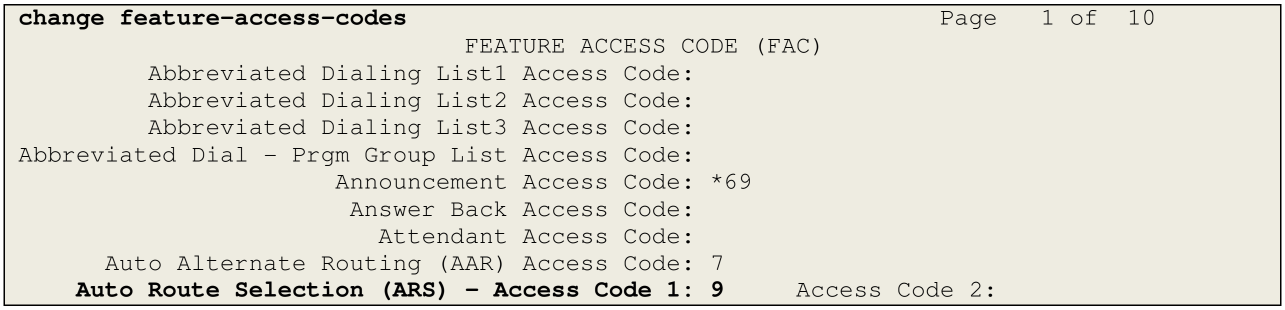
Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number in national format with leading zero. In the test configuration, individual stations were mapped to send numbers allocated from the Completel Direct Dial-In (DDI) range supplied. This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



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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  2000             2          02765nnnn0       10    Total Administered: 7
 4  2298             2          02765nnnn3       10       Maximum Entries: 540
 4  2316             2          02765nnnn5       10
 4  2346             2          02765nnnn2       10
 4  2396             2          02765nnnn1       10
 4  2402             2          02765nnnn5       10
 4  2611             2          02765nnnn4       10
```

5.8. Administer Route Selection for Outbound Calls

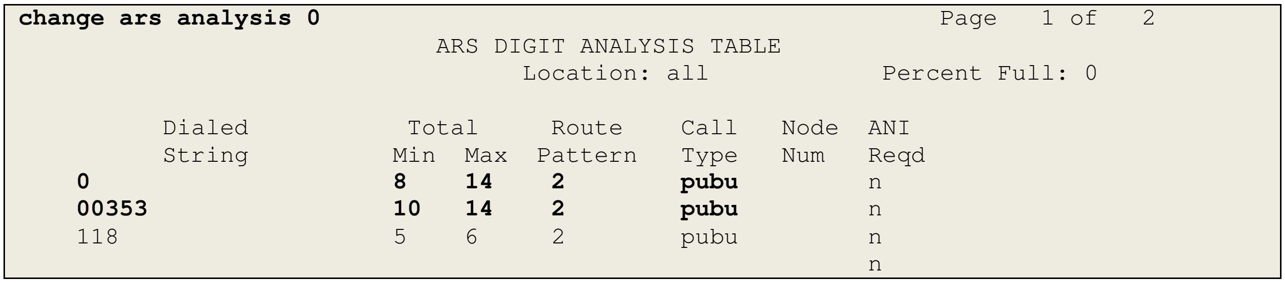
In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to the Completel UCM service. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** 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:
```

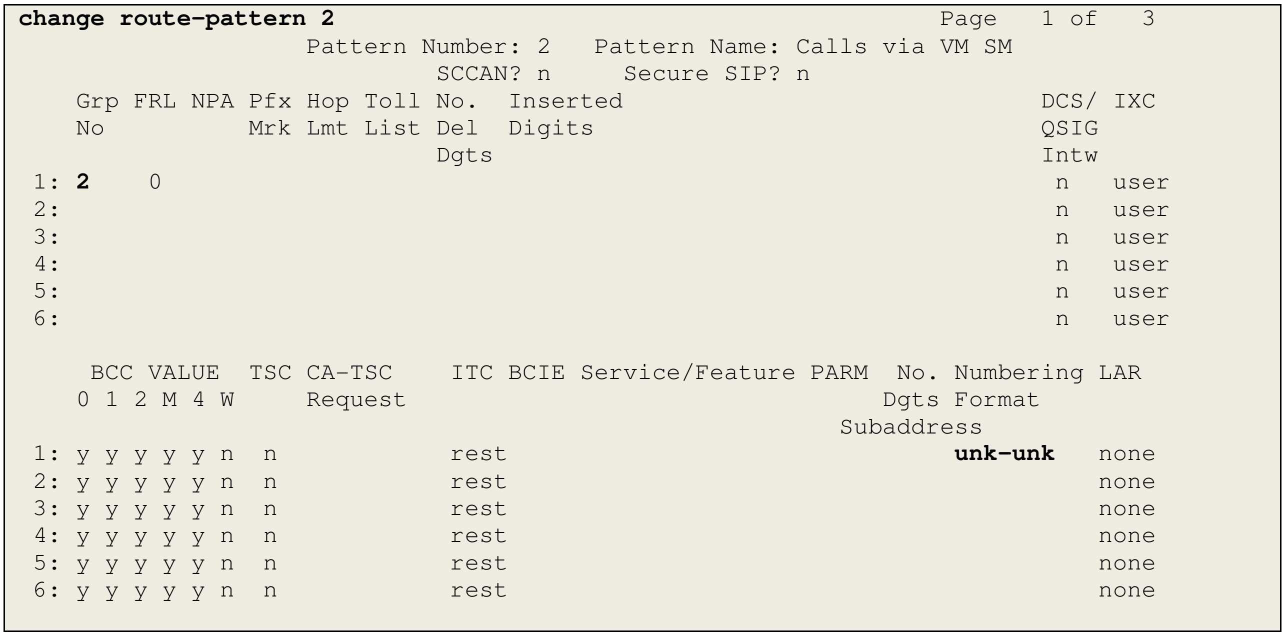
Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0 or 00353. Calls are sent to **Route Pattern 2**.

Note: that exact maximum number lengths should be used where possible to reduce post-dial delay.



```
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     2        pubu         n
    00353                10   14     2        pubu         n
    118                  5    6      2        pubu         n
                                                           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 **2** is used to route calls to trunk group **2**. CLI is set to a private format and the private numbering table used by setting the **Numbering Format** to **unk-unk**.



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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                 unk-unk   none
 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 Communication Manager extensions. The incoming digits sent in the INVITE message from Completel can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by Completel for testing are assigned to the internal extensions of the test equipment configured within Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **02765nnnn0** to **02765nnnn5** to the 4 digit extension by deleting all (**10**) of the incoming digits and inserting the extension number.

Note: that the significant digits beyond the area code have been obscured.

```
change inc-call-handling-trmt trunk-group 2                    Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 02765nnnn0       10  2000
 public-ntwrk    10 02765nnnn1       10  2396
 public-ntwrk    10 02765nnnn2       10  2346
 public-ntwrk    10 02765nnnn3       10  2298
 public-ntwrk    10 02765nnnn4       10  2611
 public-ntwrk    10 02765nnnn5       10  6101
```

5.10. EC500 Configuration

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

- 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 **2** so that Trunk Group 2 will be used for routing
- Set the **Config Set** to **1**

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

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 2396             EC500        -     0035386nnnnnnn   2          1
                               -
```

Save Communication Manager changes by entering **save translation.**

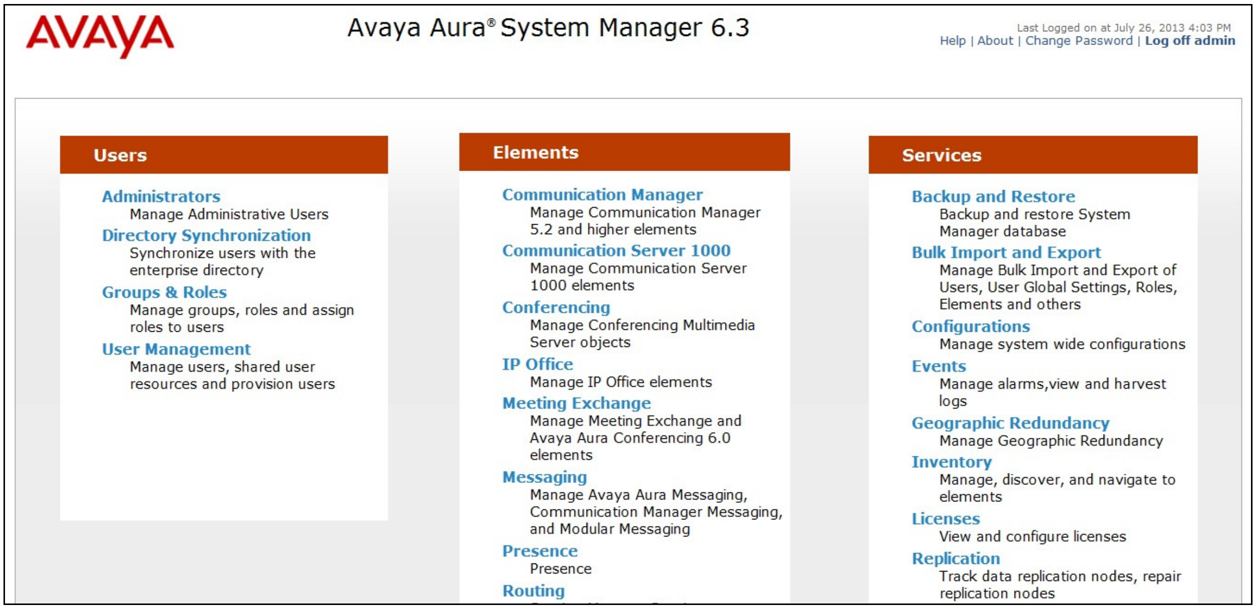
6. Configuring Avaya Aura® Session Manager

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

6.1. Log in to Avaya Aura® System Manager

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



Avaya Aura® System Manager 6.3

Last Logged on at July 26, 2013 4:03 PM
Help | About | Change Password | Log off admin

Users

Administrators
Manage Administrative Users
Directory Synchronization
Synchronize users with the enterprise directory
Groups & Roles
Manage groups, roles and assign roles to users
User Management
Manage users, shared user resources and provision users

Elements

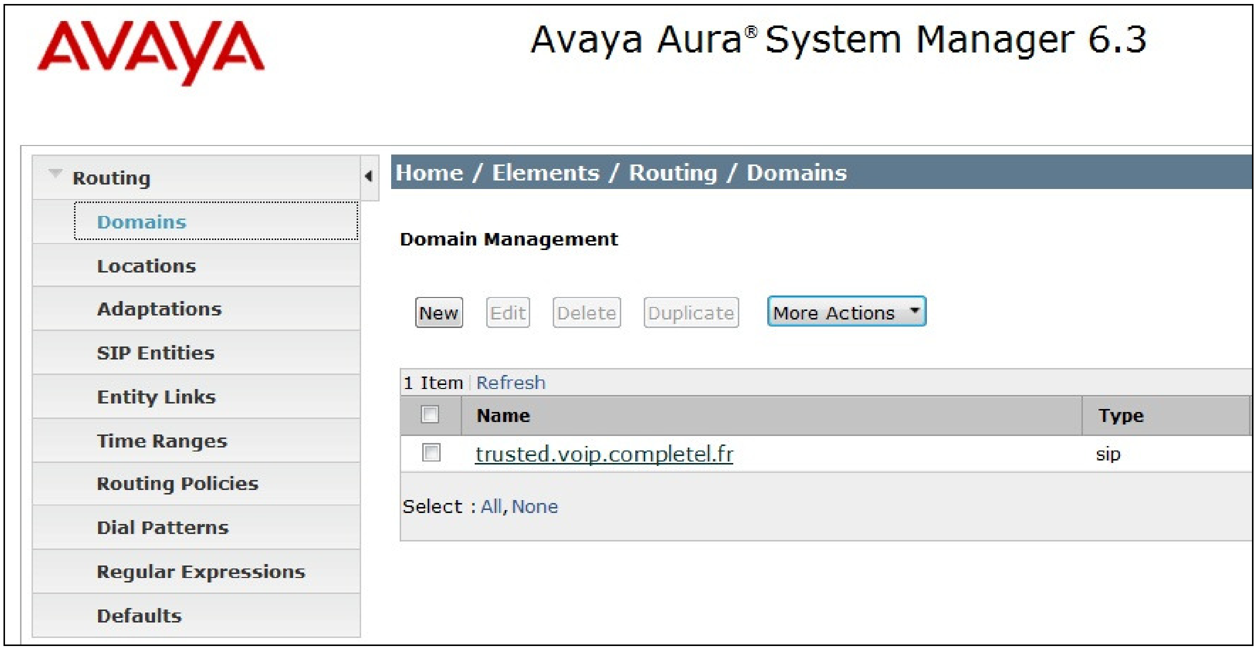
Communication Manager
Manage Communication Manager 5.2 and higher elements
Communication Server 1000
Manage Communication Server 1000 elements
Conferencing
Manage Conferencing Multimedia Server objects
IP Office
Manage IP Office elements
Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements
Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging
Presence
Presence
Routing

Services

Backup and Restore
Backup and restore System Manager database
Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Configurations
Manage system wide configurations
Events
Manage alarms,view and harvest logs
Geographic Redundancy
Manage Geographic Redundancy
Inventory
Manage, discover, and navigate to elements
Licenses
View and configure licenses
Replication
Track data replication nodes, repair replication nodes

6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name agreed with Completel; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on the Communication Manager. Refer to **Section 5.3** for details. In test, **trusted.voip.completel.fr** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.



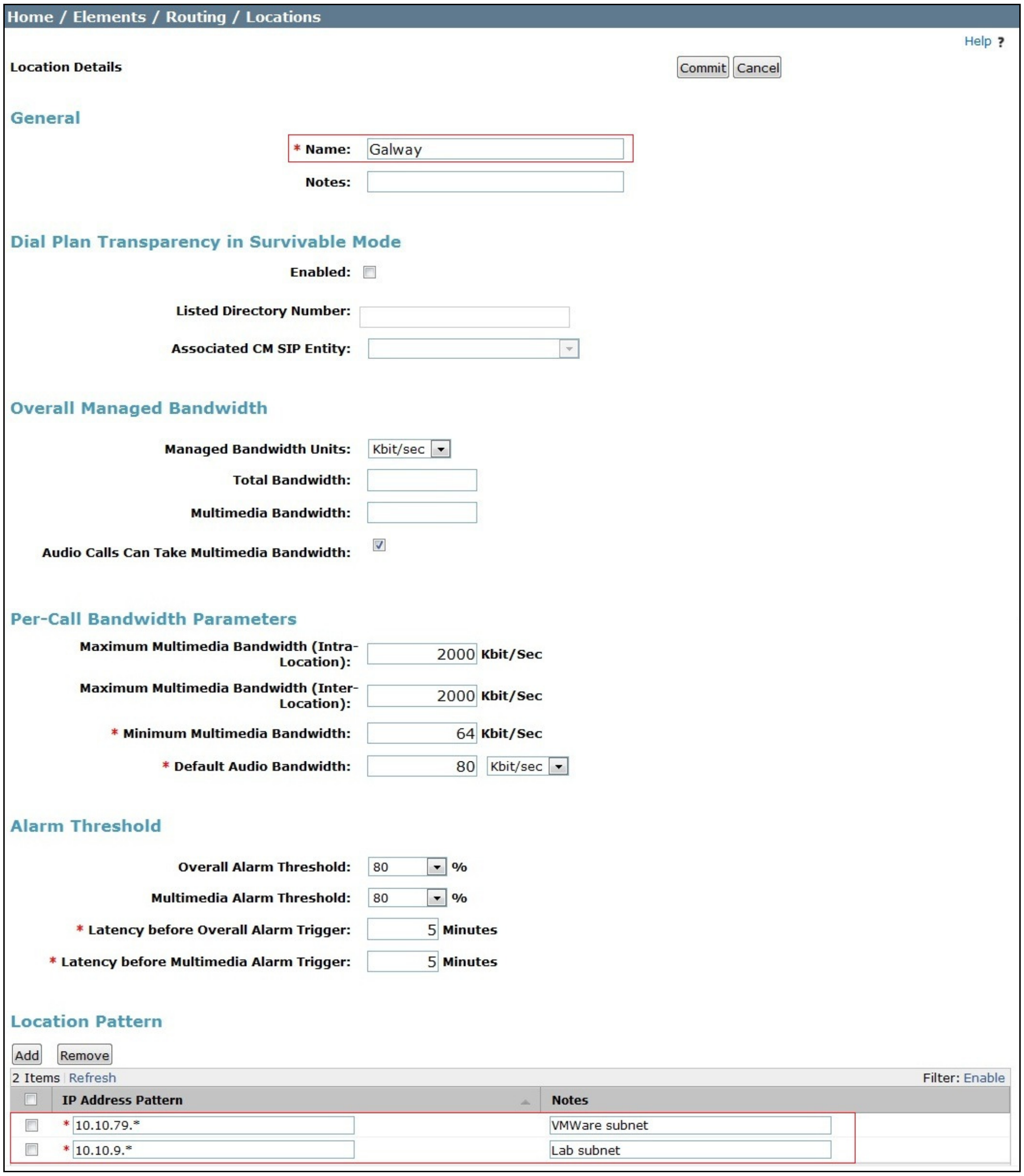
Domain Management

□	Name	Type
□	trusted.voip.completel.fr	sip

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row. Below is the location configuration used for the test enterprise.

Note: "*" is used to specify any number of allowed characters at the end of the string.



