Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Acme Packet Net-Net 4250 SBC to support SFR SIP Trunk (Collecte SIP) - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the SFR Collecte SIP service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Acme Packet Net-Net 4250, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. SFR 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 SFR Collecte SIP and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server and Acme Packet Net-Net 4250 SBC. Customers using this Avaya SIP-enabled enterprise solution with SFR Collecte SIP 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 Acme Packet Net-Net 4250 SBC. The enterprise site was configured to use the Collecte SIP service provided by SFR.

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 general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Acme Packet Net-Net 4250. The Communication Manager and Session Manager used in test were at Release 6.2, though the configuration described is applicable to Release 6.0.1 as well. The enterprise site was configured to use the Collecte SIP service provided by SFR. The interoperability tests included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DDI numbers assigned by SFR. The calls were made to H.323 and SIP telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via SFR to PSTN destinations. The calls were made from H.323 and SIP telephones.
- Calls using G.711A and G.729A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful 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 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 SFR requiring Avaya response and sent by Avaya requiring SFR response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for SFR Collecte SIP with the following observations:

- No inbound toll free numbers were tested as none were available from the Service Provider
- Emergency Services numbers were not tested as part of the Avaya GSSCP testing but were tested separately by Avaya France. The configuration is described in these Application Notes.
- SIP REFER and "302 Moved Temporarily" are not supported.
- Early media did not work on inbound calls when Direct IP-IP Audio Connections was configured. Direct IP-IP Audio Connections is required to avoid capacity constraints on the Media Gateway.
- Intermittent call failures were observed on outgoing calls where a "503 Service Unavailable" message was received from the network. This was assumed to be a local issue.
- During the CLI presentation test on outgoing calls, the number seen on the called phone had two leading zeros. The configuration of the enterprise equipment was not considered to be at fault as the format of the CLI between the customer and network SBC was consistent with that described in the STAS.
- Calls forwarded to the PSTN contain the calling party's number in the "From" and "P Asserted ID" headers. In the STAS document, it is mentioned that the diverting number should be present. This would currently only be available from the History Info or Diverting Number headers.
- The EC500 Confirmed Answer test failed as when the answer was pressed on the mobile phone, it did not wait until another button was pressed before connecting the call. This was not seen as critical for SIP certification.
- Due to a licensing issue and time constraints, the Call Centre tests were not run. As there is no significant difference in signalling between these calls and all the tests that were completed, this was not seen as critical for SIP certification. In addition, Call Centre calls use SIP REFER for some call flows and these are not supported by SFR.

2.3. Support

Le Service Technique SFR Business Team est joignable 24H/24, 7J/7 par un numéro gratuit pour signalisation des incidents techniques sur le service Collecte SIP.

CENTRE SERVICE CLIENT SFR Business Team
0 800 950 920

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the SFR Collecte SIP. Located at the Enterprise site is an Acme Packet Net-Net 4250 and a single HP Proliant server with System Manager, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones with SIP and H.323 firmware 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 H.323.

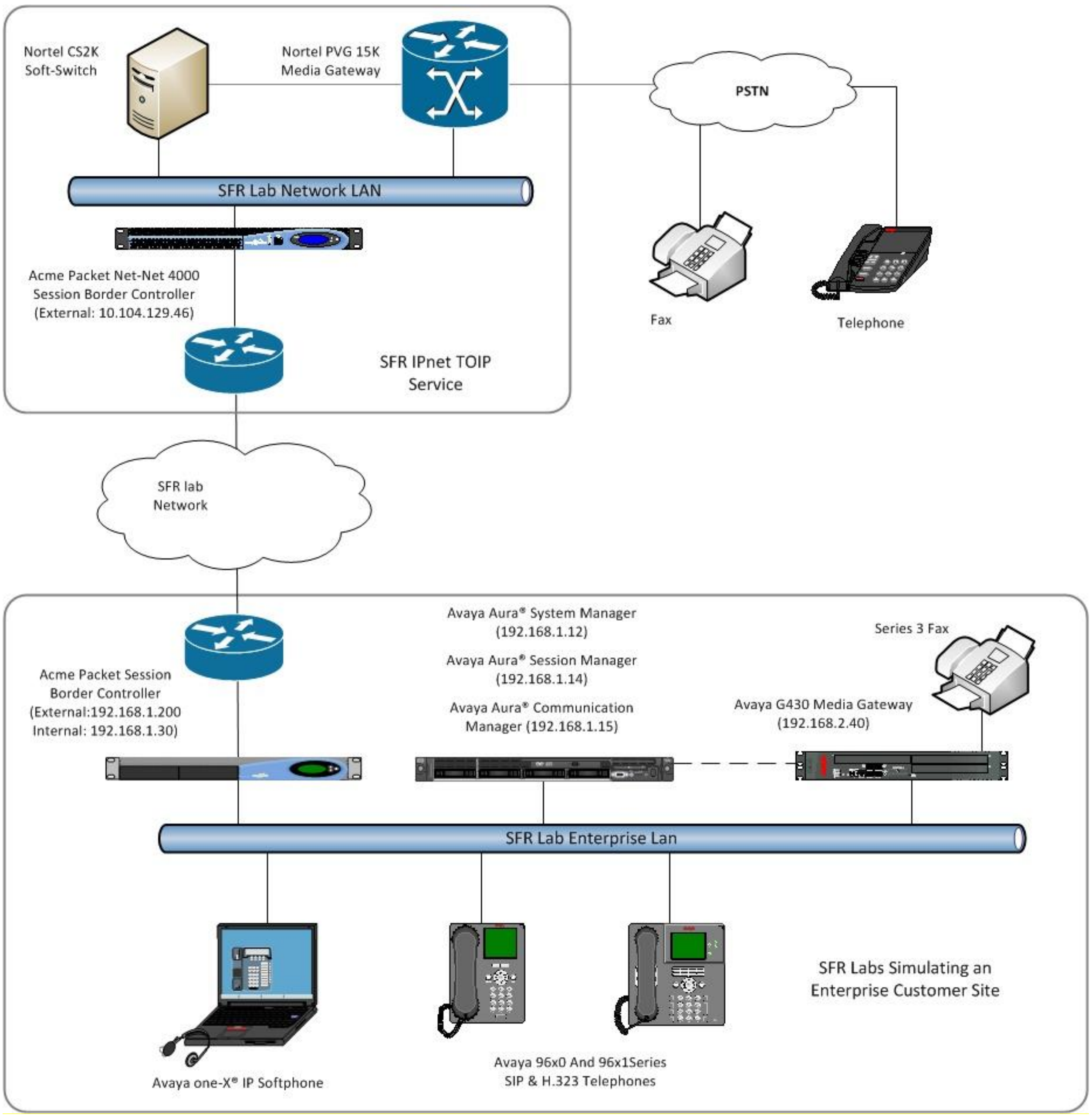


Figure 1: Test Set-up SFR Collecte SIP to Avaya Enterprise

4. Equipment and Software Validated

Equipment/Software	Release/Version
Avaya	
HP Proliant DL360 Server running Session Manager	R6.2 Build 6.2.0.0.620120
HP Proliant DL360 Server running System Manager	R6.2 SP3 Build 6.2.0.0.15669-6.2.12.307
HP Proliant DL360 Server running Communication Manager	R6.2 Build R016x.02.0.823.0
Acme Packet Net-Net 4250 Session Border Controller	6.2.0
Avaya 9601 series Handsets SIP	 9601-IPT-SIP-R6_1_4-070412
Avaya 9611 & 9608 Handsets - SIP - H.323	 96x1-IPT-SIP-R6_2_0-082012 96x1-IPT-H323-R6_2_2_09-071012
Analogue Fax	N/A
Avaya one–X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.3.08-SP3-Patch2-35791
SFR	
Nortel CS2k Softswitch	CVM13
Nortel PVG 15K TGW	Not known
Acme Packet Net-Net SD 4500 SBC	6.2

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 SFR Collecte SIP service. For incoming calls, the Session Manager receives SIP messages from the Acme Packet Net-Net 4250 SBC 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 messages are routed to Session Manager. Session Manager directs the outbound SIP messages to the Acme Packet Net-Net 4250 at the enterprise site that then sends the SIP messages to the SFR 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 HP Proliant DL360 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 or features. 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 SFR network, and any other SIP trunks being 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 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 24    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 0
                   Maximum Video Capable IP Softphones: 24    0
                       Maximum Administered SIP Trunks: 12000 255
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

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

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

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

           IP Attendant Consoles? y
```

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM** and **192.168.1.14** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM                    192.168.1.14
default               0.0.0.0
meaes                 192.168.1.17
procr                 192.168.1.15
procr6                ::
```

5.3. Administer IP Network Region

Use the **change ip-network-region x** 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 **sip.lab.sfr.fr**.
- By default, **IP-IP Direct Audio** (both **Intra**- and **Inter-Region**) are enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. The media stream is established directly between the enterprise end-point and the internal media interface of the Acme Packet SBC.
- 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.

```
display ip-network-region 1                                         Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: sip.lab.sfr.fr
    Name: MAIN
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: 3029
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 codecs supported by SFR were configured, namely **G.729A** and **G.711A**.

```
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:
```

The SFR Collecte SIP 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 SFR Collecte SIP service. During test, this was configured to use **TLS** (Transport Layer Security) and the default TLS port of **5061** for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tls**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SM** 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**)
- Set **Far-end Domain** to the value agreed with SFR, in test this was **sip.lab.sfr.fr**
- Set **Direct IP-IP Audio Connections** to **y**
- Set **Initial IP-IP Direct Media?** to **y** so that SIP endpoints are connected directly to the internal side of the SBC at call set-up and shuffling is not used.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

Default values were used for other fields.

```
add signaling-group 3                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3              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
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: sip.lab.sfr.fr
                                                 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? y
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 **tie**
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

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

Group Number: 3                    Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SM             COR: 1        TN: 1        TAC: *03
   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: 3
                                                     Number of Members: 255
```

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 SFR to prevent unnecessary SIP messaging during call setup.

