Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R5.2.1 and Avaya Aura® Session Manager R5.2 to support Cable and Wireless SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Cable and Wireless SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Aura® Communication Manager connected to the Cable and Wireless SIP Trunk Service via an Acme Packet 3820 Session Border Controller. Cable and Wireless 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 to configure Session Initiation Protocol (SIP) trunking between Cable and Wireless SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 5.2 and Avaya Aura® Communication Manager 5.2.1 connected to an Acme Packet 3820 Session Border Controller. Customers using this Avaya SIP-enabled enterprise solution with the Cable and Wireless SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower costs 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 with all SIP traffic routed through the Acme Packet 3820 SBC. The enterprise site was configured to use the SIP Trunk Service provided by Cable and Wireless.

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 assigned by Cable and Wireless. Incoming PSTN calls were made to H.323, SIP, Digital and Analogue telephones at the enterprise side.
- Outgoing calls from the enterprise side were completed via Cable and Wireless to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and Analogue telephones.
- Calls were made using G.729A and G.711A codecs.
- 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.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Cable and Wireless requiring Avaya response and sent by Avaya requiring Cable and Wireless response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Cable and Wireless SIP Trunk Service with the following observations:

- The Calling Line Identity (CLI) set at the enterprise is hidden if the number is withheld at the enterprise in this case no number is presented to the called party.
- 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 999) was not tested.

2.3. Support

For technical support on Cable and Wireless products please use the following web link.
http://www.cw.com/contact-us/

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Cable and Wireless SIP Trunk Service. Located at the enterprise site are a Session Manager and Communication Manager. Endpoints are Avaya 9600 series IP telephones (H323 and SIP), Avaya 4600 series IP telephones (with H.323 firmware), Avaya 5400 series Digital telephone, an Analogue Telephone and a Fax machine. All SIP traffic from the enterprise site is via the Acme Packet 3820 SBC. For test purposes only, the Avaya enterprise site and the Cable and Wireless site were connected using a VPN tunnel across the Internet. VPN connectivity is not a facet of this application note and is transparent to the test activity. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

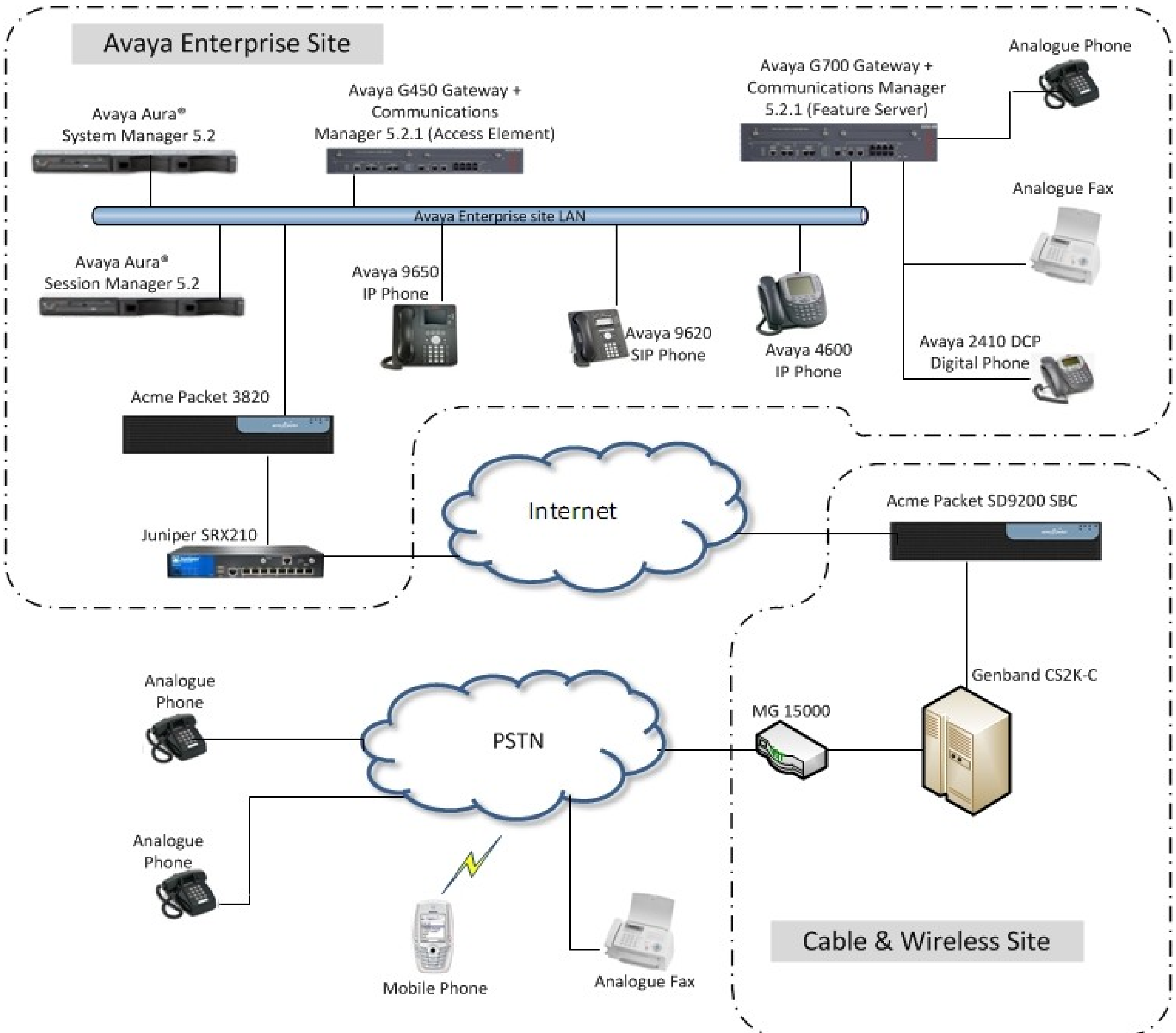


Figure 1: Cable and Wireless Test Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya G650 Media Gateway S8500	FW30.18.1 R015x.02.1.016.4
Avaya G700 Media Gateway MM711 Analogue MM712 Digital MM710 DSP S8300B	FW 30.10.3 HW31 FW093 HW04 FW009 HW11 FW047 R015x.02.1.016.4
Avaya Server S8510	Avaya Aura® Session Manager R5.2 (5.2.2.0.522007)
Avaya Server S8510	Avaya Aura® System Manager R5.2 (5.2.2.0.522002)
Avaya 9650 Phone (H.323)	3.11
Avaya 9620 Phone (SIP)	2.6.4.0
Avaya 4621 Phone (H.323)	2.9.1
Avaya 2420 Digital Phone	N/A
Analogue Phone	N/A
Acme Packet 3820 Net-Net SBC	Firmware SCX6.1.0 MR-6 GA (Build 738)
Service Provider	
ACME SD9200 SBC	rel 7 (nnSD700m7)
C&W SIP Trunk Service CS2k-C	CVM12

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 the Cable and Wireless SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Cable and Wireless via the Acme Packet 3820 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 signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Acme Packet 3820 SBC and on to the Cable and Wireless 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 S8300 Server and Avaya G700 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 Cable and Wireless network, and any other SIP trunks used.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 3
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 5
```

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? n                        ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? n
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? n
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? n               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? n                     Malicious Call Trace? n
     External Device Alarm Admin? n                 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? n                 Multifrequency Signaling? y
      Global Call Classification? n         Multimedia Call Handling (Basic)? n
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? n               Multimedia IP SIP Trunking? n
                       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. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **sm100** and **192.168.186.46** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the interface that the Communication Manager will use as the SIP signaling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
CMM                 10.10.16.82
default               0.0.0.0
procr               192.168.186.47
sm100               192.168.186.46
```

5.3. Administer IP Network Region

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

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

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Default
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1             Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? n
 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. Enter the list of audio codecs eligible to be used in order of preference. For the interoperability test the codecs supported by Cable and Wireless were configured, namely G.711A and G.729A.

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

                          IP Codec Set

    Codec Set: 1

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

On **Page 2** of the **IP Codec Set form**, configure the fax protocol by setting the **Fax Mode** to **off,** as shown in the next screenshot.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

5.5. Administer SIP Signaling Group 2

This signaling group (and trunk group) will be used for inbound and outbound PSTN calls to the Cable and Wireless SIP Trunk Service and will be configured using TCP (Transmission Control Protocol) and the default SIP port of 5060. Configure the **Signaling Group** using the **add signaling-group 2** 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 **sm100**), also shown in **Section 5.2**.
- Ensure that the recommended 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**.
- Set the **Far-end Domain** field to the domain of the enterprise (**avaya.com** in this setup).
- The **Direct IP-IP Audio Connections** field is set to **y**.

```
display signaling-group 2
                                SIGNALING GROUP

 Group Number: 2              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n




 Near-end Node Name: procr               Far-end Node Name: sm100
 Near-end Listen Port: 5060              Far-end Listen Port: 5060
                                         Far-end Network Region: 2
Far-end Domain: avaya.com

                                              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? n                      Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

5.6. Administer SIP Trunk Group 2

A trunk group is associated with the signaling group described in **Section 5.5.** Configure the trunk group using the **add trunk-group 2** command. 2. On **Page 1** of this form:

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

Group Number: 2                  Group Type: sip          CDR Reports: y
  Group Name: CM<>SM                   COR: 1        TN: 1        TAC: 702
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                     Signaling Group: 2
                                                   Number of Members: 5
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a reasonable value to prevent unnecessary SIP messages during call setup. A value of **1800** was used in this reference configuration.

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

TRUNK PARAMETERS

     Unicode Name: auto
                                           Redirect On OPTIM Failure: 5000

            SCCAN? n                              Digital Loss Group: 18
                       Preferred Minimum Session Refresh Interval(sec): 1800
```

On **Page 3** set the **Numbering Format** field to **public**.