Location Details

General

* Name: Galway
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
* Minimum Multimedia Bandwidth: 64 Kbit/Sec
* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %
Multimedia Alarm Threshold: 80 %
* Latency before Overall Alarm Trigger: 5 Minutes
* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

2 Items

□	IP Address Pattern	Notes
□	* 10.10.79.*	VMWare subnet
□	* 10.10.9.*	Lab subnet

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**:

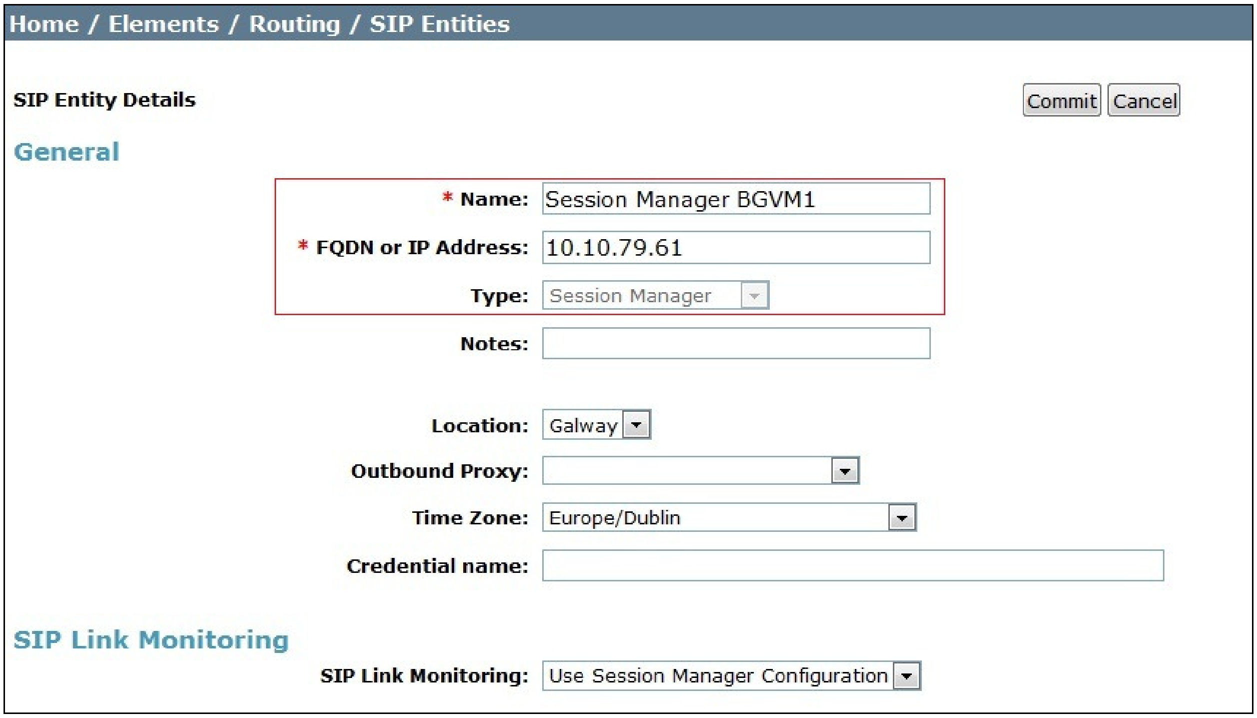
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP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

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller for Enterprise (Avaya SBCE)

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 SIP signalling interface of Session Manager.



SIP Entity Details

General

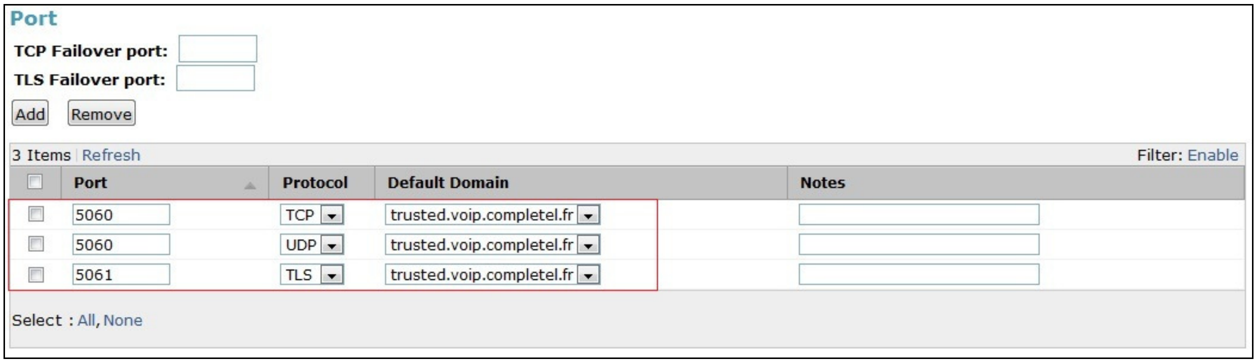
* Name:	Session Manager BGVM1
* FQDN or IP Address:	10.10.79.61
Type:	Session Manager
Notes:	
Location:	Galway
Outbound Proxy:	
Time Zone:	Europe/Dublin
Credential name:	

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The Session Manager must be configured with the port numbers and transport 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 SIP domain



Port

TCP Failover port:

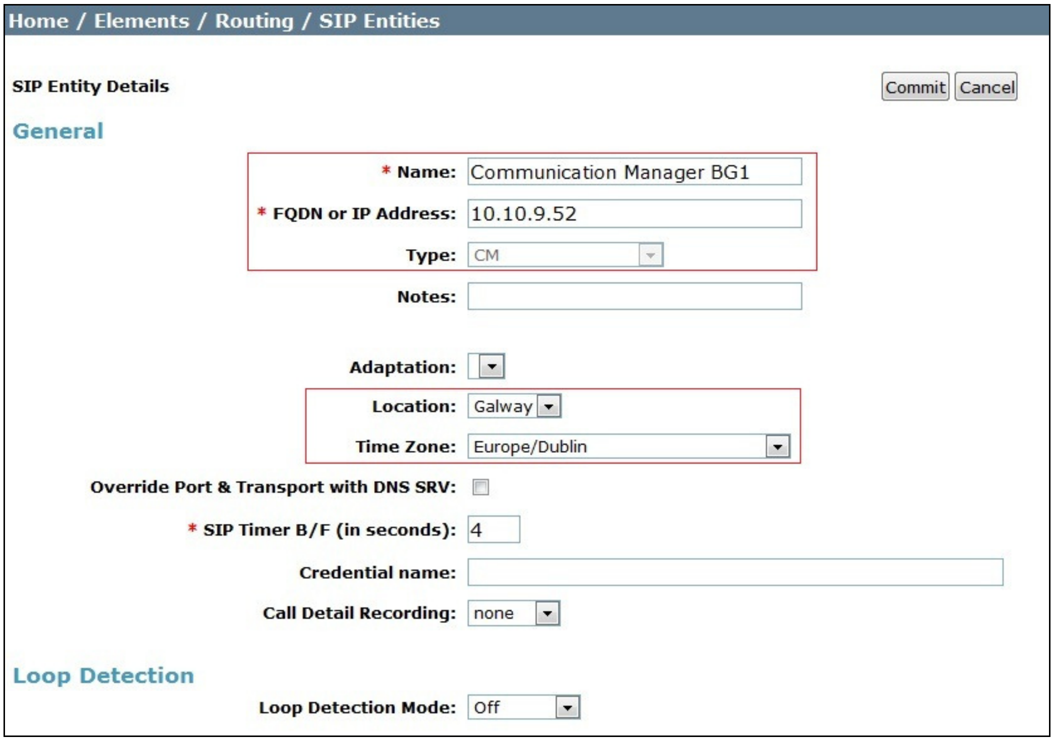
TLS Failover port:

3 Items

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	trusted.voip.completel.fr	
□	5060	UDP	trusted.voip.completel.fr	
□	5061	TLS	trusted.voip.completel.fr	

6.4.2. Avaya Aura® Communication Manager SIP Entity

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



SIP Entity Details

General

* Name: Communication Manager BG1

* FQDN or IP Address: 10.10.9.52

Type: CM

Notes:

Adaptation:

Location: Galway

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: □

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

Credential name:

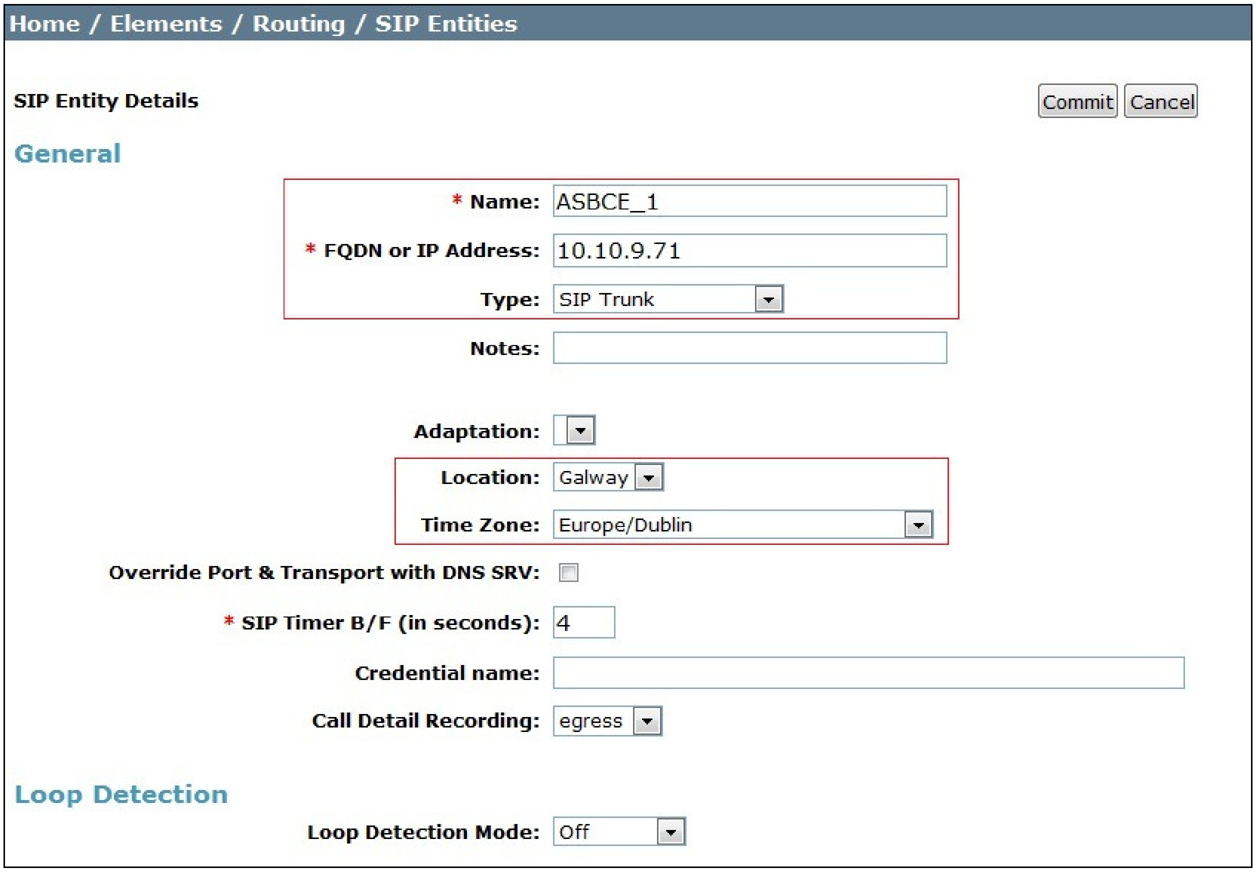
Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

6.4.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP Entity for 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 the location as defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



SIP Entity Details

General

* Name:	ASBCE_1
* FQDN or IP Address:	10.10.9.71
Type:	SIP Trunk
Notes:	
Adaptation:	
Location:	Galway
Time Zone:	Europe/Dublin
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	egress

Loop Detection

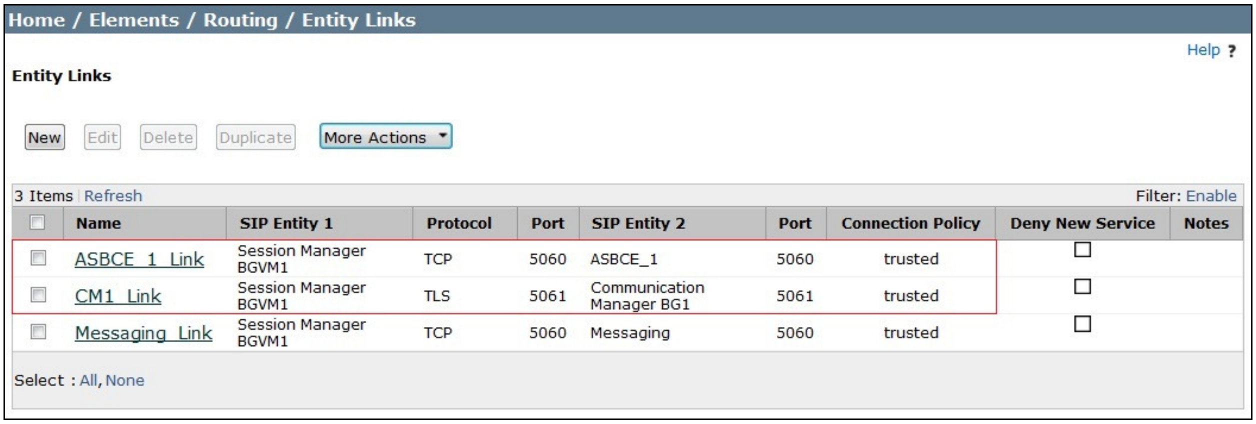
Loop Detection Mode:	Off

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 the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

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



□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
□	ASBCE_1_Link	Session Manager BGVM1	TCP	5060	ASBCE_1	5060	trusted	□	
□	CM1_Link	Session Manager BGVM1	TLS	5061	Communication Manager BG1	5061	trusted	□	
□	Messaging_Link	Session Manager BGVM1	TCP	5060	Messaging	5060	trusted	□	

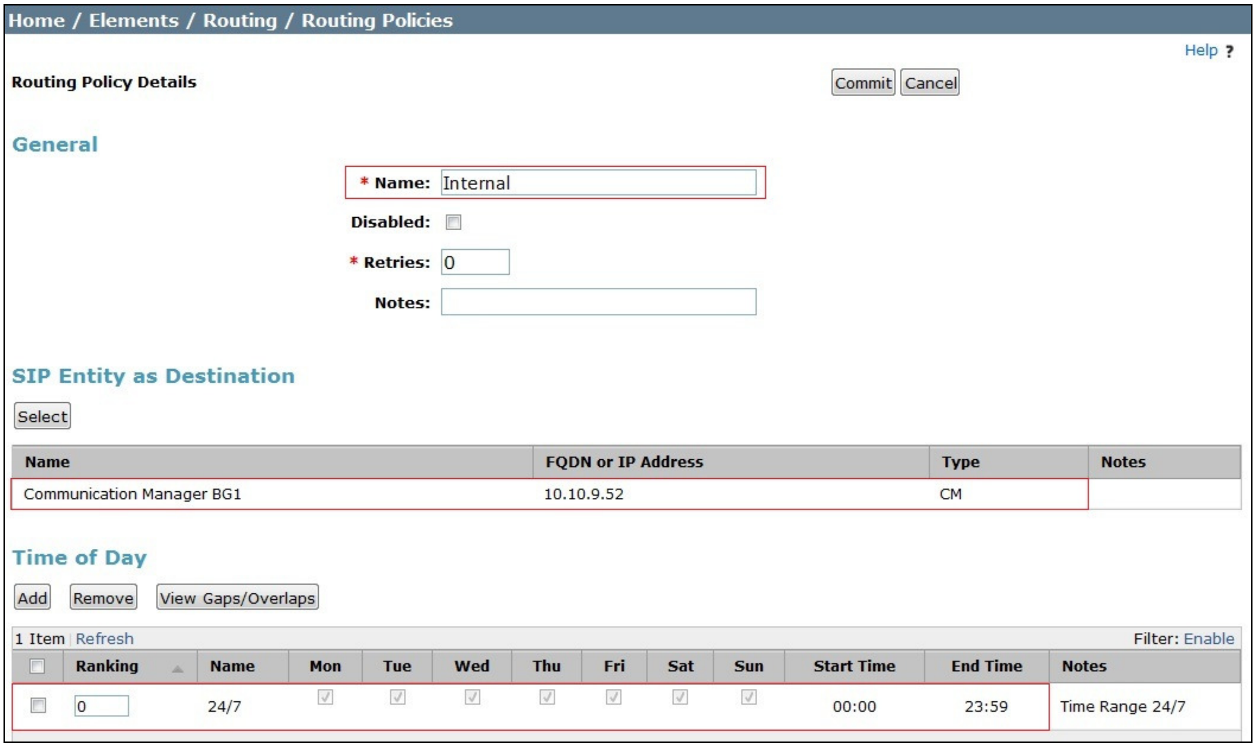
6.6. Administer Routing Policies

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

Under **General**:

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

The following screen shows the routing policy for Communication Manager.



