Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise to Support Vodafone Netherlands (NL) SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone NL SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise. Vodafone NL is a member of the DevConnect Global SIP Service Provider program. These Application Notes are the result of a retest of the Vodafone NL SIP Trunk Service and supersede the previous Application Notes.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server and Avaya Session Border Controller for Enterprise. Customers using this Avaya SIP-enabled enterprise solution with the Vodafone NL SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. The Vodafone solution incorporates routing for calls placed to and from their Mobile and Fixed networks separately and offer short dialing from dedicated mobile telephones. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers and Fixed short dial numbers assigned by Vodafone NL. Incoming PSTN calls were made to H.323, SIP, Digital and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Vodafone NL to PSTN and Vodafone Mobile destinations using short dial and full number. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and Analogue telephones.
- Calls using G.729, G.711A and G.711Mu codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the pass-through mode. T.38 was also tested and this is an optional feature.
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones was turned used during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

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

- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X Communicator was used to test soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers (such as 112) was not tested.
- When CM responds with 488 "Not Acceptable Here" during codec rejection, the network re-attempts to establish the call during which the caller gets dead air and no indication of call failure.
- When CLID is restricted, the user part of the From and P-Asserted-ID fields is set to "anonymous" and the Privacy header is not sent. This header is not correct but is not visible to the user as the endpoints display the caller is "Private" as appropriate.
- T.38 fax transmission is not supported. Faxing may or may not work in this environment..
- When signalling fails and a 500 "Server Link Monitor Status Down" is received from the Session Manager, the network attempts to re-establish the call during which the caller gets dead air and no indication of call failure.
- When a call is silent for 35 to 40 minutes during a long duration call, the media stream fails, but the call will stay connected with a one way audio condition.

2.3. Support

For technical support on Vodafone Netherlands SIP trunking services, contact Vodafone Netherlands support at http://www.vodafone.nl/zakelijk/totaal_oplossingen/vast_en_mobiel/.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone NL SIP Trunk Service. Located at the enterprise site is a Session Manager and Communication Manager. Endpoints are Avaya 9600 series IP telephones, Avaya 2400 series Digital Telephone, an Avaya Desktop Video Device, a PC running Avaya one-X® Communicator an Analogue Telephone and Fax Machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

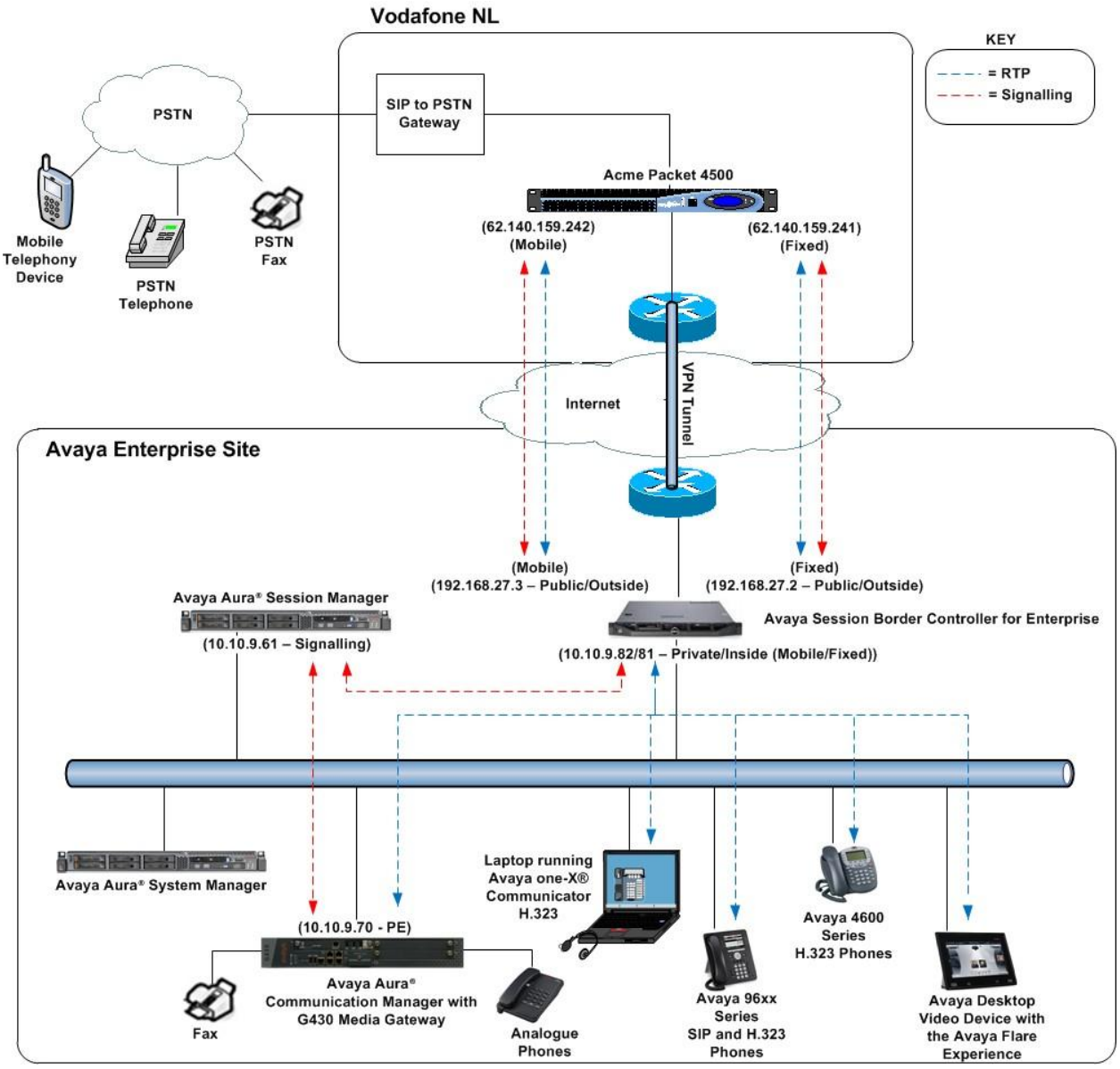


Figure 1: Vodafone NL SIP Solution Topology

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya S8300 Server	Avaya Aura® Communication Manager R6.0.1 (R016x.00.1.510.1-19009)
Avaya G430 Media Gateway	FW 30.12.1
Avaya S8800 Server	Avaya Aura® Session Manager R6.2 (6.2.0.0.620120)
Avaya S8800 Server	Avaya Aura® System Manager R6.2 (System Platform 6.2.0.0.27, Template 6.2.12.0)
Avaya Session Border Controller for Enterprise Server	Avaya Session Border Controller for Enterprise 4.0.5.Q02
Avaya 1616 Phone (H.323)	1.301
Avaya 4621 Phone (H.323)	2.902
Avaya 9630 Phone (H.323)	3.103
Avaya 9630 Phone (SIP)	R2.6 SP6
Avaya A175 Desktop Video Device	Flare Experience Release 1.1
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	Avaya one–X® Communicator 6.1.3.08-SP3-Patch2-35791
Analogue Phone	N/A
Vodafone Netherlands	
Vodafone Office Voice	1.0
Vodafone OneVoice Corporate	1.0
Cisco UBE	15.2.3
Acme Packet Net-Net 4500	SCX6.2.0 MR-6 Patch 2 (Build 876)

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signaling associated with Vodafone NL SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Vodafone NL via the ASBCE and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Vodafone NL network. Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya S8800 Server and Avaya 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 Vodafone NL network, and any other SIP trunks used.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  10
```

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

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

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

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Type **change node-names ip** to make changes to the **IP Node Names**. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **ASM9** and **10.10.9.61** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                  IP Address
ASM7                  10.10.7.61
ASM9                  10.10.9.61
SM100                 10.10.8.56
default               0.0.0.0
procr                 10.10.8.67
procr6                ::
```

5.3. Administer IP Network Region

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

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is set to yes to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources
- 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** was used

```
change ip-network-region 1                                    Page   1 of  20
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

Use the **change ip-codec-set** command 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 Vodafone NL were configured, namely **G.729A**, **G.711A** and **G.711MU**

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

Vodafone NL SIP Trunk Service uses pass-through which is not a method supported by Avaya. Configure the pass-through fax protocol by setting the **Fax Mode** to **pass-through** on **Page 2** of the codec set form as shown below.

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

                           IP Codec Set

                               Allow Direct-IP Multimedia? n

                     Mode                Redundancy
    FAX              pass-through         0
    Modem            off                  0
    TDD/TTY          US                   3
    Clear-channel    n                    0
```

Note: Avaya only support T.38 fax interoperability with other third parties. Even though **pass-through** was tested and no issues were found during testing, Avaya cannot guarantee reliable fax transmission using this protocol.

5.5. Administer SIP Signalling Groups

Add a signalling group and trunk group for inbound and outbound PSTN calls to Vodafone NL SIP Trunk Service and configure using TCP (Transmission Control Protocol) and tcp port of 5060. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set the **Group Type** field to **sip**
- The **Transport Method** field is set to **tcp**
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2**
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **asm9**), also shown in **Section 5.2**
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.3.** This field logically establishes the **far-end** for calls using this signaling group as network region **1**
- The **Direct IP-IP Audio Connections** field is set to **y**
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833

The default values for the other fields may be used.

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

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
       Q-SIP? n                                          SIP Enabled LSP? n
    IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                Far-end Node Name: ASM9
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1

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

5.6. Administer SIP Trunk Group

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

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan, i.e. **101**
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **tie**
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

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

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

On **Page 2** of the trunk-group form set the **Preferred Minimum Session Refresh Interval(sec)** to **900** as the optimum value for interworking with the Vodafone NL network. This results in a minimum session expiration (Min-SE) time of 1800 seconds. Min-SE indicates the minimum value for the session interval in seconds. When used in an INVITE or UPDATE request, it indicates the smallest value of the session interval that can be used for that session.