```
Add trunk-group 3                                              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): 600

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

On **Page 3**, set the **Numbering Format** field to **public**. This allows delivery of CLI in E.164 format with a leading “+”.

```
add trunk-group 3                                                  Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: internal
                                                   Maintenance Tests? y




                     Numbering Format: public
                                                 UUI Treatment: service-provider

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

On **Page 4** of this form:

- Set **Support Request History** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by SFR

```
add trunk-group 3                                                  Page   4 of  21
                              PROTOCOL VARIATIONS

                           Mark Users as Phone? n
                 Prepend '+' to Calling Number? n
           Send Transferring Party Information? n

                         Send Diversion Header? n
                       Support Request History? y
                  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: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                  Enable Q-SIP? n
```

5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the test configuration, individual stations were mapped to send numbers allocated from the SFR 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 public-unknown-numbering 0                                 Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk        CPN             CPN
Len Code           Grp(s)     Prefix          Len
                                                   Total Administered: 6
 4  4000           3          33427nnnnn0     11      Maximum Entries: 9999
 4  4001           3          33427nnnnn1     11
 4  4002           3          33427nnnnn2     11   Note: If an entry applies to
 4  4004           3          33427nnnnn4     11   a SIP connection to Avaya
 4  4005           3          33427nnnnn5     11   Aura(R) Session Manager,
 4  4009           3          33427nnnnn9     11   the resulting number must
                                                   be a complete E.164 number.
```

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 SFR Collecte SIP service. The single digit **0** was used as the ARS access code providing a facility for telephone users to dial 0 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: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 0     Access Code 2:
```

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 0. 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 **00**. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 3**.

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

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max   Pattern    Type   Num   Reqd
    0                     9    12     3         pubu         n
    00                    9    14     3         pubu         n
    01                    10   10     3         pubu         n
    118                   3    6      3         pubu         n
    1xx                   3    3      3         pubu         n
    99                    12   12     99        pubu         n
```

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **3** is used to route calls to trunk group **3**.

```
change route-pattern 3                                         Page   1 of   3
                    Pattern Number: 3   Pattern Name: SIP Trunk
                             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: 3    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                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
```

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from SFR can be manipulated as necessary to route calls to the desired extension. In the example, the incoming DDI numbers provided by SFR for testing are assigned to the internal extensions of the test equipment configured within the Communication Manager. The **change inc-call-handling-trmt trunk-group x** command is used to translate numbers **0427nnnnn0** to **0427nnnnn9** to the 4 digit extension by deleting **9** digits of the incoming number and inserting the first three digits of the extension number (**400**). An exception shown below is where all digits are deleted and replaced with a Virtual Directory Number (VDN **4833**) used for DTMF testing. Note that the significant digits beyond the city code have been obscured.

```
change inc-call-handling-trmt trunk-group 3                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 tie             10 0427nnnnn8       10  4833
 tie             10 0427nnnnn        9   400
 tie
 tie
```

5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 4002. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 0) 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 **aar** so for call routing
- Set the **Config Set** to **1**

```
change off-pbx-telephone station-mapping 4002                   Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 4002             EC500        -      00353867818308   aar        1
-
```

5.11. Emergency Number handling

The short number is defined as a **dialed string** and the **Call Type** set to **emer** (emergency)

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

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    0                     9    12    3         pubu         n
    00                    9    14    3         pubu         n
    01                    10   10    3         pubu         n
    118                   3    6     3         pubu         n
    1xx                   3    3     3         pubu         n
    15                    2    2     3         emer         n
    17                    2    2     3         emer         n
    18                    2    2     3         emer         n
    99                    12   12    99        pubu         n
                                                            n
```

On each site, define the number to be sent as the calling party when an emergency number is dialled. Example:
Site 1 Extension 4000 and 4001 are defined with DDI numbers 0427418050 and 0427418051. To define 4000 as the emergency location number for 4001, type **change station 4001** and on **Page** 2, change the **Emergency Location Ext** to **4000**

```
change station 4001                                                     Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
             CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single
                                                        EMU Login Allowed? n
        H.320 Conversion? n         Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                      EC500 State: enabled
         Multimedia Mode: enhanced                Audible Message Waiting? n
     MWI Served User Type:                     Display Client Redirection? n
              AUDIX Name:                     Select Last Used Appearance? n
                                                Coverage After Forwarding? s
                                                  Multimedia Early Answer? n
                                              Direct IP-IP Audio Connections? y
  Emergency Location Ext: 4000         Always Use? n IP Audio Hairpinning? n
```

Configure the IP network mapping using the **change ip-network-map** command and define an **Emergency Location Extension**. This can be done using a static IP address for a single phone or one or more subnets for an IP network region. The example shows Emergency Location Extensions for two sites, both in the IP network region defined in **Section 5.3**.

```
change ip-network-map                                            Page   1 of  63
                              IP ADDRESS MAPPING

