Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 5.2.1, Avaya Aura™ Session Manager 5.2.1.1, and Acme Packet 4500 Net-Net Session Director integration with Metaswitch MetaSphere CFS – Issue 1.0

Abstract

These Application Notes describe the steps to configure an Avaya Aura™ SIP trunk solution with Metaswitch MetaSphere Call Feature Server (CFS). The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager (version 5.2.1), and Avaya Aura™ Session Manager (version 5.2.1.1), and an Acme Packet 4500 Net-Net Session Director (6.1.0).

The Metaswitch MetaSphere CFS solution referenced within these Application Notes is designed for customers with an Avaya SIP trunk solution. The Metaswitch MetaSphere CFS solution provides access to service providers for local and/or long Distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Interoperability Test Lab, utilizing a connection to the Metaswitch Test Lab over the public network.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure an Avaya Aura™ SIP trunk solution with Metaswitch MetaSphere Call Feature Server (CFS). The Avaya SIP trunk architecture consists of Avaya Aura™ Communication Manager (version 5.2.1), and Avaya Aura™ Session Manager (version 5.2.1.1), and an Acme Packet 4500 Net-Net Session Director (6.1.0). Various Avaya analog, digital, H.323, and SIP stations are also included in the configuration.

The Acme Packet 4500 Net-Net Session Director is used as an edge device between the Avaya Customer Premises Equipment (CPE) and the Metaswitch MetaSphere solution.

Session Manager performs as the SIP trunking "hub" where all inbound and outbound SIP call routing (and other call processing) decisions are made. Communication Manager SIP trunks and Acme Packet "session-agents" are provisioned to terminate at Session Manager.

The Metaswitch MetaSphere CFS solution described in these Application Notes is designed for customers using Communication Manager and Session Manager. The Metaswitch MetaSphere CFS solution provides access to service providers for local and/or long Distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

1.1. Interoperability Compliance Testing

A simulated enterprise site consisting of Communication Manager (version 5.2.1), Session Manager (version 5.2.1.1), System Manager (version 5.2.1.1), and an Acme Packet 4500 Net-Net Session Director (version 6.1.0) supporting SIP trunking was connected to the public internet. The enterprise site was configured to use a generally available SIP trunking solution provided by Metaswitch. This allowed the enterprise site to use SIP trunking for calls to and from the PSTN.

The following features and functionality were covered during the SIP trunking interoperability compliance testing:

- Incoming calls to the enterprise site from the PSTN (using the DID numbers assigned by Metaswitch).
- Outgoing calls from the enterprise site to PSTN destinations via Metaswitch.
- Calls using various analog, digital, H.323, and SIP endpoints supported by the Avaya IP telephony solution.
- Various call types including: local, long distance, and toll free calls.
- Calls using various codecs.
- Inbound and outbound fax calls.
- DTMF tone transmission using RFC 2833 with successful voice mail navigation.
- Telephone features such as hold, transfer, conference, and call forwarding.
- EC500 Features
- Calls using Avaya one-X Communicator (softphone).

1.2. Support

For technical support for Metaswitch, contact your Metaswitch Networks support representative.

2. Reference Configuration

Figure 1 illustrates the reference configuration used for the DevConnect compliance testing. The reference configuration is comprised of Avaya Customer Premises Equipment (CPE) located in the Solution Interoperability Test Lab in Westminster, Colorado. The Avaya CPE location simulates an enterprise customer site and uses private IP addressing. At the edge of the Avaya CPE location, an Acme Packet Session Border Controller (SBC) provides Network Address Translation (NAT) functionality that converts the private IP addressing to public addressing that is passed to Metaswitch. The "inside" interface of the Acme Packet SBC is connected to a private subnet. The "outside" interface of the Acme Packet SBC is connected to a Juniper edge router providing access to the Metaswitch Test Lab network via the public internet.

Metaswitch provided a Direct Inward Dial (DID) 10 digit number for use during the testing. The DID was mapped by Session Manager to an associated Communication Manager extension.

Metaswitch used the domain *208.xxx.xxx.135*. The Avaya CPE environment was assigned the domain *avaya.com*. See **Section 2.1** for more details regarding the domains.

The following components were used in the reference configuration and are discussed in detail in subsequent sections.

- Session Manager on a Avaya S8800 Server
- Avaya Aura™ System Manager non an Avaya S8800 Server
- Communication Manager on an Avaya S8300 Server, with an Avaya G450 Media Gateway
- Communication Manager on an Avaya S8800 Server, with an Avaya G430 Media Gateway

Note – This Communication Manager serves as a Feature Server in the reference configuration for the Avaya 9600 Series SIP Telephones. SIP phones (requiring advanced calling features) and non-SIP phones configured on the same Communication Manager is currently not supported. This restriction will be lifted in future releases of Session Manager and Communication Manager.

- Avaya 9600 Series IP Telephones (SIP)
- Avaya 9600 Series IP Telephones (H.323)
- Avaya one-X Communicator (H.323 softphone)
- Avaya 6400 Series Digital Telephone
- Avaya 6210 Analog Telephone
- Fax Machine
- Acme Packet Net-Net 4500 Session Director
- Metaswitch Networks MetaSphere CFS

Since public IP addresses were used during compliance testing, IP addresses are not shown in the figure below and the public IP addresses are masked (at least partially) throughout the document.