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

TRUNK PARAMETERS

     Unicode Name: auto
                                         Redirect On OPTIM Failure: 5000

            SCCAN? n                                Digital Loss Group: 18
                    Preferred Minimum Session Refresh Interval(sec): 900
```

On **Page 3,** set the **Numbering Format** field to **private.** This allows the number to be sent to Vodafone NL in national format with the leading 0.

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



                     Numbering Format: private
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n


                                   Modify Tandem Calling Number: no
```

On **Page 4,** set the **Support Request History** to **n** as History Info is not used by Vodafone NL. Set **Telephone Event Payload Type** to **101**.

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

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

5.7. Administer Calling Party Number Information

In this section the Calling Party Number sent when making a call using the SIP trunk is specified

5.7.1. Set Private Unknown Numbering

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, stations with a **4**-digit extension **8000** and **8396** will send the calling party numbers **038xxxxxx0** and **038xxxxxx1** to Vodafone NL SIP Trunk Service. These calling party numbers will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Public DID numbers have been masked for security purposes.

```
change private-unknown-numbering 0                              Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN           CPN
Len Code          Grp(s)    Prefix        Len
 4  8000          1           038xxxxxx0    10    Total Administered: 2
 4  8396          1           038xxxxxx1    10       Maximum Entries: 540
```

5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to Vodafone NL SIP Trunk Service. In the sample configuration, the single digit **9** is used as the ARS access code. Avaya telephone users will dial **9** to reach an outside line. Use the **change feature-access-codes** command to configure or observe **9** as the **Auto Route Selection (ARS) - Access Code 1.**

```
change feature-access-codes                                    Page   1 of  10
                            FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *69
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 7
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

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 illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning **0** or **00**. The entry for **06** is used to route to the Vodafone Mobile network. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group.

```
change ars analysis 02                                         Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                 Location:  all           Percent Full:    1

          Dialed           Total     Route     Call    Node  ANI
          String          Min  Max  Pattern   Type    Num   Reqd
    0                     8    8    1         pubu          n
    00                    13   14   1         pubu          n
    06                    10   10   1         pubu          n
```

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group 1. Set the **Numbering Format** to **unk-unk** to avoid conversion to E.164 format.

```
change route-pattern 1                                          Page   1 of   3
                     Pattern Number: 1   Pattern Name: tosm100
                           SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                           Dgts                                     Intw
 1: 1    0                                                           n   user
 2:                                                                  n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user
 6:                                                                  n   user

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

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Vodafone NL can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by Vodafone NL correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **038xxxxxxx** to a 4 digit extension by deleting all of the incoming digits and inserting an extension. The 209x entries are used to allow incoming calls from the Vodafone Mobile network to be directed to assigned extensions. Public DID numbers have been masked for security purposes.

```
change inc-call-handling-trmt trunk-group 1                     Page   1 of   3
                    INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             10 038xxxxxx0       all 8000
 tie             10 038xxxxxx1       all 8396
 tie             10 038xxxxxx2       all 8346
 tie             10 038xxxxxx3       all 8296
 tie             10 038xxxxxx4       all 8601
 tie             10 038xxxxxx5       all 8316
 tie             4  2090             all 8000
 tie             4  2091             all 8396
 tie             4  2092             all 8346
 tie             4  2093             all 8296
 tie             4  2094             all 8601
```

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

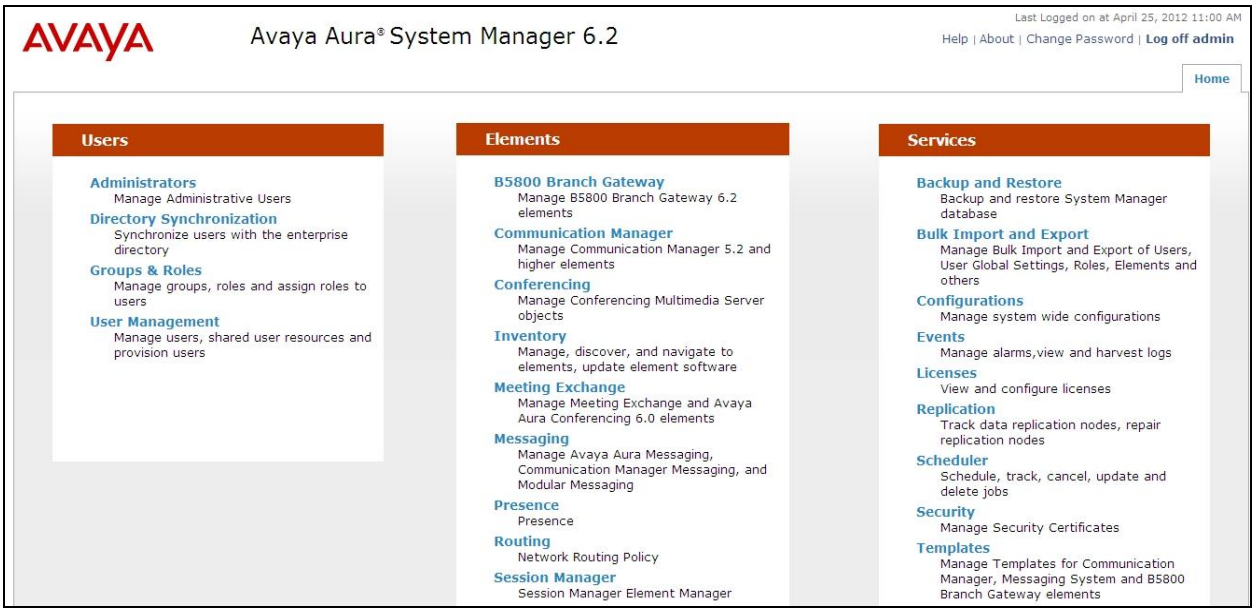
6. Configuring Avaya Aura® Session Manager

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

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

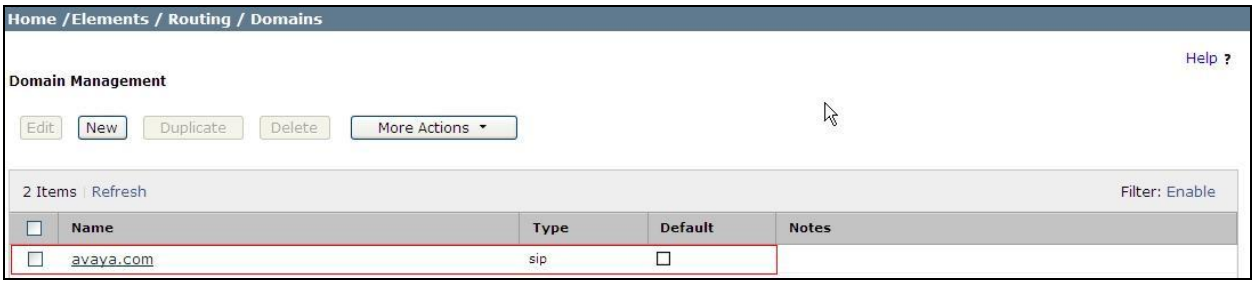
6.1. Log in to Avaya Aura® System Manager