                                              Subnet Network      Emergency
 IP Address                                   Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 192.168.1.0                            /24    1      n    4002
   TO: 192.168.1.254
 FROM: 192.168.2.0                            /24    1      n    4000
   TO: 192.168.2.254
 FROM:                                        /             n
   TO:
 FROM:                                        /             n
```

When an emergency call is made, the CM identifies the mapping from the IP address of the phone. It then compares the Emergency Location Extension defined in the IP network map with the one defined for the station. If the two are the same, the CM sends the station extension. If the two are different, it sends the IP Address Mapping extension. Refer to [4] for more detailed information.

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

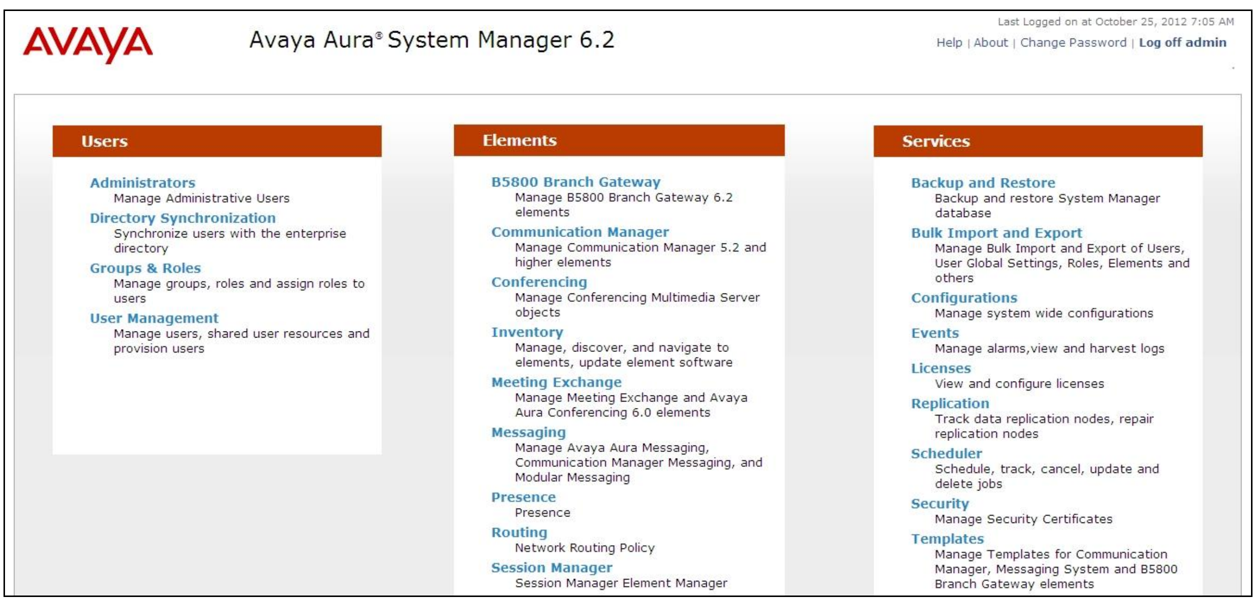
6. Configuring Avaya Aura® Session Manager

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

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

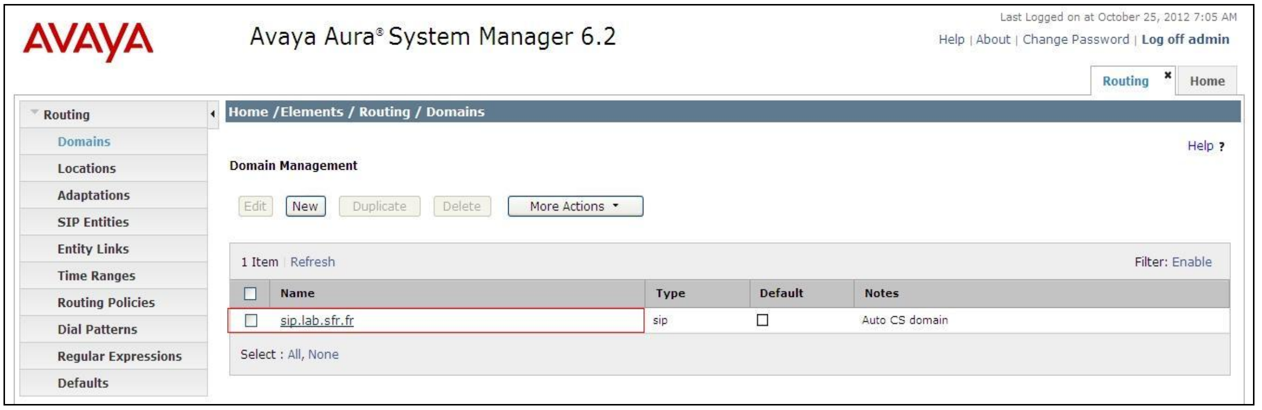
6.1. Log in to Avaya Aura® System Manager

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 opening screen will be presented with menu options shown below.



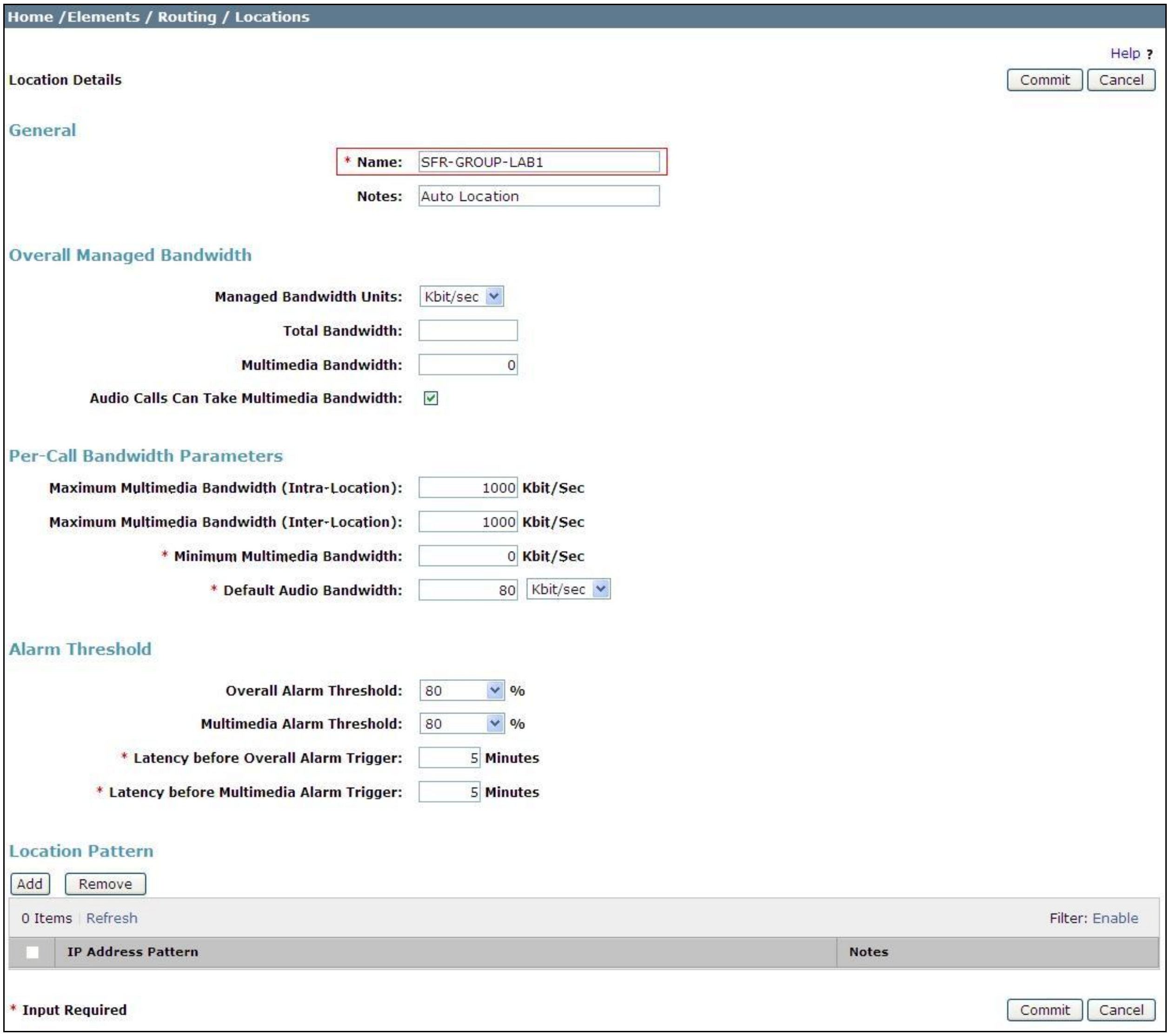
6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu 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., **sip.lab.sfr.fr**) and optionally a description for the domain in the Notes field. Click **Commit** [not shown] to save changes.



6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of 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. Below is the location configuration used for the test enterprise.

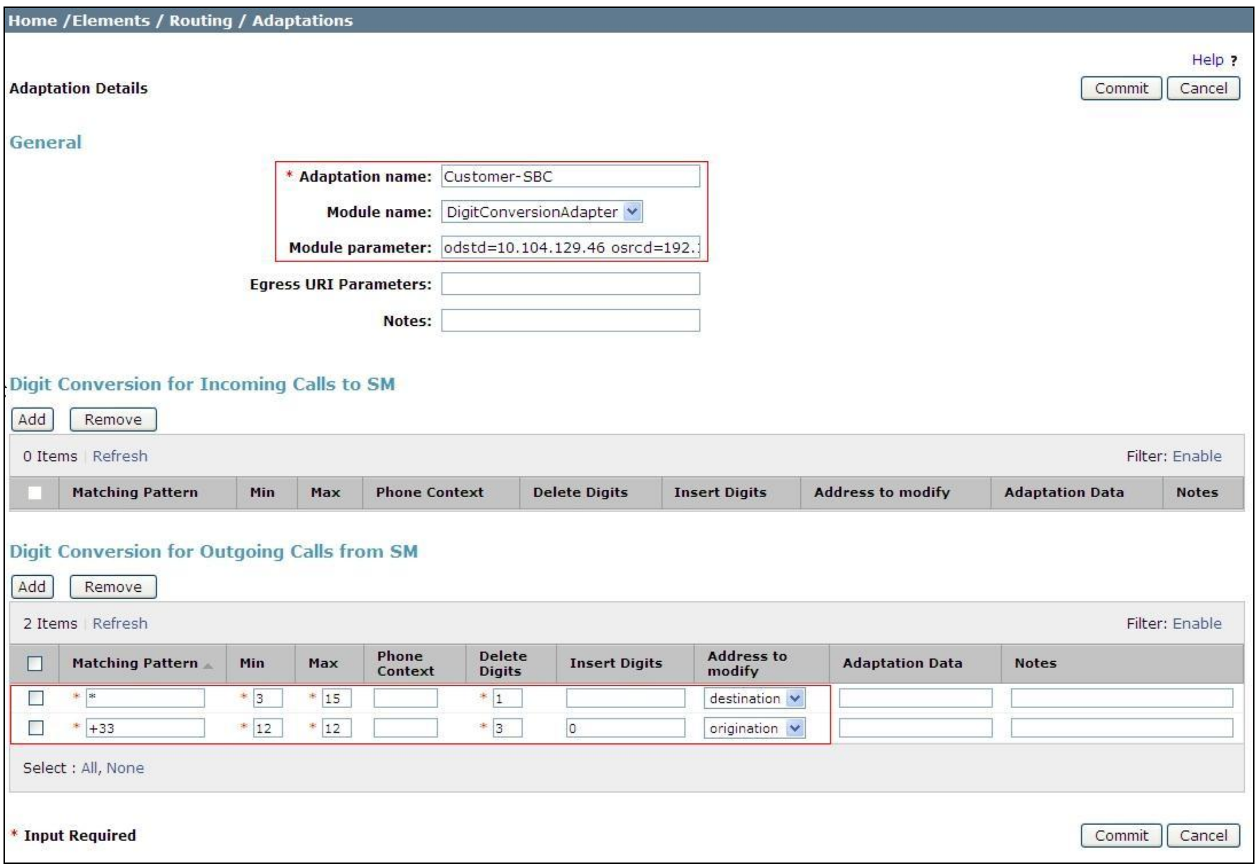