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

                     Numbering Format: public
                                                UUI Treatment: service-provider

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

On **Page 4** set the **Mark Users as Phone** to **y**, this field inserts a parameter to SIP requests indicating to any receiving SIP entity that the user part of the request URI should be treated as a telephone number. Set **Send Transferring Party Information** to **y,** to allow trunk to trunk transfers.

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

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

                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 101
```

5.7. 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 the Cable and Wireless SIP Trunk Service. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise 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   9
                               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: *01
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    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 is 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. Calls are sent to Route Pattern 2, which contains the previously configured **SIP Trunk Group 2**.

```
change ars analysis                                             Page   1

                          ARS DIGIT ANALYSIS REPORT

                           Location:  all

              Dialed            Total        Route     Call       Node
              String          Min    Max    Pattern    Type      Number

        0                      8      8      deny      op
        0                      9      16     2         pubu
```

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, **Route Pattern 2** is used to route calls to trunk group 2.

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

     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
```

5.8. 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 Cable and Wireless 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 Cable and Wireless correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers starting with **0149** to a 4 digit extension by deleting the first seven incoming digits, leaving a four digit extension number.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len     Digits
 public-ntwrk    11     0149         7
```

5.9. Administer Public Unknown Numbering

The final configuration step for Communication Manager is to set the Public Unknown numbering table. To ensure outgoing calls have the correct Caller Line ID, each outgoing call must be prefixed with the area code. The full public number is composed of the **CPN Prefix** plus the four digit extension. Use the change **public-unknown-numbering 0** command to configure the table to prefix all outgoing numbers. A value of 0149160 was used for the **CPN Prefix**.