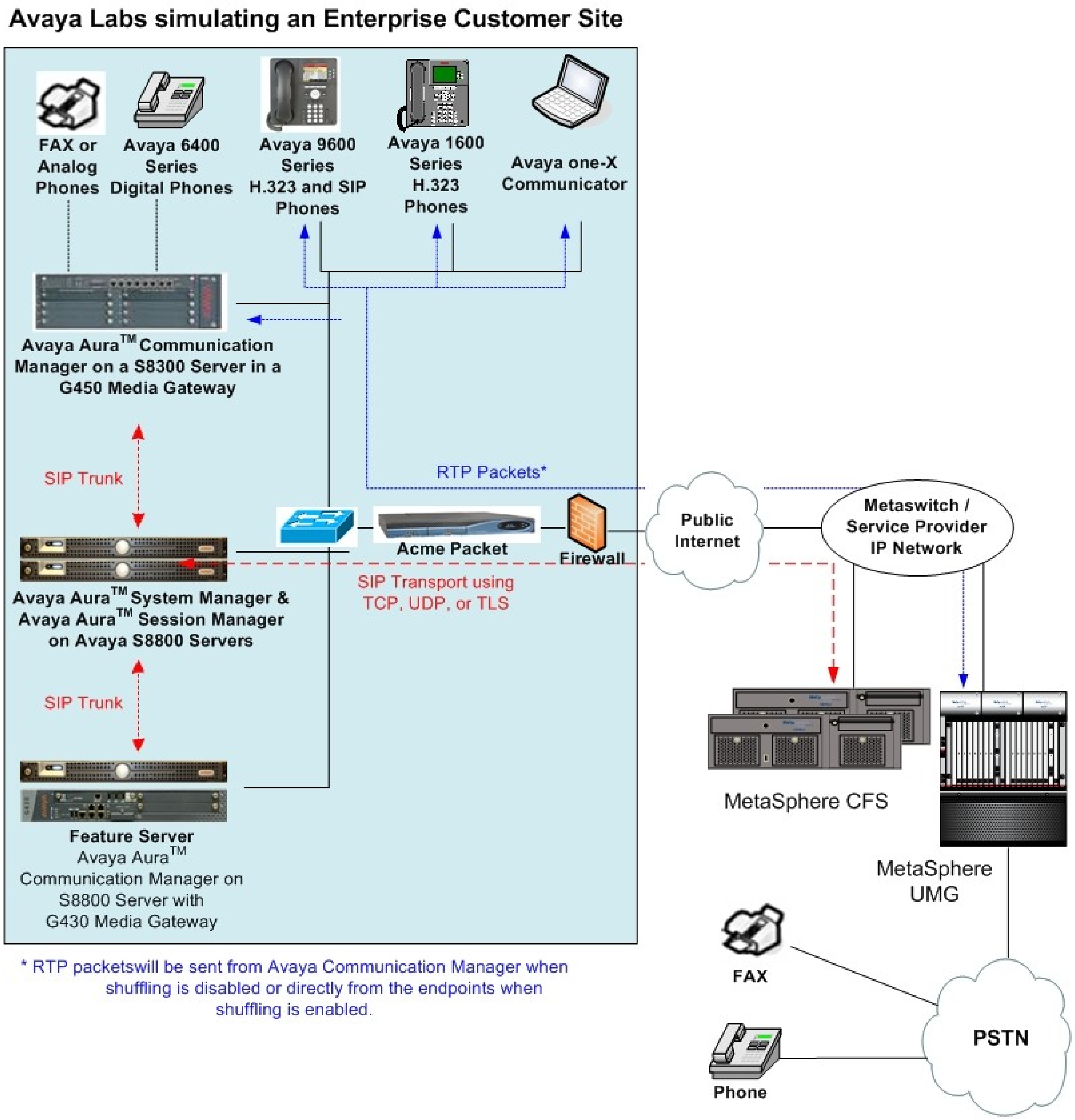

Figure 1: Avaya Interoperability Test Lab Reference Configuration

2.1. Local to Foreign Domain Conversion for Outbound Calls

The Avaya CPE environment was assigned the domain *avaya.com*, and the Metaswitch domain is *208.xxx.xxx.135*. For outbound calls from the Avaya CPE, the destination specified in the SIP request URI should be *208.xxx.xxx.135*. There are two methods to accomplish this.

1. Communication Manager method – Communication Manager would specify the Metaswitch domain in the Far-End Domain field of the Signaling Group form. This would result in Communication Manager sending a SIP request URI to Session Manager with the following format:

   <called number>@208.xxx.xxx.135

   Session Manager would forward this URI to the Acme Packet for transmission to Metaswitch.

2. Session Manager method – Communication Manager would specify the Avaya domain (or blank) in the Far-End Domain field of the Signaling Group form. This would result in Communication Manager sending a SIP request URI to Session Manager with the following format:

   <called number>@avaya.com

   By assigning an adaptation to the Acme Packet SIP Entity (**see Sections 6.3.2** and **6.3.4**), Session Manager will convert the Avaya CPE domain to the Metaswitch domain and send the following request URI to the Acme Packet:

   <called number>@ 208.xxx.xxx.135

Note - In the reference configuration, method 2 was chosen.

3. Equipment and Software Validated

The following equipment and software were used in the reference configuration.

Equipment	Software/Firmware
Avaya Aura™ Session Manager – Avaya S8800 Server w/ SM100 Board	5.2.1.1
Avaya Aura™ System Manager – Avaya S8800 Server	5.2.1.1
Avaya Aura™ Communication Manager - Avaya S8300 Server	5.2.1 with Avaya Aura™ Communication Manager Messaging
Avaya G450 Media Gateway	-
Avaya 9600 Series IP Telephones (SIP) Avaya 9600 Series IP Telephones (H.323)	2.5.0 3.0
Avaya one-X Communicator (H.323 softphone)	5.2
Avaya 64xx Digital Telephone	-
Avaya 6210 Analog Telephone	-
Fax Machine	-
Acme Packet Net-Net 4500 Session Director	SCX6.1.0 MR-1 Patch 1 (WS Build 282)
Metaswitch Networks MetaSphere CFS	7.1.01 SU0

Table 1: Equipment and Software Used in the Reference Configuration

4. Configure Avaya Aura™ Communication Manager for SIP Trunking

This Section describes the steps for configuring Communication Manager with the necessary signaling and media characteristics for the SIP trunk connection with the Metaswitch solution.

Note - The initial installation, configuration, and provisioning of the Avaya servers for Communication Manager, Avaya Media Gateways and their associated boards, as well as the Avaya telephones, are presumed to have been previously completed and are not discussed in these Application Notes.

The Avaya CPE site utilized a Communication Manager running on an Avaya S8300 server with an Avaya G450 Media Gateway.

Note – The Communication Manager commands described in these Application Notes were administered using the System Access Terminal (SAT). SSH was used to connect to the SAT via the appropriate IP address, login and password.

4.1. Verify System Capacity and Features

The Communication Manager license file controls the customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

1. On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** value is sufficient for the combination of trunks to the Metaswitch solution and any other SIP trunking applications. Be aware that for each call from a non-SIP endpoint to the Metaswitch solution, one SIP trunk is used for the duration of the call.

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

IP PORT CAPACITIES                                                USED
                    Maximum Administered H.323 Trunks: 450   50
          Maximum Concurrently Registered IP Stations: 450   3
            Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
             Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                 Maximum Video Capable H.323 Stations: 0     0
                  Maximum Video Capable IP Softphones: 0     0
                      Maximum Administered SIP Trunks: 450   270
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                            Maximum TN2501 VAL Boards: 0     0
                    Maximum Media Gateway VAL Sources: 0     0
          Maximum TN2602 Boards with 80 VoIP Channels: 0     0
         Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 2: System-Parameters Customer-Options Form – Page 2

Note – If any changes are made to the **system-parameters customer-options** form, you must log out of the SAT and log back in for the changes to take effect.

2. On **Page 3** of the **System-Parameters Customer-Options** form, verify that the **ARS** feature is enabled.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? n
        Access Security Gateway (ASG)? n              Authorization Codes? n
        Analog Trunk Incoming Call ID? n                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                         CAS Main? n
Answer Supervision by Call Classifier? n                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? n
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? n
          ASAI Link Core Capabilities? y                DCS Call Coverage? n
          ASAI Link Plus Capabilities? y               DCS with Rerouting? n
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n                          DS1 MSP? n
                                ATMS? n             DS1 Echo Cancellation? n
                  Attendant Vectoring? n




        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 3: System-Parameters Customer-Options Form – Page 3

3. On **Page 4** of the **System-Parameters Customer-Options** form, verify that the **Enhanced EC500**, **IP Trunks,** and **ISDN-PRI** features are enabled.

```
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? n
        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 4: System-Parameters Customer-Options Form – Page 4

4.1.1 Dial Plan

In the reference configuration, five digit extensions for analog, digital, and H.323 stations were provisioned with the format 7xxxx. Five digit extensions for SIP stations were provisioned with the format 531xx. Trunk Access Codes (TAC) are 3 digits in length and begin with 1. The Feature Access Code (FAC) to access ARS is one digit in length (the number "9").

The dial plan is modified with the ***change dialplan analysis*** command.

1. On **Page 1** of the form, configure the following:
   - Local extensions (analog, digital, and H.323 stations):
     1. In the **Dialed String** field, enter **7**.
     2. In the **Total Length** field, enter **5**.
     3. In the **Call Type** field, enter **ext**.
   - Local extensions (SIP stations):
     1. In the **Dialed String** field, enter **5**.
     2. In the **Total Length** field, enter **5**.
     3. In the **Call Type** field, enter **ext**.
   - TAC codes:
     1. In the **Dialed String** field, enter **1**.
     2. In the **Total Length** field, enter **3**.
     3. In the **Call Type** field, enter **dac**.
   - FAC code – ARS access:
     1. In the **Dialed String** field, enter **9**.
     2. In the **Total Length** field, enter **1**.
     3. In the **Call Type** field, enter **fac**.

```
change dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all         Percent Full:    2

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     1            3    dac
     2            5    ext
     4            4    ext
     5            5    ext
     7            5    ext
     8            5    ext
     9            1    fac
     *            3    fac
```

Figure 5: Change Dialplan Analysis Form – Page 1

4.1.2 Uniform Dialplan

The uniform dial plan is modified with the ***change uniform-dialplan*** command.

1. On **Page 1** of the form, configure the following:
   - Local extensions (SIP stations):
     1. In the **Matching Pattern** field, enter **531**
     2. In the **Len** field, enter **5**
     3. In the **Del** field, enter **0**
     4. In the **Net** field, enter **aar**
     5. In the **Conv field**, enter **n**

```
change uniform-dialplan 0                                         Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                Percent Full: 0

  Matching                  Insert              Node
  Pattern        Len Del    Digits     Net Conv Num
531              5   0                 aar  n
```

Figure 6: Change Uniform Dialplan Form – Page 1

4.1.3 Node Names

In the **IP Node Names** form, verify (or assign) the node names to be used in this configuration using the ***change node-names ip*** command.

- **SM2** and **10.64.20.31** are the **Name** and **IP Address** of Session Manager.
- **procr** and **10.64.21.41** are the **Name** and **IP Address** of the processor interface for Communication Manager.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
CM-B1               192.45.108.55
CM-B2               192.45.108.57
SES-A               10.64.21.61
SM1                 10.64.40.42
SM2                 10.64.20.31
default             0.0.0.0
procr               10.64.21.41
```

Figure 7: IP Node Names Form

4.1.4 IP-Network-Regions

One network region was defined in the reference configuration.