Routing Policy Details

General

* Name:	Internal
Disabled:	□
* Retries:	0
Notes:	

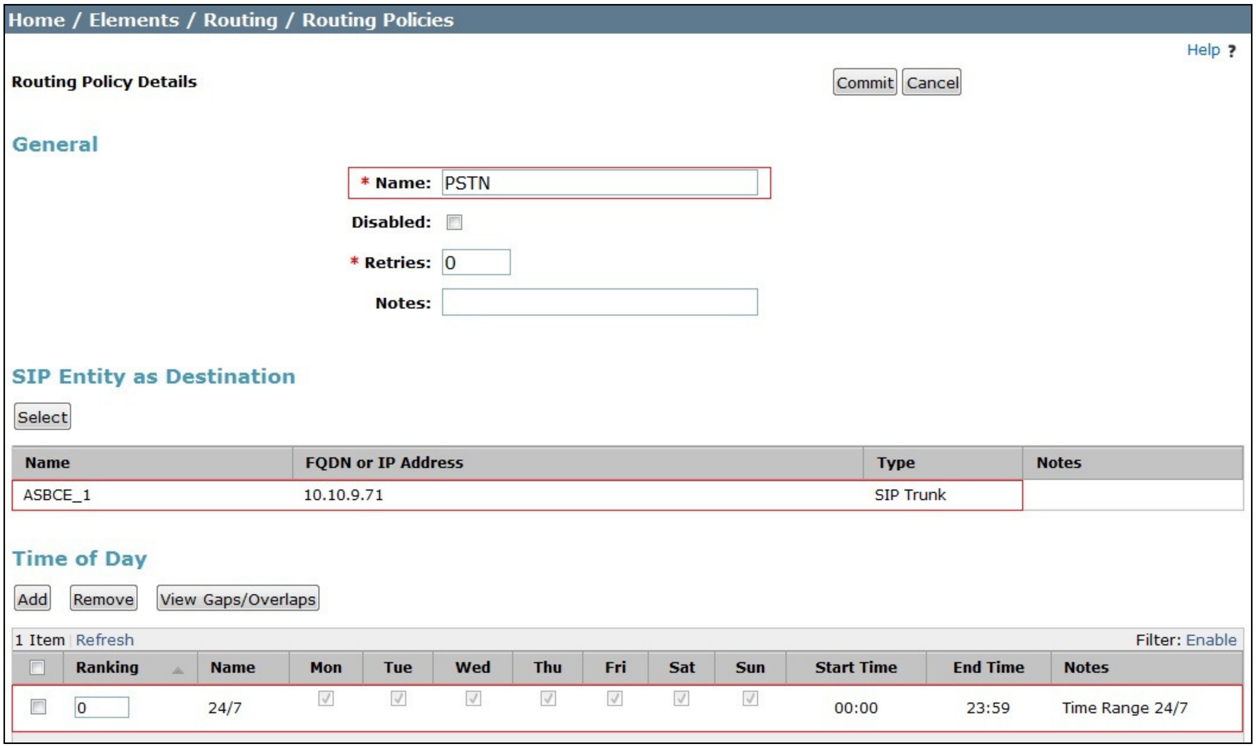
SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Communication Manager BG1	10.10.9.52	CM	

Time of Day

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

The following screen shows the routing policy for Avaya SBCE.



Home / Elements / Routing / Routing Policies

Help ?

Routing Policy Details

Commit Cancel

General

* Name: PSTN

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ASBCE_1	10.10.9.71	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

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

6.7. Administer Dial Patterns

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

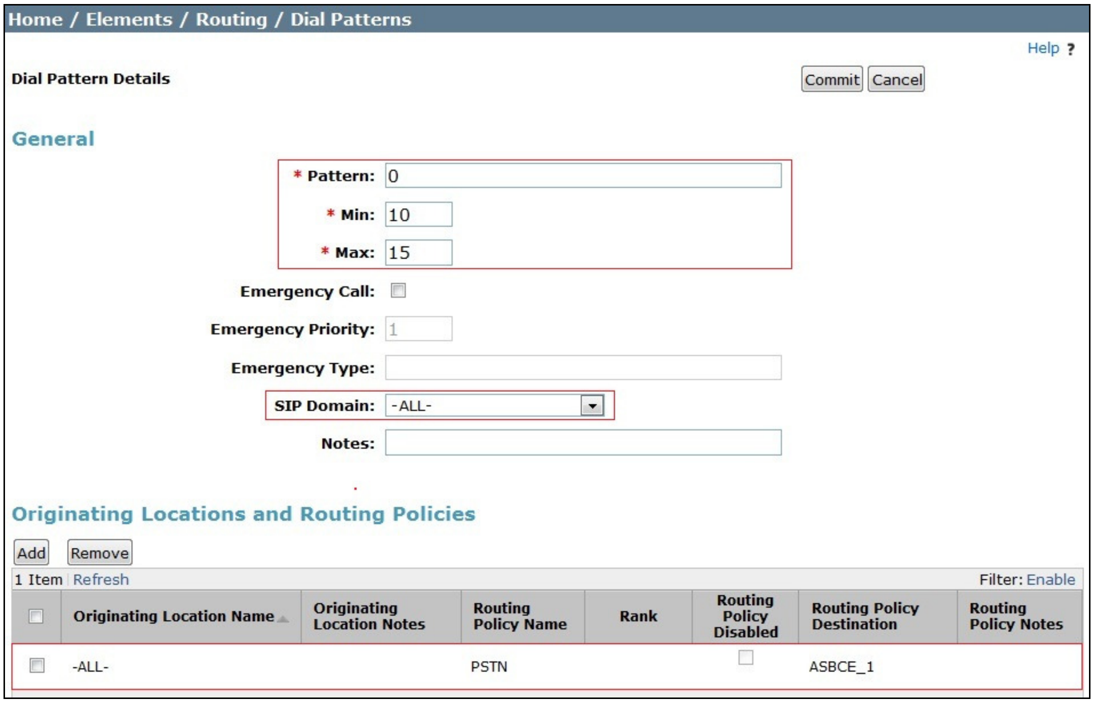
Under **General**:

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

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown)
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**
- Under **Routing Policies** select one of the routing policies defined in **Section 6.6.**
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the Completel UCM service.



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

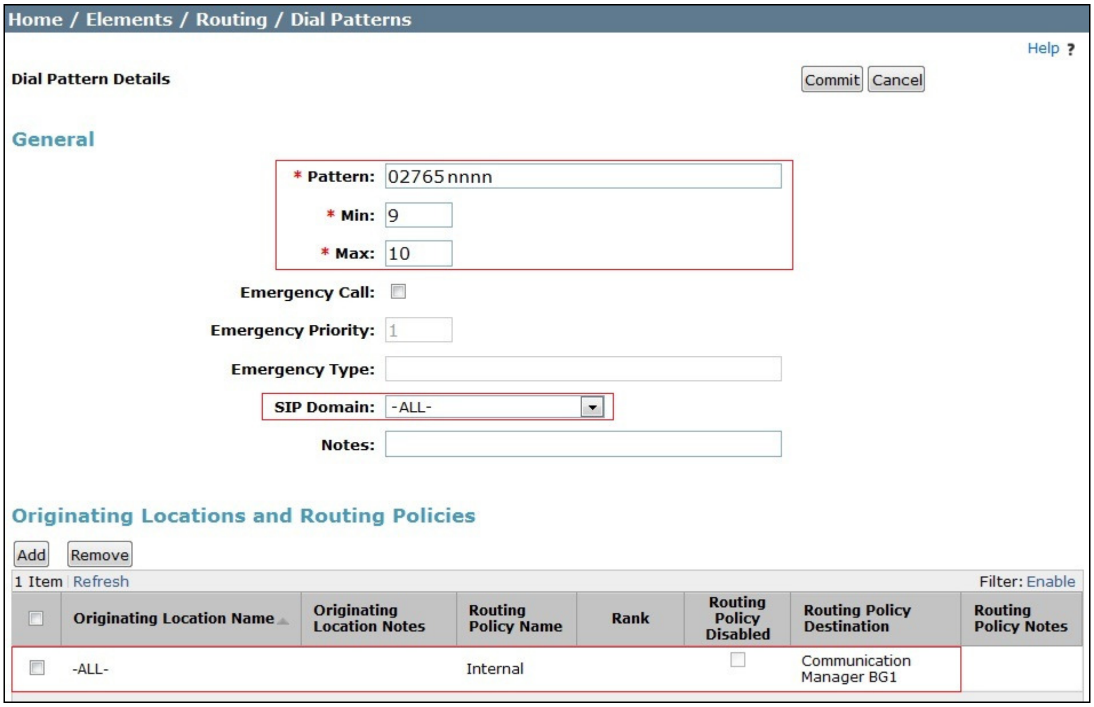
* Pattern:	0
* Min:	10
* Max:	15
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		PSTN		□	ASBCE_1	

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



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern:	02765nnnn
* Min:	9
* Max:	10
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

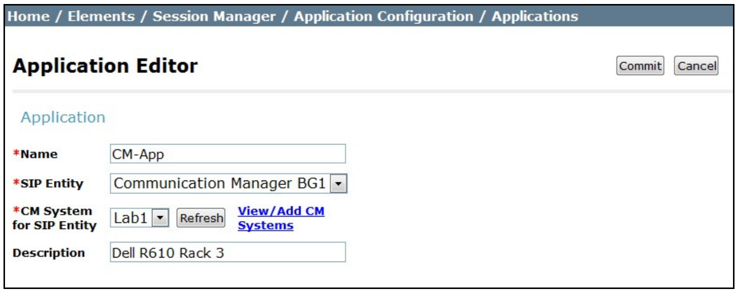
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		Internal		□	Communication Manager BG1	

Note: the pattern to be matched has been obscured.

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** (not shown).

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for Communication Manager and select **Commit** to save the configuration.



Home / Elements / Session Manager / Application Configuration / Applications

Application Editor

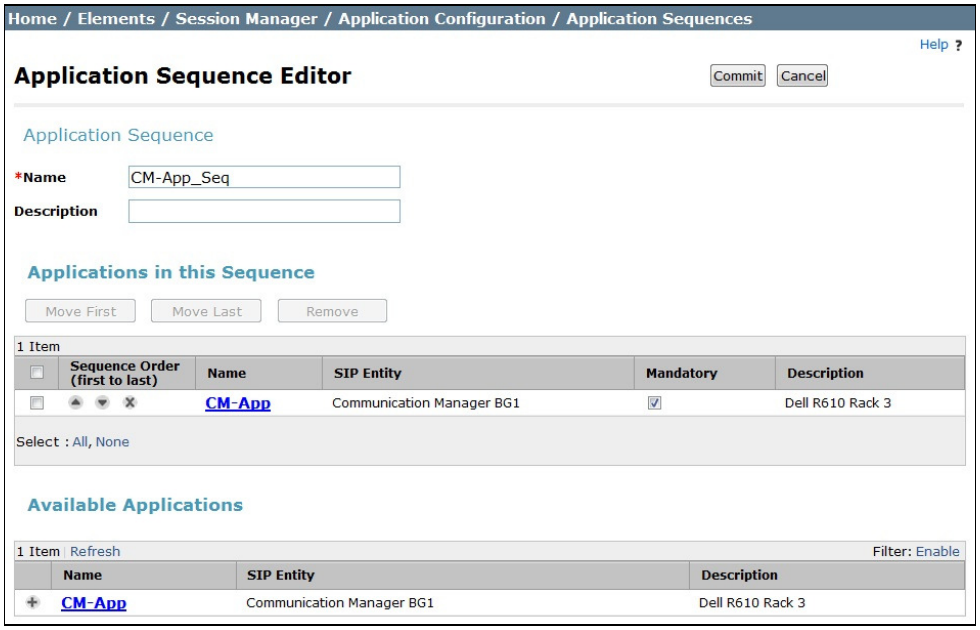
Application

*Name	CM-App
*SIP Entity	Communication Manager BG1
*CM System for SIP Entity	Lab1 Refresh View/Add CM Systems
Description	Dell R610 Rack 3

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** (not shown)..

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



Home / Elements / Session Manager / Application Configuration / Application Sequences

Application Sequence Editor

Application Sequence

*Name	CM-App_Seq
Description	

Applications in this Sequence

1 Item

☐	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
☐	▲ ▼ ✕	CM-App	Communication Manager BG1	☑	Dell R610 Rack 3

Select : All, None

Available Applications

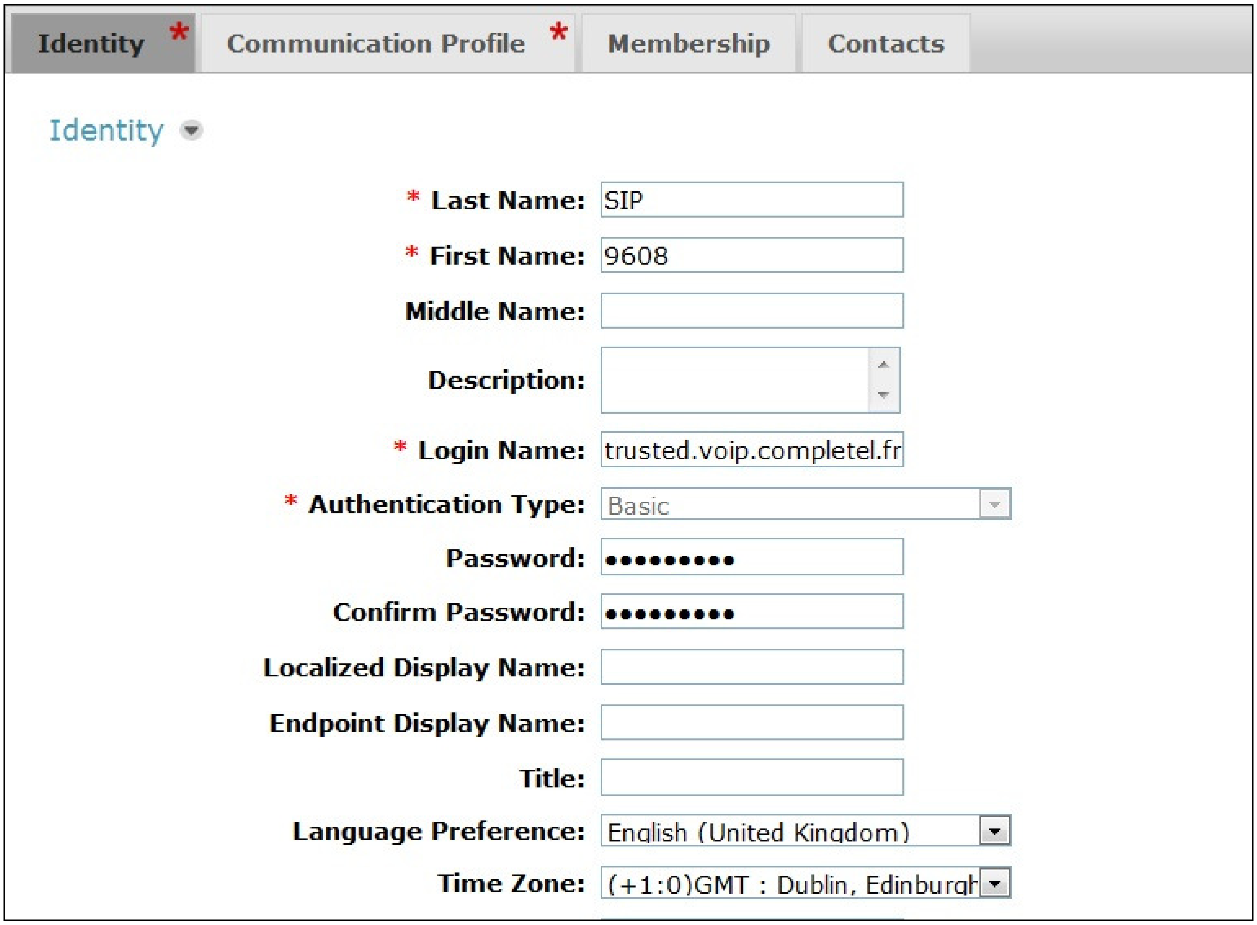
1 Item Refresh Filter: Enable

	Name	SIP Entity	Description
+	CM-App	Communication Manager BG1	Dell R610 Rack 3

6.10. Administer SIP Extensions

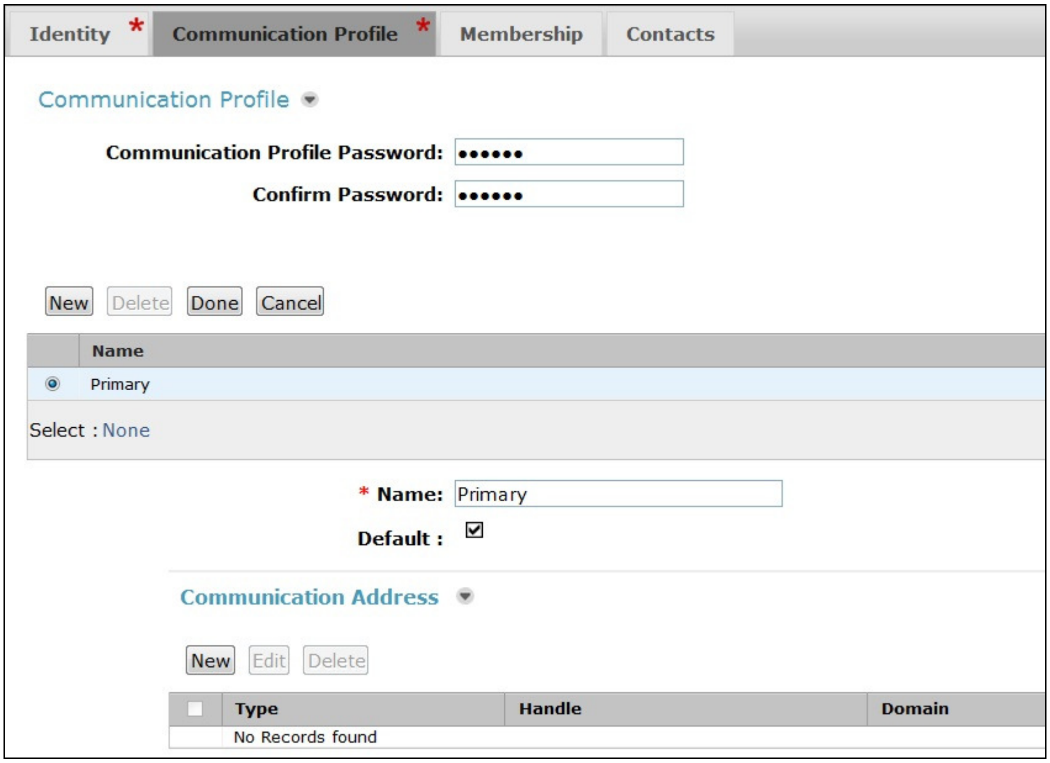
SIP extensions are registered with Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).
On the **Identity** tab:

- 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. **2208@trusted.voip.completel.fr** (entire name could not be displayed in the screenshot) 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
- Set the **Language Preference** and **Time Zone** as required



* Last Name:	SIP
* First Name:	9608
Middle Name:	
Description:	
* Login Name:	trusted.voip.completel.fr
* Authentication Type:	Basic
Password:	•••••••••
Confirm Password:	•••••••••
Localized Display Name:	
Endpoint Display Name:	
Title:	
Language Preference:	English (United Kingdom)
Time Zone:	(+1:0)GMT : Dublin, Edinburgh

On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it.