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



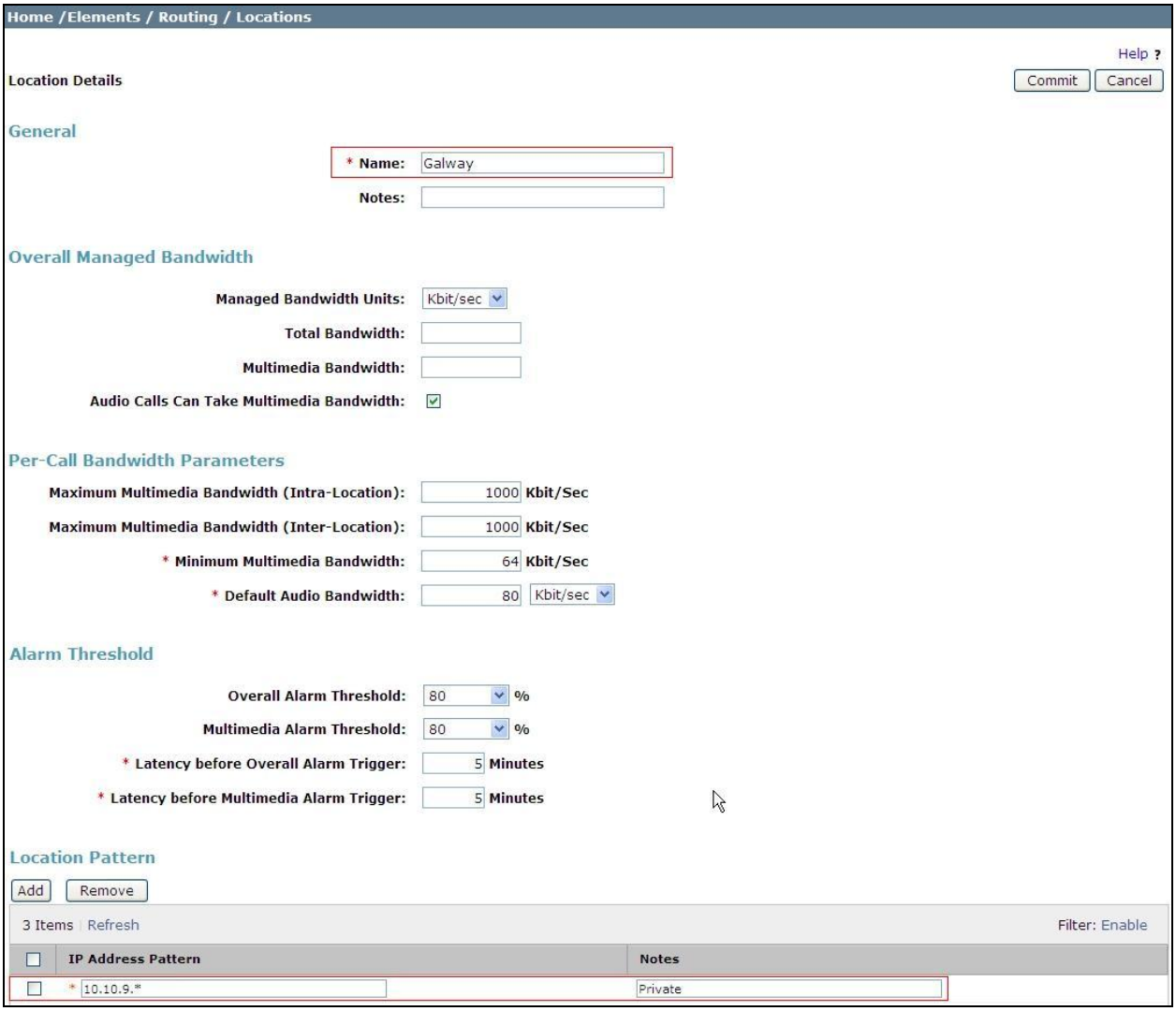
6.2. Administer SIP domain

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



6.3. Administer Locations

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



6.4. Administer SIP Entities

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

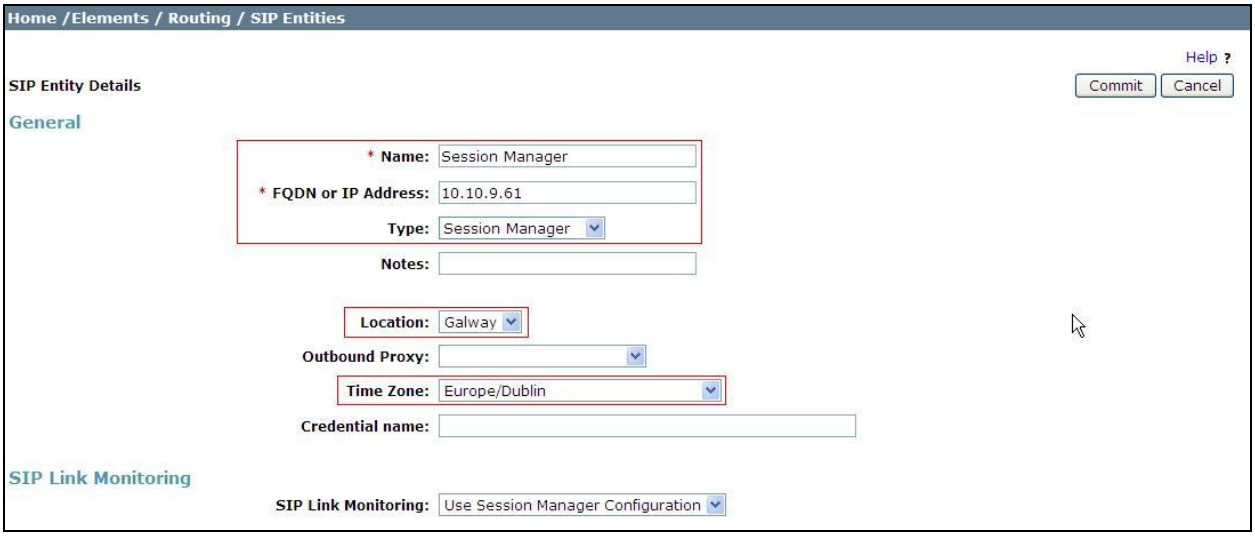
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP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

In this configuration there are three SIP Entities.

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

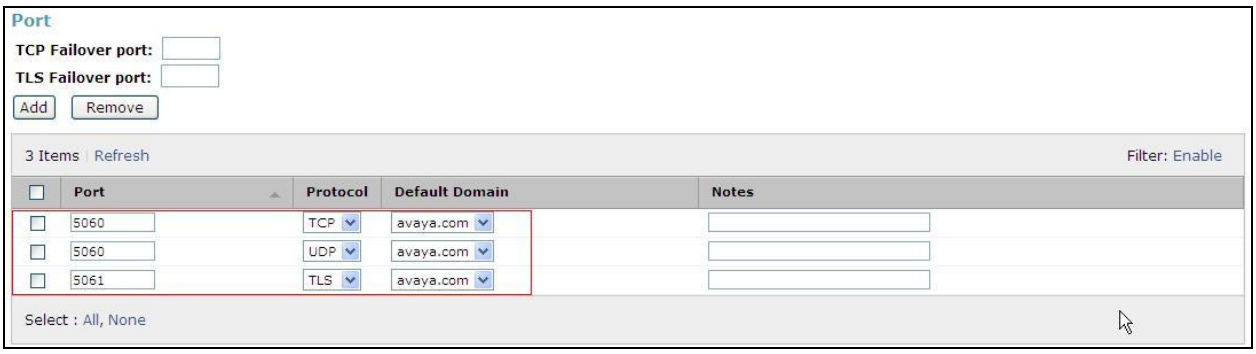
6.4.1. Avaya Aura® Session Manager SIP Entity

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



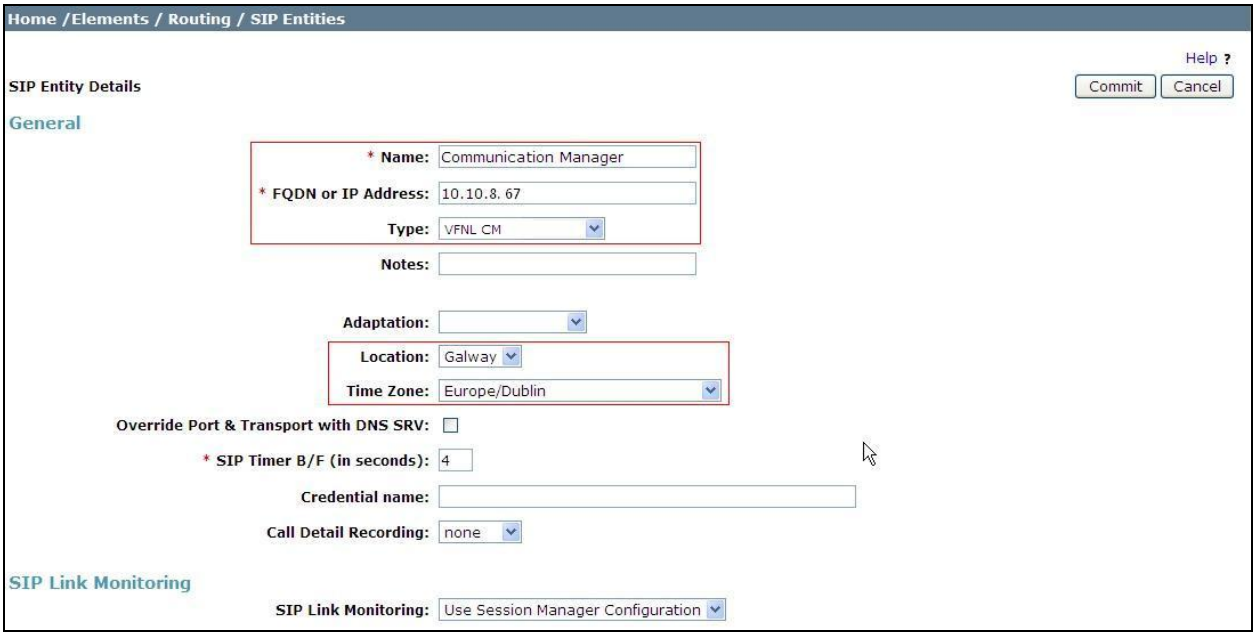
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

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



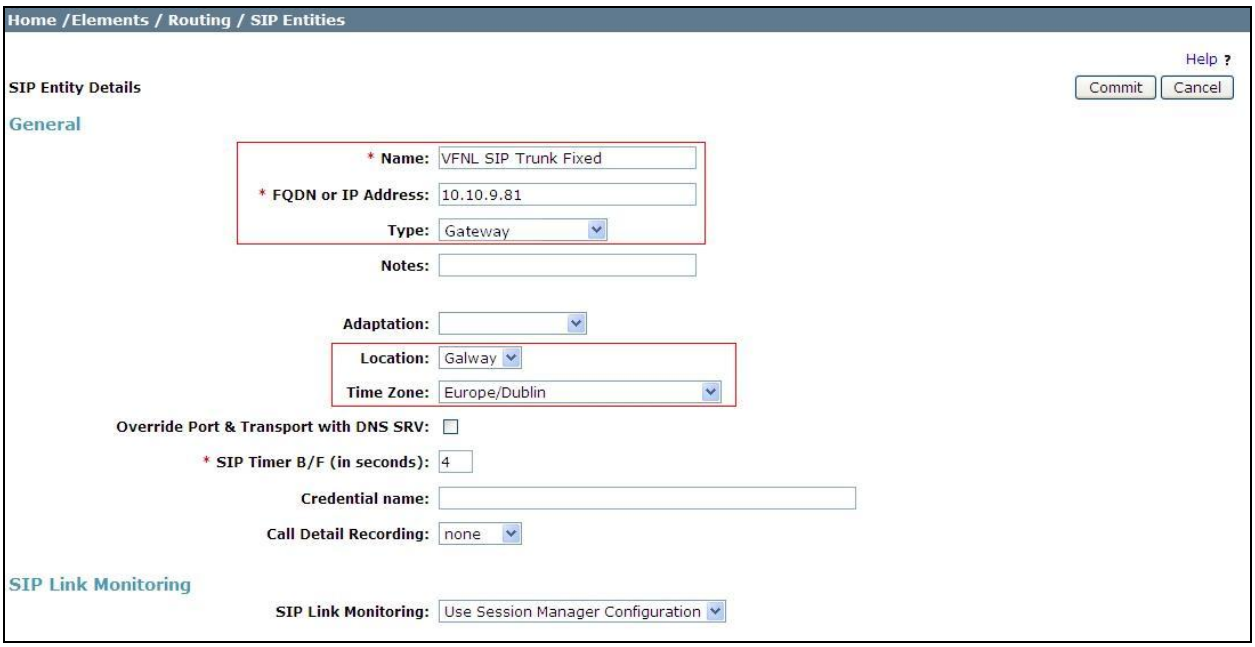
6.4.2. Avaya Aura® Communication Manager SIP Entity