The SIP trunk ip-network-regions are defined in the SIP Signaling Group form with the Far-end Region parameter (see **Section 4.1.6**).

Network region assignments for ip-interfaces may be verified with the ***list ip-interface all*** command.

```
list ip-interface all

                                IP INTERFACES

                                                                 Net
ON Type   Slot  Code/Sfx      Node Name/       Mask  Gateway Node     Rgn  VLAN
                              IP-Address
-- ------ ----- --------      ---------------  ----  ---------------  ---  ----
 y PROCR                      10.64.21.41      /24   10.64.21.1       1
```

Figure 8: IP-Interface IP-Network-Region Assignments

The network-region for an ip-interface may be modified with the ***change ip-interface x*** command where **x** is the board location or **procr**.

```
change ip-interface procr                                     Page   1 of   1
                                  IP INTERFACES


                  Type: PROCR
                                                       Target socket load: 1700

      Enable Interface? y                           Allow H.323 Endpoints? y
                                                     Allow H.248 Gateways? y
        Network Region: 1                             Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /24
```

Figure 9: IP-Interface IP-Network-Region Assignment

The **IP-Network-Region** form specifies the parameters used by the Communication Manager components and how components defined to different regions interact with each other. In the reference configuration, only one ip-network region was used; however, other combinations are possible.

Note – Avaya IP telephones inherit the ip-network-region of the procr (or C-LAN) they register to. As a result, if an IP phone registers to the procr in the reference configuration, that phone will become part of region 1. If an IP phone needs to be defined to a different region regardless of registration, this may be performed with the ***change ip-network-map*** command (not shown).

4.1.4.1 IP-Network-Region 1

Ip-network-region 1 is defined for Communication Manager components. The network regions are modified with the ***change ip-network-region x*** command, where x is the network region number.

1. On **Page 1** of the **IP Network Region** form:
   - Configure the **Authoritative Domain** field to *avaya.com*.
   - By default, **Intra-region** and **Inter-region IP-IP Direct Audio** (media shuffling) are set to **yes** to allow audio traffic to be sent directly between IP endpoints to reduce the use of media resources.
   - Set the **Codec Set** to **1** for the corresponding calls within the IP Network Region.
   - All other values are the default values.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Compliance Testing
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? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

Figure 10: IP Network Region 1 – Page 1

4.1.5 IP Codec Sets

One IP codec set is defined in the reference configuration.

4.1.5.1 IP-Codec-Set 1

G.711MU is typically used within the same location and is often specified first. Other codecs could be specified as well depending on local requirements. Codec set 1 is associated with ip-network-region 1 (see **Section 4.1.4.1**).

The **IP-Codec-Set** form is modified with the ***change ip-codec-set x*** command, where ***x*** is the codec set number.

1. On **Page 1** of the form:
   - Configure the **Audio Codec** field **1** to **G.711MU**. During compliance testing G.729B and G.729AB were also tested.

```
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.711MU          n          2        20
 2:
```

Figure 11: IP Codec Set 1

2. On **Page 2** of the form:
   - Configure the **FAX** field to **t.38-standard**.
   - Configure the **Fax Redundancy** field to **0**.
   - Use the default settings for all other fields.

```
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
```

Figure 12: IP Codec Set 1 – Page 2

4.1.6 SIP Trunk Groups

SIP trunks are defined for internal calls as well as off network calls to and from the PSTN via Metaswitch. A SIP trunk is created in Communication Manager by provisioning a SIP Trunk Group as well as a SIP Signaling Group.

Note – In the SIP trunk configurations below (and in the corresponding Session Manager configuration), TLS was selected as the transport protocol in the reference configuration. The TCP protocol could have been used instead.

4.1.6.1 Configure SIP Trunk for internal calls

1. Using the ***change signaling-group 8*** command, configure the Signaling Group as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** field to **tls**.

Note – This specifies the transport method used between Communication Manager and Session Manager, not the transport method used to the Metaswitch network.

- Specify the procr (or C-LAN) used for SIP signaling (node name **procr**) and the Session Manager (node name **SM2**) as the two ends of the signaling group in the **Near-end Node Name** and **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Section 4.1.3.**
- Specify **5061** in the **Near-End** and **Far-end Listen Port** fields.
- Enter the value **1** into the **Far-end Network Region** field. This value is for the **IP Network Region** defined in **Section 4.1.4.1**.
- Set the **Far-end Domain** field to *avaya.com*.
- The **Direct IP-IP Audio Connections** field should be set to **y** to allow RTP voice paths to be established directly between IP telephones and the Metaswitch network.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF tones using RFC 2833.
- The default values for the other fields may be used.

```
change signaling-group 8                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 8              Group Type: sip
                        Transport Method: tls
  IMS Enabled? n





   Near-end Node Name: procr                  Far-end Node Name: SM2
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1
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? y                       Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

Figure 13: Internal calls SIP Trunk - Signaling Group 8

2. Using the ***change trunk-group 8*** command, change the Trunk Group as follows:
   a. On **Page 1** of the Trunk Group form:
      - Set the **Group Type** field to **sip**.
      - Choose a descriptive **Group Name.**
      - Specify an available trunk access code (**TAC**) (e.g. **108**).
      - Set the **Service Type** field to **public-ntwrk.**
      - Enter **8** as the **Signaling Group** number.
      - Specify the **Number of Members** used by this SIP trunk group (e.g. **10**).

```
change trunk-group 8                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 8                    Group Type: sip           CDR Reports: y
  Group Name: to SM (avaya.com)           COR: 1        TN: 1        TAC: 108
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                       Signaling Group: 8
                                                     Number of Members: 10
```

Figure 14: Internal calls Trunk Group 8 – Page 1

   b. On **Page 3** of the **Trunk Group** form:
      - Set the **Numbering Format** field to **public.** This field specifies the format of the calling party number sent to the far-end.

```
change trunk-group 8                                              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








 Show ANSWERED BY on Display? y
```

Figure 15: Internal calls Trunk Group 8 – Page 3

4.1.6.2 Configure SIP Trunk for off network calls

The SIP trunk for off network calls is configured in the same fashion as the internal call SIP Trunk except that the Far-end Domain is set to blank.

1. Using the ***change signaling-group 9*** command, configure the Signaling Group as follows:

   - Set the **Group Type** field to **sip**.
   - Set the **Transport Method** field to **tls**.

Note – This specifies the transport method used between Communication Manager and Session Manager, not the transport method used to the Metaswitch network.

   - Specify the procr (or C-LAN) used for SIP signaling (node name **procr**) and the Session Manager (node name **SM2**) as the two ends of the signaling group in the **Near-end Node Name** and **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Section 4.1.3.**
   - Specify **5061** in the **Near-End** and **Far-end Listen Port** fields.
   - Enter the value **1** into the **Far-end Network Region** field. This value is for the **IP Network Region** defined in **Section 4.1.4.1**.
   - Leave the **Far-end Domain** field blank. This permits inbound calls from any foreign domain (e.g. the Metaswitch network).
   - The **Direct IP-IP Audio Connections** field should be set to **y** to allow RTP voice paths to be established directly between IP telephones and the Metaswitch network.
   - The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF tones using RFC 2833.
   - The default values for the other fields may be used.