6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. Domain names used n the request URI and various headers are overwritten with local IP addresses using module parameters **odstd** and **osrcd**. The example shown was used in the test environment for the following functions:

- Conversion of the calling party number to a national format with leading 0
- Removal of the leading digit from the called party number
- Override of the destination domain in the Request URI and To header with IP address
- Override of the source domain in the From, P-Asserted-ID and History-Info headers with IP address

The module **DigitConversionAdaptor** is used with module parameters **odstd** and **osrcd**



Note: This is an example only. Private numbering in the Communication Manager and header manipulation in the enterprise SBC could be used to have similar effect.

6.5. Administer SIP Entities

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

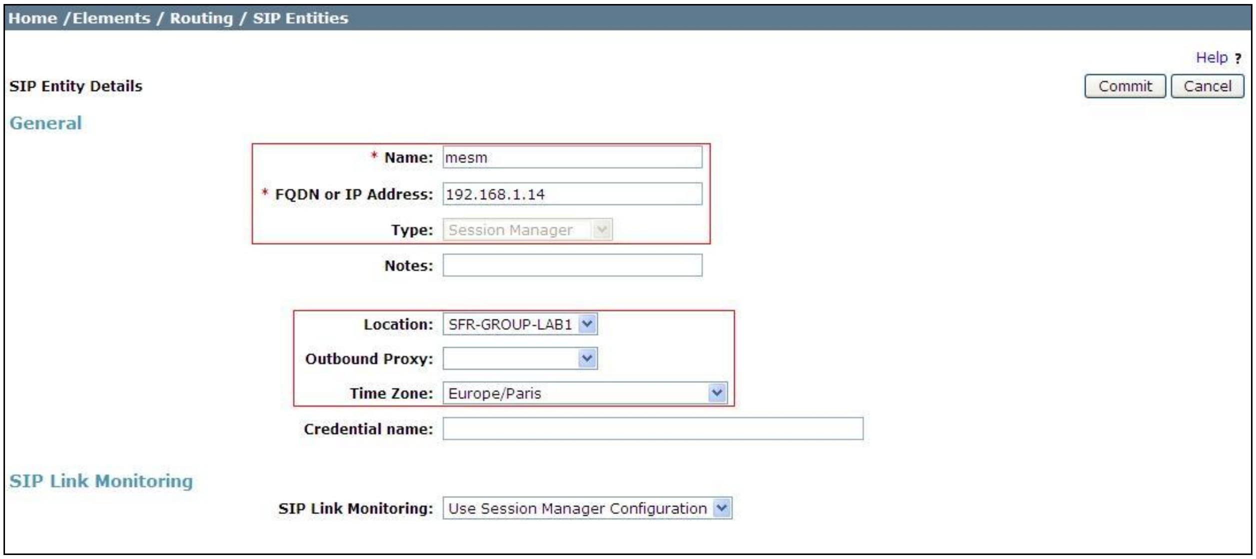
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the Session Border Controller SIP entity (Note that **Gateway** was used in test, there is not currently a significant difference in functionality between the two settings)
- In the **Adaptation** field, enter the adaptation defined in **section 6.4** where appropriate. In this test it was applied to the Acme Packet SBC entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone where SIP Entity resides

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Acme Packet Net-Net 4250 SBC SIP Entity

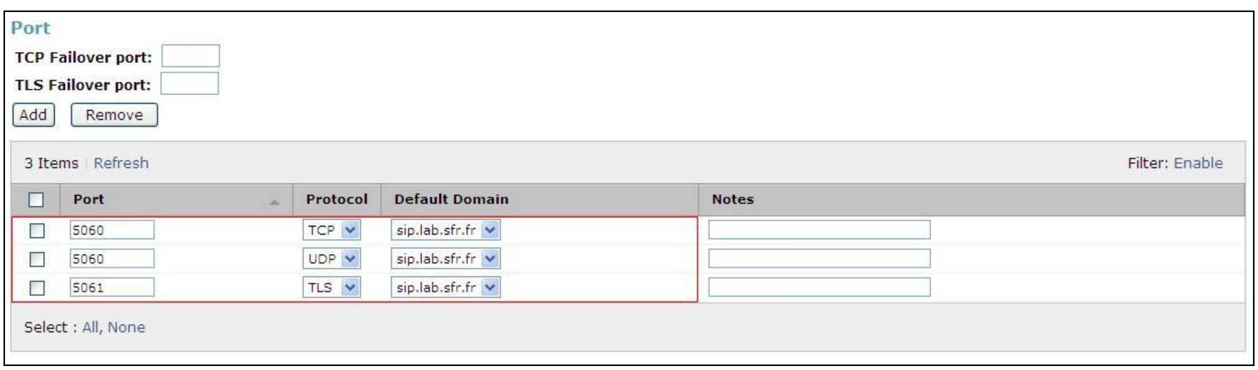
6.5.1. Avaya Aura® Session Manager SIP Entity

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



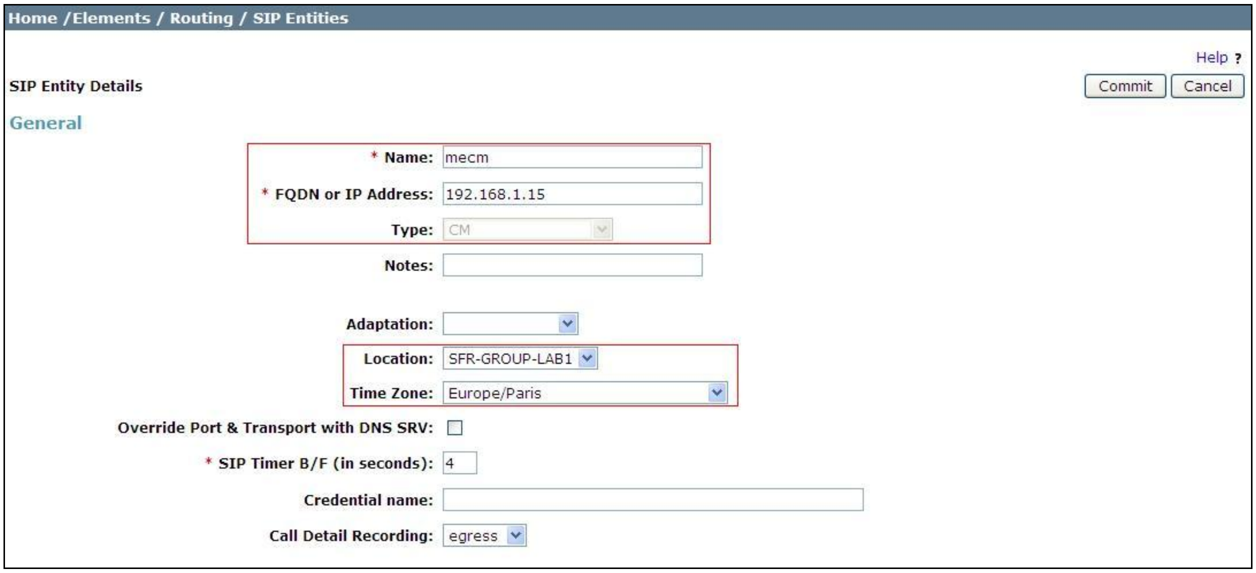
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- 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 a previously defined SIP domain, in this case **sip.lab.sfr.fr** as the default domain