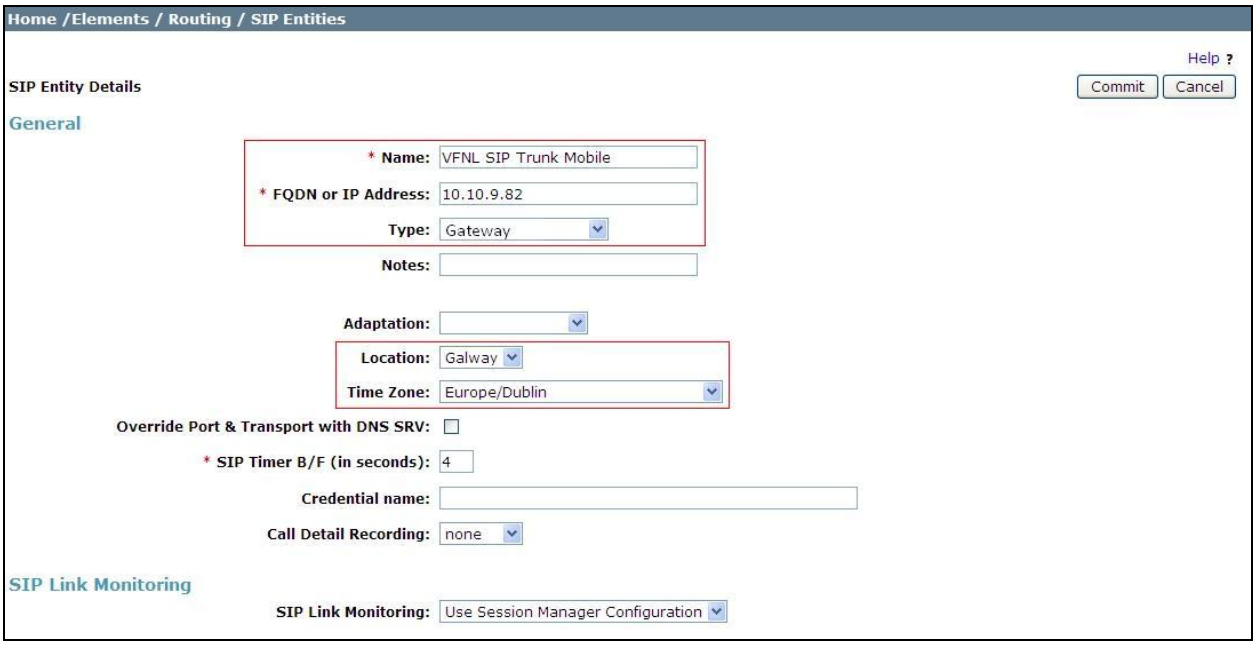
The following screens show the SIP entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling. The entity **Type** is set to **CM**.



6.4.3. Avaya Session Border Controller for Enterprise SIP Entities

The following screen shows the SIP entity for the Avaya Session Border Controller for Enterprise used for routing Fixed and Mobile calls. The **FQDN or IP Address** field is set to the IP address of the private interfaces administered in **Section 7** of this document.





6.5. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu 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 **Protocol** field enter the transport protocol to be used to send SIP requests
- 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

Click **Commit** (not shown) to save changes. The following screen shows the Entity Links used in this configuration.

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* VFNL CM Link	* Session Manager	TCP	* 5060	* VFNL CM	* 5060	Trusted	

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* VFNL Fixed Link	* Session Manager	TCP	* 5060	* VFNL SIP Trunk Fixed	* 5060	Trusted	

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* VFNL Mobile Link	* Session Manager	TCP	* 5060	* VFNL SIP Trunk Mobile	* 5060	Trusted	

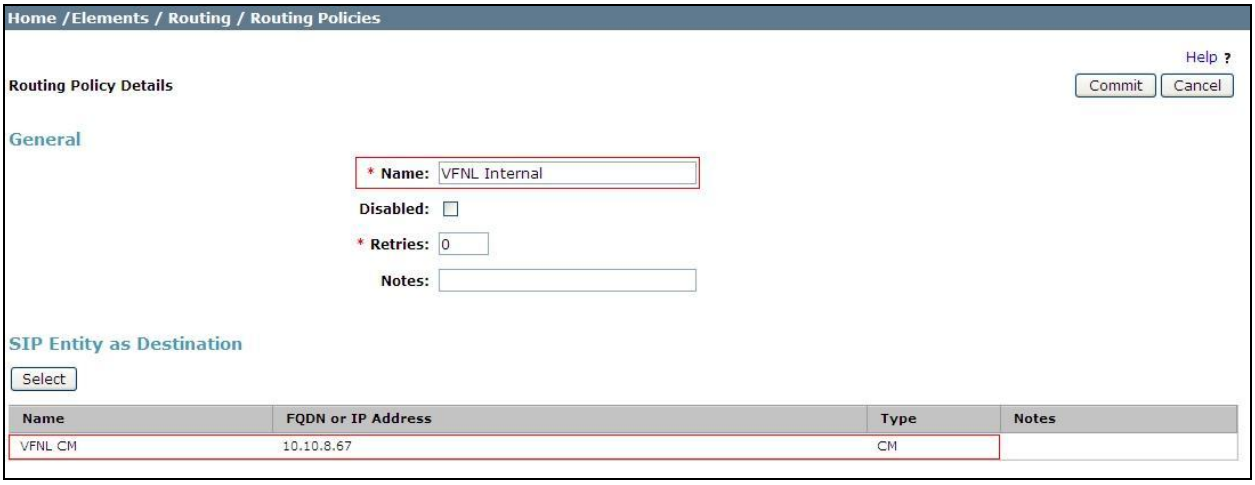
6.6. Administer Routing Policies

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).

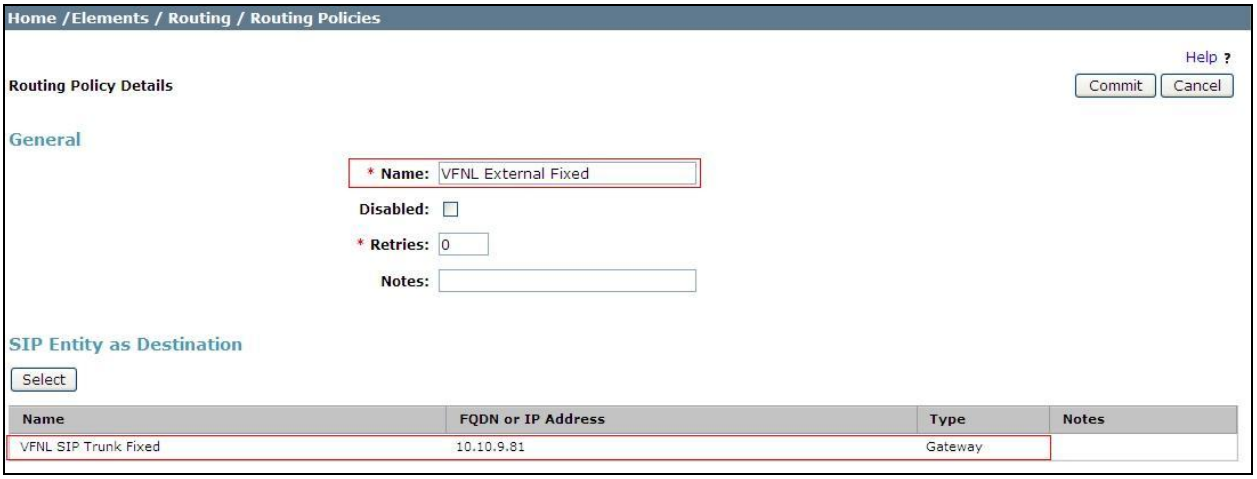
Under **General**:

- 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

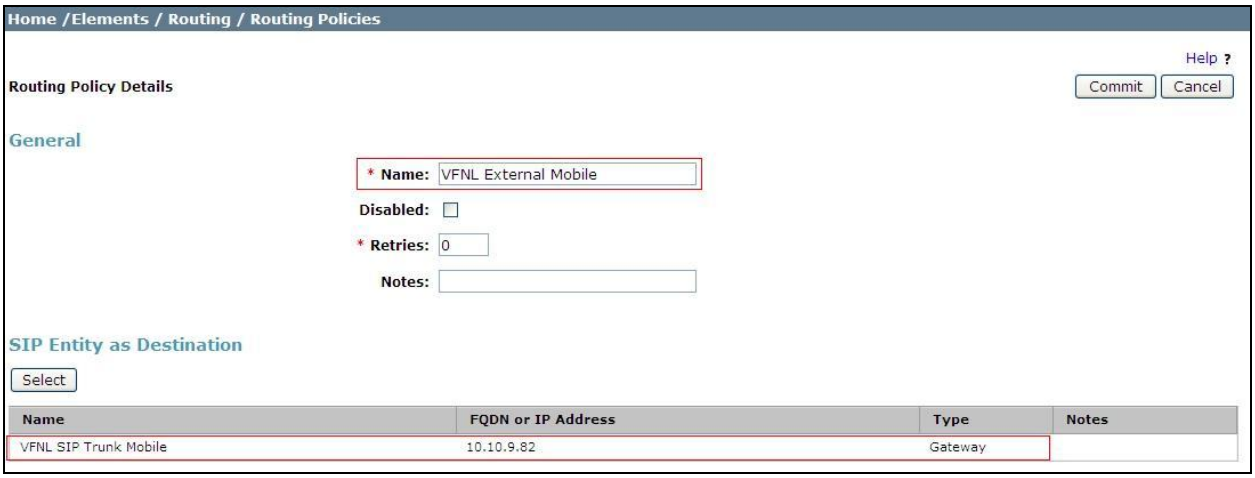
The following screen shows the routing policy for Communication Manager:



The following screen shows the routing policy for Avaya Session Border Controller for Enterprise Fixed:



The following screen shows the routing policy for Avaya Session Border Controller for Enterprise Mobile:



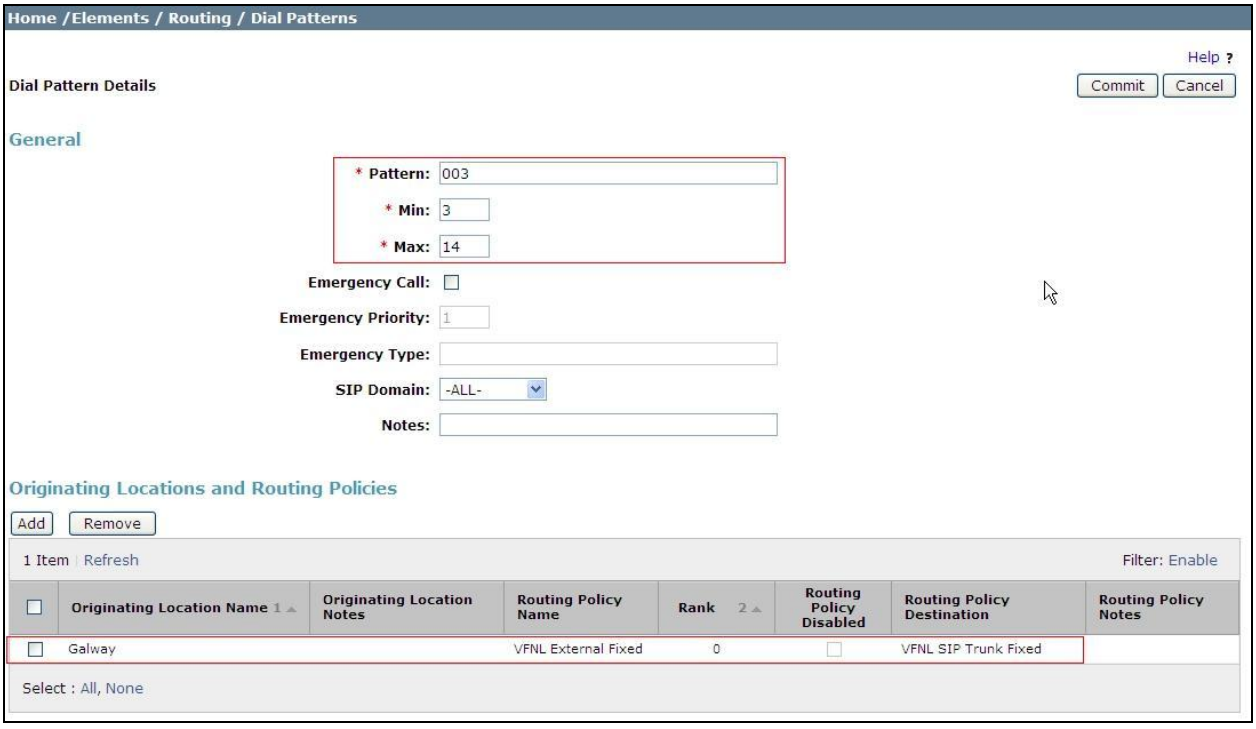
6.7. Administer Dial Patterns

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).

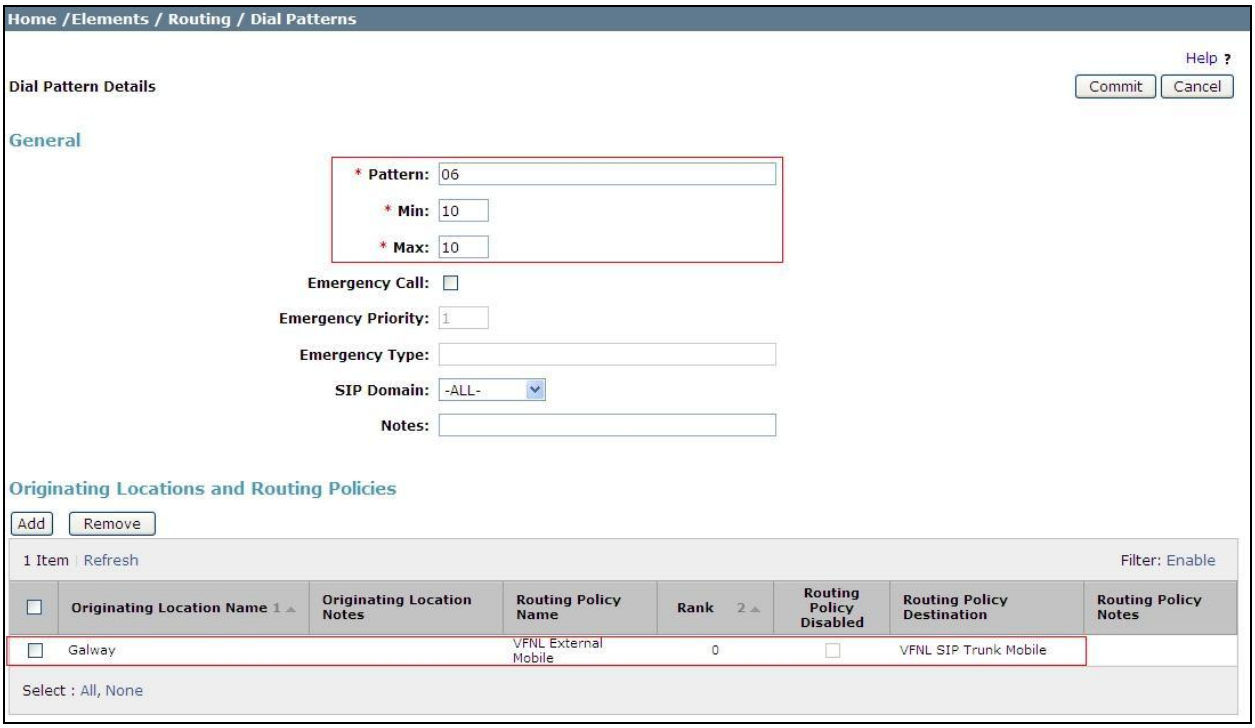
Under **General**:

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

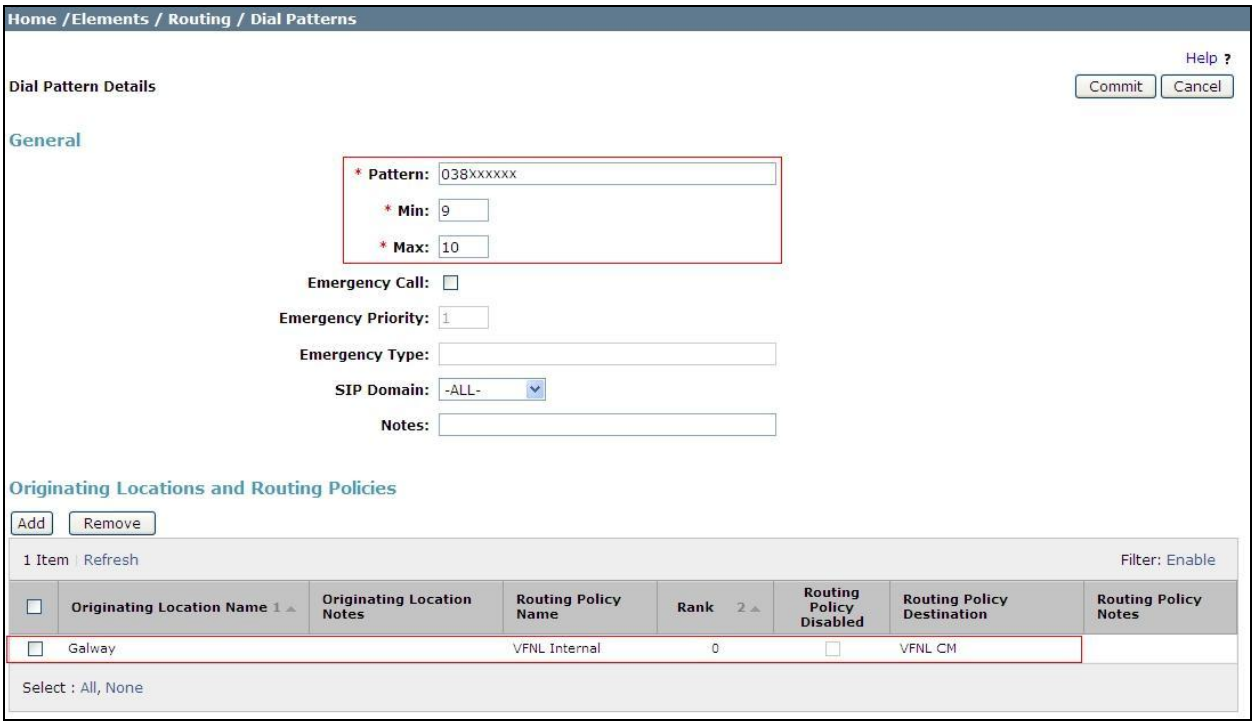
Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.6.** Click **Select** button to save (not shown). The following screen shows an example dial pattern configured for Vodafone NL SIP Trunk Service Fixed.



The following screen shows an example dial pattern configured for Vodafone NL SIP Trunk Service Mobile.



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



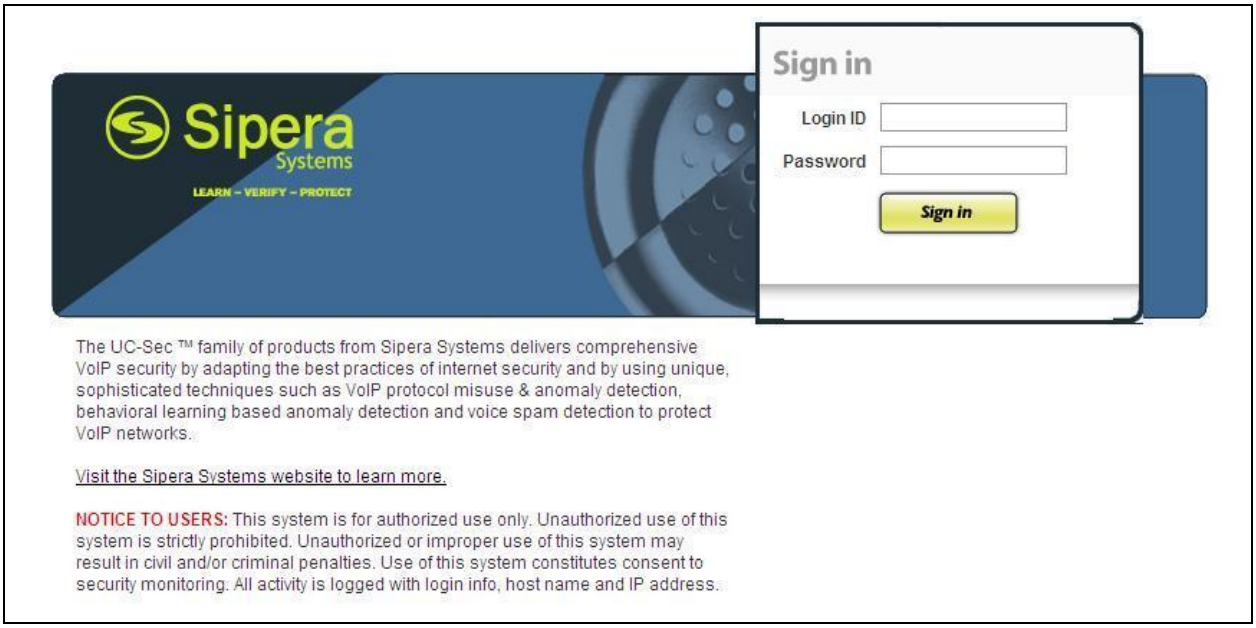
7. Avaya Session Border Controller for Enterprise Configuration

This section provides the procedures for configuring Session Border Controller for Enterprise.