```
change signaling-group 9                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 9             Group Type: sip
                       Transport Method: tls
  IMS Enabled? n





   Near-end Node Name: procr                  Far-end Node Name: SM2
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1
Far-end Domain:

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

Figure 16: Off network calls SIP Trunk - Signaling Group 9

2. Using the ***change trunk-group 9*** command, change the Trunk Group as follows:
    a. On **Page 1** of the Trunk Group form:
        - Set the **Group Type** field to **sip**.
        - Choose a descriptive **Group Name.**
        - Specify an available trunk access code (**TAC**) (e.g. **109**).
        - Set the **Service Type** field to **public-ntwrk.**
        - Enter **9** as the **Signaling Group** number.
        - Specify the **Number of Members** used by this SIP trunk group (e.g. **10**).

```
change trunk-group 9                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 9                    Group Type: sip          CDR Reports: y
  Group Name: to SM (blank)              COR: 1        TN: 1        TAC: 109
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                    Signaling Group: 9
                                                  Number of Members: 10
```

Figure 17: Off network calls Trunk Group 9 – Page 1

    b. On **Page 3** of the **Trunk Group** form:
        - Set the **Numbering Format** field to **public.** This field specifies the format of the calling party number sent to the far-end.

```
change trunk-group 9                                            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







 Show ANSWERED BY on Display? y
```

Figure 18: Off network calls Trunk Group 9 – Page 3

4.1.7 Public Unknown Numbering – Basic Configuration

In the reference configuration, Communication Manager uses a 5 digit dialing plan with extensions 7xxxx for analog, digital, and H.323 stations. The **Public-Unknown-Numbering** form allows Communication Manager to use these extensions as the calling party number for outbound calls. Otherwise, *Anonymous* is displayed as the calling number. Each extension string is defined for the trunk group(s) that the extensions may use. These trunks may be defined individually or in contiguous ranges.

In the reference configuration, in order for a station to place off network calls (to the PSTN), the calling number must match the DID provided by Metaswitch, or the call will be rejected by Metaswitch. The public-unknown-numbering form was configured to convert a local calling extension to its associated Metaswitch DID.

Use the ***change public-unknown-numbering x*** command, where *x* is the leading digit of the dial plan extensions (e.g. **7**).

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to **7**.
- Set the **Trk Grp(s)** field to **9.**
- Set the **CPN Prefix** field to the leading digits of the Metaswitch DID (e.g. **51021**)
- Set the **Total CPN Len** field to **10**. This is the total number of digits in the DID.

With this configuration, Communication Manager will insert 51021 for calls from a 5 digit extension (starting with digit 7), going over trunk 9. This allows the station with the extension that matches the last 5 digits of the Metaswitch DID to place calls to the PSTN.

For internal calls:

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to **7**.
- Set the **Trk Grp(s)** field to **8**.
- Set the **Total CPN Len** field to **5**. This is the total number of digits in the extension.

All provisioned public-unknown-numbering entries can be displayed by entering the command ***display public-unknown-numbering 0*** as show below.

```
display 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: 4
 5  5                                       5           Maximum Entries: 240
 5  7             8                         5
 5  7             9         51021           10
```

Figure 19: Public-unknown-numbering Form – Basic Configuration

4.1.8 Call Routing

4.1.8.1 Outbound Calls

The following sections describe the Communication Manager provisioning required for outbound dialing. Although Session Manager routes all inbound and outbound SIP trunk calls, Communication Manager uses ARS and AAR to direct outbound calls to Session Manager.

4.1.8.1.1 ARS

The Automatic Route Selection feature is used to route calls via a SIP trunk, configured in **Section 4.1.6.2**, to Session Manager, which in turn completes the calls to the Metaswitch. In the reference configuration, ARS is triggered by dialing a 9 (feature access code or FAC) and then dialing the called number. ARS matches on the called number and sends the call to a specified route pattern.

1. Use the ***change feature-access-codes*** command to specify **9** as the access code for external dialing.
   - Set **Auto Route Selection (ARS) – Access Code 1:** to **9**.

```
change feature-access-codes                                        Page   1 of   8
                              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:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *11    All: *22    Deactivation: *33
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

Figure 20: Feature-Access-Codes Form – Page 1

2. Use the ***change ars analysis*** command to configure the route pattern selection rule based upon the number dialed following the ARS access digit "9". In the reference configuration, outbound calls are placed to the following numbers:

    - 1732 (calls to area code 732 by dialing 9 1 732 xxx xxxx)
    - 1303 (calls to area code 303 by dialing 9 1 303 xxx xxxx)

    For example, to specify 732 area code calls, enter the command ***change ars analysis 173*** and enter the following values:
    - Set the **Dialed String** field to **173**.
    - Set the **Total Min** field to **11**.
    - Set the **Total Max** field to **11**.
    - Set the **Route Pattern** field to **9** (will direct to off network calls trunk).
    - Set the **Type** field to **fnpa**.

    Different values may be used. These were the values used for the reference configuration.

```
display ars analysis 173                                       Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    2

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    173                   11   11     9        fnpa         n
```

Figure 21: ARS Analysis Form

3. Using the same procedure, specify the other called number patterns in the ARS table.

4.1.8.1.2 AAR

The Automatic Alternate Routing feature is used to route calls to the SIP trunk, configured in **Section 4.1.6.1**, to the Session Manager, which in turn completes the calls to local SIP stations. AAR matches on the called number and sends the call to a specified route pattern.

1. Use the ***change aar analysis*** command to configure the route pattern selection rule based upon the number dialed. In the reference configuration 5 digit SIP stations were provisioned with the extension format 531xx.

```
change aar analysis 531                                        Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    2

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    531                   5    5      8        aar          n
```

Figure 22: AAR Analysis Form

4.1.8.1.3 Route Patterns

The reference configuration used route-pattern 9 for ARS calls to Session Manager.

Note - Route patterns may also be used to add or delete digits prior to sending them out the specified trunk(s). This feature was not used in the reference configuration.

1. Use the ***change route-pattern*** command to define the SIP trunk group to be used in the route pattern that ARS selects.
   - Set the **Grp No** field to ***9***.
   - Set the **FRL** field to ***0***.
   - The default values for the other fields may be used.

```
change route-pattern 9                                          Page   1 of   3
                    Pattern Number: 9   Pattern Name: Outbound-SM2
                             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: 9    0                                                               n   user
 2:                                                                      n   user
```

Figure 23: Route Pattern 9 – Outbound Calls to Metaswitch

2. Use the **change route-pattern** command to define the SIP trunk group to be used in the route pattern that AAR selects.
   - Set the **Grp No** field to ***8***.
   - Set the **FRL** field to ***0***.
   - The default values for the other fields may be used.

```
change route-pattern 8                                          Page   1 of   3
                    Pattern Number: 8   Pattern Name: to SIP stations
                             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: 8    0                                                               n   user
 2:                                                                      n   user
```

Figure 24: Route Pattern 8 –Calls to SIP stations

4.1.8.2 Incoming Calls

Session Manager is used to convert the inbound Metaswitch DID number to a Communication Manager extension. Therefore, no incoming digit manipulation was required on Communication Manager.

Note - Incoming called numbers may be changed to match a provisioned extension, if necessary, with the Communication Manager ***change inc-call-handling-trmt trunk-group x*** command, where **x** is the receiving trunk.

4.1.9 Avaya Aura™ Communication Manager Stations (non-SIP)

In the reference configuration, 5-digit non-SIP stations were provisioned with the extension format 7xxxx.

4.1.9.1 Voice Stations

The figures below show an example of an extension (Avaya H.323 IP phone). Since the phone is an IP device, a virtual port **S00027** is automatically assigned by the system. By default, three call appearances are defined on Page 4 of the form.

1. On **Page 1** of the form:
    - Set the **Type** field to match the station type (e.g. **9620**)
    - Set the **Name** field to a desired value (e.g. **Metaswitch**)
    - Set the **Security Code** (optional) to a desired value (e.g. **123456**)

```
change station 74567                                            Page   1 of   5
                                     STATION

Extension: 74567                         Lock Messages? n              BCC: 0
     Type: 9620                          Security Code: 123456          TN: 1
     Port: S00027                      Coverage Path 1:                COR: 1
     Name: Metaswitch                  Coverage Path 2:                COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 74567
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                              IP Video Softphone? n



                                             Customizable Labels? y
```

Figure 25: Avaya H.323 IP Phone – Page 1

2. On **Page 4** of the form:
    - Select an empty button assignment and enter **ec500.** Let the **timer** field default to **n**. This button will enable the EC500 capability on the phone (see **Section 4.1.10**).
    - Select an empty button assignment and enter **extnd-call**. This button will allow a user of this station to extend an active call to another phone number mapped to this extension (see **Section 4.1.10**).