Communication Profile

Communication Profile Password: ••••••

Confirm Password: ••••••

	Name
●	Primary

Select : None

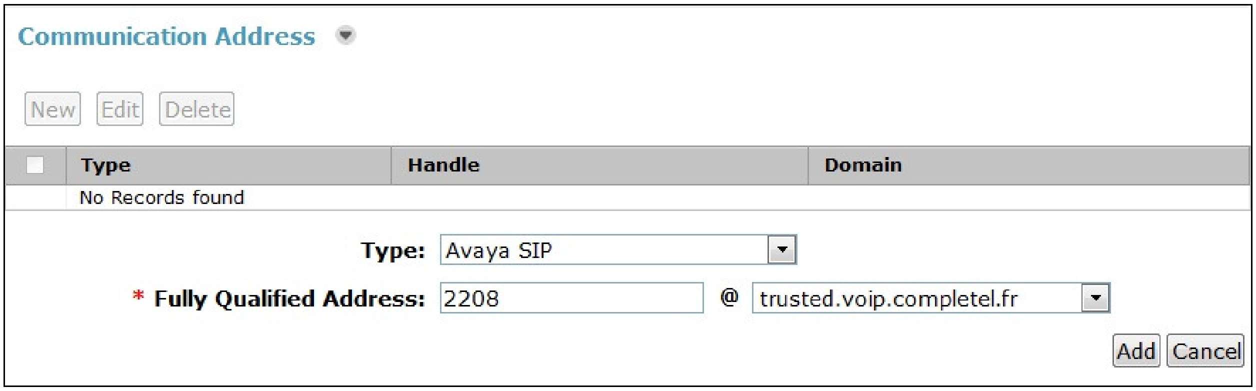
* Name: Primary

Default : ☑

Communication Address

□	Type	Handle	Domain
	No Records found		

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.



Communication Address

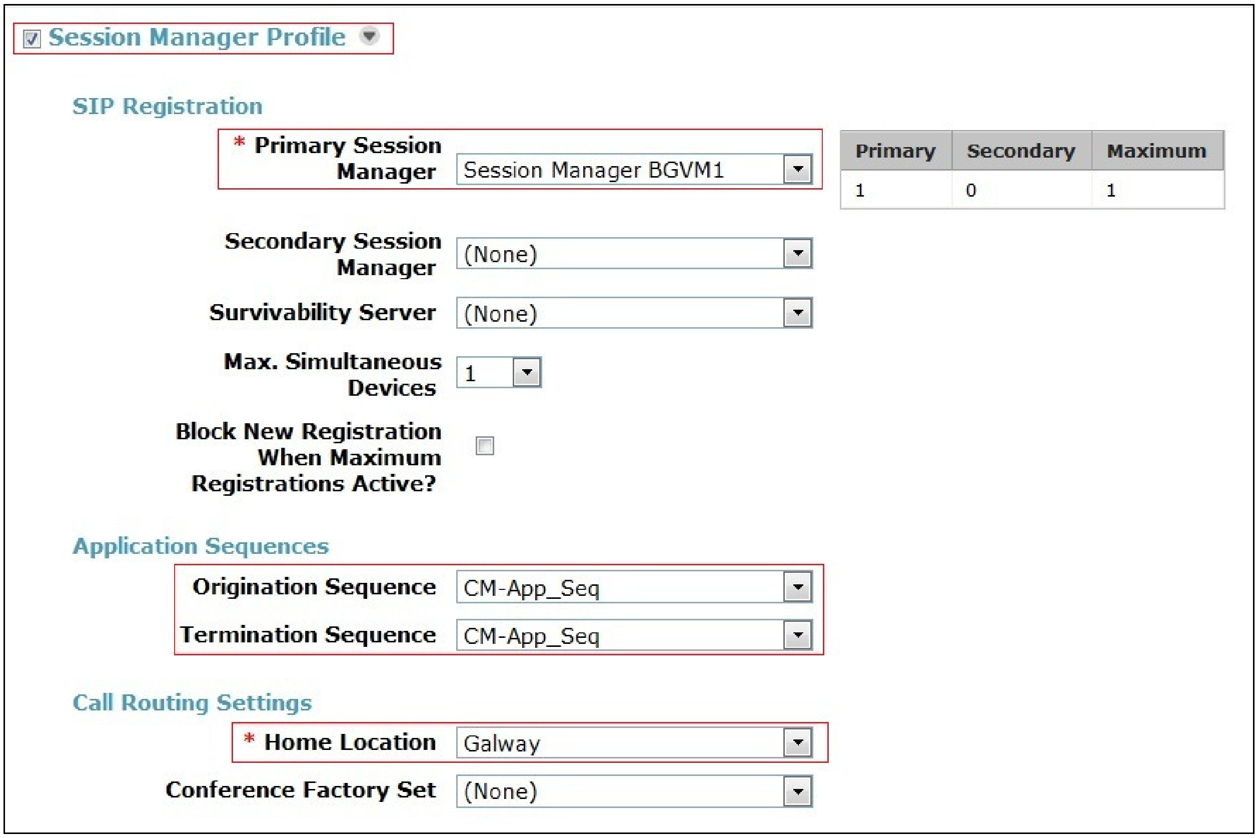
□	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: 2208 @ trusted.voip.completel.fr

Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** 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 Sequence** field configured in **Section 6.9**
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.9**
- Select the appropriate location from the drop-down menu in the **Home Location** field



☑ Session Manager Profile

SIP Registration

Primary	Secondary	Maximum
1	0	1

* Primary Session Manager	Session Manager BGVM1
Secondary Session Manager	(None)
Survivability Server	(None)
Max. Simultaneous Devices	1
Block New Registration When Maximum Registrations Active?	□

Application Sequences

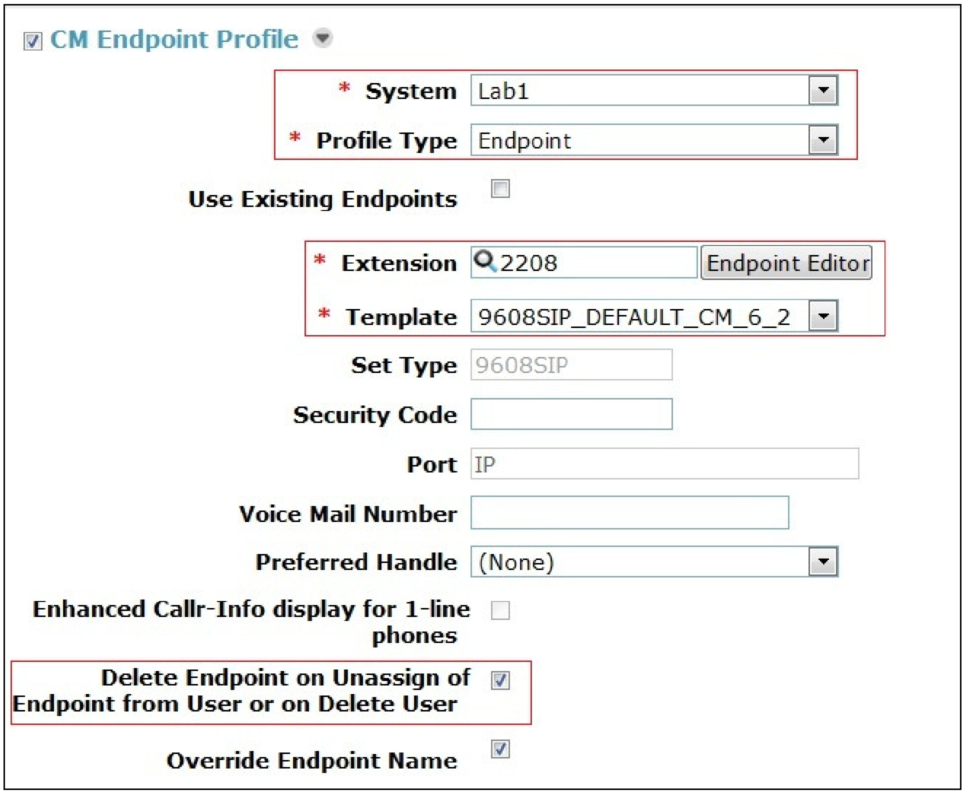
Origination Sequence	CM-App_Seq
Termination Sequence	CM-App_Seq

Call Routing Settings

* Home Location	Galway
Conference Factory Set	(None)

Expand the **Endpoint Profile** section.

- Select the SIP Entity for Communication Manager 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
- In the **Port** field **IP** is automatically inserted
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** (Not Shown) to save changes and System Manager will add the user configuration automatically to Communication Manager.



☑ CM Endpoint Profile

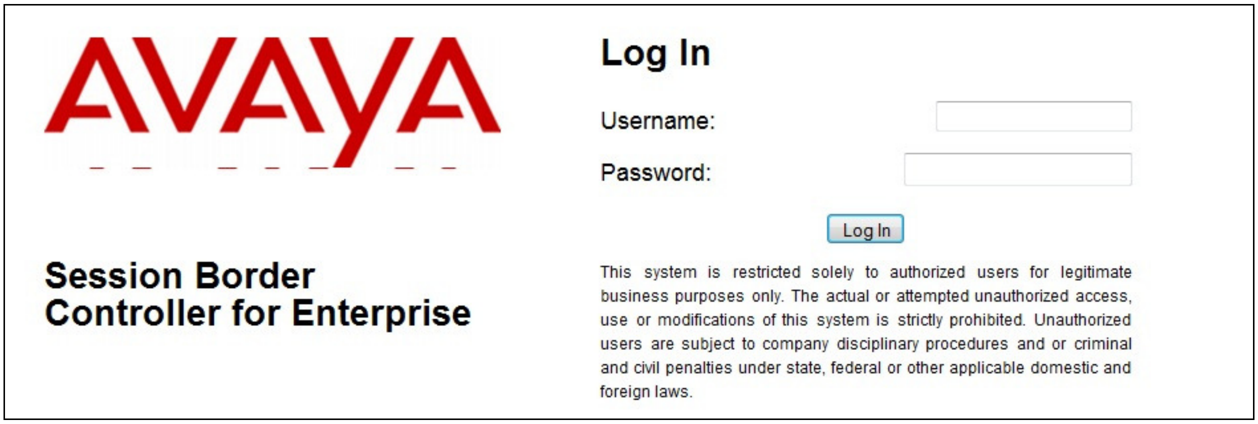
* System	Lab1
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	2208
* Template	9608SIP_DEFAULT_CM_6_2
Set Type	9608SIP
Security Code	
Port	IP
Voice Mail Number	
Preferred Handle	(None)
Enhanced Callr-Info display for 1-line phones	□
Delete Endpoint on Unassign of Endpoint from User or on Delete User	☑
Override Endpoint Name	☑

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using username **ucsec** and the appropriate password.



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.

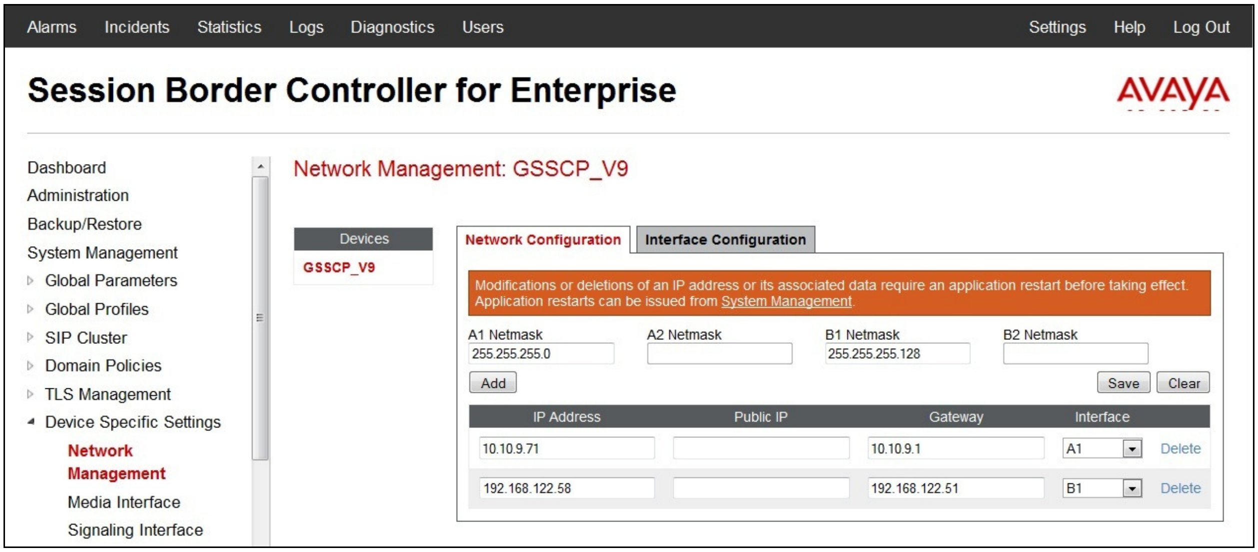
Once logged in, a dashboard is presented (not shown) with a menu on the left-hand side. The menu is used as a starting point for all administration of the Avaya SBCE.

7.2. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and netmasks 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 main menu on the left hand side and click on **Add**. Enter details in the blank box that appears at the end of the list

- Define the internal IP address with netmask and assign to interface **A1**
- Select **Save** to save the information
- Click on **Add**
- Define the external IP address with netmask and assign to interface **B1**
- Select **Save** 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)



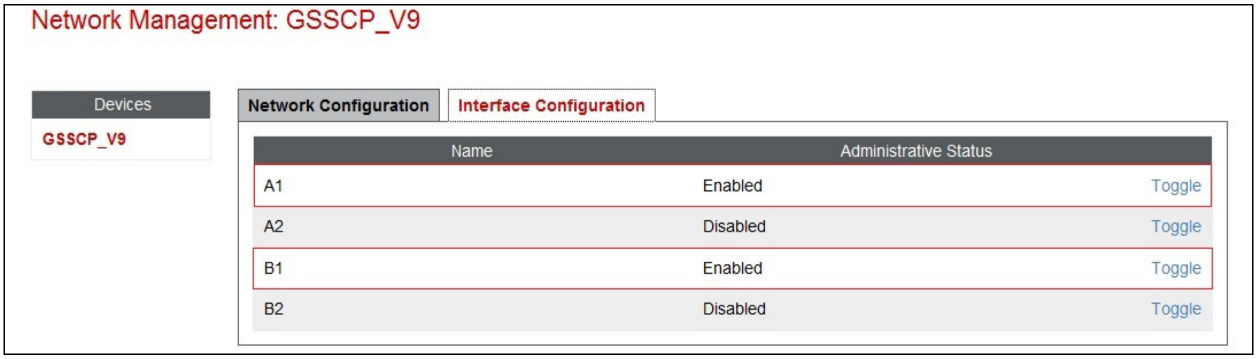
Network Management: GSSCP_V9

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	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.128	

IP Address	Public IP	Gateway	Interface	
10.10.9.71		10.10.9.1	A1	Delete
192.168.122.58		192.168.122.51	B1	Delete

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



Network Management: GSSCP_V9

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

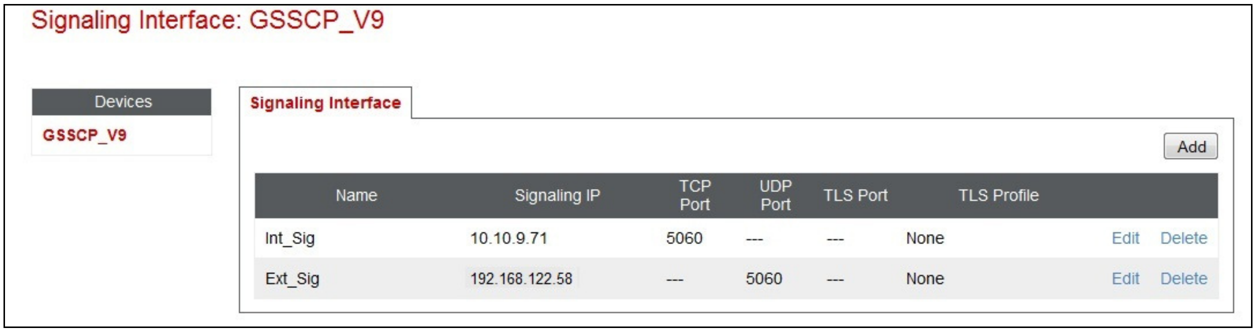
7.3. Define Interfaces

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

7.3.1. Signalling Interfaces

To define the signalling interfaces on Avaya SBCE, navigate to **Device Specific Settings → Signaling Interface** (not shown) in the main menu on the left hand side. Details of transport protocol and ports for the internal and external SIP signalling interfaces are entered here