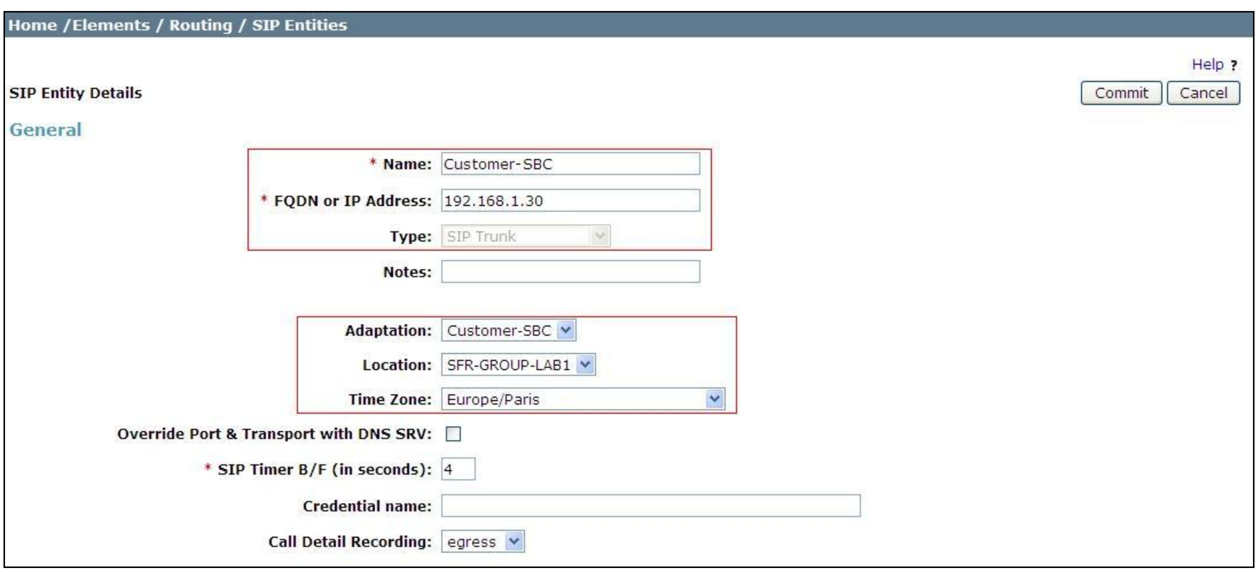
6.5.2. Avaya Aura® Communication Manager SIP Entity

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



6.5.3. Acme Packet Net-Net 4250 SIP Entity

The following screen shows the SIP Entity for the Session Border Controller. The **FQDN or IP Address** field is set to the internal IP address of the Acme Packet SBC enterprise network interface. Assign the **Adaptation** previously defined in **Section 6.4** and the location defined in **Section 6.3**

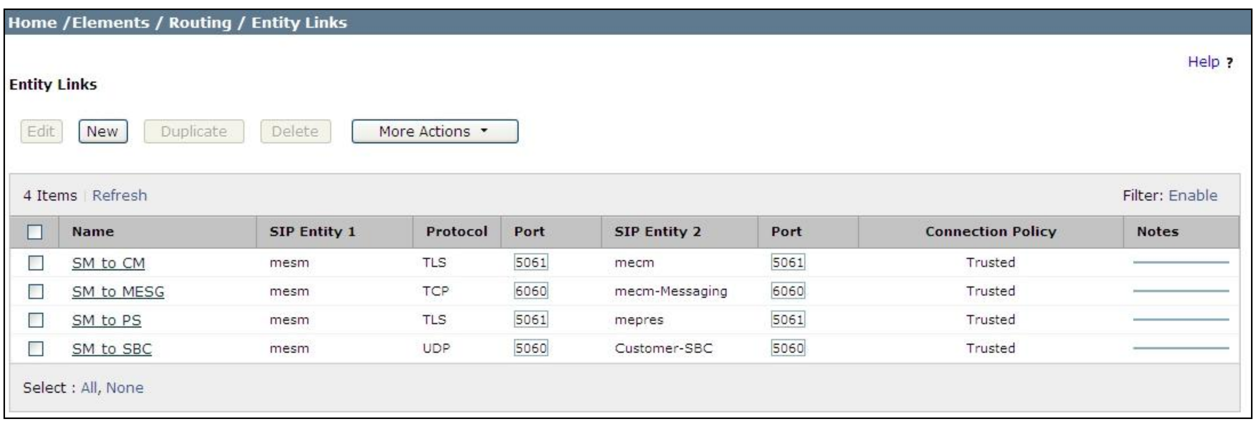


6.6. Administer Entity Links

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

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select the name given to the Session Manager Entity, in this case **mesm**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** for **Connection Policy** field to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** (not shown) 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	Notes
SM to CM	mesm	TLS	5061	mecm	5061	Trusted	
SM to MESG	mesm	TCP	6060	mecm-Messaging	6060	Trusted	
SM to PS	mesm	TLS	5061	mepres	5061	Trusted	
SM to SBC	mesm	UDP	5060	Customer-SBC	5060	Trusted	

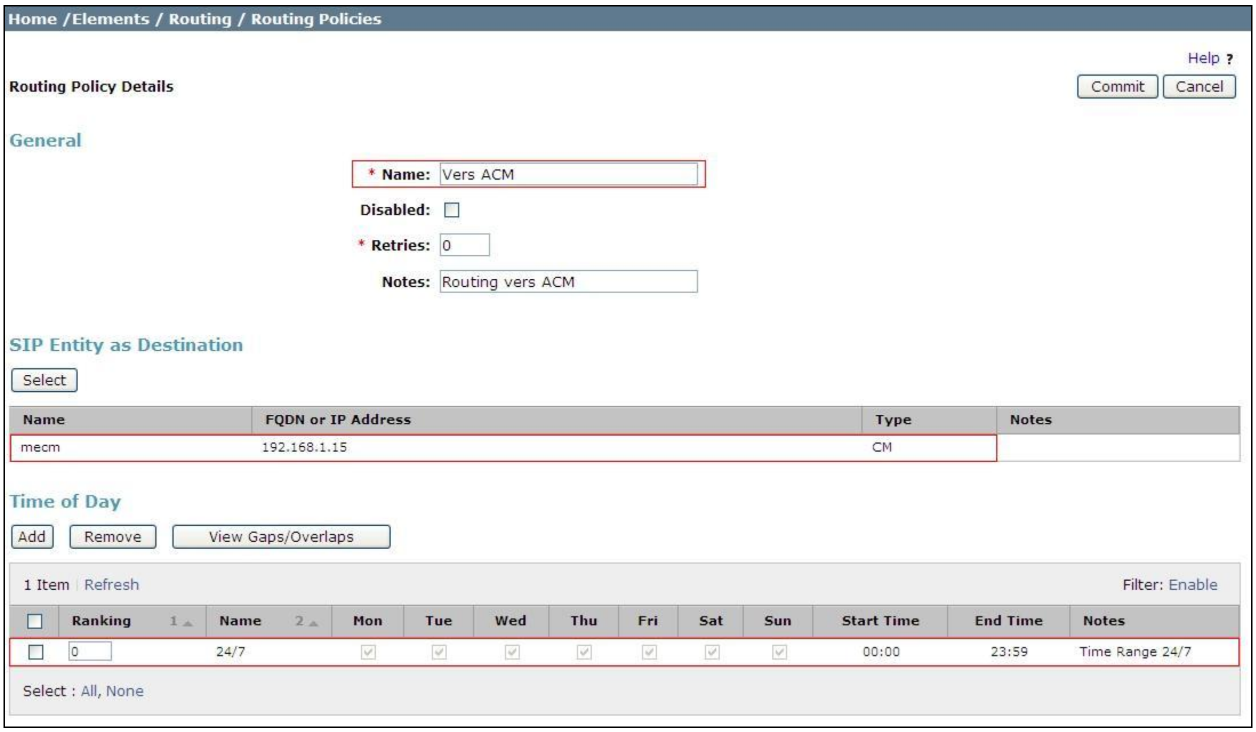
6.7. Administer Routing Policies

Routing policies are 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).

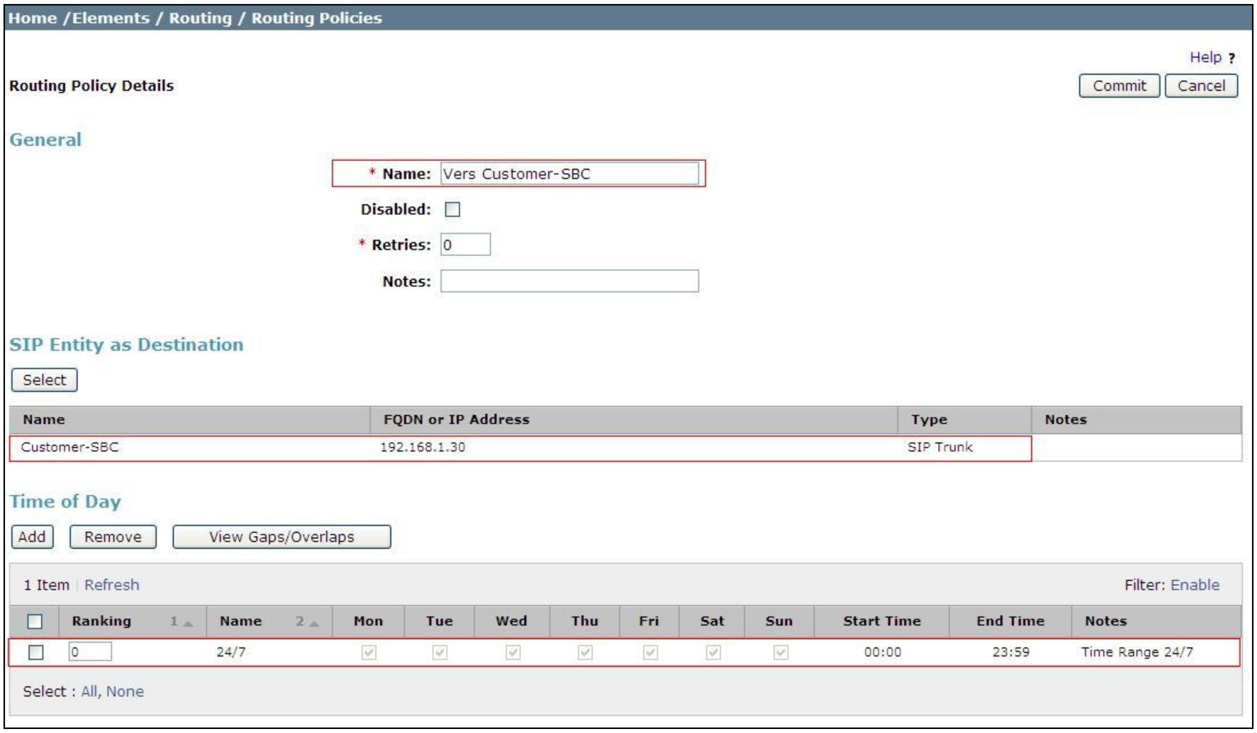
Under **General**:

- 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 in a pop-up screen (not shown)
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.



The following screen shows the routing policy for the Acme Packet SBC.



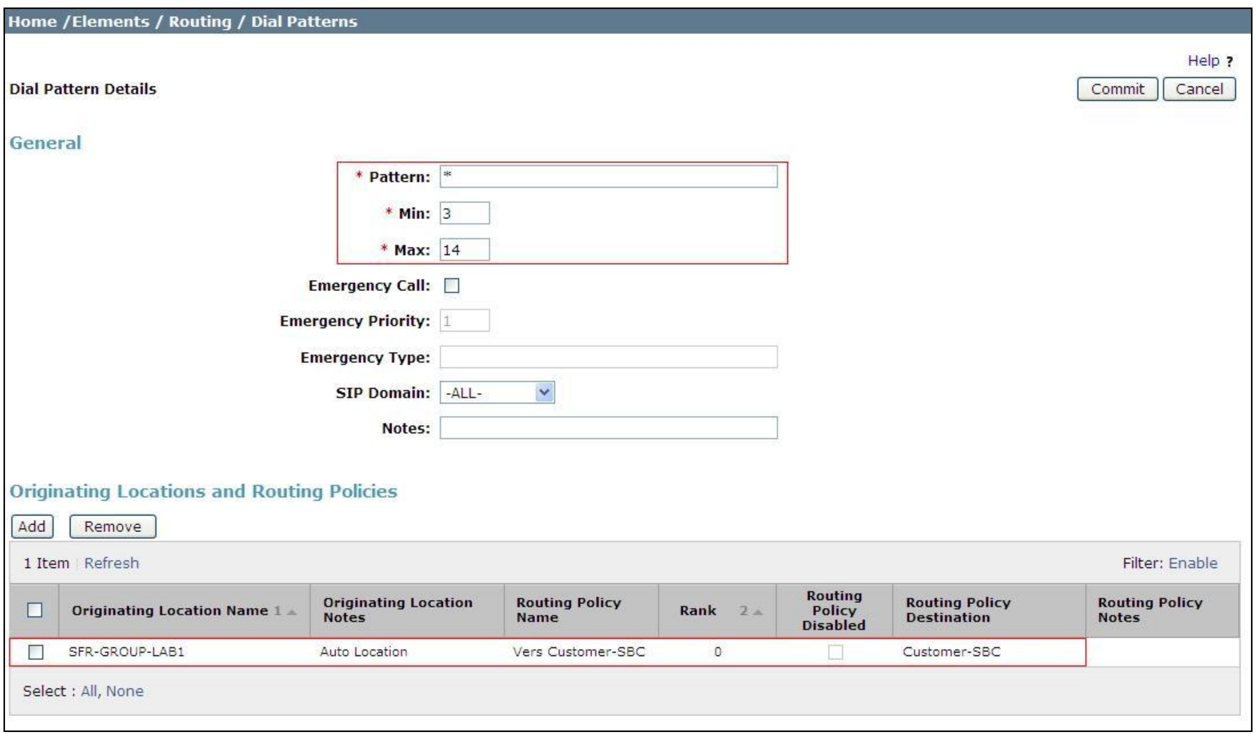
6.8. Administer Dial Patterns

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

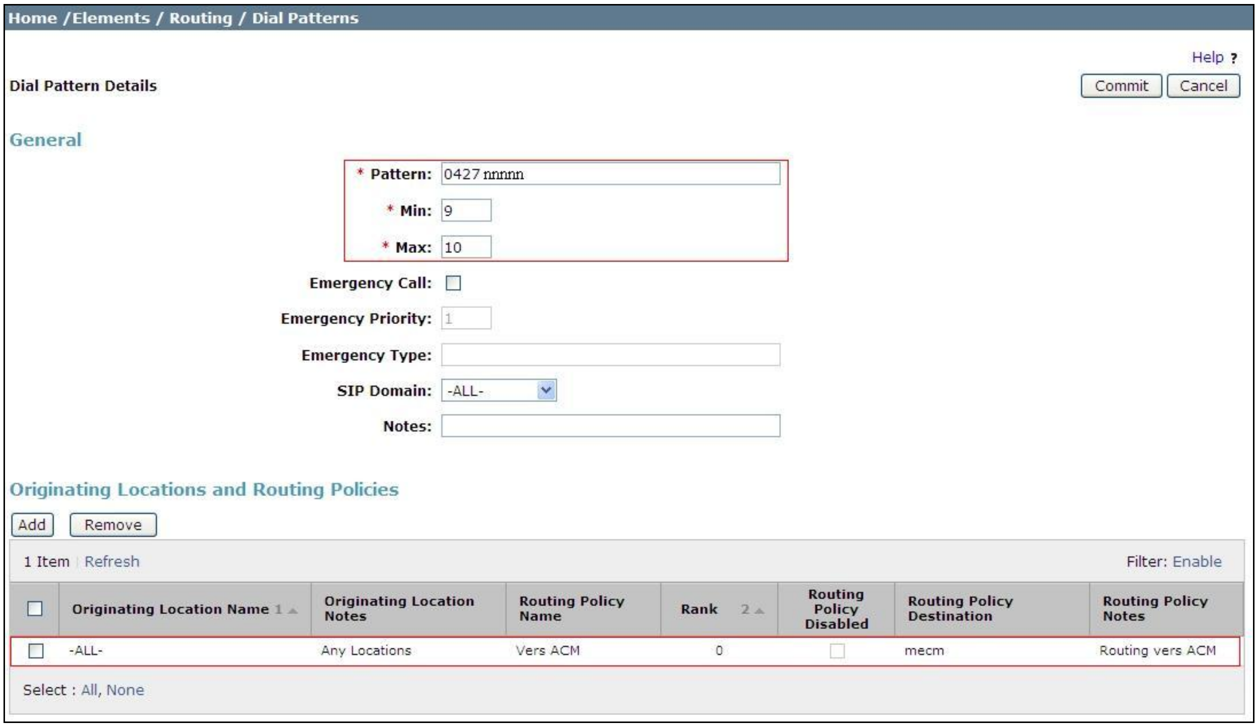
Under **General**:

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