```
change station 74567                                            Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                          Headset? n
       Jack:                                          Speaker? n
      Cable:                                         Mounting: d
      Floor:                                      Cord Length: 0
   Building:                                        Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            4: ec500      Timer? n
 2: call-appr                            5: extnd-call
 3: call-appr                            6:


    voice-mail Number:
```

Figure 26: Avaya H.323 IP Phone – Page 4

4.1.10 EC500 Provisioning

The Communication Manager EC500 feature was used to during compliance testing. EC500 provides calls for a Communication Manager station to be extended to a second destination endpoint. Typically this endpoint is a cell phone. When EC500 is enabled on the Communication Manager station (by pressing the **ec500** button), any inbound call to that station will generate a new outbound call from Communication Manager to the provisioned EC500 destination endpoint. Similarly, if there is an existing active call at the station, pressing the **extnd-call** button will generate a new outbound call from Communication Manager to the provisioned EC500 destination endpoint.

Note – Only the basic EC500 call redirection functionality was used in the reference configuration. EC500 supports significantly more features.

1. Use the command **change off-pbx-telephone station mapping x** where *x* is the Communication Manager station (e.g. **74567**).
   - **Station Extension** – This field will automatically populate.
   - **Application** – Enter **EC500**.
   - **Phone Number** – Enter the phone that will also be called (e.g. **7325555555**).
   - **Trunk Selection** – Enter **9** to route the call over trunk 9.

Note – **ARS** could also be entered depending on the configuration. This means ARS will be used to determine how Communication Manager will place the new outbound call.

   - **Config Set** – Enter **1**.
   - Use the default values for all other fields.

```
change off-pbx-telephone station-mapping 74567                 Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 74567            EC500        -     7325555555        9          1
```

Figure 27: EC500 Station Mapping

4.1.11 Save Avaya Aura™ Communication Manager Provisioning

Enter the ***save translation*** command to make the changes permanent.

5. Configure Avaya Aura™ Communication Manager as a Feature Server for SIP Trunking

This Section describes the steps for configuring Communication Manager as a Feature Server with the necessary signaling and media characteristics for the SIP trunk connection with the Metaswitch solution. The Feature Server provides advanced feature capabilities to Avaya 9600 Series SIP Telephones.

Note - The initial installation, configuration, and provisioning of the Avaya servers for Communication Manager, Avaya Media Gateways and their associated boards, as well as Avaya telephones, are presumed to have been previously completed and are not discussed in these Application Notes.

The Avaya CPE site utilized Communication Manager running on an Avaya S8800 server with an Avaya G430 Media Gateway as a Feature Server for SIP endpoints.

Note – The Communication Manager commands described in these Application Notes were administered using the System Access Terminal (SAT). SSH was used to connect to the SAT via the appropriate IP address, login and password.

5.1. Verify System Capacity and Features

The Communication Manager license file controls the customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

1. On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Metaswitch solution and any other SIP trunking applications.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 450    0
           Maximum Concurrently Registered IP Stations: 18000 0
             Maximum Administered Remote Office Trunks: 0      0
Maximum Concurrently Registered Remote Office Stations: 0      0
              Maximum Concurrently Registered IP eCons: 0      0
  Max Concur Registered Unauthenticated H.323 Stations: 0      0
                  Maximum Video Capable H.323 Stations: 0      0
                   Maximum Video Capable IP Softphones: 0      0
                       Maximum Administered SIP Trunks: 300    20
  Maximum Administered Ad-hoc Video Conferencing Ports: 0      0
   Maximum Number of DS1 Boards with Echo Cancellation: 0      0
                             Maximum TN2501 VAL Boards: 10     0
                     Maximum Media Gateway VAL Sources: 0      0
           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
```

Figure 28: System-Parameters Customer-Options Form – Page 2

Note – If any changes are made to the **system-parameters customer-options** form, you must log out of the SAT and log back in for the changes to take effect.

2. On **Page 3** of the **System-Parameters Customer-Options** form, verify that the **ARS** feature is enabled.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? n          Audible Message Waiting? n
        Access Security Gateway (ASG)? n              Authorization Codes? n
        Analog Trunk Incoming Call ID? n                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                         CAS Main? n
Answer Supervision by Call Classifier? n                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? n
         ARS/AAR Dialing without FAC? y                      DCS (Basic)? n
         ASAI Link Core Capabilities? y                DCS Call Coverage? n
         ASAI Link Plus Capabilities? y               DCS with Rerouting? n
      Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
             ATM WAN Spare Processor? n                          DS1 MSP? n
                               ATMS? n             DS1 Echo Cancellation? n
                 Attendant Vectoring? n



        (NOTE: You must logoff & login to effect the permission changes.)
```

Figure 29: System-Parameters Customer-Options Form – Page 3

3. On **Page 4** of the **System-Parameters Customer-Options** form, verify that the **IP Trunks** feature is enabled.

```
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? 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
```

Figure 30: System-Parameters Customer-Options Form – Page 4

5.1.1 Dial Plan

In the reference configuration, five digit extensions for analog, digital, and H.323 stations were provisioned with the format 7xxxx. Five digit extensions for SIP stations were provisioned with the format 531xx. Trunk Access Codes (TAC) are 3 digits in length and begin with 1. The Feature Access Code (FAC) to access ARS is one digit in length (the number “9”).

The dial plan is modified with the ***change dialplan analysis*** command.

1. On **Page 1** of the form:
    - Local extensions (analog, digital, and H.323 stations):
        1. In the **Dialed String** field enter **7**.
        2. In the **Total Length** field enter **5**.
        3. In the **Call Type** field enter **ext**.
    - Local extensions (SIP stations):
        1. In the **Dialed String** field enter **5**.
        2. In the **Total Length** field enter **5**.
        3. In the **Call Type** field enter **ext**.
    - TAC codes:
        1. In the **Dialed String** field enter **1**.
        2. In the **Total Length** field enter **3**.
        3. In the **Call Type** field enter **dac**.
    - FAC code – ARS access:
        1. In the **Dialed String** field enter **9**.
        2. In the **Total Length** field enter **1**.
        3. In the **Call Type** field enter **fac**.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     1            3    dac
     2            5    ext
     4            4    ext
     5            5    ext
     6            5    aar
     7            5    ext
     8            5    aar
     9            1    fac
```

Figure 31: Change Dialplan Analysis Form – Page 1

5.1.2 Uniform Dialplan

The uniform dial plan is modified with the ***change uniform-dialplan*** command.

1. On **Page 1** of the form, configure the following:
   - Local extensions (non-SIP stations):
     1. In the **Matching Pattern** field, enter **7**
     2. In the **Len** field, enter **5**
     3. In the **Del** field, enter **0**
     4. In the **Net** field, enter **aar**
     5. In the **Conv field**, enter **n**

```
change uniform-dialplan 0                                     Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                            Percent Full: 0

  Matching                   Insert              Node
  Pattern       Len Del      Digits      Net Conv Num
7               5   0                    aar  n
```

Figure 32: Change Uniform Dialplan Form – Page 1

5.1.3 Node Names

In the **IP Node Names** form, verify (or assign) the node names to be used in this configuration using the ***change node-names ip*** command.

- **SM01** and **10.64.20.31** are the **Name** and **IP Address** of Session Manager.
- **procr** and **10.64.20.25** are the **Name** and **IP Address** of the processor interface for Communication Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
SM01                10.64.20.31
default             0.0.0.0
procr               10.64.20.25
```

Figure 33: IP Node Names Form

5.1.4 IP-Network-Regions

One network region was defined in the reference configuration.

The SIP trunk ip-network-regions are defined in the SIP Signaling Group form with the Far-end Region parameter (see **Section 4.1.6**).

Network region assignments for ip-interfaces may be verified with the ***list ip-interface all*** command.

```
list ip-interface all

                                IP INTERFACES

                                                                       Net
ON Type   Slot  Code/Sfx      Node Name/       Mask  Gateway Node     Rgn  VLAN
                              IP-Address
-- ------ ----- --------      ---------------  ----  ---------------  ---  ----
 y PROCR                      10.64.20.25      /24   10.64.20.1       1
```

Figure 34: IP-Interface IP-Network-Region Assignments

The network-region for an ip-interface may be modified with the ***change ip-interface x*** command where **x** is the board location or **procr**.