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the internal signalling interface used for Session Manager
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.2**
- Select **TCP** port number **5060**
- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the external signalling interface used for Completel
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.2**
- Select **UDP** port number **5060**

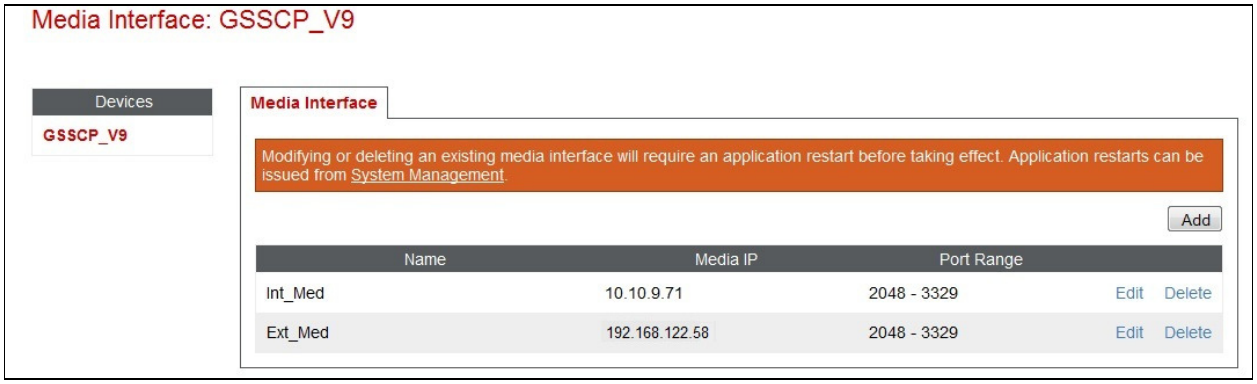


Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig	10.10.9.71	5060	---	---	None	Edit	Delete
Ext_Sig	192.168.122.58	---	5060	---	None	Edit	Delete

7.3.2. Media Interfaces

To define the media interfaces on Avaya SBCE, navigate to **Device Specific Settings → Media Interface** in the main menu on the left hand side (not shown). 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** and enter details of the internal media interface 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 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add** and enter details of the external media interface 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 7.2**
- Select **RTP port** ranges for the media path with the Completel network



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_Med	10.10.9.71	2048 - 3329	Edit	Delete
Ext_Med	192.168.122.58	2048 - 3329	Edit	Delete

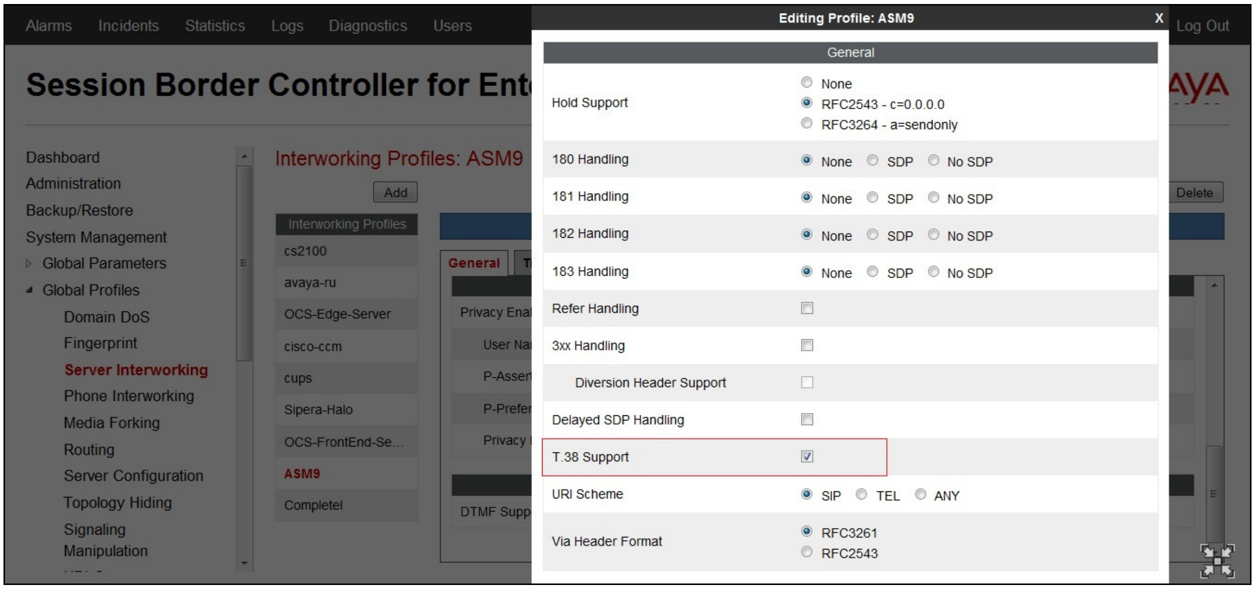
Note: during test the port ranges for the internal and external media interfaces were defined as the default values used by Communication Manager,

7.4. Define Server Interworking

Server interworking is defined for each server connected to Avaya SBCE. In this case, the Completel SBC is connected as the Trunk Server and Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM9** was used (not shown)
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box then click **Next** and **Finish** (not shown)

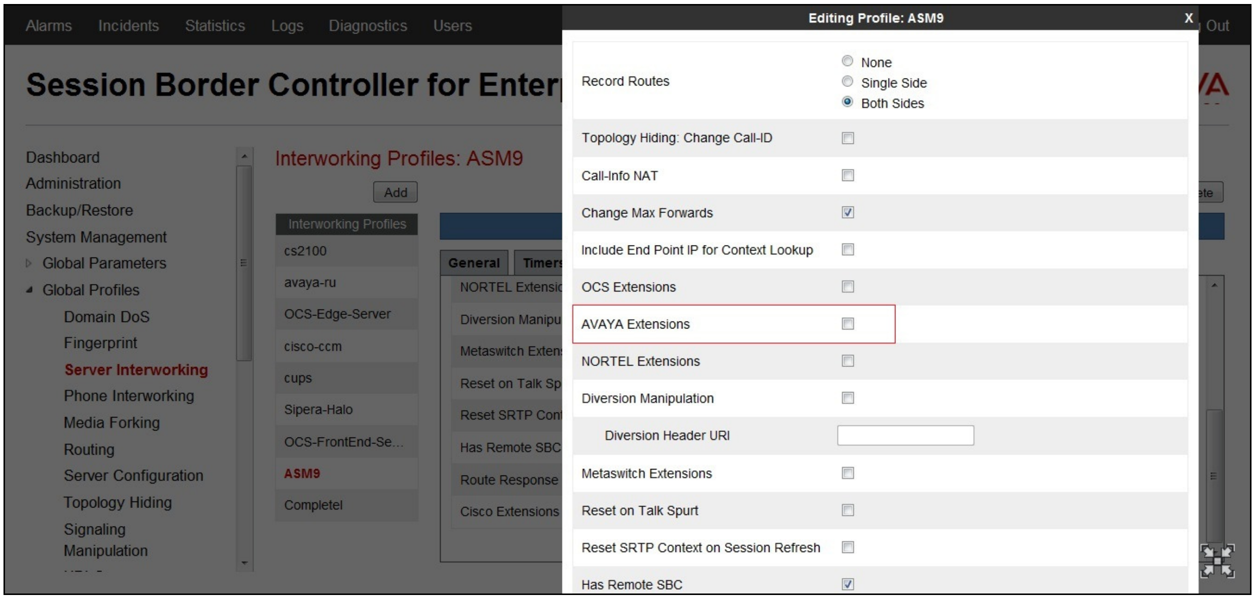


Editing Profile: ASM9

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	□
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

- In the **Advanced** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Uncheck the **AVAYA Extensions** box



Editing Profile: ASM9

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	☑

To define Server Interworking for the Completel SBC, highlight the previously defined profile for Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown).

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

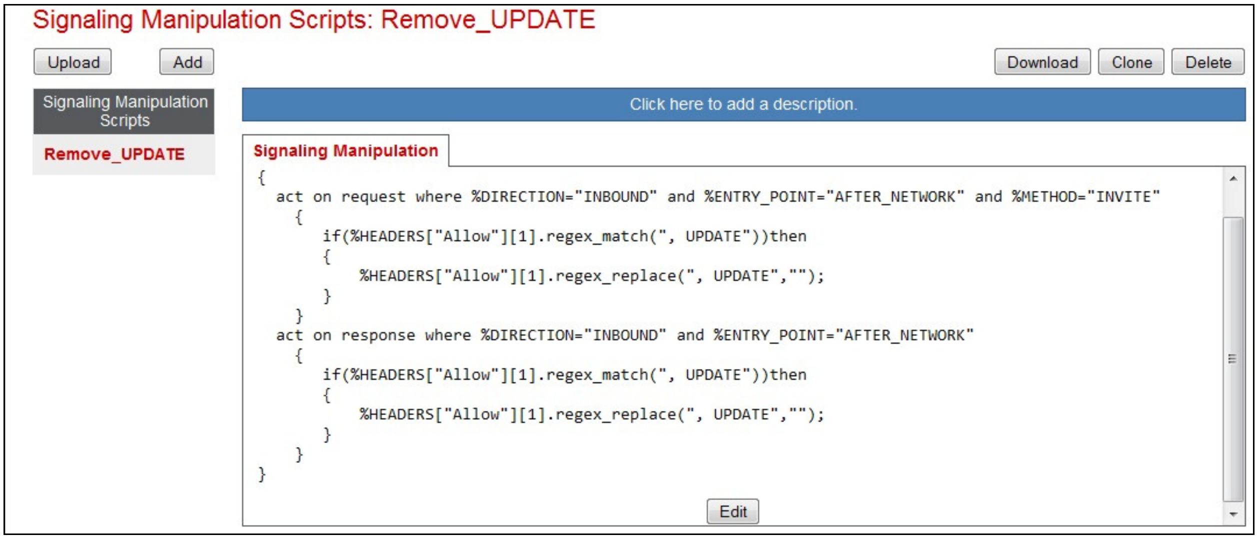
7.5. Define Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. During test, an issue was found in the use of the UPDATE message between Completel UCM service and the enterprise that could not be resolved by other methods such as Server Interworking and Signaling Rules. The issue occurred when the UPDATE message was sent from the Completel network to change the codec to T.38 for fax calls. The enterprise was not successfully changing the codec and the fax calls were failing. The solution was to remove UPDATE from the Supprted header in messages going from the enterprise to the network. This prompts the network to use re-INVITE instead of UPDATE.

To define the signalling manipulation to remove UPDATE from the Supported header in outgoing messages, navigate to **Global Profiles → Signaling Manipulation** in the main menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor (not shown). The title in the example is **Remove_UPDATE**. The script text is as follows:

```
within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and
%METHOD="INVITE"
    {
       if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
       {
           %HEADERS["Allow"][1].regex_replace(", UPDATE","");
       }
    }
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
       if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
       {
           %HEADERS["Allow"][1].regex_replace(", UPDATE","");
       }
    }
}
```

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


Signaling Manipulation Scripts: Remove_UPDATE
Upload
Add
Download
Clone
Delete
Signaling Manipulation Scripts
Remove_UPDATE
Click here to add a description.
Signaling Manipulation
Edit

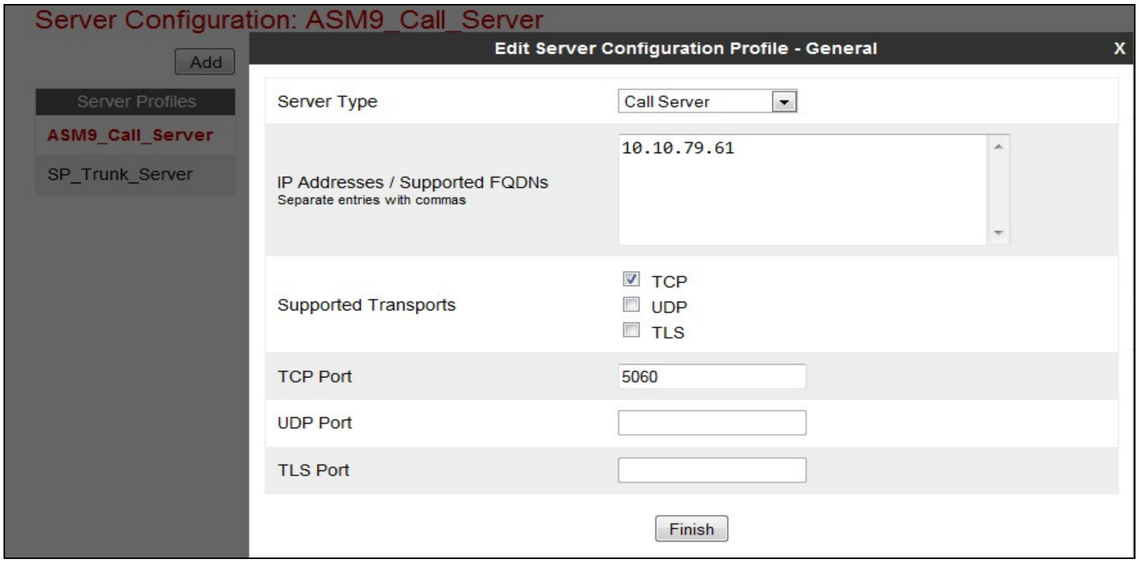
```
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and %METHOD="INVITE"
    {
       if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
       {
           %HEADERS["Allow"][1].regex_replace(", UPDATE","");
       }
    }
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
       if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
       {
           %HEADERS["Allow"][1].regex_replace(", UPDATE","");
       }
    }
}
```

7.6. Define Servers

Servers are defined for each server connected to Avaya SBCE. In this case, the Completel SBC is connected as the Trunk Server and Session Manager is connected as the Call Server. To define Session Manager, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side (not shown).

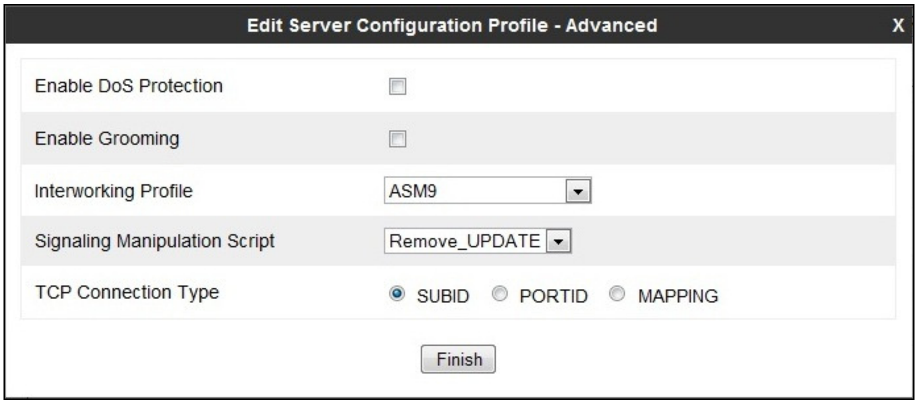
Click on **Add** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for Session Manager and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the SIP signalling interface of Session Manager. This is the same IP address as defined on Communication Manager in **Section 5.2**
- Check **TCP** in **Supported Transports**
- Define the **TCP** port for SIP signalling, **5060** is used for Session Manager and click **Finish**


Server Configuration: ASM9_Call_Server
Add
Server Profiles
ASM9_Call_Server
SP_Trunk_Server
Edit Server Configuration Profile - General
X
Finish

Server Type	Call Server
IP Addresses / Supported FQDNs Separate entries with commas	10.10.79.61
Supported Transports	☑ TCP □ UDP □ TLS
TCP Port	5060
UDP Port	
TLS Port	