7.1. Accessing UC-Sec Control Centre

Access the web interface by typing **https://x.x.x.x** (where x.x.x.x is the management IP of the E-SBC).

Select **UC-Sec Control Center** and enter the **Login ID** and **Password**.

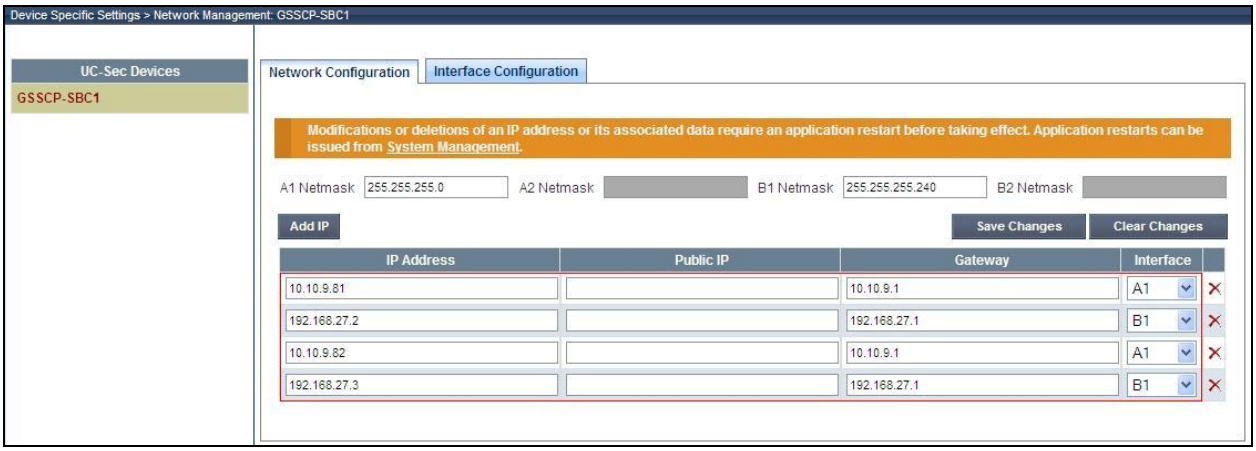


7.2. Define Network Information

Network information is required on the ASBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the ASBCE can have only one interface assigned. Two internal interface addresses and two external interface addresses are required for Vodafone NL fixed and mobile networks. To define the network information, navigate to **Device Specific Settings → Network Management** in the **UC-Sec Control Center** menu on the left hand side and click on **Add IP**. Enter details in the blank box that appears at the end of the list

- Define the internal IP addresses with screening mask and assign to interface **A1**
- Select **Save** (not shown) to save the information
- Click on **Add IP**
- Define the external IP addresses with screening mask and assign to interface **B1**
- Select **Save** (not shown) to save the information
- Select the **Network Configuration** tab and change the state of interfaces **A1** and **B1** to **Enabled** (not shown)
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar

Note: Multiple IP addresses defined on a single interface must be in the same subnet.



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

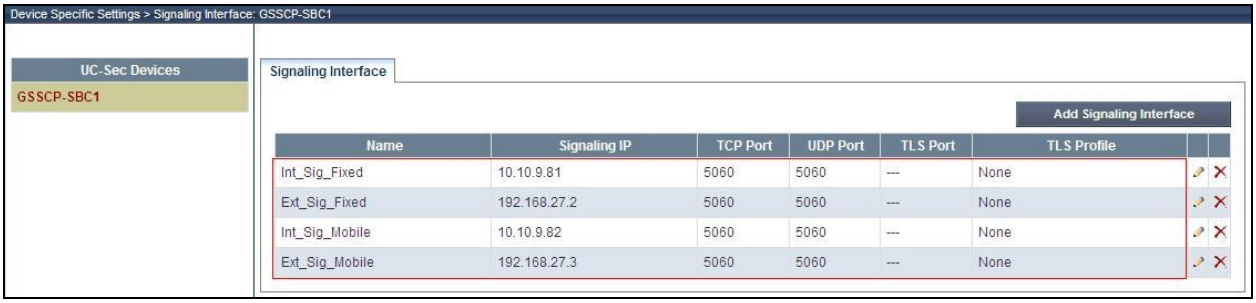
7.3. Define Interfaces

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

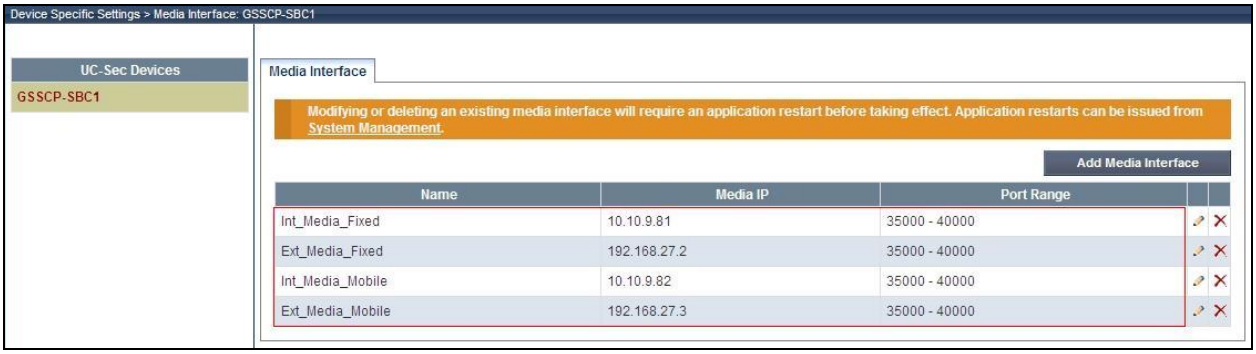
- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal signalling interface for the Vodafone NL fixed network
- Select an **internal** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for Vodafone NL
- Select **Add Signalling Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external signalling interface for the Vodafone NL fixed network
- Select an **external** interface IP address (not shown) defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for Vodafone NL
- Repeat this process for the internal and external signalling interfaces for the Vodafone NL mobile network.



7.3.2. Media Interfaces

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

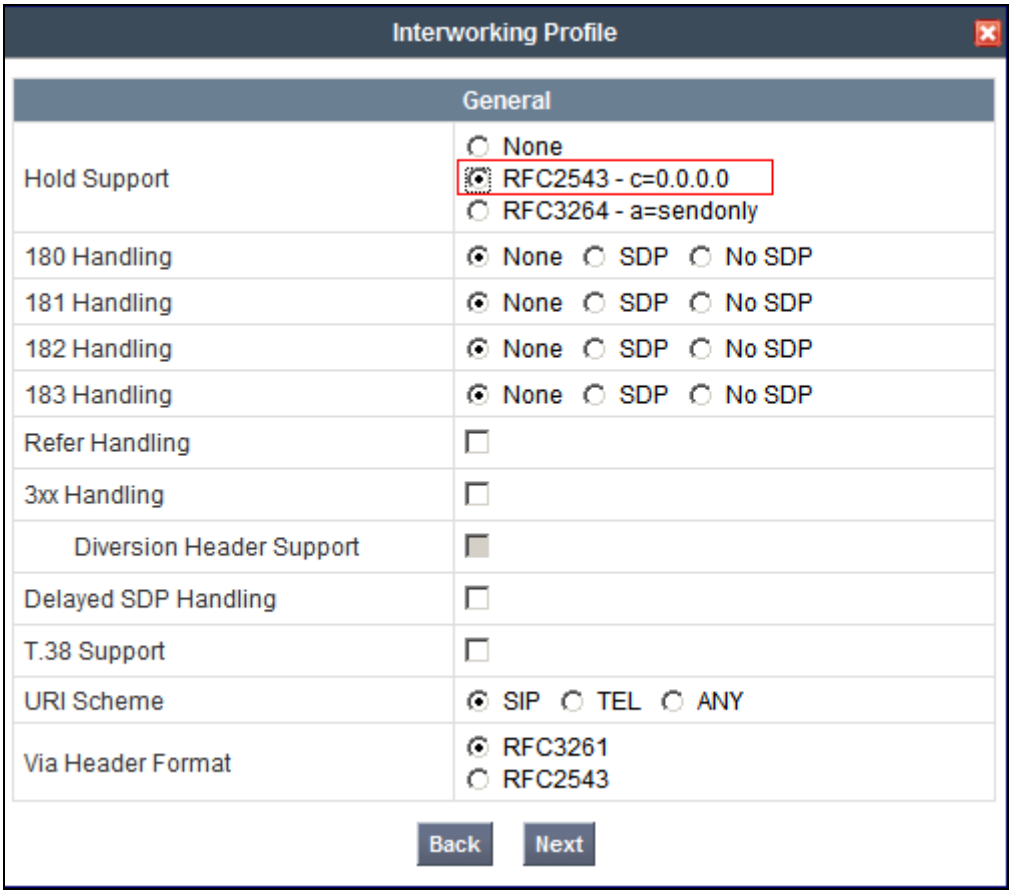
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface for the Vodafone NL fixed network
- Select an **internal** interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface for the Vodafone NL fixed network
- Select an **external** interface IP address (not shown) defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the Vodafone NL SBC
- Repeat this process for the internal and external signalling interfaces for the Vodafone NL mobile network.