```
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: 2
 4  1                     0149160        11         Maximum Entries: 240
 4  2                                      4
```

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

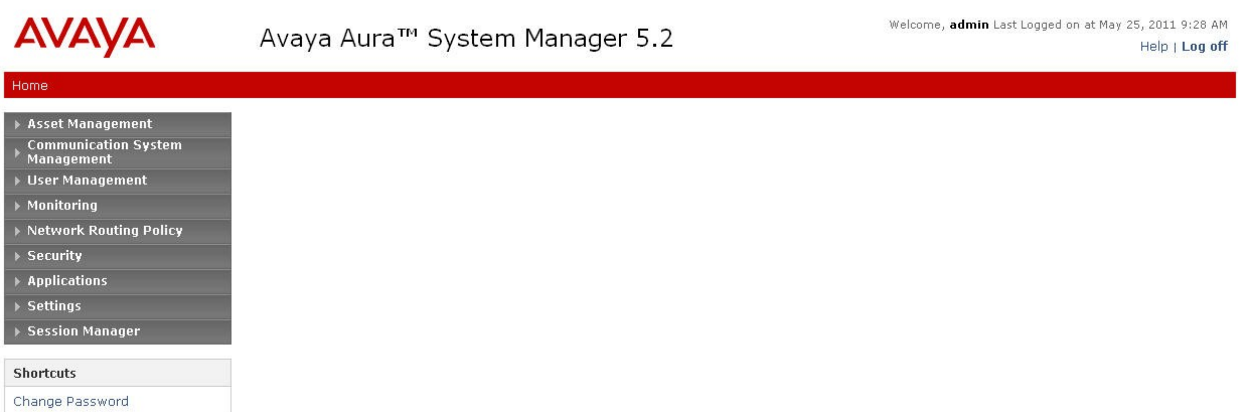
6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® Session 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
- Configure a SIP phone

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 page will be presented with menu options shown below.

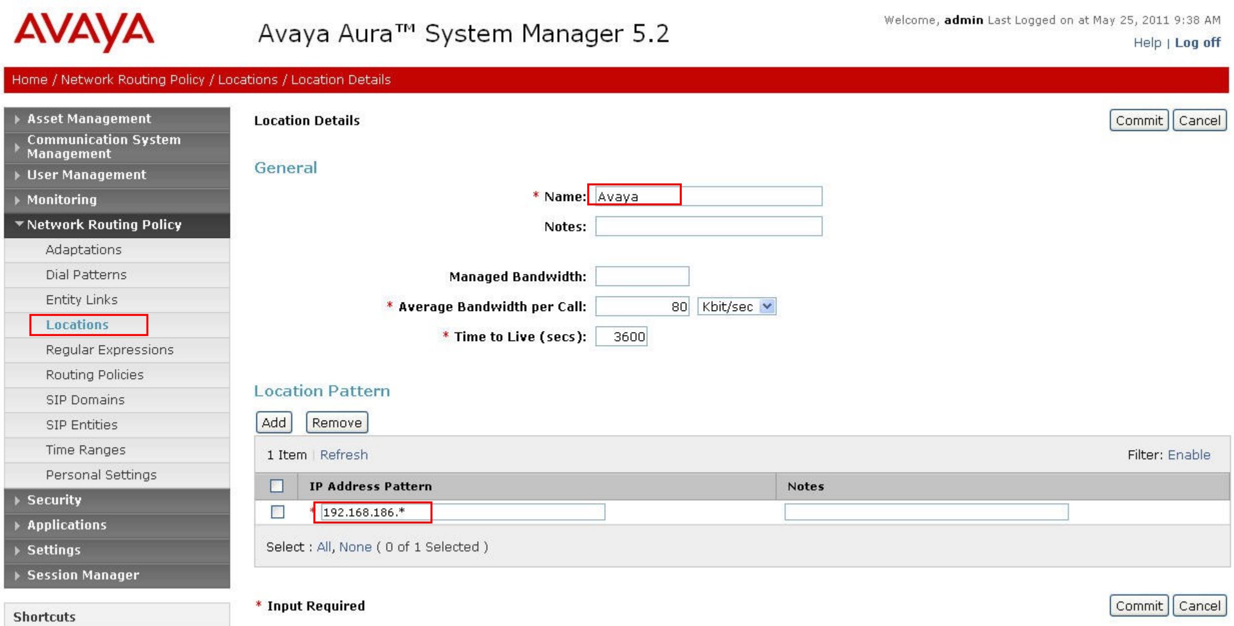


6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Network Routing Policy** from the left hand side menu and in the resulting drop down list select **SIP Domains**. Click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes. See the following screenshot for details.

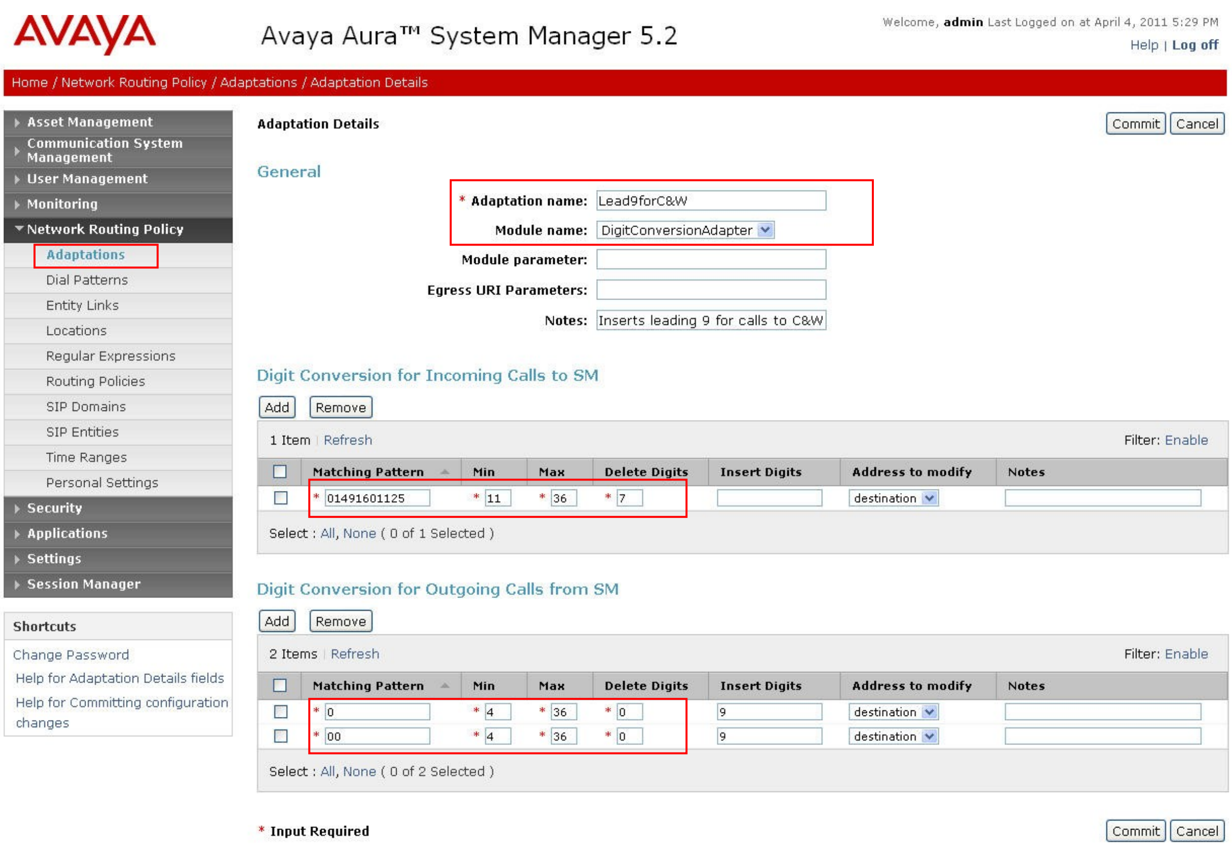
6.3. Administer Locations

For bandwidth management purposes, locations are used to identify logical and/or physical locations where SIP Entities reside. To add a location, select **Network Routing Policy** from the left hand side menu, then select **Locations** from the resulting drop down list. 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. A '*' is used to specify any number of allowed characters at the end of the string. Click **Commit** to save. Below is the location configuration used for the simulated enterprise site.



6.4. Administer Adaptions

An adaptation module is used to perform digit manipulation. In this example the incoming PSTN E.164 numbering format must be converted to a four digit local extension for SIP telephones and a leading digit 9 must be added to all outgoing PSTN calls. To add an adaptation, select **Adaptions** from the left panel menu (see the following screenshot) and then click on the **New** button (not shown). Under **General**, enter **DigitConversionAdapter** for the **Module Name**. Next, select **DigitConversionAdapter** from the **Module name** drop down list.