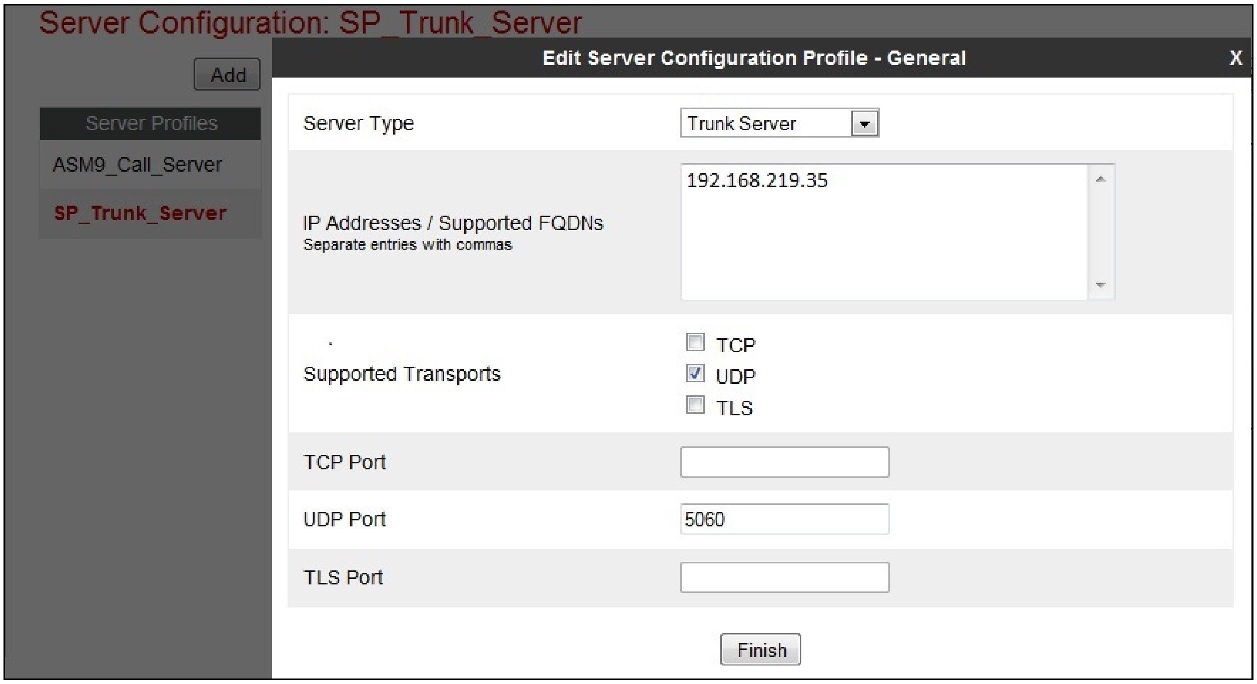
- Select the **Advanced** tab (not shown)
- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for Session Manager as defined in **Section 7.4**
- In the **Signaling Manipulation Script** drop down menu, select the script defined in **Section 7.5**
- Click **Finish**



Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	ASM9
Signaling Manipulation Script	Remove_UPDATE
TCP Connection Type	● SUBID ○ PORTID ○ MAPPING

To define the Completel SBC as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Completel SBC and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the Completel SBC
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for Completel

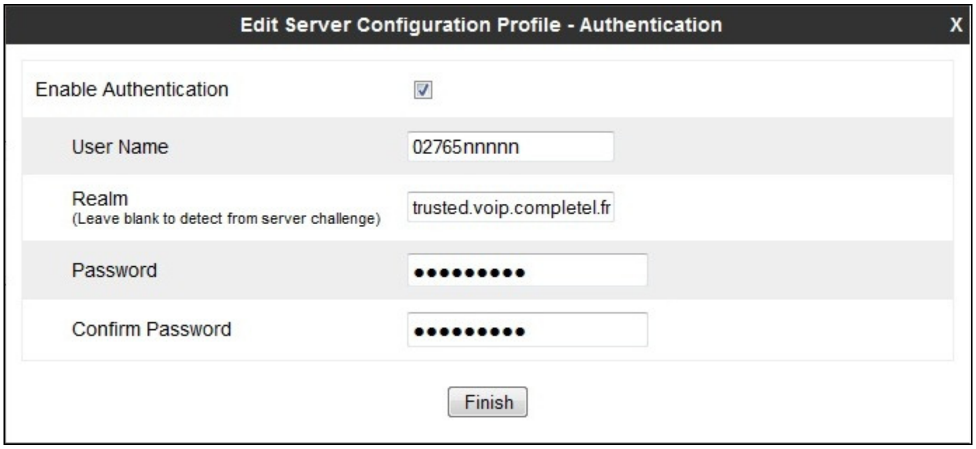


Server Configuration: SP_Trunk_Server

Edit Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs Separate entries with commas	192.168.219.35
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5060
TLS Port	

- Click **Next** and check the **Enable Authentication** box
- Define the Authentication parameters as provided by Completel.

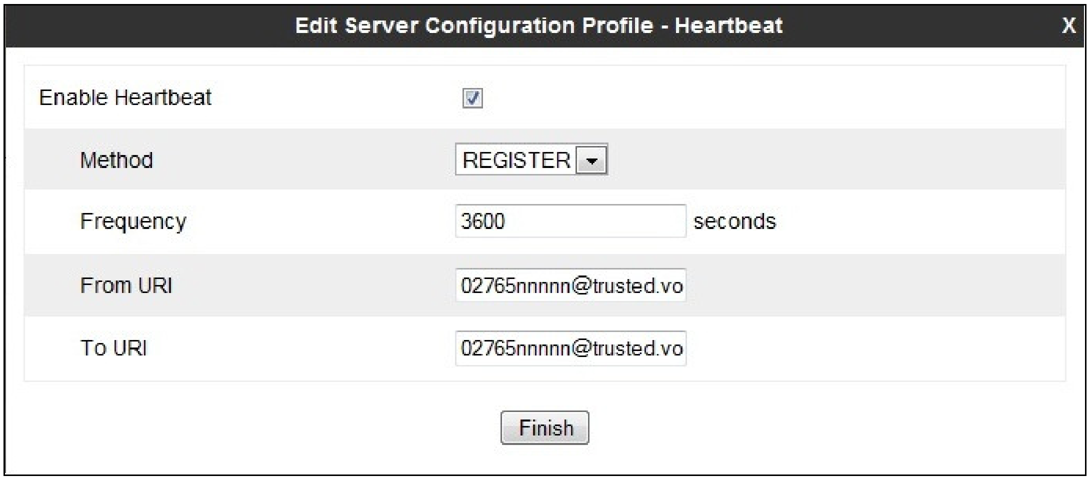


Edit Server Configuration Profile - Authentication

Enable Authentication	☑
User Name	02765nnnnn
Realm (Leave blank to detect from server challenge)	trusted.voip.completel.fr
Password	●●●●●●●●●
Confirm Password	●●●●●●●●●

Periodic REGISTER messages are required on the SIP trunk along with authentication for security. The REGISTER messages are defined using the heartbeat feature on Avaya SBCE. The heartbeat feature is defined in the Server configuration.

- Click **Next** and check the **Enable Heartbeat** box
- In the **Method** drop down menu, select **REGISTER**
- In the Frequency field, an arbitrary value of **3600** was set for test.
- In the **From URI** and **To URI** fields, use the username and domain as defined for authentication

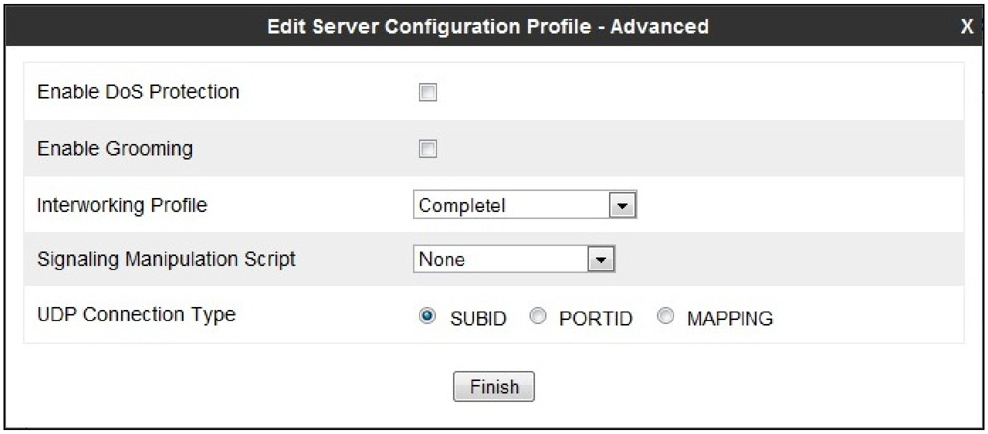


Edit Server Configuration Profile - Heartbeat

Enable Heartbeat	☑
Method	REGISTER
Frequency	3600 seconds
From URI	02765nnnnn@trusted.vo
To URI	02765nnnnn@trusted.vo

Note: the REGISTER requests are sent at regular intervals defined by the expires parameter in the 200 OK response to the REGISTER request. The expires parameter is in the Contact Header of the 200 OK and during test was set to 45 (seconds). The interval defined in **Frequency** field in the above configuration does not have any effect on the timing of REGISTER requests.

- Click **Next** again then select the **Interworking Profile** for the Completel SBC defined in **Section 7.4** from the drop down menu



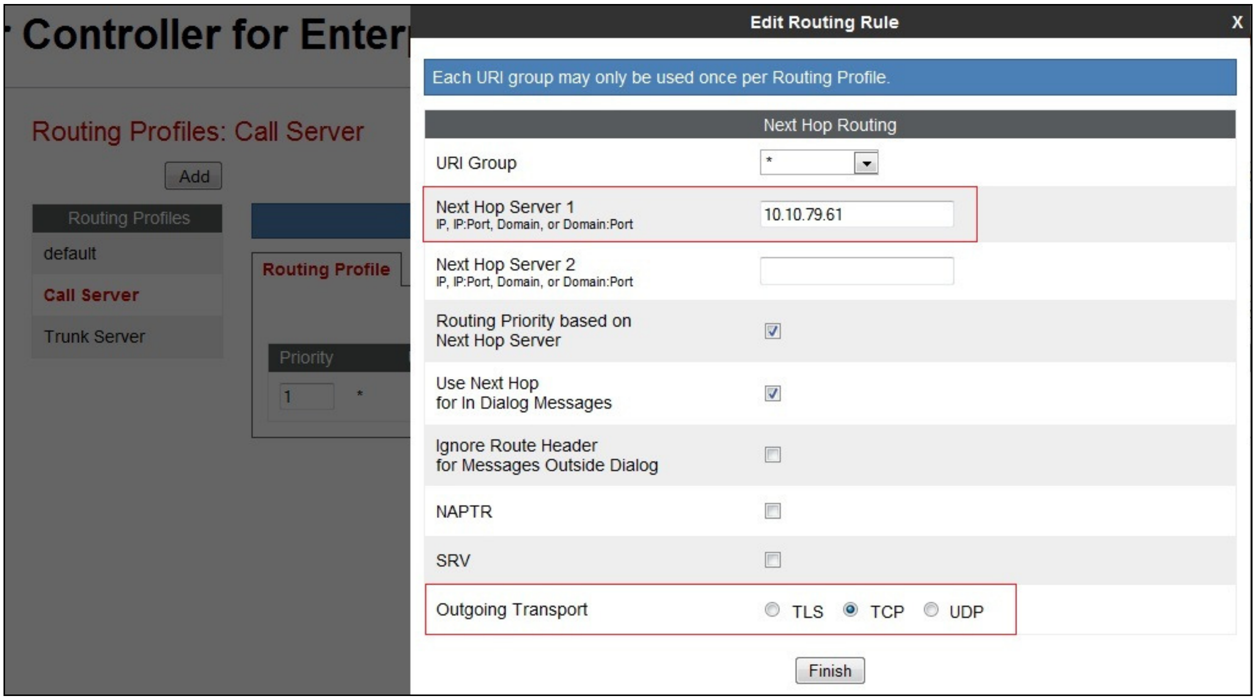
Edit Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Completel
Signaling Manipulation Script	None
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

7.7. Define Routing

Routing information is required for routing to Session Manager on the internal side and the Completel SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to Session Manager, navigate to **Global Profiles → Routing** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for Session Manager, in this case **Call Server**, and click **Next** (not shown)
- Enter the IP address and port of the SIP signalling interface for Session Manager in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**



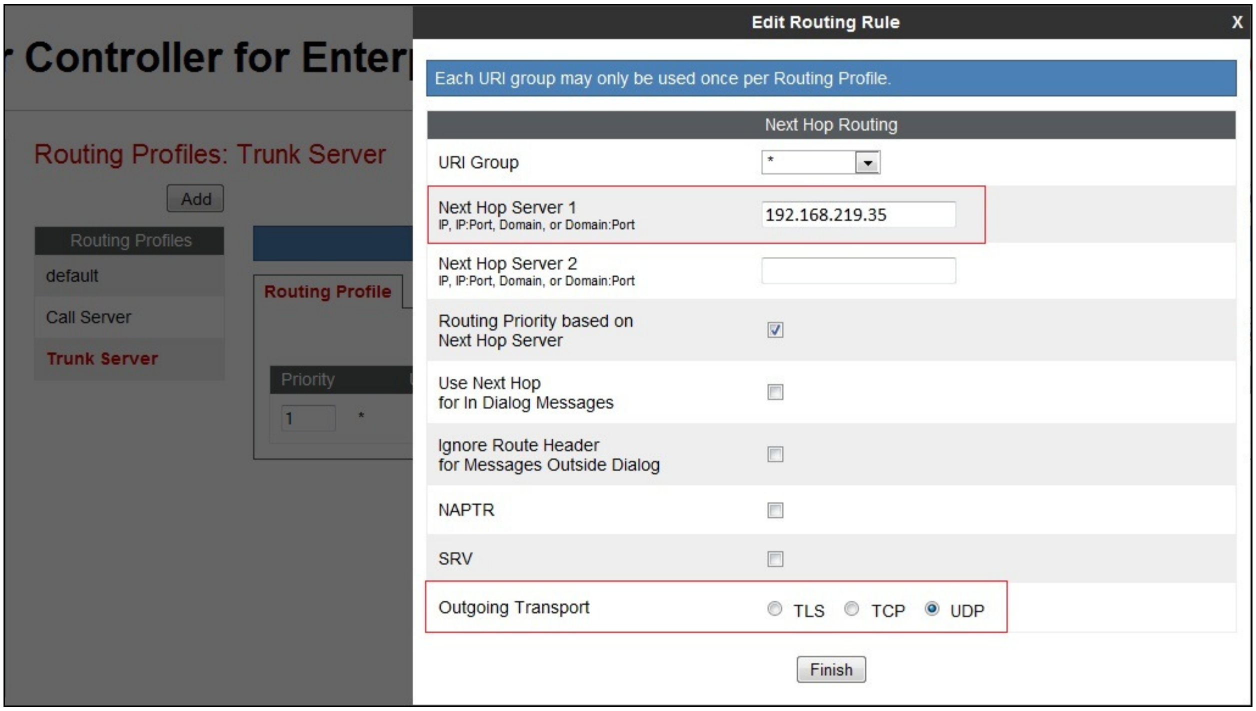
Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.10.79.61
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

To define routing to the Completel SBC, navigate to **Global Profiles → Routing** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Completel SBC, in this case a generic name of **Trunk Server** was used, and click **Next**
- Enter the Completel SBC IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**



Edit Routing Rule

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

Next Hop Routing

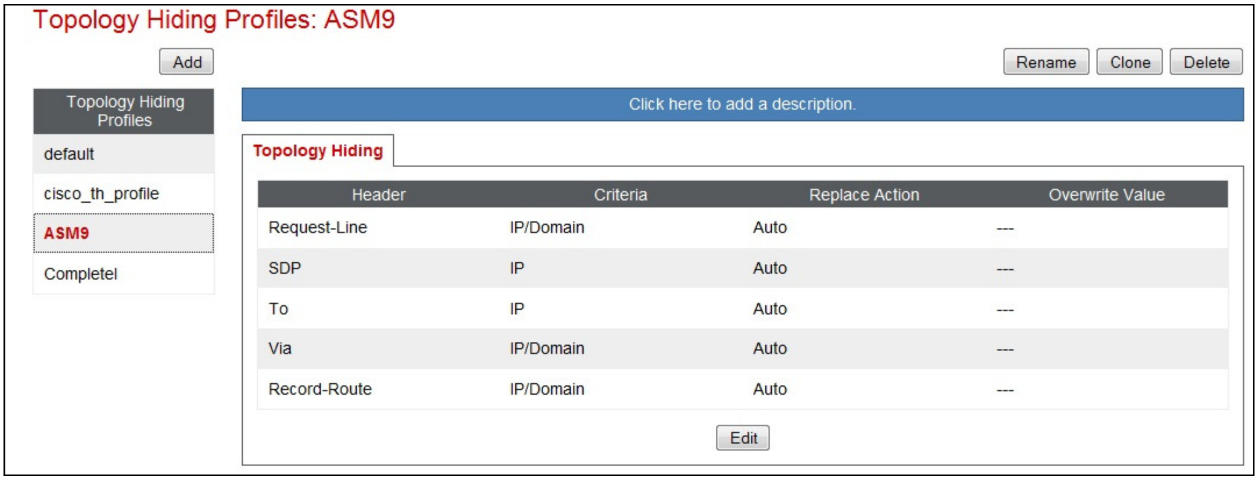
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.219.35
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ○ TCP ● UDP

7.8. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten 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 Session Manager. In some cases where Topology Hiding can’t be applied, in particular the Contact header, IP addresses are translated to Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side (not shown). Click on **Add** 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 **Request-Line**, **Record-Route** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **To** and **SDP** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**



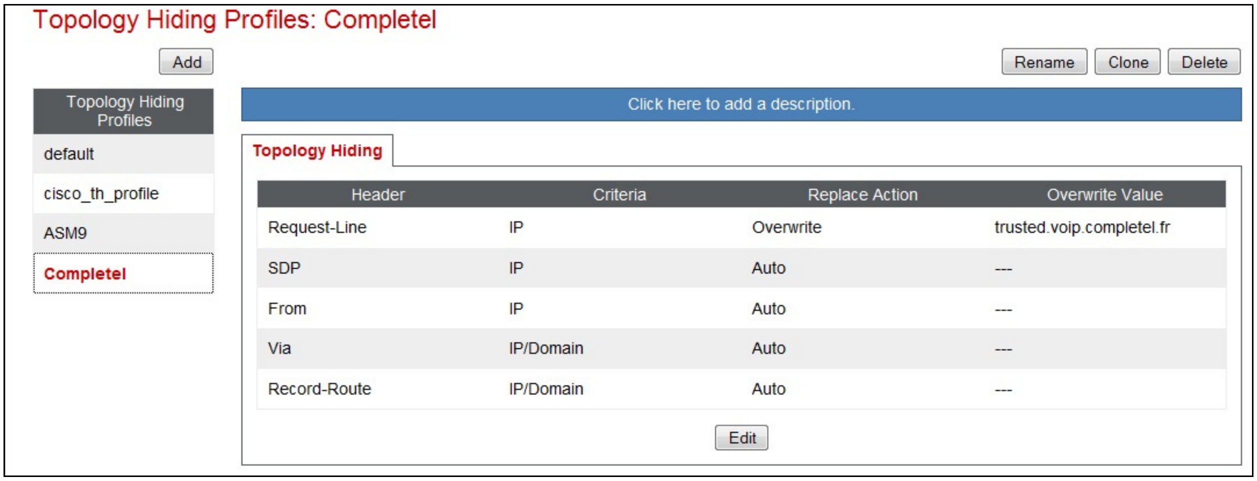
Topology Hiding Profiles: ASM9

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

Note: the use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names can be used for the enterprise and the Completel network.