7.4. Define Server Interworking

Server interworking is defined for each server connected to the ASBCE. In this case, the Vodafone NL SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define server interworking on the ASBCE, navigate to **Global Profiles → Server interworking** in the **UC-Sec Control Center** 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 **SM9_Call_Server** was used
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Change the **Hold Support** RFC to **RFC2543** then click **Next** and **Finish**



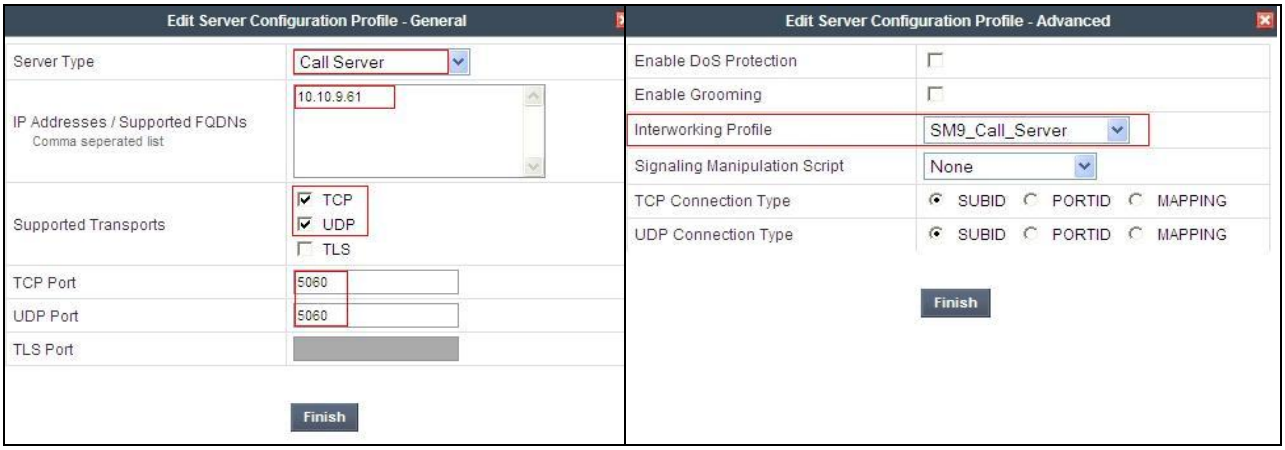
To define Server Interworking for the Vodafone Netherlands SBC, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile**

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

7.5. Define Servers

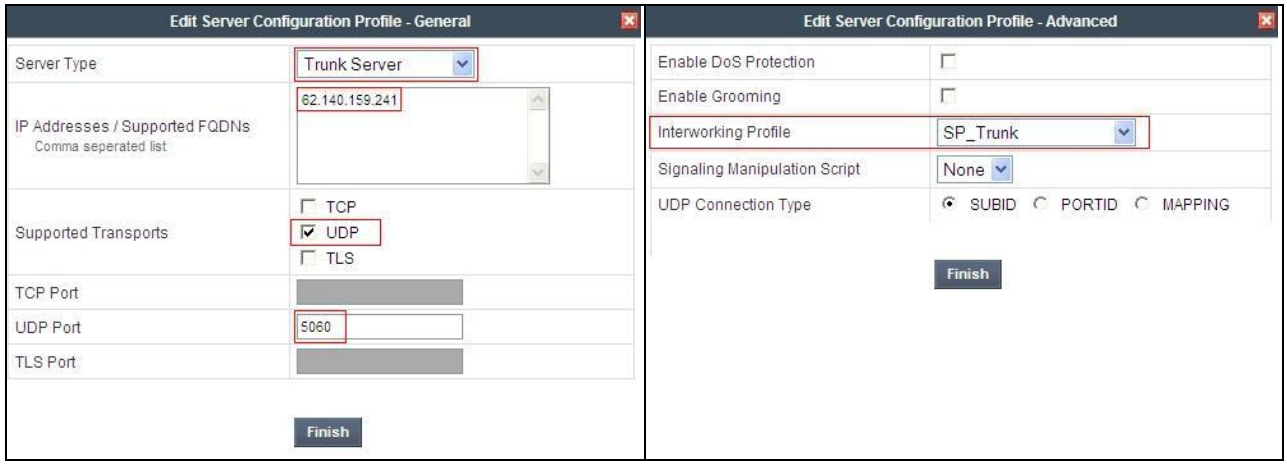
Servers are **define**d for each server connected to the ASBCE. In this case, the Vodafone NL SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on the Communication Manager in **Section 5.2**
- Check **TCP** and **UDP** in **Supported Transports**
- Define the **TCP** and **UDP** ports for SIP signalling, **5060** is used for Vodafone NL
- Click **Next** three times then select the **Interworking Profile** for the Session Manager defined in **Section 7.4** from the drop down menu

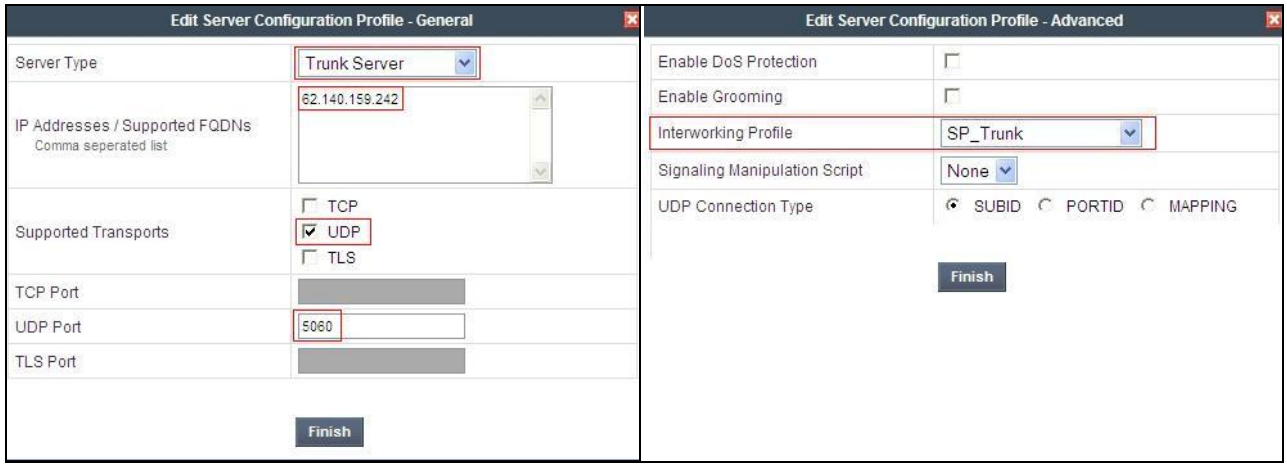


To define the Vodafone NL SBC as two separate Trunk Servers for the fixed and mobile networks, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Vodafone NL SBC and click Next
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the Vodafone NL SBC that's to be used for the fixed network
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for Vodafone NL
- Click **Next** three times then select the **Interworking Profile** for the Vodafone NL SBC defined in **Section 7.4** from the drop down menu



Repeat the process for the mobile Trunk Server and in the **IP Addresses / Supported FQDNs** box, type the IP address of the Vodafone NL SBC that's to be used for the mobile network



7.6. Define Routing

Routing information is required for routing to the Session Manager on the internal side and the Vodafone NL SBC fixed and mobile addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Communication Manager, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

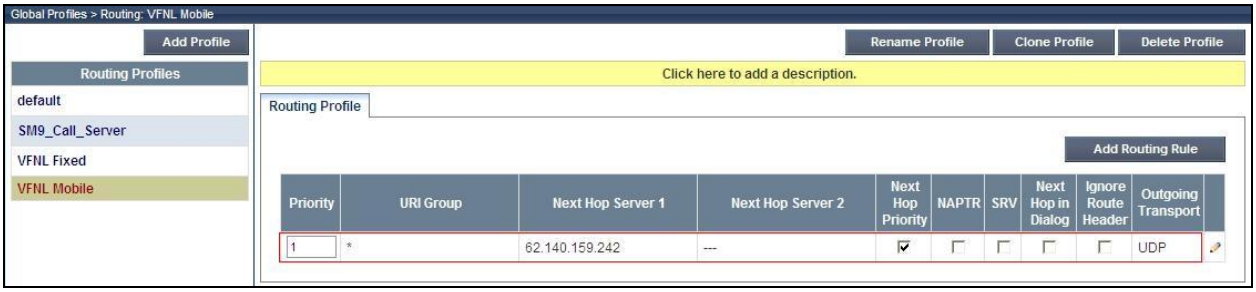
Note: Unless default port 5060 is used, this must be included in the next hop IP address.

To define routing to the Vodafone NL SBC for the fixed network, navigate to **Global Profiles Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Vodafone NL SBC fixed address and click **Next**
- Enter the SBC IP address for the fixed network and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**

To define routing to the Vodafone NL SBC for the mobile network, navigate to **Global Profiles Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Vodafone NL SBC mobile address and click **Next**
- Enter the SBC IP address for the fixed network and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**



7.7. 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 or next hop IP addresses can be used. As IP addressing was used in test instead of domain names, there was little requirement for topology hiding. IP addresses are translated to the ASBCE external addresses using NAT. To define Topology Hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu.