Under **Digit Conversion for Incoming Calls to SM**, click on the **Add** button and for **Matching Pattern**; enter some digits that will be tested for a match against all incoming calls. Next, enter the **Min** digit string length, the **Max** digit string length and the **Delete Digits** value. The example given shows that incoming calls with a number between 11 and 36 digits long will be tested, and if the first elevenigits match the string '0149160', then these digits will be removed and the remaining digits are checked by Session Manager. Normally, these would be sent to Communication Manager for further processing, in this scenario number 1125 represents a SIP telephone which is registered to Session Manager.

Under **Digit Conversion for Outgoing Calls from SM,** it is required to add the leading digit 9 to all outgoing PSTN calls. This is accomplished by testing all numbers dialed for digit pattern '0' or '00' and inserting a digit '9' if a match is found. Click on **Commit** when finished.

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:**

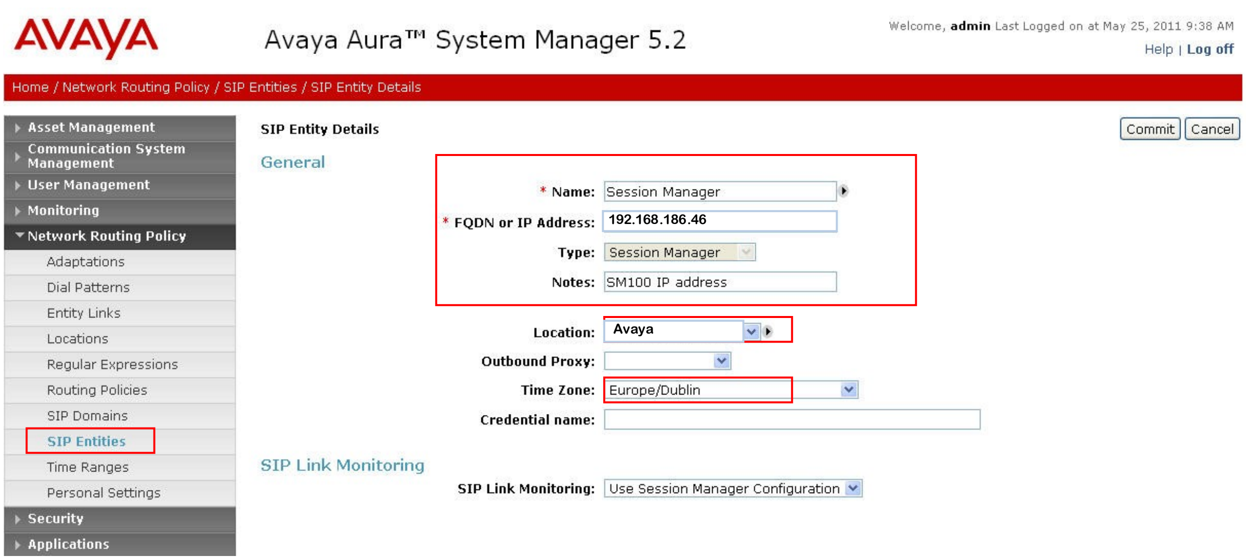
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of the SIP entity being configured.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the SBC 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 test configuration there are four SIP Entities configured.

- Session Manager SIP Entity
- Communication Manager SIP Entity (access element)
- Communication Manager SIP Entity (feature server)
- Acme Packet 3820 Session Border Controller SIP Entity (SBC)

6.5.1. Avaya Aura® Session Manager SIP Entity

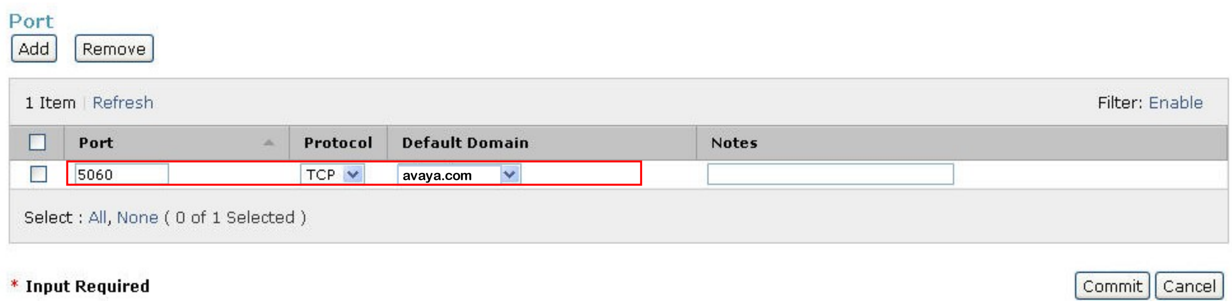
The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface.



The Session Manager must be configured with the port numbers and the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the **SIP Entity Details** 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**.

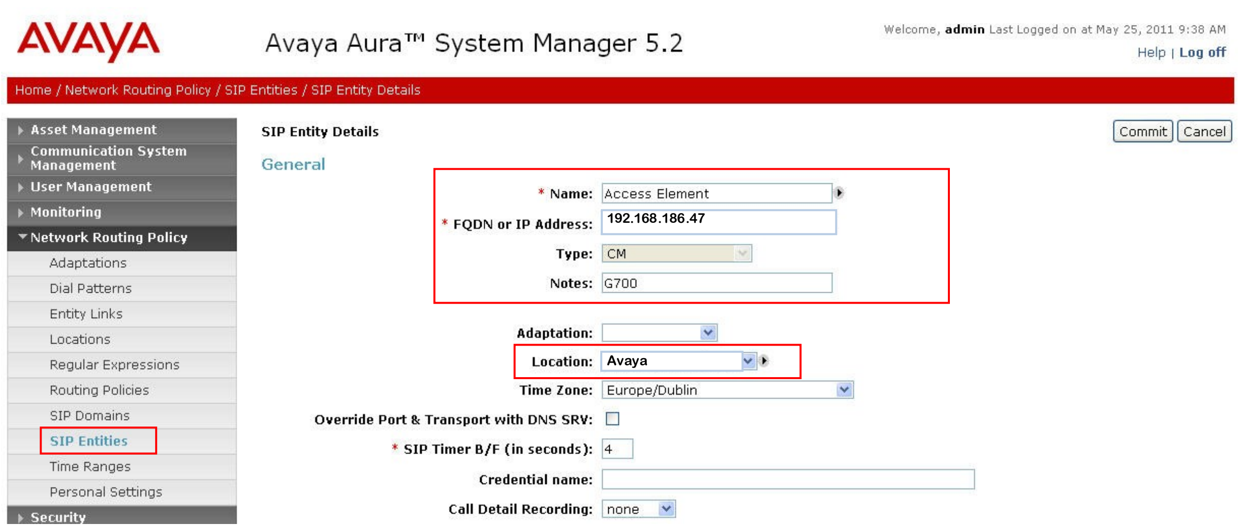
When finished, click of the **Commit** button. See the following screenshot for an example.



6.5.2. Avaya Aura® Communication Manager SIP Entity (access element)

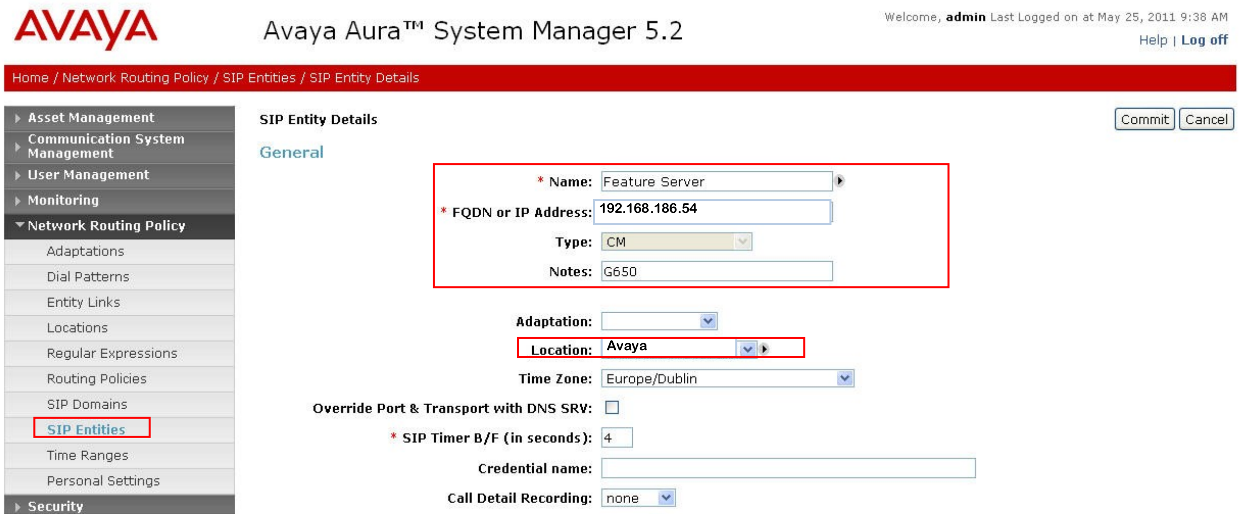
The following screen show the SIP entity for Communication Manager which is configured as an Access Element. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling.

Set the **Type** field to CM and click on the **Commit** button to save.



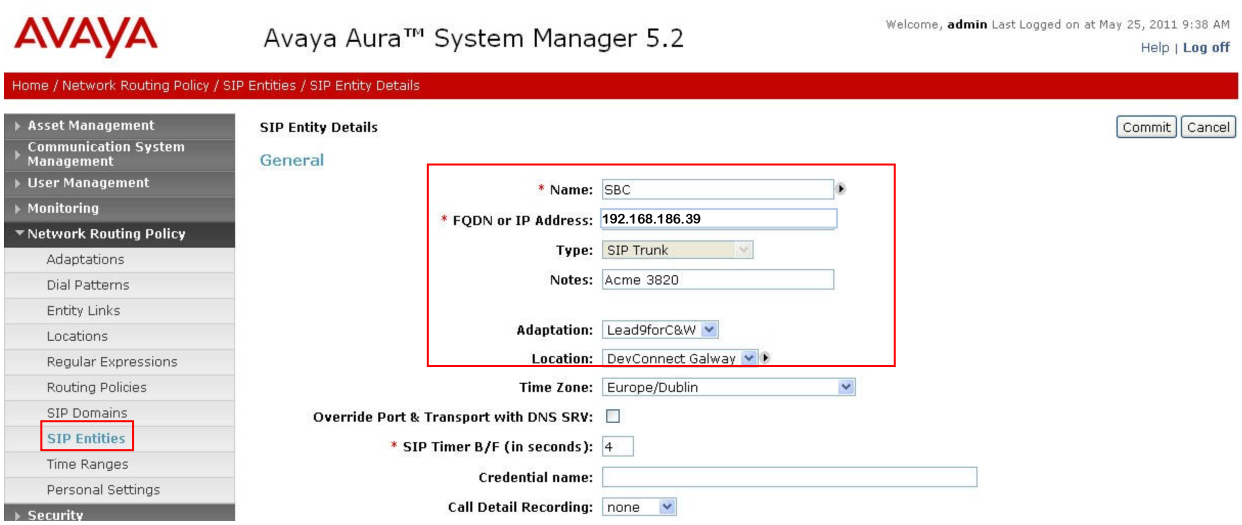
6.5.3. Avaya Aura® Communication Manager SIP Entity (feature server)

The next screenshot shows a SIP entity for Communication Manager which is configured as a Feature Server. The **FQDN or IP Address** field is set to the IP address of the Interface that provides SIP signaling. Set the **Type** field to CM and click on the **Commit** button to save.