To define Topology Hiding for the Completel SBC, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Completel SBC and click **Next**
- If the **Record-Route** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From** and **SDP** and **Request-Line** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For the **From** and **SDP** headers leave the **Replace Action** at the default value of **Auto**
- Set the **Replace Action** for the **Request-Line** Header to **Overwrite** and set the **Overwrite Value** to the Completel domain name. In test **trusted.voip.completel.fr** was used.



Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP	Overwrite	trusted.voip.completel.fr
SDP	IP	Auto	---
From	IP	Auto	---
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

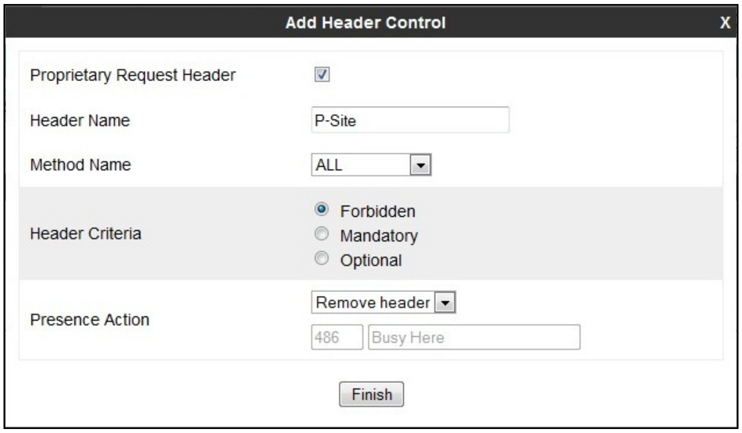
7.9. Signalling Rules

Signalling rules are a mechanism on Avaya SBCE to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. In the case of Completel, the network is sending a re-INVITE to change the codec for fax calls to T.38 after the enterprise has already sent its own re-INVITE. This is causing the enterprise to send a "491 Request Pending - another fax request in progress" message. When the network receives this message, it is clearing the call. Signalling Rules can be used to convert the 491 message to a 200 OK which prevents the network from clearing the call.

In addition to the above scenario, signalling rules can be used to convert the network response to OPTIONS, which is "503 Not Implemented – Fake Return Code", to a 200 OK which is accepted by Session Manager. They can also be used to remove proprietary headers from the SIP messages coming from the enterprise.

During test, signalling rules were used on both Session Manager and Completel network. The signalling rule on Session Manager was used to remove proprietary headers. To define the signalling rule, navigate to **Domain Policies →Signalling Rules** in the main menu on the left hand side (not shown). Click on **Add** and enter details in the Signalling Rule pop-up box

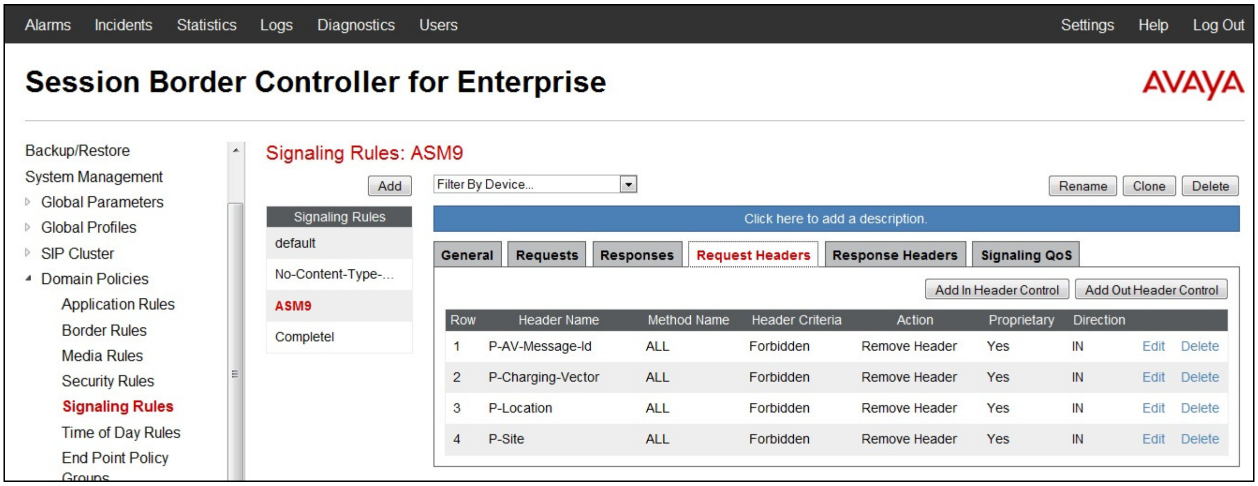
- In the **Rule Name** field enter a descriptive name for Session Manager signalling rule and click **Next** and **Next** again, then **Finish** (not shown)
- Click on the **Request Headers** tab and then click on **Add In Header Control** (not shown)
- Check the **Proprietary Request Header** box
- Enter the name of the proprietary header in the Header Name field, in the example shown **P-Site** is used and **ALL** in the Method Name field
- Check **Forbidden** in the Header Criteria options
- In the **Presence Action** drop down menu, select **Remove Header**
- Click **Finish**



Proprietary Request Header	☑
Header Name	P-Site
Method Name	ALL
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Remove header 486 Busy Here

Note: the above is an example of the proprietary headers. During test, the same was done for P-AV-Message-Id, P-Charging-Vector and P-Location headers.

When finished, all the Request Headers defined will be shown under the Request Headers tab as shown in the screenshot.

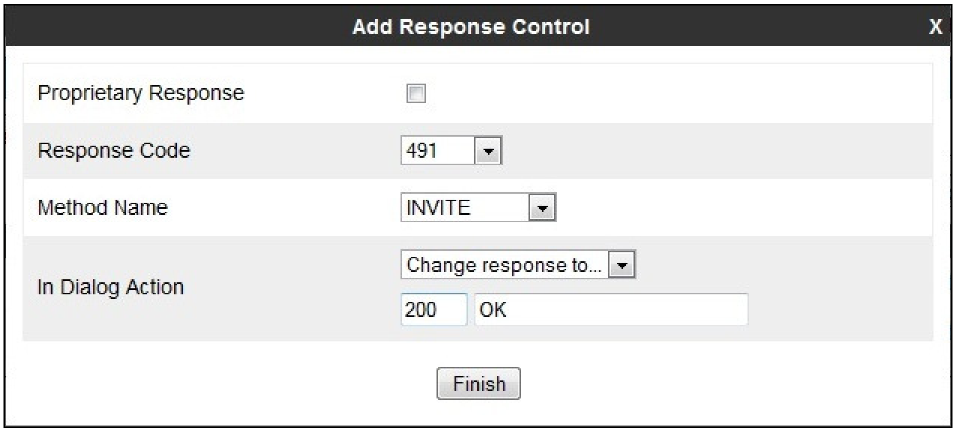


Signaling Rules: ASM9

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Site	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

The signalling rule on the Completel network was used to change the responses to "SIP OPTIONS" messages and the "491 Request Pending - another fax request in progress" messages . To define the signalling rule, navigate to **Domain Policies →Signalling Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Signalling Rule pop-up box (not shown)

- In the **Rule Name** field enter a descriptive name for the Completel network signalling rule and click **Next** and **Next** again, then **Finish** (not shown)
- Click on the **Responses** tab and then click on **Add Out Response Control** (not shown)
- In the **Response Code** drop down box, select **491**
- In the **Method Name** enter the method of the original request, in this case **INVITE**
- In the **Dialog Action** drop down box, select **Change response to…**
- In the two **Dialog Action fields**, enter **200** and **OK**
- Click **Finish**



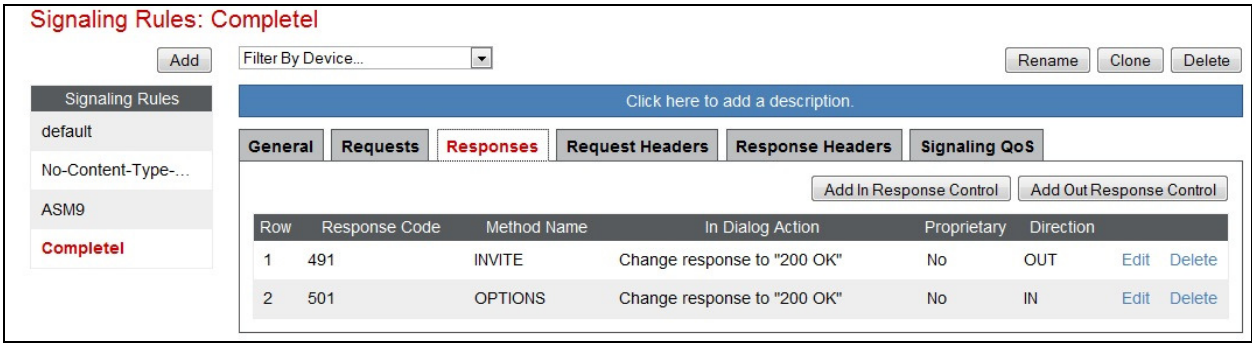
Proprietary Response	□
Response Code	491
Method Name	INVITE
In Dialog Action	Change response to... 200 OK

- Click on the **Responses** tab again and this time then click on **Add In Response Control**
- In the **Response Code** drop down box, select **503**
- In the **Method Name**, enter the method of the original request, in this case **OPTIONS**
- In the **Dialog Action** drop down box, select **Change response to**
- In the two **Dialog Action fields**, enter **200** and **OK**

- Click **Finish**

The screenshot for the Response Control for the OPTIONS message is not shown.

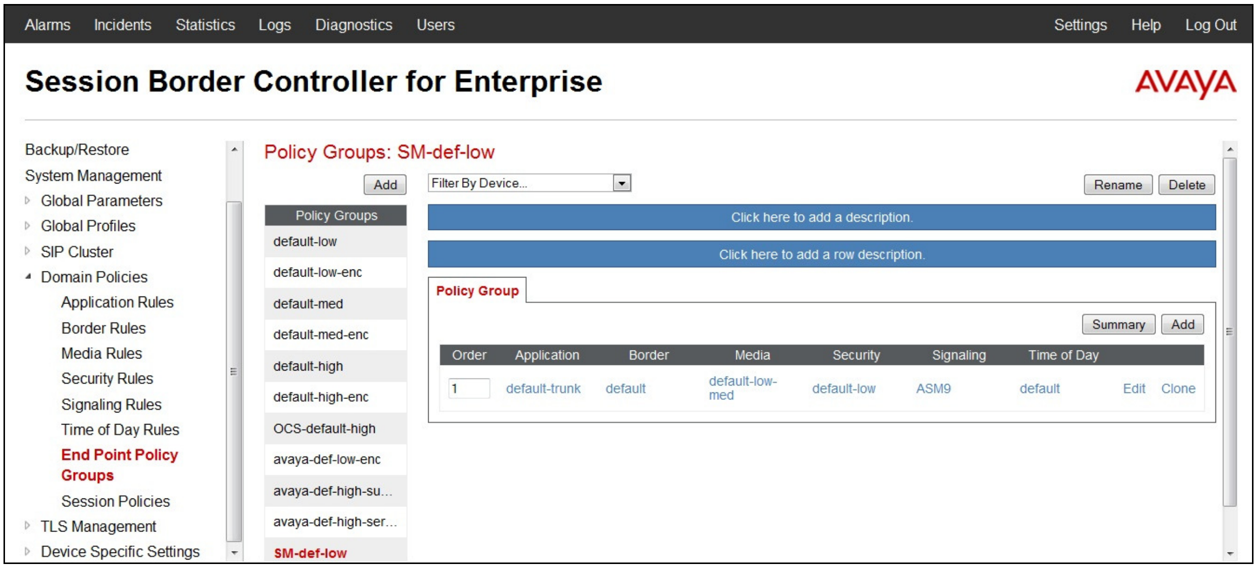
When finished, all the Request Headers defined will be shown under the Request Headers tab as shown in the screenshot.



Row	Response Code	Method Name	In Dialog Action	Proprietary	Direction		
1	491	INVITE	Change response to "200 OK"	No	OUT	Edit	Delete
2	501	OPTIONS	Change response to "200 OK"	No	IN	Edit	Delete

End Point Policy Groups are required to implement the signalling rules. To define one for Session Manager, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown)

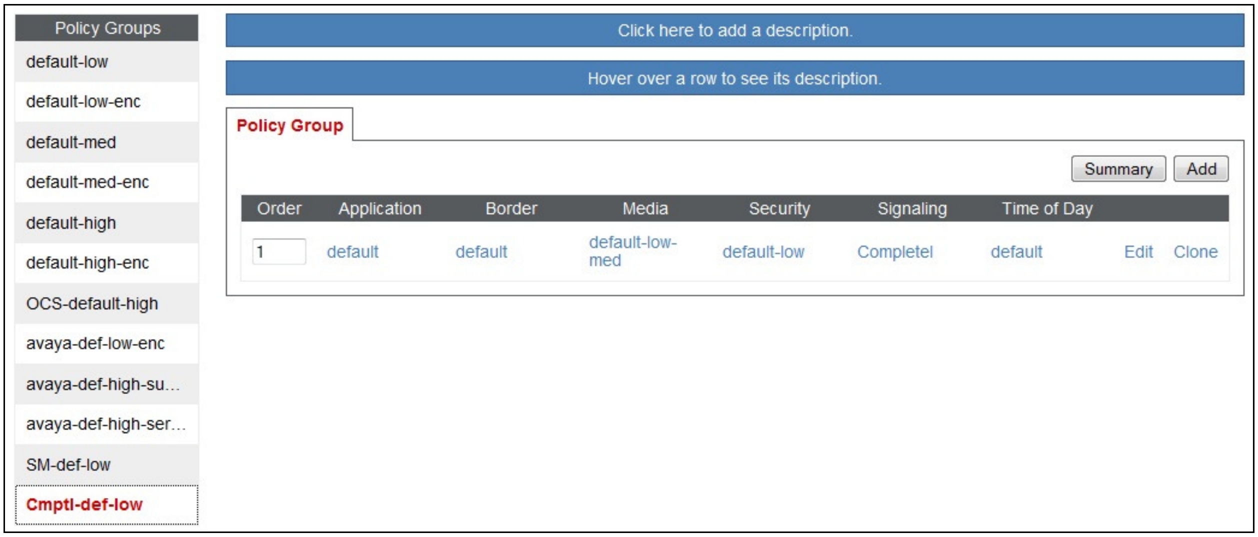
- In the **Group Name** field enter a descriptive name for the Session Manager Policy Group, in this case **SM-def-low**, and click **Next**
- Leave the **Application**, **Border**, **Media**, **Security** and **Time of Day** fields at their default values
- In the **Signaling** drop down menu, select the recently added signalling rule for Session Manager (**ASM9**)
- Leave the Time of Day field at its default value



Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-low	ASM9	default	Edit	Clone

To define an End Point Policy Group for the Completel network, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown)

- In the **Group Name** field enter a descriptive name for the Completel network, in this case **Cmptl-def-low**, and click **Next**
- Leave the **Application**, **Border**, **Media**, **Security** and **Time of Day** fields at their default values
- In the **Signaling** drop down menu, select the recently added signalling rule for the Completel network (**Completel**)
- Leave the Time of Day field at its default value



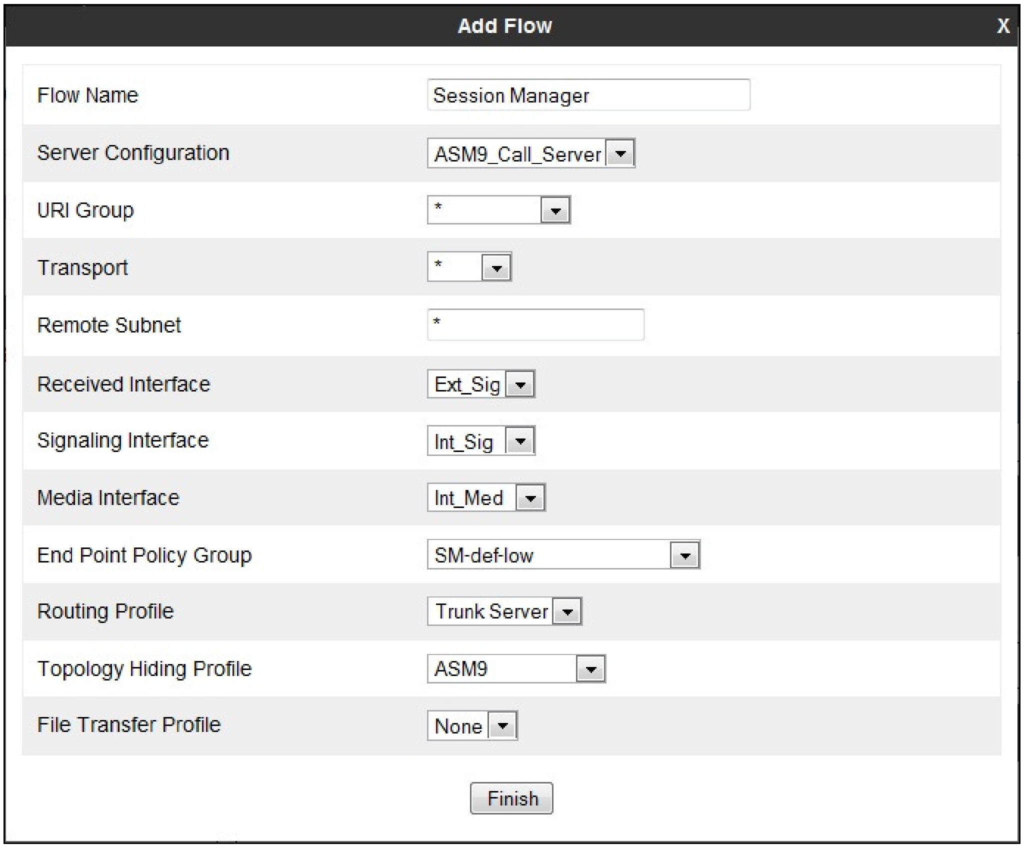
Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default	default	default-low-med	default-low	Completel	default	Edit	Clone

7.10. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from Session Manager to the Completel SBC and an incoming flow from the Completel SBC to Session Manager. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to the Completel SBC and vice versa.