Under **Originating Locations and Routing Policies** click **Add**, and in the resulting screen (not shown), under **Originating Location,** select **ALL.** Under **Routing Policies** select one of the routing policies defined in **Section 6.7** and click **Select** button to save. The following screen shows an example dial pattern configured for the Acme Packet SBC which will route the calls out to the SFR Collecte SIP service.



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

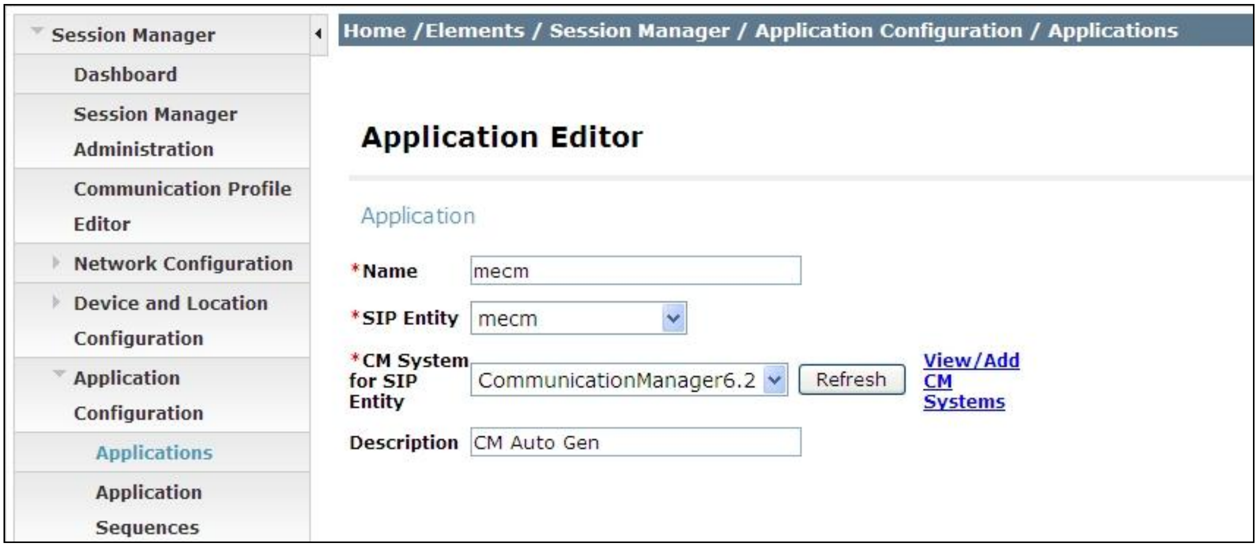


6.9. Administer Application for Avaya Aura® Communication Manager

From the Session Manager home screen, select **Session Manager** under the Elements menu. In the resulting **Session Manager** tab, select **Application Configuration → Applications** from the left panel menu 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 the Communication Manager configured in **Section 6.5.2**
- In the **CM System for SIP Entity** field select the Communication Manager defined under **Inventory → Manage Elements** (not shown)

Select **Commit** to save the configuration.

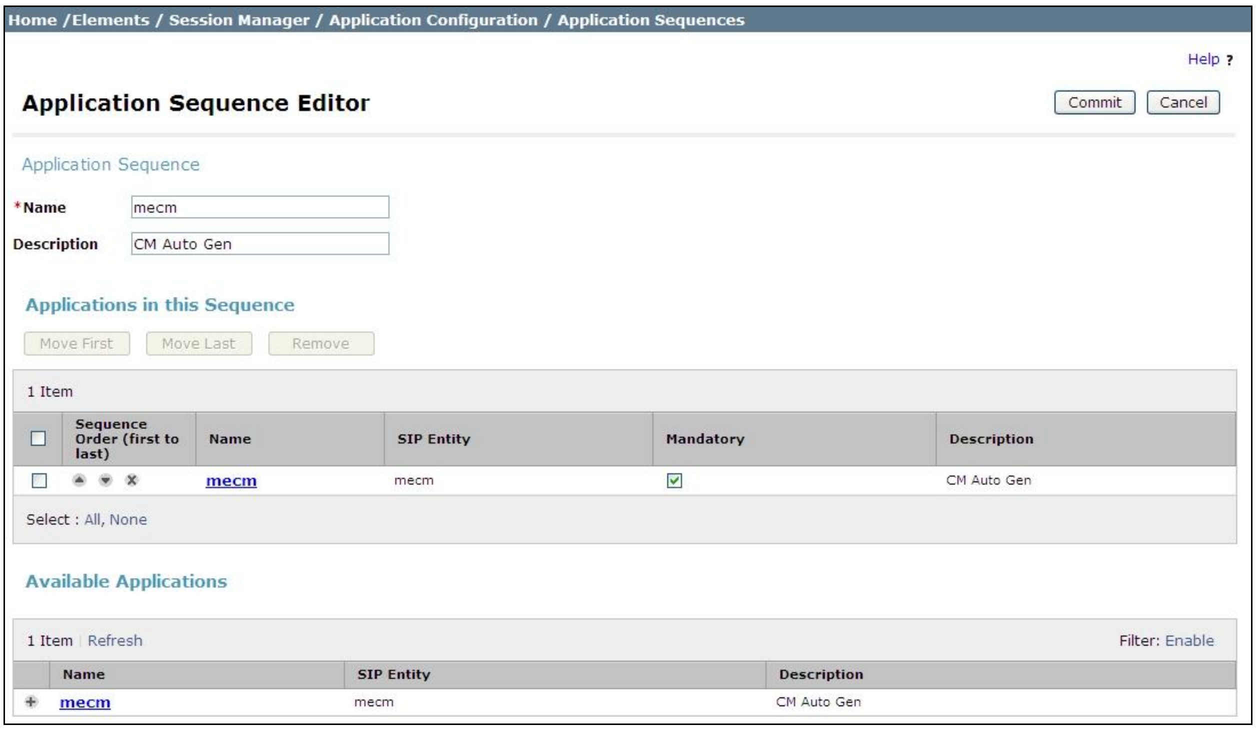


6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Application Configuration → Application Sequences** and click on **New** (not shown) and configure as follows in the resultant screen:

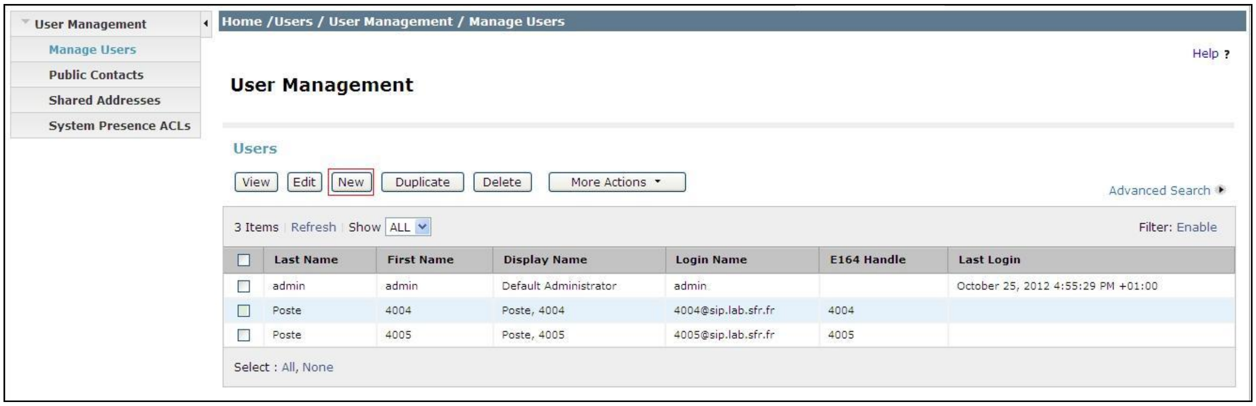
- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the **+** sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading

Select **Commit**.



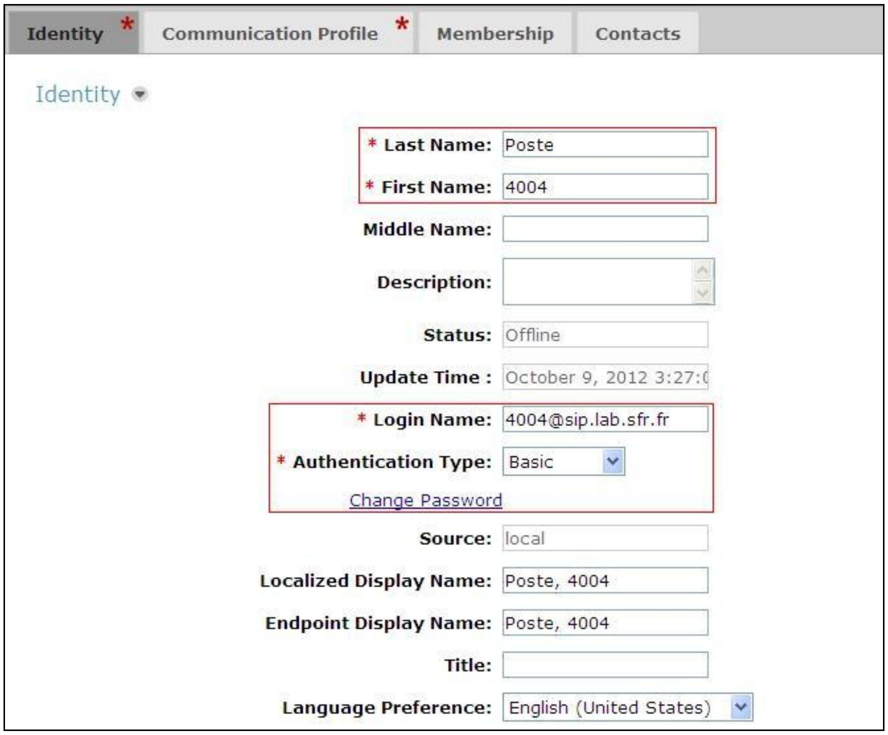
6.11. Administer SIP Extensions

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

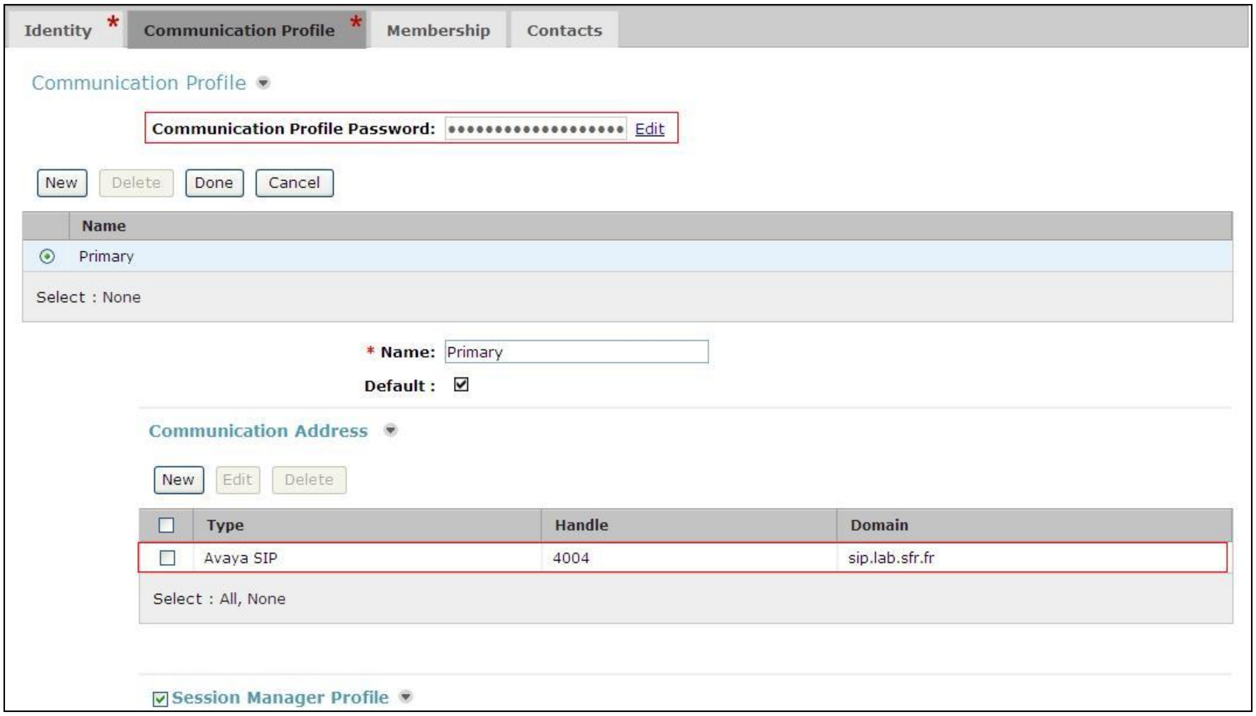


Under the **Identity** tab:

- 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. **4004@sip.lab.sfr.fr**) which is used to create the user's primary handle
- The **Authentication Type** should be **Basic** (default)