```
change ip-interface procr                                      Page   1 of   1
                                  IP INTERFACES


                  Type: PROCR
                                                     Target socket load: 1700

      Enable Interface? y                         Allow H.323 Endpoints? y
                                                   Allow H.248 Gateways? y
        Network Region: 1                           Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /24
```

Figure 35: IP-Interface IP-Network-Region Assignment.

The **IP-Network-Region** form specifies the parameters used by the Communication Manager components and how components defined to different regions interact with each other. In the reference configuration, only one ip-network region was used; however, other combinations are possible.

Note – Avaya IP telephones inherit the ip-network-region of the procr (or C-LAN) they register to. As a result, if an IP phone registers to the procr in the reference configuration, that phone will become part of region 1. If an IP phone needs to be defined to a different region regardless of registration, this may be performed with the ***change ip-network-map*** command.

5.1.4.1 IP-Network-Region 1

Ip-network-region 1 is defined for Communication Manager components. The network regions are modified with the ***change ip-network-region x*** command, where x is the network region number.

1. On **Page 1** of the **IP Network Region** form:
   - Configure the **Authoritative Domain** field to *avaya.com*.
   - By default, **Intra-Region** and **Inter-Region IP-IP Direct Audio** (media shuffling) is set to **yes** to allow audio traffic to be sent directly between IP endpoints to reduce the use of media resources.
   - Set the **Codec Set** to **1** for the corresponding calls within the IP Network Region.
   - All other values are the default values.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

Figure 36: IP Network Region 1 – Page 1

5.1.5 IP Codec Sets

One codec set is defined in the reference configuration.

5.1.5.1 IP-Codec-Set 1

G.711MU is typically used within the same location and is often specified first. Other codecs could be specified as well depending on local requirements. Codec set 1 is associated with ip-network-region 1 (see **Section 5.1.4.1**).

The **IP-Codec-Set** form is modified with the ***change ip-codec x*** command, where ***x*** is the codec set number.

1. On **Page 1** of the form:
   - Configure the **Audio Codec** field **1** to **G.711MU.** During compliance testing G.729B and G.729AB were also tested.

```
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.711MU          n          2        20
 2:
```

Figure 37: IP Codec Set 1

2. On **Page 2** of the form:
   - Configure the **FAX** field to **t.38-standard**.
   - Configure the **Fax Redundancy** field to **0**.
   - Use the default settings for all other fields.

```
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
```

Figure 38: IP Codec Set 1 – Page 2

5.1.6 SIP Trunk Groups

SIP trunks are defined for internal calls as well as network calls to and from the PSTN via Metaswitch. A SIP trunk is created in Communication Manager by provisioning a SIP Trunk Group as well as a SIP Signaling Group.

Note – In the SIP trunk configurations below (and in the corresponding Session Manager configuration), TCP was selected as the transport protocol in the reference configuration. The TLS protocol could have been used instead.

5.1.6.1 Configure SIP Trunk for internal calls

1. Using the ***change signaling-group 1*** command, configure the Signaling Group as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** field to **tcp**.

Note – This specifies the transport method used between Communication Manager and Session Manager, not the transport method used to the Metaswitch network.

- Set the **IMS Enabled?** field to **y**.
- Specify the procr (or C-LAN) used for SIP signaling (node name **procr**) and the Session Manager (node name **SM01**) as the two ends of the signaling group in the **Near-end Node Name** and **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Section 5.1.3.**
- Specify **5060** in the **Near-End** and **Far-end Listen Port** fields.
- Enter the value **1** into the **Far-end Network Region** field. This value is for the **IP Network Region** defined in **Section 5.1.4.1**.
- Set the **Far-end Domain** field to *avaya.com*.
- The **Direct IP-IP Audio Connections** field should be set to **y** to allow RTP voice paths to be established directly between IP telephones and the Metaswitch network.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF tones using RFC 2833.
- The default values for the other fields may be used.

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

 Group Number: 1              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? y





   Near-end Node Name: procr                Far-end Node Name: SM01
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 1
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? y                    Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```

Figure 39: Internal calls SIP Trunk - Signaling Group 1

2. Using the ***change trunk-group 1*** command, change the Trunk Group as follows:
   a. On **Page 1** of the Trunk Group form:
      - Set the **Group Type** field to **sip**.
      - Choose a descriptive **Group Name.**
      - Specify an available trunk access code (**TAC**) (e.g. **101**).
      - Set the **Service Type** field to **tie.**
      - Enter **1** as the **Signaling Group** number.
      - Specify the **Number of Members** used by this SIP trunk group (e.g. **10**).

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

Group Number: 1                    Group Type: sip         CDR Reports: y
  Group Name: to SM (avaya.com)           COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                      Signaling Group: 1
                                                    Number of Members: 10
```

Figure 40: Internal calls Trunk Group 1 – Page 1

b. On **Page 3** of the **Trunk Group** form:
   - Set the **Numbering Format** field to **private.** This field specifies the format of the calling party number sent to the far-end.

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



                     Numbering Format: private
                                                  UUI Treatment: service-provider

                                                   Replace Restricted Numbers? n
                                                  Replace Unavailable Numbers? n







 Show ANSWERED BY on Display? y
```

Figure 41: Internal calls Trunk Group 1 – Page 3

5.1.6.2 Configure SIP Trunk for off network calls

The SIP trunk for off network calls is configured in the same fashion as the internal call SIP Trunk except that the Far-end Domain is set to blank.

1. Using the ***change signaling-group 2*** command, configure the Signaling Group as follows:

   - Set the **Group Type** field to **sip**.
   - Set the **Transport Method** field to **tcp**.

Note – This specifies the transport method used between Communication Manager and Session Manager, not the transport method used to the Metaswitch network.

   - Set the **IMS Enabled?** field to **y**.
   - Specify the procr (or C-LAN) used for SIP signaling (node name **procr**) and the Session Manager (node name **SM01**) as the two ends of the signaling group in the **Near-end Node Name** and **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Section 5.1.3.**
   - Specify **5060** in the **Near-End** and **Far-end Listen Port** fields.
   - Enter the value **1** into the **Far-end Network Region** field. This value is for the **IP Network Region** defined in **Section 5.1.4.1**.
   - Leave the **Far-end Domain** field blank. This permits inbound calls from any foreign domain (e.g. the Metaswitch network).
   - The **Direct IP-IP Audio Connections** field should be set to **y** to allow RTP voice paths to be established directly between IP telephones and the Metaswitch network.

- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF tones using RFC 2833.
- The default values for the other fields may be used.

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

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





   Near-end Node Name: procr                  Far-end Node Name: SM01
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1
Far-end Domain:

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

Figure 42: Off network calls SIP Trunk - Signaling Group 2

2. Using the ***change trunk-group 2*** command, change the Trunk Group as follows:
   a. On **Page 1** of the Trunk Group form:
      - Set the **Group Type** field to **sip**.
      - Choose a descriptive **Group Name.**
      - Specify an available trunk access code (**TAC**) (e.g **102**).
      - Set the **Service Type** field to **tie.**
      - Enter **2** as the **Signaling Group** number.
      - Specify the **Number of Members** used by this SIP trunk group (e.g. **10**).

```
change trunk-group 2                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 2                   Group Type: sip          CDR Reports: y
  Group Name: to SM (blank)              COR: 1        TN: 1        TAC: 102
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                       Signaling Group: 2
                                                     Number of Members: 10
```

Figure 43: Off network calls Trunk Group 2 – Page 1

b. On **Page 3** of the **Trunk Group** form:
   - Set the **Numbering Format** field to **private.** This field specifies the format of the calling party number sent to the far-end.

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




                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n








 Show ANSWERED BY on Display? y
```

Figure 44: Off network calls Trunk Group 2 – Page 3

5.1.7 Private Unknown Numbering – Basic Configuration

In the reference configuration, Communication Manager uses a 5 digit dialing plan with extensions 531xx for SIP stations. The **Private-Unknown-Numbering** form allows Communication Manager to use these extensions as the calling party number for outbound calls. Otherwise, *Anonymous* is displayed as the calling number. Each extension string is defined for the trunk group(s) that the extensions may use. These trunks may be defined individually or in contiguous ranges.