To define a Server Flow for Session Manager, navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab. Select **Add Flow** (not shown). Enter details in the pop-up menu.

- 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 server flow for Session Manager, in this case **Session Manager** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.6** for Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Session Manager is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Completel network defined in **Section 7.7.**
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for Session Manager defined in **Section 7.9**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.8** and click **Finish.**

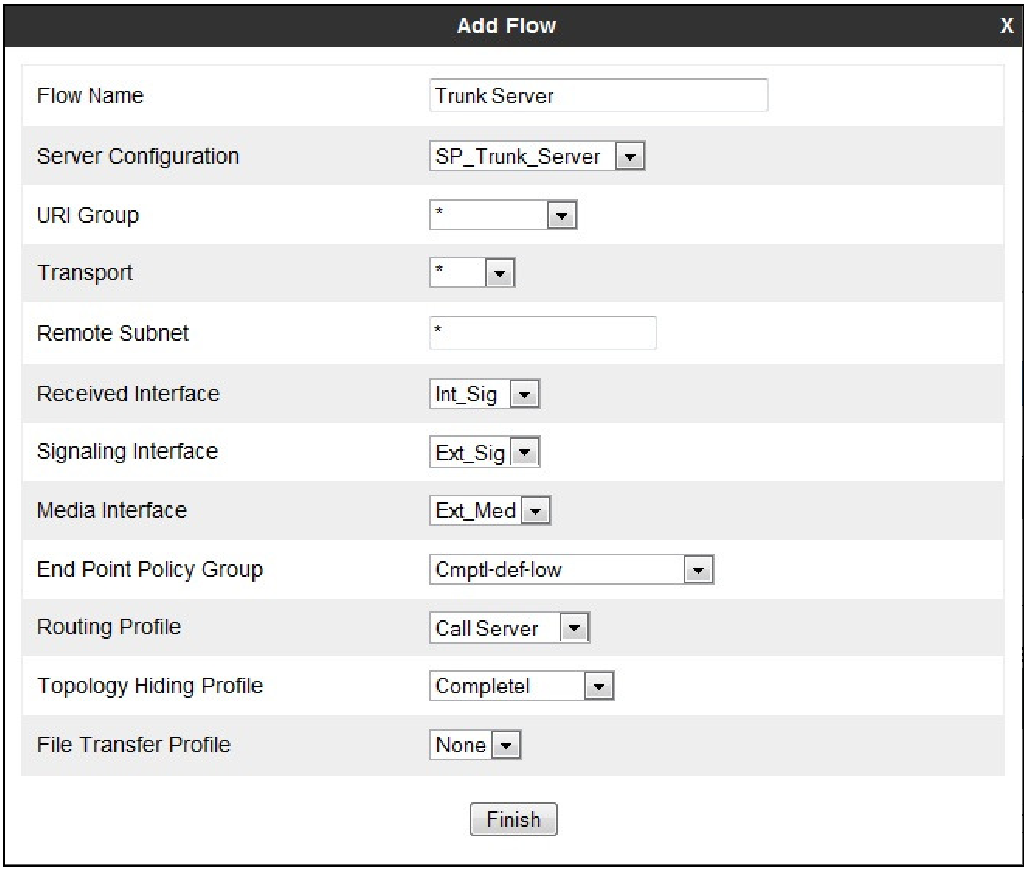


Add Flow

Flow Name	Session Manager
Server Configuration	ASM9_Call_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Med
End Point Policy Group	SM-def-low
Routing Profile	Trunk Server
Topology Hiding Profile	ASM9
File Transfer Profile	None

To define a Server Flow for the Completel network,
navigate to **Device Specific Settings → End Point Flows**. Click on the **Server Flows** tab. Select **Add Flow** (not shown). Enter details in the pop-up menu.

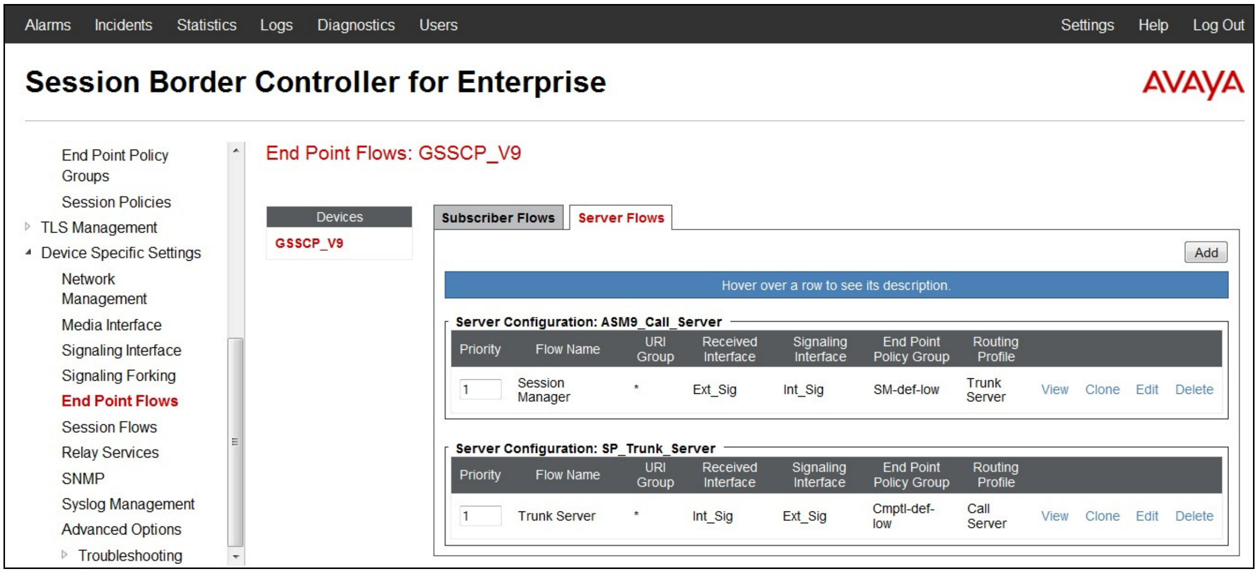
- In the **Name** field enter a descriptive name for the server flow for the Completel network, in this case a generic name of **Trunk Server** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.6** for the Completel network
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Completel network is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Completel network is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the Completel network is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.7.**
- In the **End Point Policy Group** drop down menu, select the End Point Policy Group that contains the Signalling Rules for Completel defined in **Section 7.9**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Completel network defined in **Section 7.8** and click **Finish.**



Add Flow

Flow Name	Trunk Server
Server Configuration	SP_Trunk_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Med
End Point Policy Group	Cmptl-def-low
Routing Profile	Call Server
Topology Hiding Profile	Completel
File Transfer Profile	None

The information for all Server Flows is shown on a single screen on Avaya SBCE.



Session Border Controller for Enterprise

End Point Flows: GSSCP_V9

Hover over a row to see its description.

Server Configuration: ASM9_Call_Server

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Session Manager	*	Ext_Sig	Int_Sig	SM-def-low	Trunk Server	View	Clone	Edit	Delete

Server Configuration: SP_Trunk_Server

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk Server	*	Int_Sig	Ext_Sig	Cmptl-def-low	Call Server	View	Clone	Edit	Delete

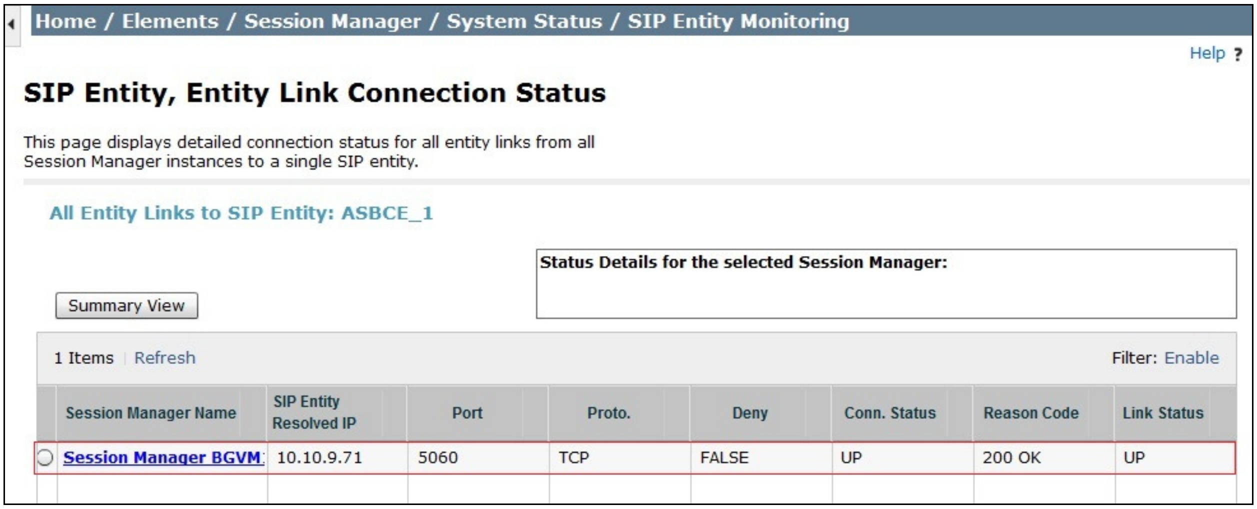
8. Configure Completel Equipment

The configuration of the Completel equipment used to support the Completel UCM service is outside of the scope of these Application Notes and will not be covered. To obtain further information on Completel equipment and system configuration please contact an authorised Completel 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** (not shown). Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.



Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

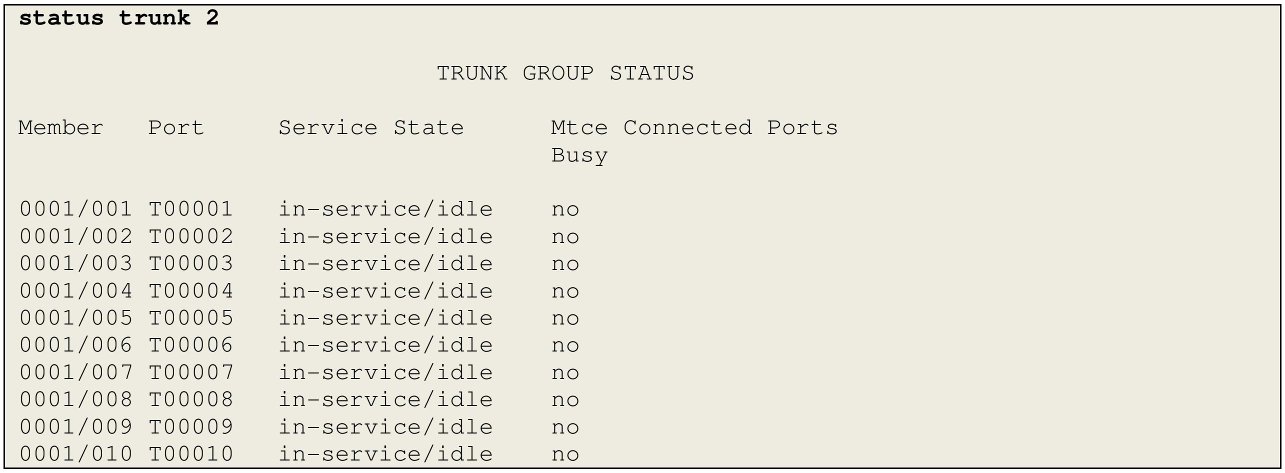
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: ASBCE_1

Status Details for the selected Session Manager:

	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	Session Manager BGVM	10.10.9.71	5060	TCP	FALSE	UP	200 OK	UP

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



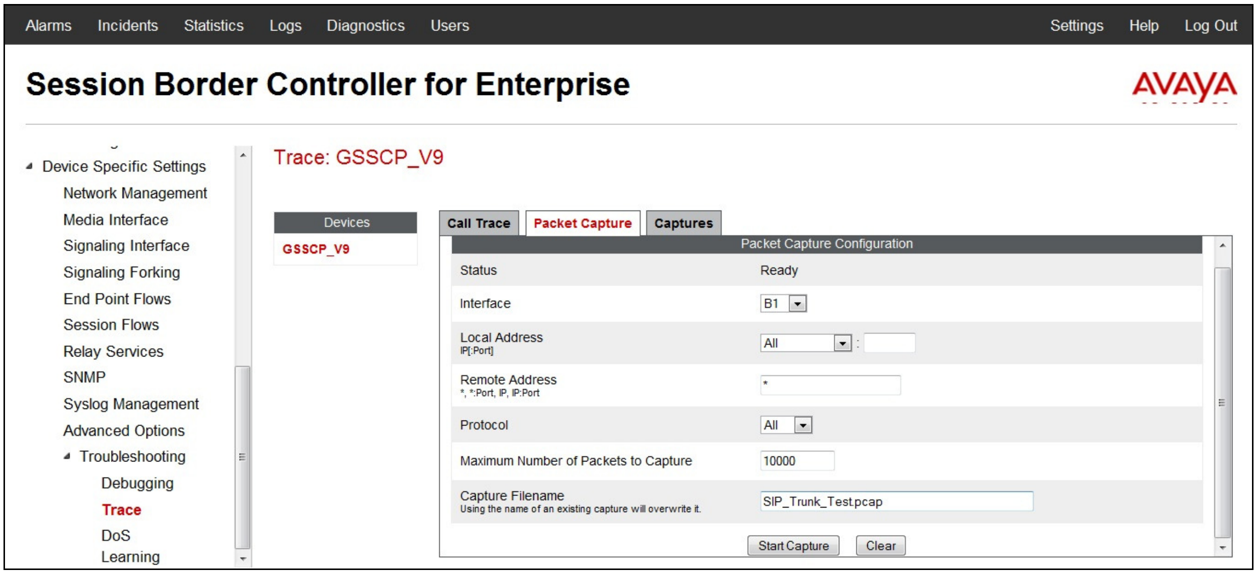
```
status trunk 2

                                 TRUNK GROUP STATUS

Member    Port      Service State      Mtce Connected Ports
                                       Busy

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 Avaya SBCE trace facility to check that the REGISTER requests sent from Avaya SBCE are receiving a response.

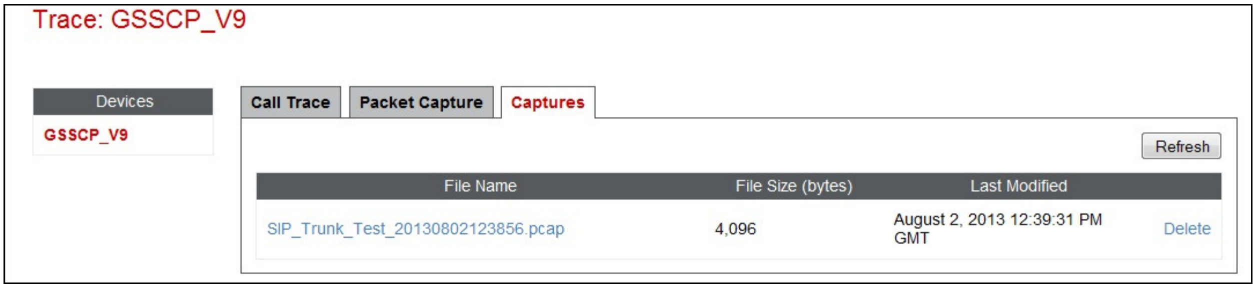
   To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

   - 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 R6.2 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise to the Completel UCM service. Completel UCM 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] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.2, December 2012.

[2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.

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

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

[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/

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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