- In the **Password/Confirm Password** fields (not shown) enter an alphanumeric password

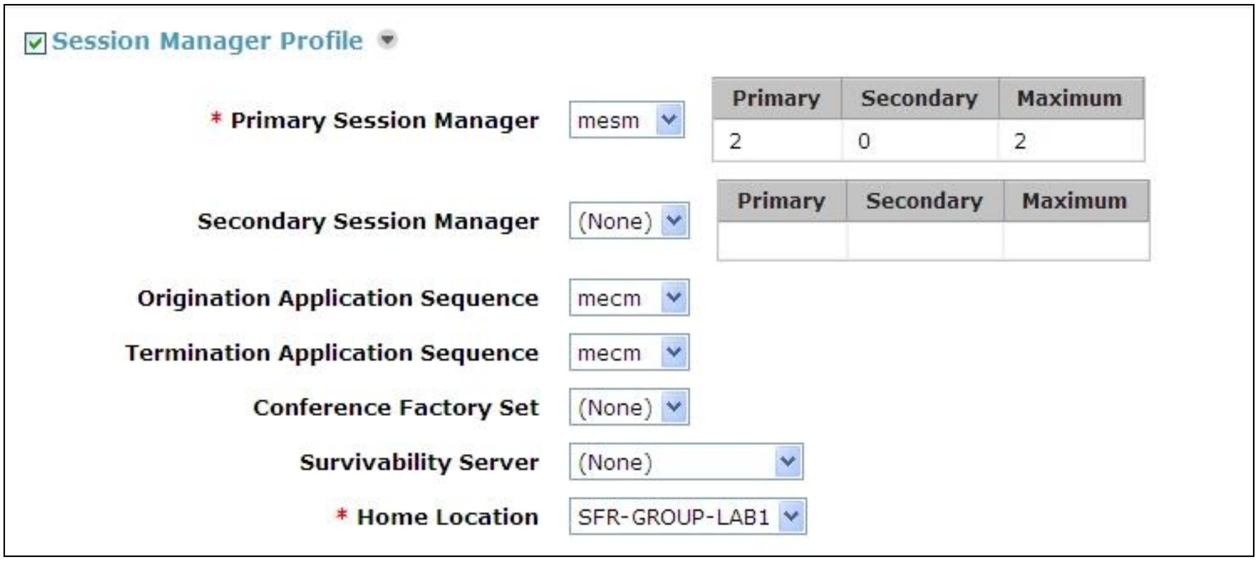


Under the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it (not shown), then expand the **Communication Address** section (not shown) and click **New**. For the **Type** field, select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.



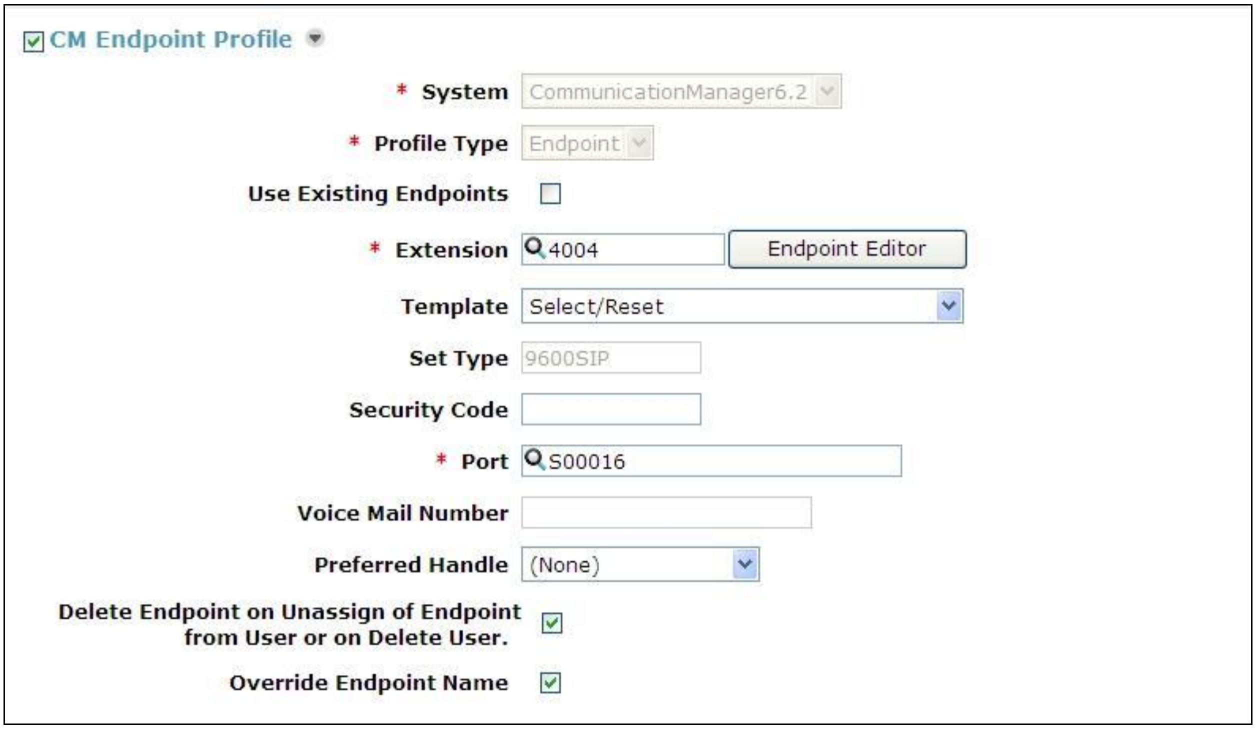
Expand the **Session Manager Profile** section.

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



Expand the **Endpoint Profile** section.

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



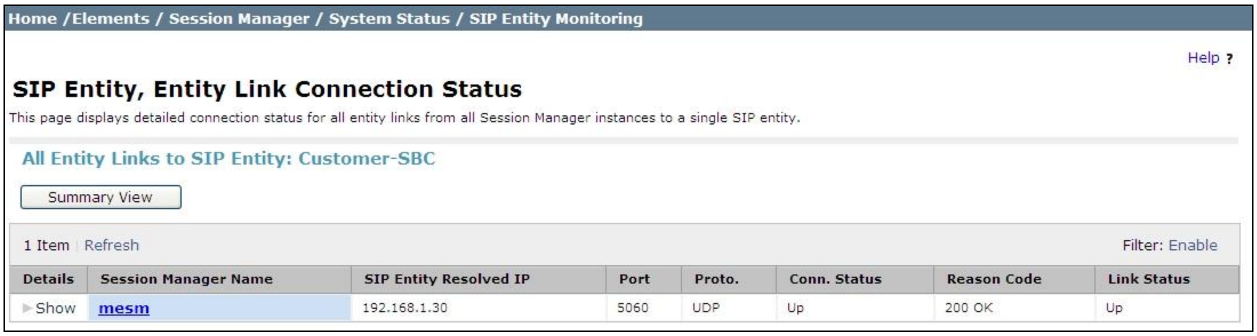
7. Configure SFR Collecte SIP

The configuration of the SFR equipment used to support the Collecte SIP service is outside of the scope of these Application Notes and will not be covered. To obtain further information on SFR equipment and system configuration please contact an authorised SFR representative.

8. 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**.



Note: This is also an indication that the SIP trunk between the Acme packet SBC and the SFR network is working effectively as OPTIONS are passed by the SBC from the Session Manager to the 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 3

                                    TRUNK GROUP STATUS

Member    Port     Service State       Mtce Connected Ports
                                       Busy

0003/001 T00043   in-service/idle    no
0003/002 T00001   in-service/idle    no
0003/003 T00002   in-service/idle    no
0003/004 T00003   in-service/idle    no
0003/005 T00004   in-service/idle    no
0003/006 T00005   in-service/idle    no
0003/007 T00006   in-service/idle    no
0003/008 T00007   in-service/idle    no
0003/009 T00008   in-service/idle    no
0003/010 T00009   in-service/idle    no
0003/011 T00010   in-service/idle    no
```