Use the ***change private-unknown-numbering x*** command, where *x* is the leading digit of the dial plan extensions (e.g. **5**).

- Set the **Ext Len** field to **5**.
- Set the **Ext Code** field to **5**.
- Set the **Trk Grp(s)** field to **1.**
- Set the **Total CPN Len** field to **5**

All provisioned private-unknown-numbering entries can be displayed by entering the command ***display private-unknown-numbering 0*** as show below.

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

Ext Ext              Trk         Private          Total
Len Code             Grp(s)      Prefix           Len
 4  4                1                            4     Total Administered: 3
 4  4                2                            4       Maximum Entries: 540
 5  5                1                            5
```

Figure 45: Private-unknown-numbering Form – Basic Configuration

5.1.8 Call routing

5.1.8.1 Internal Calls

The following sections describe the Communication Manager provisioning required for dialing internal non-SIP extensions.

Note –Metaswitch only assigned one DID number that had access to the PSTN. The configuration required for inbound and outbound PSTN calls to and from an H.323 station on Communication Manager was shown in **Section 4.1.8**. Although, not shown here, similar administration can be done for a SIP station on Communication Manager as a Feature Server.

5.1.8.1.1 AAR

The Automatic Alternate feature is used to route calls via a SIP trunk, configured in **Section 5.1.6.1**, to the Session Manager, which in turn completes the calls to local stations. AAR matches on the called number and sends the call to a specified route pattern.

1. Use the ***change aar analysis*** command to configure the route pattern selection rule based upon the number dialed. In the reference configuration, calls are placed to non-SIP stations with 5 digit extensions (7xxxx).

```
change aar analysis 7                                              Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