6.5.4. Acme Packet 3820 SIP Entity

The Acme 3820 SBC used for the SIP trunk connection to Cable and Wireless must be added to Session Manager as a SIP entity. The **FQDN or IP Address** field is set to the private side IP address of the SBC. Note the **Adaption** is the one configured in **Section 6.4** and this is applied to all incoming and outgoing calls which pass through the Acme 3820 SBC. See the following screenshot for **SBC** entity configuration details.

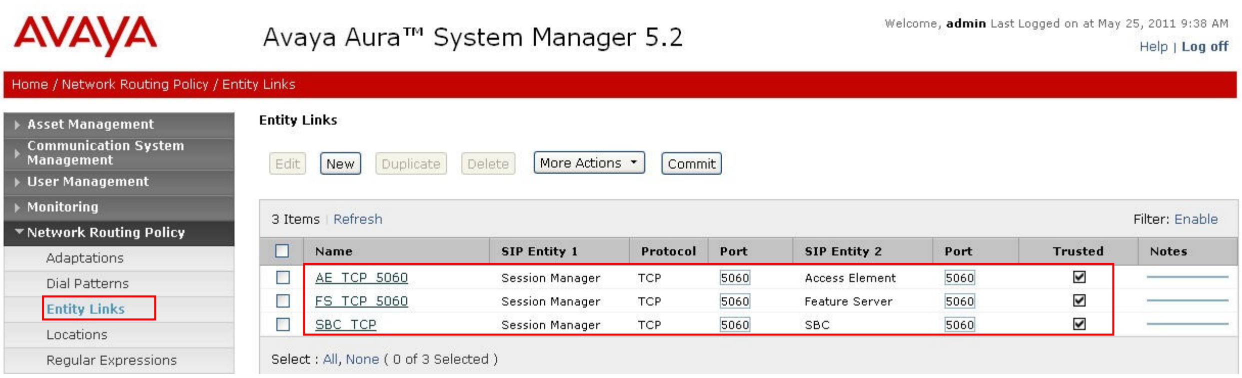


6.6. Administer Entity Links

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 of the following screenshot and click on the **New** button. 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 always select **Session Manager.**
- In the **Port** field **for SIP Entity 1**, enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter one of the other SIP Entities created in **Sections 6.5**.
- In the **Port** field for **SIP Entity 2**, enter the port number to which the other system expects to receive SIP requests.
- Select the **Trusted** tick box to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.

Repeat this step until all three SIP Entities are configured (i.e., the access element, the feature server and the Acme 3820 SBC). Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration.

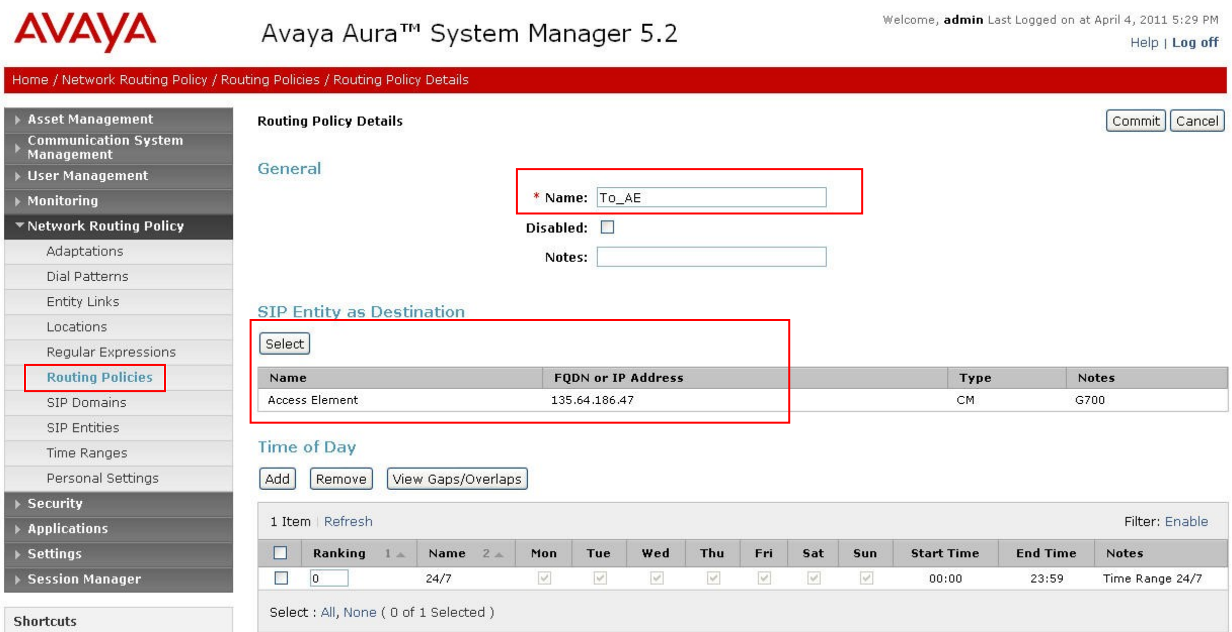


6.7. Administer Routing Policies

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

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

The following screen shows the routing policy for Communication Manager configured as an access element. Repeat the above procedure to configure the Acme 3820 SBC.



The next screenshot shows both routing policies used during compliance testing.

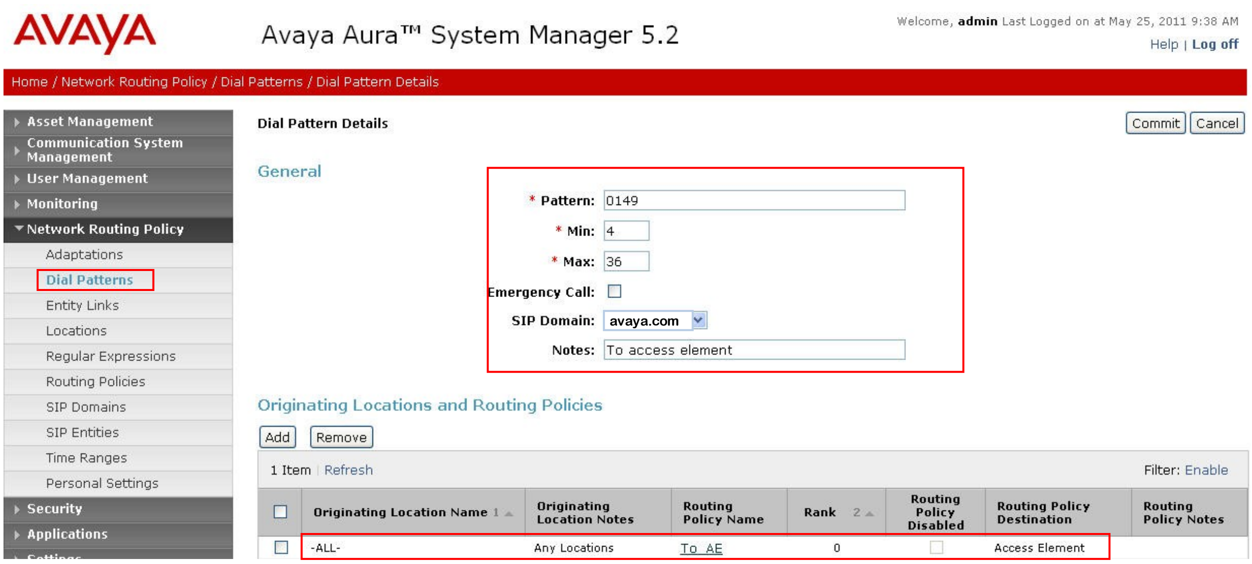
6.8. Administer Dial Patterns

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).

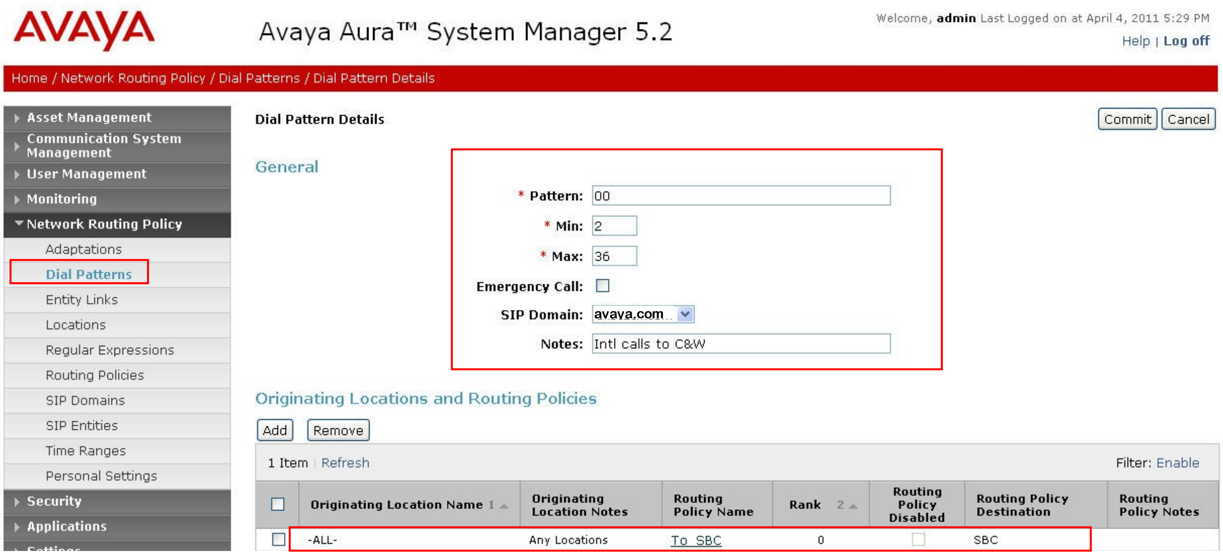
Under **General:**

- In the **Pattern** field, enter a 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**, and in the resulting screen (not shown) under **Originating Location** select the location created in **Section 6.3** (**All** in this example) and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save (not shown). The following screen shows an example dial pattern configured for the access element.