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

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet Net-Net 4250 SBC to SFR Collecte SIP service. The service was successfully tested with a number of observations listed in **Section 2.2**.

10. 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,* March 2012.
[2] *Administering Avaya Aura® System Platform Release 6.2,* February 2012.
[3] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012.
[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] *Net-Net 4000 S-CX6.2.0 Maintenance and Troubleshooting Guide.pdf*, https://support.acmepacket.com/
[9] *Net-Net Session Director C[xz]6.3.9Final User Guide.pdf*, https://support.acmepacket.com/
[10] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

Appendix A

The configuration details provided here are the Acme Packet 4250 Net-Net SBC settings used during this compliance testing.

ANNOTATION: The local policy below controls the routing of SIP messages from session manager to the SFR SIP trunk service.

```
show run
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        core-avaya [Enterprise SIP domain]
        description                     Avaya-to-SFR
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@192.168.1.50
        last-modified-date              2011-04-07 12:50:28
        next-hop                        10.104.129.46 [SIP trunk provider address]
        realm                           peer-sfr [SIP trunk provider realm]
        action                          none
        terminate-recursion             disabled
        app-protocol                    SIP
        methods
        lookup                          single
        next-key
```

ANNOTATION: The local policy below controls the routing of SIP messages from the SIP trunk service provider to the session manager.

```
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        peer-sfr [SIP trunk service provider]
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@192.168.1.50
        last-modified-date              2011-04-07 12:51:30
        next-hop                        192.168.1.14 [session manager IP address]
        realm                           core-avaya [the Enterprise realm]
        action                          none
        terminate-recursion             disabled
        app-protocol                    SIP
        methods
        lookup                          single
        next-key
media-manager
```

```
      state                          enabled [enabled to manage voice media]
      latching                       enabled
      flow-time-limit                86400
      initial-guard-timer            300
      subsq-guard-timer              300
      tcp-flow-time-limit            86400
      tcp-initial-guard-timer        300
      tcp-subsq-guard-timer          300
      tcp-number-of-ports-per-flow   2
      hnt-rtcp                       disabled
      algd-log-level                 NOTICE
      mbcd-log-level                 NOTICE
      red-flow-port                  1985
      red-mgcp-port                  1986
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      media-policing                 enabled
      max-signaling-bandwidth        10000000
      max-untrusted-signaling        100
      min-untrusted-signaling        30
      app-signaling-bandwidth        0
      tolerance-window               30
      rtcp-rate-limit                0
      trap-on-demote-to-deny         enabled
      syslog-on-demote-to-deny       disabled
      min-media-allocation           32000
      min-trusted-allocation         1000
      deny-allocation                1000
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      media-supervision-traps        disabled
      dnsalg-server-failover         disabled
      last-modified-by               admin@192.168.1.50
      last-modified-date             2011-04-07 10:57:42
```

ANNOTATION: The following network interfaces define the IP address used on the enterprise (internal) network and on the SIP trunk provider (external) network and the associated physical ports to which these addresses are mapped.

```
network-interface
      name                           M00
      sub-port-id                    0
      description                    Internal-Nwk-If [the realm using this IP addr]
      hostname
      ip-address                     192.168.1.30 [Acme Packet private IP address]
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        192.168.1.1 [private side gateway]
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
```

```
            health-score                    0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
      hip-ip-list                    192.168.1.30 [allow hip to this address]
      ftp-address                    192.168.1.30 [allow ftp to this address]
      icmp-address                   192.168.1.30 [allow icmp to this address]
      snmp-address
      telnet-address                 192.168.1.30 [allow telnet to this address]
      ssh-address
      last-modified-by               admin@console
      last-modified-date             2012-10-15 11:14:32
network-interface
      name                           M10
      sub-port-id                    0
      description                    SFR-external-Nwk-If [SIP trunk provider realm]
      hostname
      ip-address                     192.168.1.200 [Acme Packet public IP address]
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        192.168.1.1 [public side gateway]
      sec-gateway
      gw-heartbeat
            state                           disabled
            heartbeat                       0
            retry-count                     0
            retry-timeout                   1
            health-score                    0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
      hip-ip-list                    192.168.1.200 [allow hip to this address]
      ftp-address
      icmp-address                   192.168.1.200 [allow icmp to this address]
      snmp-address
      telnet-address
      ssh-address
      last-modified-by               admin@192.168.1.50
      last-modified-date             2011-04-07 11:17:24
phy-interface
      name                           M00
      operation-type                 Media
      port                           0
      slot                           0
      virtual-mac
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      overload-protection            disabled
      last-modified-by               admin@192.168.1.50
      last-modified-date             2011-04-07 10:59:21
phy-interface
      name                           M10
      operation-type                 Media
      port                           0
      slot                           1
```

```
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        overload-protection            disabled
        last-modified-by               admin@192.168.1.50
        last-modified-date             2011-04-07 10:59:50
```

ANNOTATION: The realm configuration “core-avaya” represents the enterprise network where the communication manager and session manager are located.

```
realm-config
        identifier                     core-avaya [Enterprise realm]
        description                    Real-Avaya-side [descriptive name]
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M00:0
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        fallback-bandwidth             0
        max-priority-bandwidth         0
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        cac-failure-threshold          0
        untrust-cac-failure-threshold  0
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
```

```
        restriction-mask                  32
        accounting-enable                 enabled
        user-cac-mode                     none
        user-cac-bandwidth                0
        user-cac-sessions                 0
        icmp-detect-multiplier            0
        icmp-advertisement-interval       0
        icmp-target-ip
        monthly-minutes                   0
        net-management-control            disabled
        delay-media-update                disabled
        refer-call-transfer               disabled
        dyn-refer-term                    disabled
        codec-policy
        codec-manip-in-realm              disabled
        constraint-name
        call-recording-server-id
        xnq-state                         xnq-unknown
        hairpin-id                        0
        stun-enable                       disabled
        stun-server-ip                    0.0.0.0
        stun-server-port                  3478
        stun-changed-ip                   0.0.0.0
        stun-changed-port                 3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                        disabled
        hide-egress-media-update          disabled
        last-modified-by                  admin@192.168.1.92
        last-modified-date                2012-10-24 02:26:41
```

ANNOTATION: The session agent below represents the SFR SIP trunk service network border element. The Acme will attempt to send calls to the border element based on successful responses to the OPTIONS "ping-method". SFR SIP trunk service border element is also specified in the session-group section below.

```
realm-config
        identifier                        peer-sfr [SIP trunk provider realm]
        description                       Realm-SFR-SIP-Tk [descriptive name]
        addr-prefix                       0.0.0.0
        network-interfaces
                                          M10:0
        mm-in-realm                       disabled
        mm-in-network                     enabled
        mm-same-ip                        enabled
        mm-in-system                      enabled
        bw-cac-non-mm                     disabled
        msm-release                       disabled
        qos-enable                        disabled
        generate-UDP-checksum             disabled
        max-bandwidth                     0
        fallback-bandwidth                0
        max-priority-bandwidth            0
        max-latency                       0
        max-jitter                        0
        max-packet-loss                   0
        observ-window-size                0
        parent-realm
```

```
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              ACME_NAT_TO_FROM_IP
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        cac-failure-threshold           0
        untrust-cac-failure-threshold   0
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@192.168.1.92
        last-modified-date              2012-10-24 02:12:09
```

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

```
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   core-avaya
        egress-realm-id                 core-avaya
        nat-mode                        None
        registrar-domain
        registrar-host
        registrar-port                  0
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
        extra-method-stats              disabled
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        options                         max-udp-length=0
        refer-src-routing               disabled
        add-ucid-header                 disabled
        proxy-sub-events
        pass-gruu-contact               disabled
        sag-lookup-on-redirect          disabled
        last-modified-by                admin@192.168.1.50
        last-modified-date              2011-04-07 16:22:46
```

ANNOTATION: The SIP interface below is used to communicate with the Session Manager. SIP signaling is transported using UDP.

```
sip-interface
        state                           enabled
        realm-id                        core-avaya
        description                     SIP-if-Avaya-side
        sip-port
                address                         192.168.1.30
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
```

```
        ims-aka-profile
carriers
trans-expire                   0
invite-expire                  0
max-redirect-contacts          0
proxy-mode
redirect-action
contact-mode                   none
nat-traversal                  none
nat-interval                   30
tcp-nat-interval               90
registration-caching           disabled
min-reg-expire                 300
registration-interval          3600
route-to-registrar             disabled
secured-network                disabled
teluri-scheme                  disabled
uri-fqdn-domain
trust-mode                     all
max-nat-interval               3600
nat-int-increment              10
nat-test-increment             30
sip-dynamic-hnt                disabled
stop-recurse                   401,407
port-map-start                 0
port-map-end                   0
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
sip-ims-feature                disabled
operator-identifier
anonymous-priority             none
max-incoming-conns             0
per-src-ip-max-incoming-conns  0
inactive-conn-timeout          0
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive                  none
add-sdp-invite                 disabled
add-sdp-profiles
sip-profile
sip-isup-profile
last-modified-by               admin@192.168.1.50
last-modified-date             2011-04-07 15:39:03
```

ANNOTATION: The SIP interface below is used to communicate with the SFR SIP trunk service, signalling is transported using UDP.

```
sip-interface
      state                           enabled
      realm-id                        peer-sfr
      description                     SIP-If-SFR-side
      sip-port
            address                         192.168.1.200
            port                            5060
            transport-protocol              UDP
            tls-profile
            allow-anonymous                 all
            ims-aka-profile
      carriers
      trans-expire                    0
      invite-expire                   0
      max-redirect-contacts           0
      proxy-mode
      redirect-action
      contact-mode                    none
      nat-traversal                   none
      nat-interval                    30
      tcp-nat-interval                90
      registration-caching            disabled
      min-reg-expire                  300
      registration-interval           3600
      route-to-registrar              disabled
      secured-network                 disabled
      teluri-scheme                   disabled
      uri-fqdn-domain
      trust-mode                      all
      max-nat-interval                3600
      nat-int-increment               10
      nat-test-increment              30
      sip-dynamic-hnt                 disabled
      stop-recurse                    401,407
      port-map-start                  0
      port-map-end                    0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      sip-ims-feature                 disabled
      operator-identifier
      anonymous-priority              none
      max-incoming-conns              0
      per-src-ip-max-incoming-conns   0
      inactive-conn-timeout           0
      untrusted-conn-timeout          0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode            pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                  none
      implicit-service-route          disabled
      rfc2833-payload                 101
      rfc2833-mode                    transparent
```

```
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.1.92
        last-modified-date             2012-10-23 10:55:27
```

ANNOTATION: The steering pools below define the IP Addresses and RTP port ranges on the respective realms. The "peer-sfr" realm IP Address will be used as the media IP Address to communicate with SFR. Likewise, the IP Address and RTP port range defined for the "core-avaya" realm steering pool will be used to communicate with the communication manager and endpoints.

```
steering-pool
        ip-address                     192.168.1.31
        start-port                     2048
        end-port                       3329
        realm-id                       core-avaya
        network-interface
        last-modified-by               admin@192.168.1.50
        last-modified-date             2011-04-07 11:50:40
steering-pool
        ip-address                     192.168.1.201
        start-port                     2048
        end-port                       3329
        realm-id                       peer-sfr
        network-interface
        last-modified-by               admin@192.168.1.50
        last-modified-date             2011-04-07 11:51:45
system-config
        hostname
        description                    Customer-SBC
        location                       Courbevoie
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                   enabled
        enable-snmp-auth-traps         disabled
        enable-snmp-syslog-notify      disabled
        enable-snmp-monitor-traps      disabled
        enable-env-monitor-traps       disabled
        snmp-syslog-his-table-length   1
        snmp-syslog-level              WARNING
        system-log-level               WARNING
        process-log-level              NOTICE
        process-log-ip-address         0.0.0.0
        process-log-port               0
        collect
                sample-interval                5
                push-interval                  15
                boot-state                     disabled
                start-time                     now
                end-time                       never
```

```
            red-collect-state              disabled
            red-max-trans                  1000
            red-sync-start-time            5000
            red-sync-comp-time             1000
            push-success-trap-state        disabled
      call-trace                     disabled
      internal-trace                 disabled
      log-filter                     all
      default-gateway                192.168.1.1
      restart                        enabled
      exceptions
      telnet-timeout                 0
      console-timeout                0
      remote-control                 enabled
      cli-audit-trail                enabled
      link-redundancy-state          disabled
      source-routing                 disabled
      cli-more                       disabled
      terminal-height                24
      debug-timeout                  0
      trap-event-lifetime            0
      default-v6-gateway             ::
      ipv6-support                   disabled
      cleanup-time-of-day            00:00
      last-modified-by               admin@192.168.1.50
      last-modified-date             2011-04-07 10:57:18
task done
SBC-SIPLAB-01#
```

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.