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

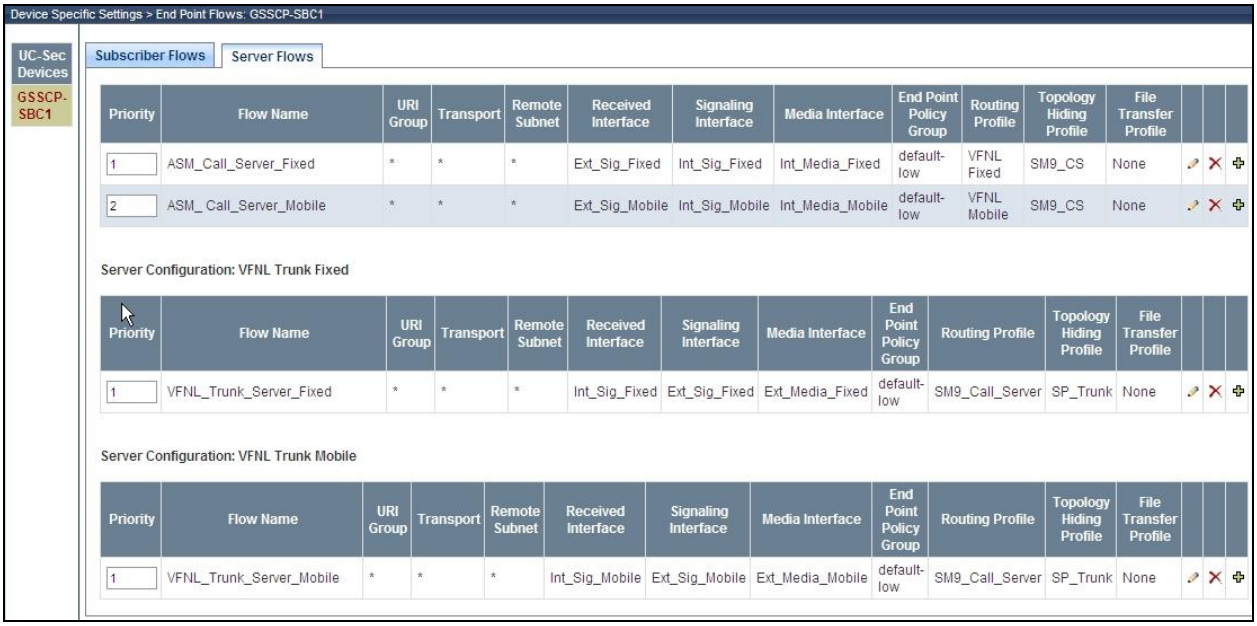
Note: The use of **Next Hop** results in the IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used for the **Request-Line** header with the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the Vodafone NL network.

To define Topology Hiding for the Vodafone NL SBC, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Vodafone NL SBC and click **Next**
- If the required Header is not shown, click on **Add Header**
- Select **Request-Line** as the required header from the **Header** drop down menu
- Select the required action from the **Required Action** drop down menu, **Next Hop** was used for test

7.8. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from the Session Manager to the Vodafone NL SBC and incoming flows from the Vodafone NL SBC to the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the Vodafone NL SBC for both fixed and mobile calls and vice versa. The following screenshot shows all flows:



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

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the outgoing server flow to the Vodafone NL SBC for the fixed network
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.6**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone NL SBC defined in **Section 7.7** and click **Finish**

Server Configuration: VFNL Trunk Fixed

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	VFNL_Trunk_Server_Fixed	*	*	*	Int_Sig_Fixed	Ext_Sig_Fixed	Ext_Media_Fixed	default-low	SM9_Call_Server	SP_Trunk	None

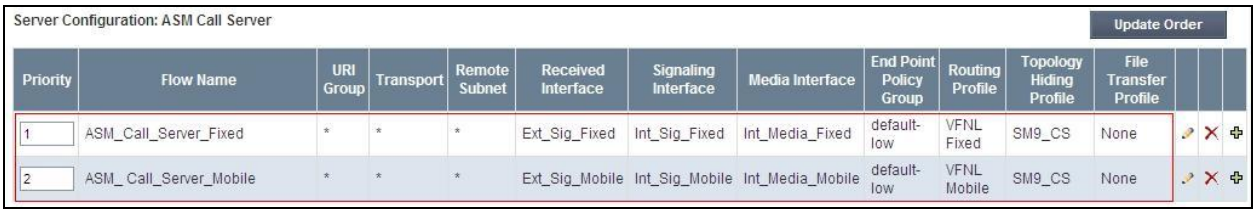
Repeat the process for an outgoing Server Flow for the mobile network. In the **Name** field enter a descriptive name for the outgoing server flow to the Vodafone NL SBC for the mobile network.

Server Configuration: VFNL Trunk Mobile

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile
1	VFNL_Trunk_Server_Mobile	*	*	*	Int_Sig_Mobile	Ext_Sig_Mobile	Ext_Media_Mobile	default-low	SM9_Call_Server	SP_Trunk	None

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

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the incoming server flow to the Session Manager
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone NL SBC defined in **Section 7.6**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**



8. Vodafone NL Configuration

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

9. Verification Steps

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

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

This is the SIP Entity link to the Vodafone NL SBC for the fixed network:

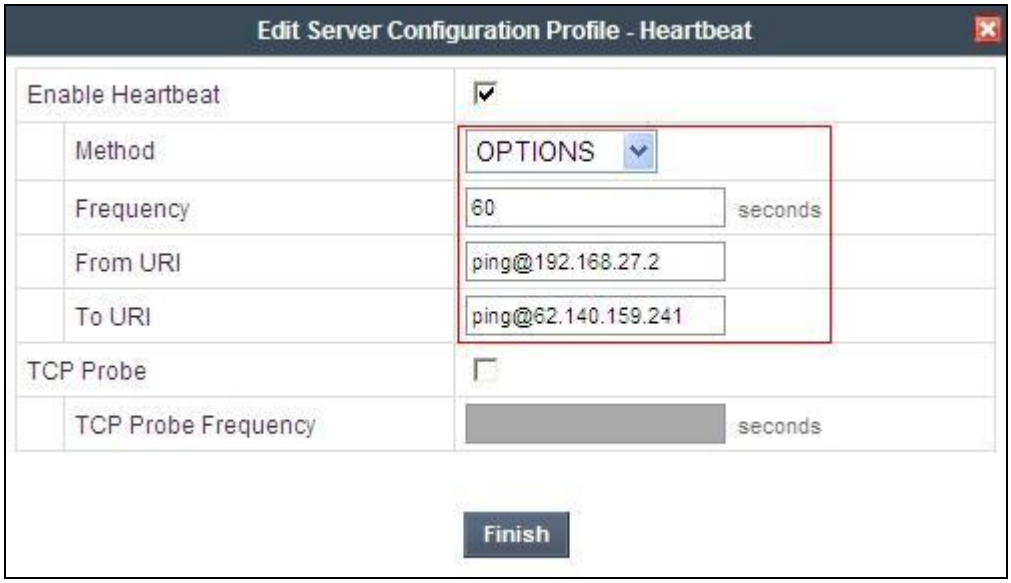
This is the SIP Entity link to the Vodafone NL SBC for the mobile network:

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

```
status trunk 1

                           TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                    Busy

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

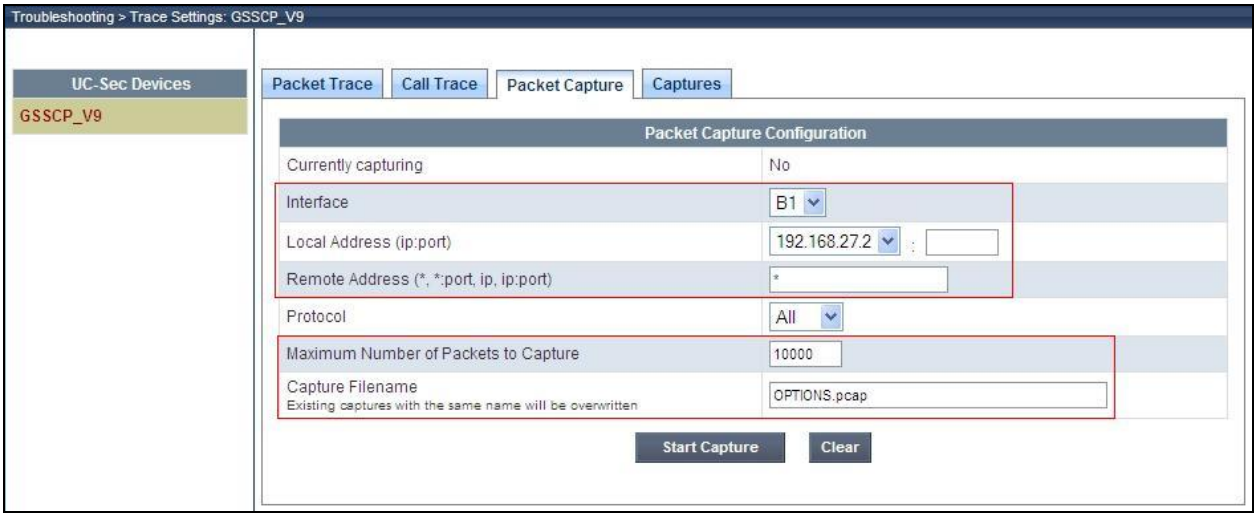
3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

7. Should issues arise with the SIP trunk, check from the ASBCE using OPTIONS. This is done by defining the heartbeat in the Server configuration then running a trace. To define the heartbeat, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side and click on the Trunk Server profile. Select the **Hearbeat** tab and click on **Edit**
   - Check the **Enable Heartbeat** box
   - Select **OPTIONS** from the **Method** drop down menu
   - Enter the **Frequency** in seconds, for convenience this can be set to the minimum value of **60** seconds
   - Enter the **From URI** in Fully Qualified Domain Name format
   - Enter the **To URI** in FQDN
   - Click on **Finish**



To define the trace, navigate to **Troubleshooting → Trace Settings** in the **UC-Sec Control Center** 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**



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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Session Border Controller for Enterprise to Vodafone NL SIP Trunk Service. The testing was successfully performed with Vodafone NL, refer to **Section 2.2** for more details.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform Release 6.2*, March 2012.

[2] *Administering Avaya Aura® System Platform Release 6.2*, February 2012.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.0.1, April 2011.

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

[5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.

[6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.

[8] *E-SBC_Admin_Guide_010-5424-405v100.pdf*, Nov 2011

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

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