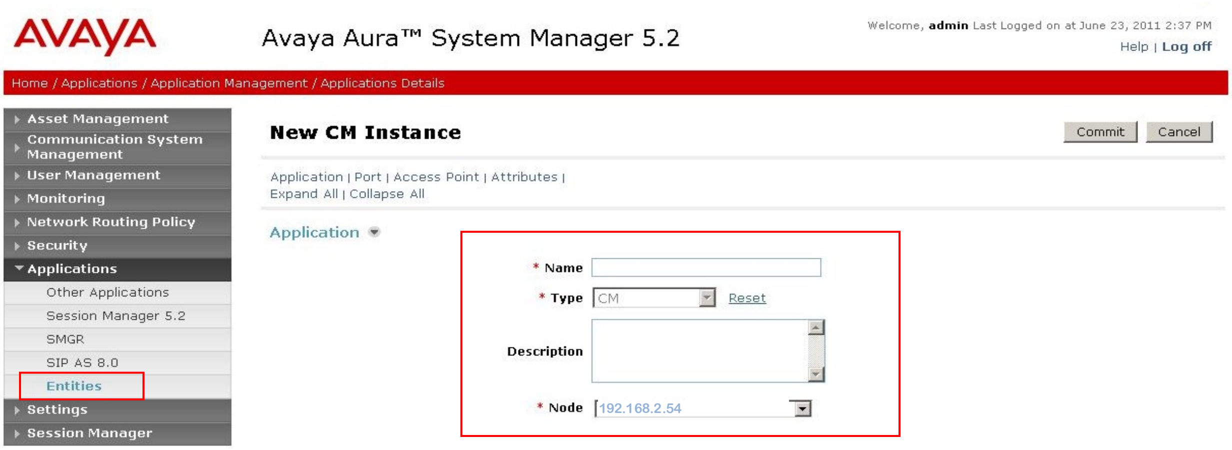


The following screen shows an example dial pattern configured for the Acme 3820 SBC.

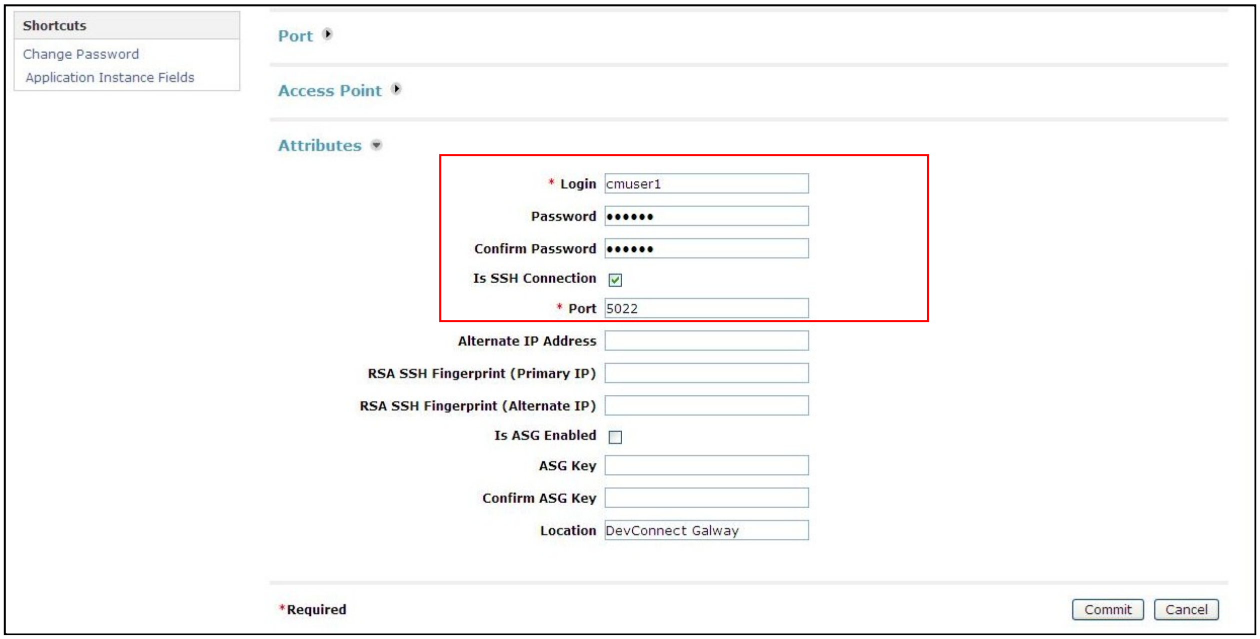


6.9. Administer Application for Avaya Aura® Communication Manager

Sip telephones require an application to be configured on Session Manager. To configure an application, click on **Applications** from the side menu then **Entities**. Click on the **New** button (not shown) then enter a **Name** for the application, select **Type** as CM. Text can be entered in the **Description** field to describe the application purpose. Type the IP address of the Feature Server configured in **Section 6.5.3** the in the **Node** field.



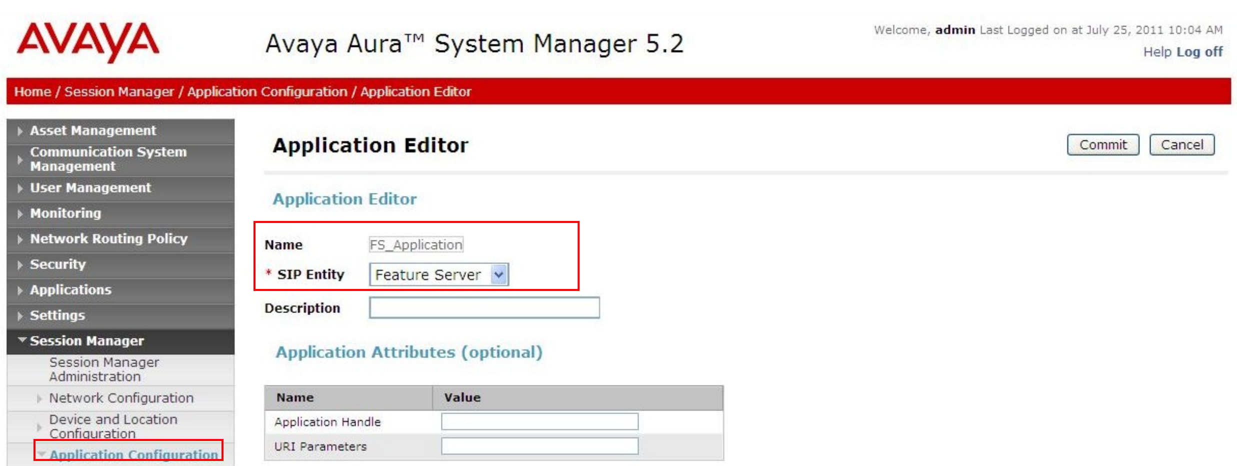
Move down the page to the attributes area and click on the arrow after **Attributes** to expand the property page. Fill in a valid profile 18 userid and password and set the port to 5022. See the following screenshot for an example.



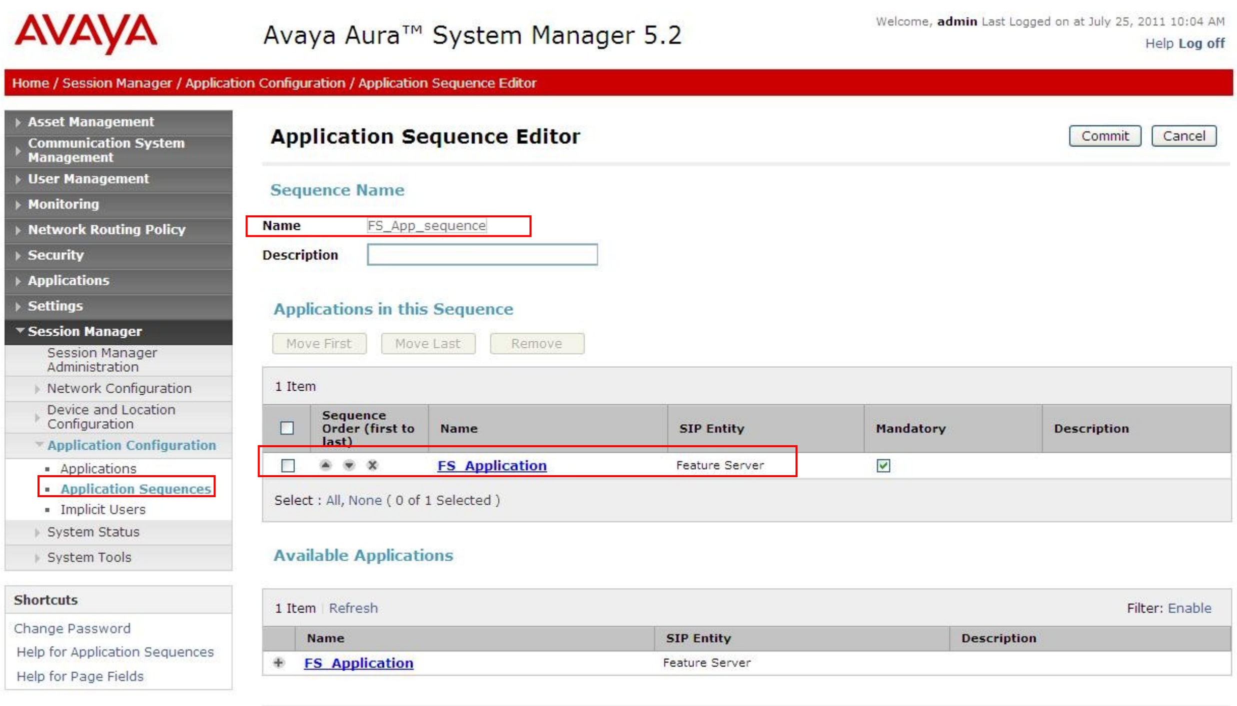
When finished, click on the **Commit** button.

6.10. Administer Application Sequence for Avaya Aura® Communication Manager

Click on **Session Manager** in the side menu, and then click on **Application Configuration**, then click on **Applications**. Click on the **New** button (not shown), then enter a **Name** for the application sequence. In the SIP Entity area select **Feature Server** from the drop down box. Enter a **Description** if required. Click on the **Commit** button when finished.

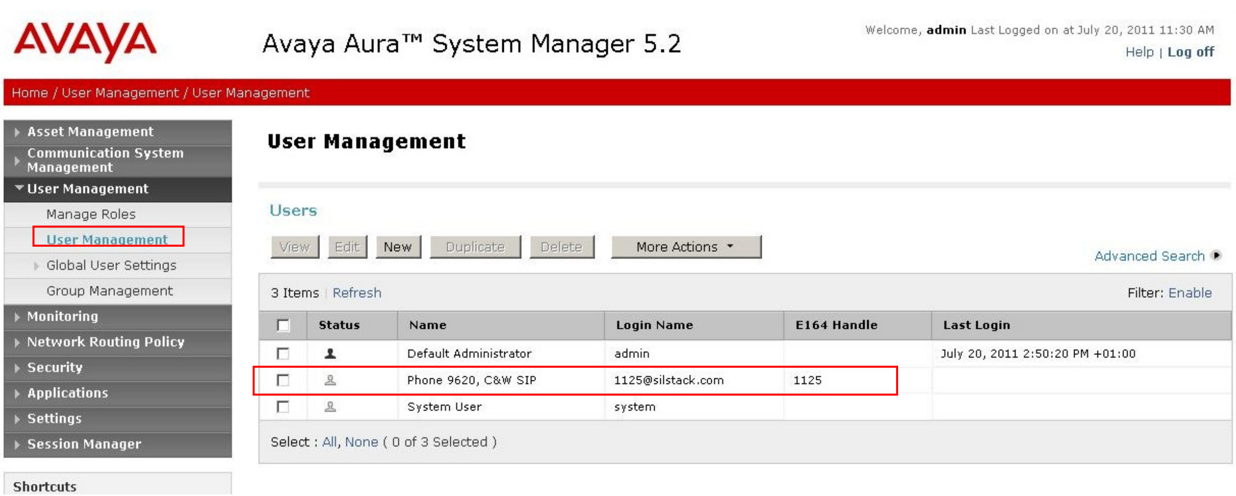


Click on the **Application Sequences** side menu and click on the **New** button (not shown). Enter a **Name** in the **Sequence Name** box. Move down the page to the **Available Applications** area and click on the plus symbol next to the application sequence you created in the previous step (see following screenshot). Ensure the sequence you just added is the first (or only) application in this sequence; use the **Move First** and **Move Last** buttons to change the application order. Click on the **Commit** button when finished.

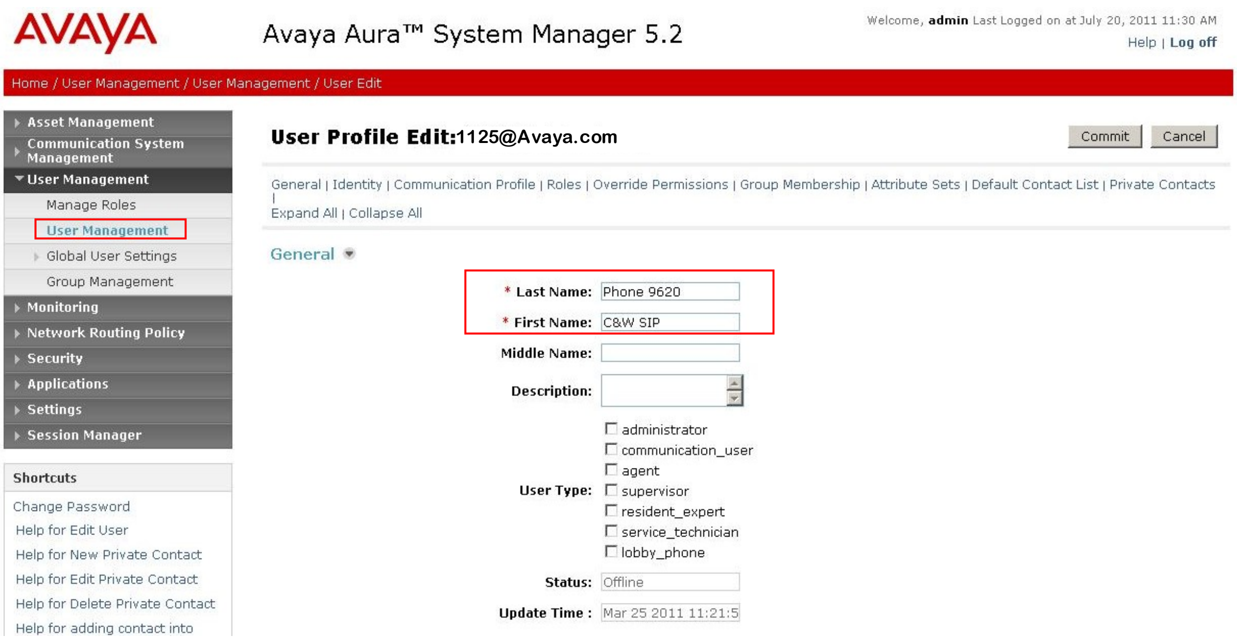


6.11. Configure a SIP phone

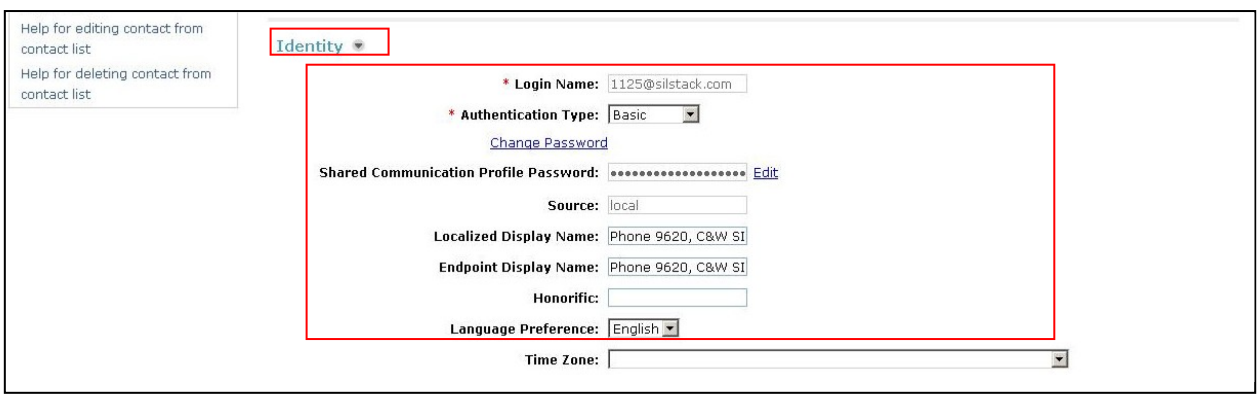
SIP telephones are configured on the Session Manager. Click on the **User Management** entry in the side menu, and then select the **User Management** entry from the drop down list. Click on the **New** button.



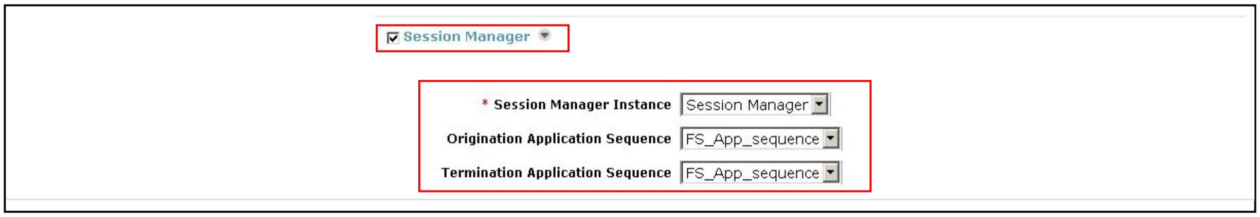
In the General area, fill in the user's first and last names, other details are not required. This section creates a new user on the System Manager.



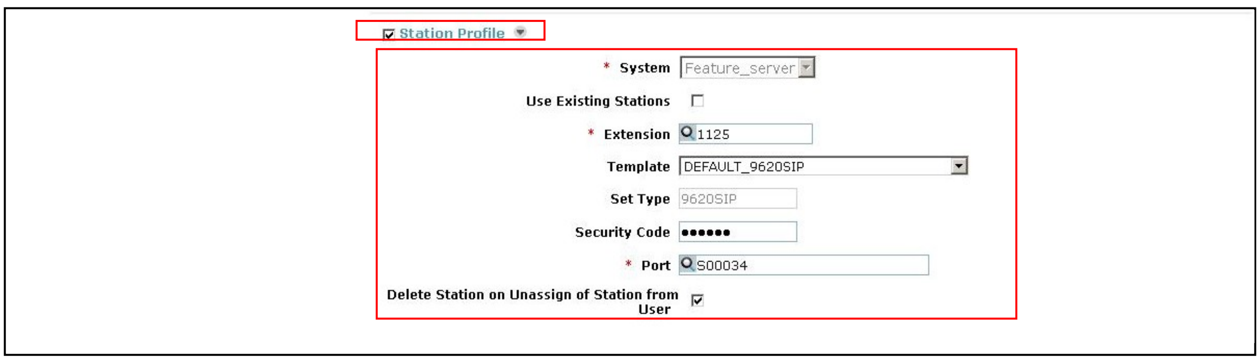
Scroll down the page and click on the arrow to the right of the **Identity** section. This section contains the SIP phones login credentials and identification details.



Scroll down to the **Session Manager** section, click the checkbox and click on the arrow to the right. Ensure the Session Manager instance is populated in the drop down box. For **Origination Application Sequence** and **Termination Application Sequence**, select the Application Sequence created in **Section 6.9** from the drop down lists.



Scroll down to the **Station Profile** section, click the checkbox and click on the arrow to the right. For **System**, select the Feature_Server previously configured in **Section 6.10**. Populate the **Extension** box with a phone number. Select the correct template for the SIP phone being configured. Enter a **Security Code** (a string of digits) and ensure the **Delete Station on Unassign of Station from User** checkbox is ticked. Finally, click on the Commit button (not shown) when finished.



This completes the configuration required for the Session Manager.

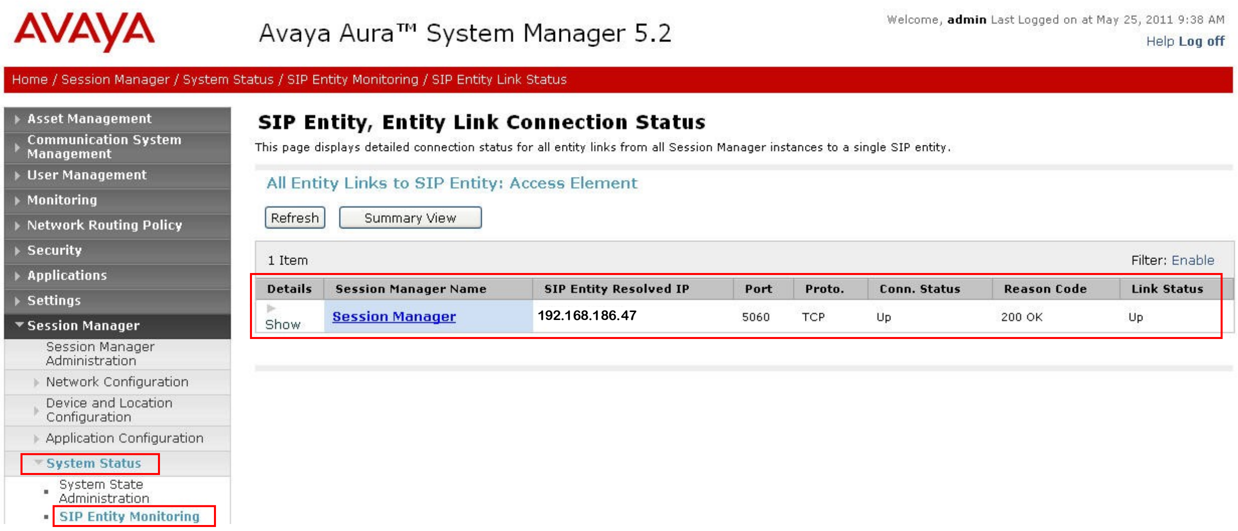
7. SIP Provider Trunk configuration

Other than the basic network diagram and general configuration for the SIP Trunk solution testing shown in **Figure 1**; specific Cable and Wireless SIP Trunk configuration and discussion of the service operational and technical characteristics are outside the scope of these Application Notes. Please contact Cable and Wireless using the contact details provide in **Section 2.3** for detailed information on their SIP Trunk product.

8. Verification Steps

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

1. From System Manager left hand side menu, click on **Session Manager** and navigate to **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.** See the following screenshot for details.



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

```
status trunk 2

                              TRUNK GROUP STATUS

Member    Port     Service State      Mtce Connected Ports
                                      Busy

0002/001 T00001   in-service/idle    no
0002/002 T00007   in-service/idle    no
0002/003 T00008   in-service/idle    no
0002/004 T00009   in-service/idle    no
0002/005 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 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.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager Access Element and Avaya Aura® Session Manager to Cable and Wireless SIP Trunk Service. Cable and Wireless SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

10. References

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

[1] *Administering Avaya Aura® Communication Manager as a Feature Server*, January 2011.

[2] *Installing and Upgrading Avaya Aura® System Manager 5.2*, July 2010.

[3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* May 2009, Document Number 555-245-205.

[5] *Administering System Manager 5.2*, January 2010.

[6] *Installing Avaya Aura® Session Manager*, October 2010.

[7] *Administering Avaya Aura® Session Manager,* August 2010, Document Number 03-603324.

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

Appendix A

The configuration details provided here are the Acme Packet 3820 Net-Net SBC settings used during compliance testing. Publicly routable IP addresses have been changed to private IP addresses for security reasons.

Acme 3820 Net-Net Session Border Controller Configuration

```
host-routes
        dest-network                   192.165.24.8              /* Far side SBC IP addres
        netmask                        255.255.255.255           /* Allow just one host
        gateway                        192.168.102.1             /* Juniper VPN gateway IP
description                            route-to-CW               /* All SIP to internet
        last-modified-by               admin
        last-modified-date             2011-03-11 16:34:38
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       OUTSIDE                   /* Far side realm
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-03-15 10:44:58
        policy-attribute
                next-hop                       192.168.186.46    /* SM100 IP address
                realm                          INSIDE            /* The Avaya side realm
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol
                state                          enabled
                methods
                media-profiles
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       INSIDE                    /* Avaya side SIP realm
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-03-07 16:42:21
        policy-attribute
                next-hop                       192.168.24.8      /* Far side SBC IP address
                realm                          OUTSIDE           /* Far side SIP realm
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
```

```
                app-protocol
                state                         enabled
                methods
                media-profiles
network-interface
        name                          S0P1                          /* Slot 0 port 1
        sub-port-id                   0
        description
        hostname
        ip-address                    192.168.102.70                /* Avaya SBC Public IP
pri-utility-addr
        sec-utility-addr
        netmask                       255.255.255.0                 /* Subnet Mask
        gateway                       192.168.102.1                 /* Juniper IP address
sec-gateway
        gw-heartbeat
                state                         enabled
                heartbeat                     10
                retry-count                   3
                retry-timeout                 1
                health-score                  30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                   11
        hip-ip-list                   192.168.102.70                /* Allow admin traffic
ftp-address
        icmp-address                  192.168.102.70                /* Allow response to pings
        snmp-address                  192.168.102.70                /* Allow SNMP
        telnet-address
        last-modified-by              admin@console
        last-modified-date            2011-03-08 14:56:08
network-interface
        name                          S0P0                          /* Slot 0 Port 0
        sub-port-id                   0
        description
        hostname
        ip-address                    192.168.186.39                /* Avaya SBC Private side IP
        pri-utility-addr
        sec-utility-addr
        netmask                       255.255.255.224               /* Subnet Mask
        gateway                       192.168.186.33                /* Local gateway
        sec-gateway
        gw-heartbeat
                state                         enabled
                heartbeat                     10
                retry-count                   3
                retry-timeout                 1
                health-score                  30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                   11
        hip-ip-list                   192.168.186.39                /* Allow admin traffic
        ftp-address
        icmp-address                  192.168.186.39                /* Allow pings
        snmp-address                  192.168.186.39                /* allow SNMP
        telnet-address                192.168.186.39                /* Permit telnet access
        last-modified-by              admin@console
        last-modified-date            2011-03-08 14:52:15
phy-interface
        name                          S0P0                          /* Slot 0 Port 0
                      */
        operation-type                Media
        port                          0
        slot                          0
        virtual-mac
        admin-state                   enabled
```

```
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-by               admin@console
        last-modified-date             2011-03-07 07:46:02
phy-interface
        name                           S0P1                         /* Slot 0 Port 1
        operation-type                 Media
        port                           1
        slot                           0
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-by               admin@console
        last-modified-date             2011-03-07 07:57:02
realm-config
        identifier                     INSIDE                       /* Avaya side realm
               */
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       S0P0:0                       /* Interface for realm INSIDE
        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
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        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
        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
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        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
        last-modified-by               admin@console
        last-modified-date             2011-03-07 14:44:01
realm-config
        identifier                     OUTSIDE                      /* Far side SIP realm
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       S0P1:0                       /* Slot 1 Port 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
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        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
        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
        codec-policy
        codec-manip-in-realm          disabled
        constraint-name
        call-recording-server-id
        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
        last-modified-by              admin@console
        last-modified-date            2011-03-07 14:45:51
session-agent
        hostname                      192.168.186.46             /* Avaya side SM100 IP
        ip-address                    192.168.186.46             /* Avaya side SM100 IP
        port                          5060
        state                         enabled
        app-protocol                  SIP
        app-type
        transport-method              UDP
        realm-id                      INSIDE                     /* Avaya side SIP realm
        egress-realm-id
        description
        carriers
        allow-next-hop-lp             enabled
        constraints                   disabled
        max-sessions                  0
        max-inbound-sessions          0
        max-outbound-sessions         0
        max-burst-rate                0
        max-inbound-burst-rate        0
        max-outbound-burst-rate       0
        max-sustain-rate              0
        max-inbound-sustain-rate      0
        max-outbound-sustain-rate     0
        min-seizures                  5
        min-asr                       0
        time-to-resume                0
        ttr-no-response               0
        in-service-period             0
        burst-rate-window             0
        sustain-rate-window           0
        req-uri-carrier-mode          None
        proxy-mode
        redirect-action
        loose-routing                 enabled
        send-media-session            enabled
        response-map
        ping-method                   OPTIONS;hops=0
        ping-interval                 60
        ping-send-mode                keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                      disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                   disabled
        in-manipulationid
```

```
        out-manipulationid
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        last-modified-by               admin@console
        last-modified-date             2011-03-15 10:48:51
session-agent
        hostname                       192.168.24.8                /* Far side SBC IP address
        ip-address                     192.168.24.8                /* Far side SBC IP address
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       OUTSIDE                     /* Far side SIP realm
        egress-realm-id
        description
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  10
        ping-send-mode                 keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
```

```
        in-manipulationid
        out-manipulationid
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        last-modified-by               admin@console
        last-modified-date             2011-03-11 17:27:22
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INSIDE
        egress-realm-id
        nat-mode                       None
        registrar-domain               *
        registrar-host                 *
        registrar-port                 5060
        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                8192
        enum-sag-match                 disabled
        extra-method-stats             disabled
        registration-cache-limit       0
        register-use-to-for-lp         disabled
        add-ucid-header                disabled
        proxy-sub-events
        last-modified-by               admin@console
        last-modified-date             2011-03-15 12:15:28
sip-interface
        state                          enabled
        realm-id                       OUTSIDE                       /* Far side SIP realm
        description                    C&W
        sip-port
                address                        192.168.102.70       /* Avaya SBC Public IP
                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
        max-udp-length=0
        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
        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
        refer-call-transfer            disabled
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        last-modified-by               admin@console
        last-modified-date             2011-03-11 17:20:45
sip-interface
        state                          enabled
        realm-id                       INSIDE                   /* Avaya side SIP realm
        description                    Manager
        sip-port
                address                        192.168.186.39       /* Avaya SBC Private IP
                port                           5060
                transport-protocol             TCP
                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
        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
        refer-call-transfer            disabled
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        last-modified-by               admin@console
        last-modified-date             2011-03-15 12:20:15
steering-pool
        ip-address                     192.168.186.39             /* Avaya SBC Private side IP
        start-port                     2048                       /* Start port matches ACM
        end-port                       3329                       /* Stop port matches ACM
        realm-id                       INSIDE                     /* Avaya side SIP realm
        network-interface
        last-modified-by               admin@console
        last-modified-date             2011-03-21 13:12:44
steering-pool
        ip-address                     192.168.24.8               /* Far side SIP realm
        start-port                     10000                      /* Start port on far side
        end-port                       20000                      /* Stop port on far side
```

```
        realm-id                       OUTSIDE                      /* Far side SIP realm
network-interface
        last-modified-by               admin@console
        last-modified-date             2011-03-21 13:13:22
system-config
        hostname
        description
        location
        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                192.168.186.33
        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
        cleanup-time-of-day            00:00
        last-modified-by               admin@console
        last-modified-date             2011-03-07 07:54:14
```

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.