          Dialed            Total      Route     Call   Node  ANI
          String          Min  Max   Pattern    Type   Num   Reqd
    7                     5    5     1          aar          n
```

Figure 46: AAR Analysis Form

5.1.8.1.2 Route Patterns

The reference configuration used route-pattern 1 for internal calls.

Note - Route patterns may also be used to add or delete digits prior to sending them out the specified trunk(s). This feature was not used in the reference configuration.

1. Use the **change route-pattern** command to define the SIP trunk group included in the route pattern that AAR selects.
    - Set the **Grp No** field to ***1***.
    - Set the **FRL** field to ***0***.
    - Let all other parameters default.

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

Figure 47: Route Pattern 1 – Internal Calls

5.1.9 Save Avaya Aura™ Communication Manager Provisioning

Enter the ***save translation*** command to make the changes permanent.

6. Avaya Aura™ Session Manager Provisioning

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager management server. All SIP call provisioning for Session Manager is performed via the System Manager web interface and is then downloaded into Session Manager.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

6.1. Network Interfaces

Session Manager is comprised of two main components, the server itself and the SM-100 card.

The Session Manager SM-100 card has four network interface ports, with one being the connection to the SIP VoIP network. This interface is used for all inbound and outbound SIP signaling and must have network connectivity to all provisioned SIP Entities.

The Session Manager server has two network interface ports with one being the port used for management/provisioning of Session Manager. This port must have network connectivity to System Manager.

Note –In the reference configuration the SM-100 interface and the Session Manager server interface were both connected to the same IP network. If desired, the System Manager/Session Manager management connection may use a different network than the SM-100 connection.

6.2. Logging into System Manager

The following provisioning is performed via System Manager to enable SIP trunking:

- **Network Routing Policy**
  - **SIP Domains** - Define domains that may send calls to Session Manager.
  - **Locations** – Logical/physical areas that may be occupied by SIP Entities
  - **SIP Entities** – Typically devices corresponding to the SIP telephony systems including Session Manager itself, however they may includes other devices such as SBCs.
  - **Entity Links** – Connection information which define the SIP trunk parameters used by Session Manager when routing calls to/from other SIP Entities.
  - **Dial Patterns** – Matching digit patterns which govern to which SIP Entity a call is routed.
  - **Routing Policies** - Policies that determine which control call routing between the SIP Entities based on applicable Dial Patterns.
  - **Time Ranges** – Specified windows during which SIP call processing is permitted for a particular Routing Policies.

- **Avaya Aura™ Session Manager** – Information corresponding to the Session Manager Server to be managed by System Manager.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL ***https://<ip-address>/SMGR***, where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials.

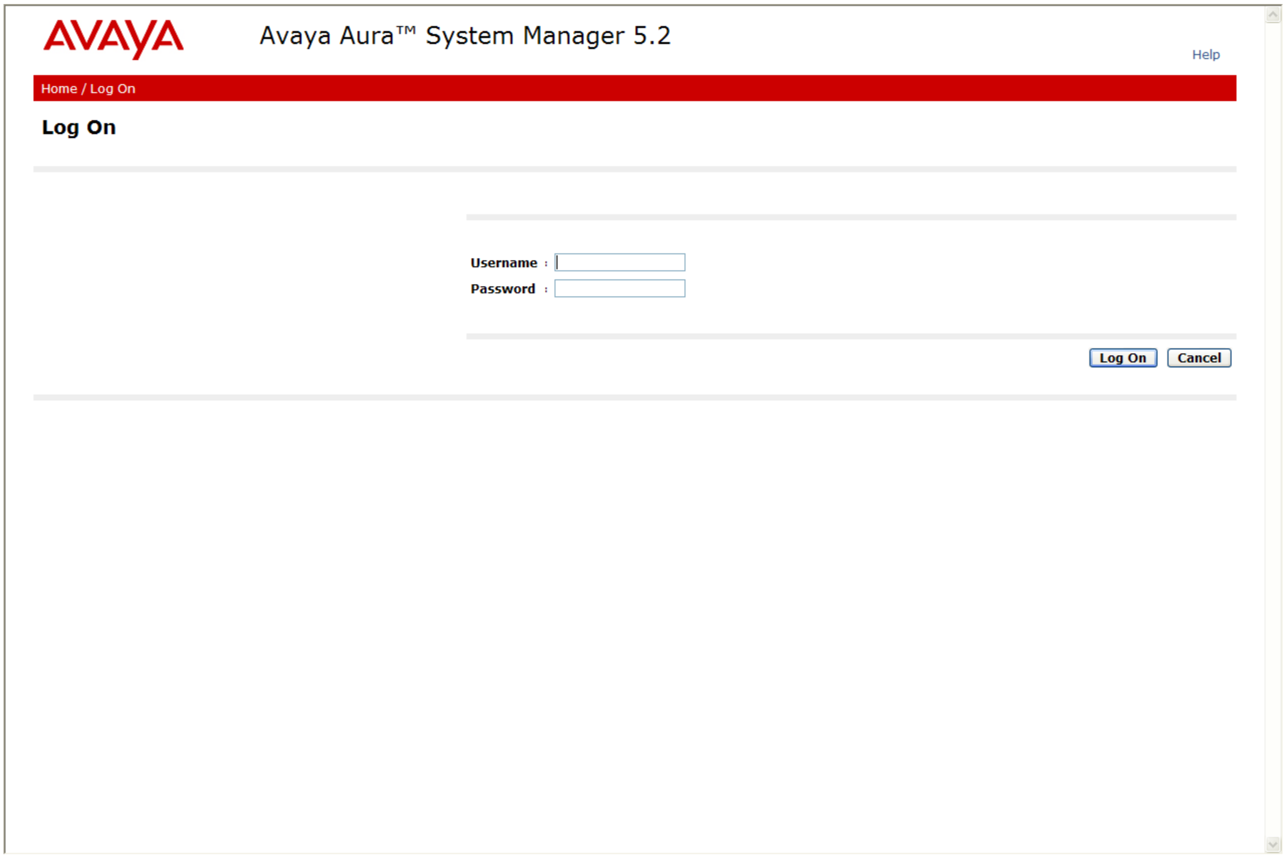

Figure 48: System Manager GUI Log On Screen

6.3. Network Routing Policy

After logging in, expand the **Network Routing Policy Link** on the left side as shown.

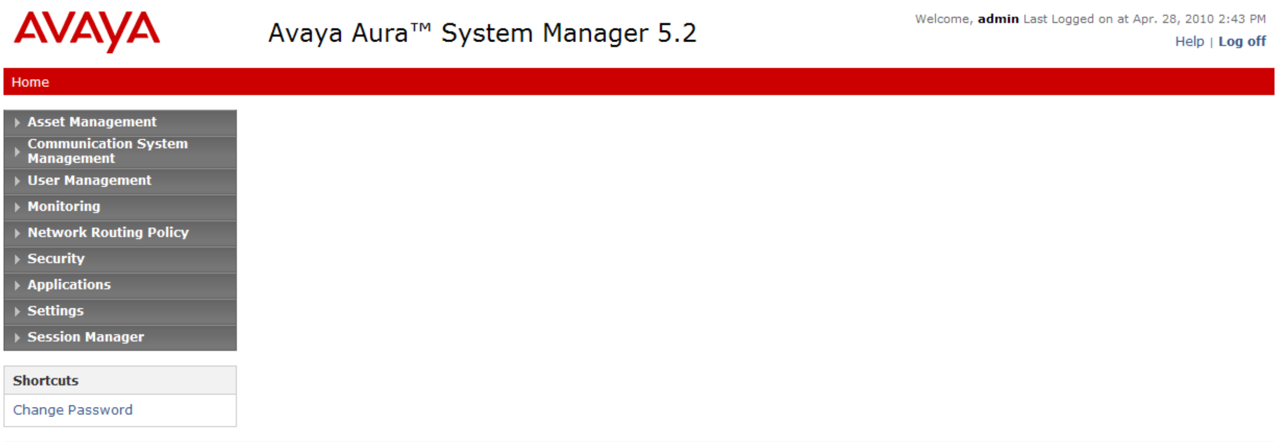

Figure 49: Network Routing Policy Menu

6.3.1 SIP Domains

In the reference configuration, one SIP domain was used. The Avaya CPE location domain is *avaya.com*.

1. Select **SIP Domains** from the menu.
2. Select **New**.
3. Enter the SIP Domain (*avaya.com*) in the **Name** field.
4. Enter a description in the **Notes** field if desired.
5. Click on the **Commit** button.

Note – On most of the following forms, to edit or delete an entry, click the box next to the item to select it. This will make the **Edit** and **Delete** buttons available.

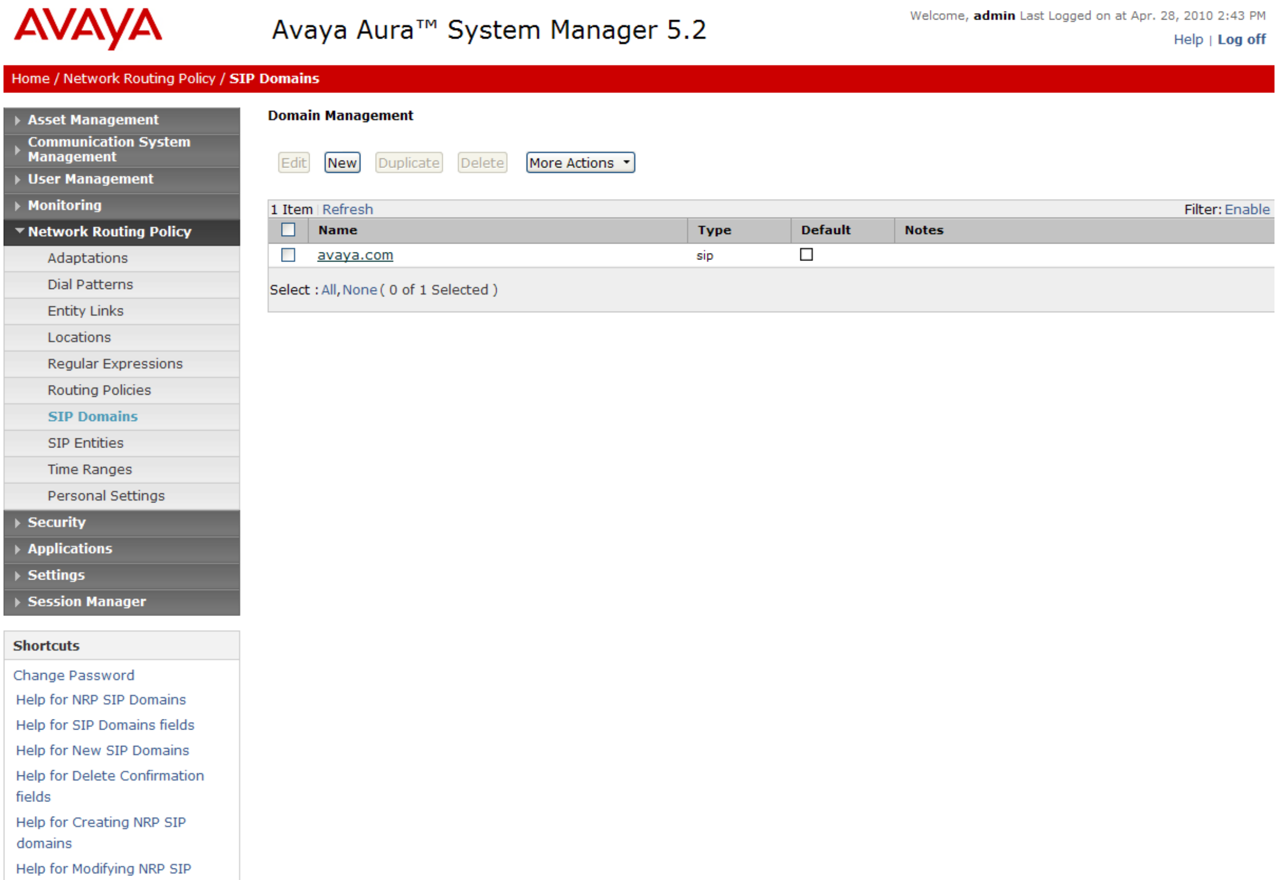

Figure 50: SIP Domain Menu

6.3.2 Adaptations

Session Manager provides for specialized code modules to process specific call processing requirements of various vendors and/or services. These modules are called adaptations.

6.3.2.1 DigitConversionAdapter

This adaptation allows Session Manager to convert inbound and/or outbound digits in SIP Request-URI, History-Info header, P-Asserted-Identity header, and Notify messages, based on the SIP Entities to which this adaptation is defined. This functionality is similar to the Communication Manager public-unknown-numbering and incoming-call-handling-treatment capabilities.

Session Manager will perform digit conversion based on whether the digits are being received (incoming) or sent (outgoing) by Session Manager with another SIP Entity. For example, on a call from Communication Manager to Metaswitch, the call leg from Communication Manager to Session Manager is incoming, while the call leg from Session Manager to the Acme Packet is outgoing.

1. Select **Adaptations** from the menu.
2. Select **New**.
   - Enter a descriptive name (e.g. **Metaswitch**).
   - Specify **DigitConversionAdapter** in the Adaptation Module field.
   - Set **Module parameter** to the domain of Metaswitch. The reference configuration required that domain contained in the Request URI to be replaced with the Metaswitch domain before being sent out to Metaswitch via the Acme Packet. The domain replacement was performed by specifying the Metaswitch domain here.
   - Leave the Egress **URI Parameters** field blank (this is for adding additional parameters such as user=phone).
   - Enter a description in the **Notes** field if desired.

For outgoing calls from Communication Manager to the PSTN, extension 74565 is converted to the Metaswitch DID 5102174567 via the public-unknown-numbering form on Communication Manager (see **Section 4.1.7**).

For incoming calls, the Metaswitch DID 5102174567 is converted to Communication Manager extension 74567 via this adaptation.

3. Click the **Add** button and enter:
   - **Matching Pattern** – The digit string to match → **5102174567**
   - **Min** – The minimum number of digits → **10**
   - **Max** – The maximum number of digits → **10**
   - **Delete Digits** – The number of digits to delete → **5**
   - **Insert Digits** – The digit to be inserted → **0**
   - **Address to Modify** - origination/destination/both – Associated headers to be monitored for matching digits. → **Both**
   - **Notes** - Enter a description in the **Notes** field if desired.
4. When completed, the Adaptation Details window for DigitConversionAdapter will look like **Figure 51**.
5. Click on the **Commit** button.

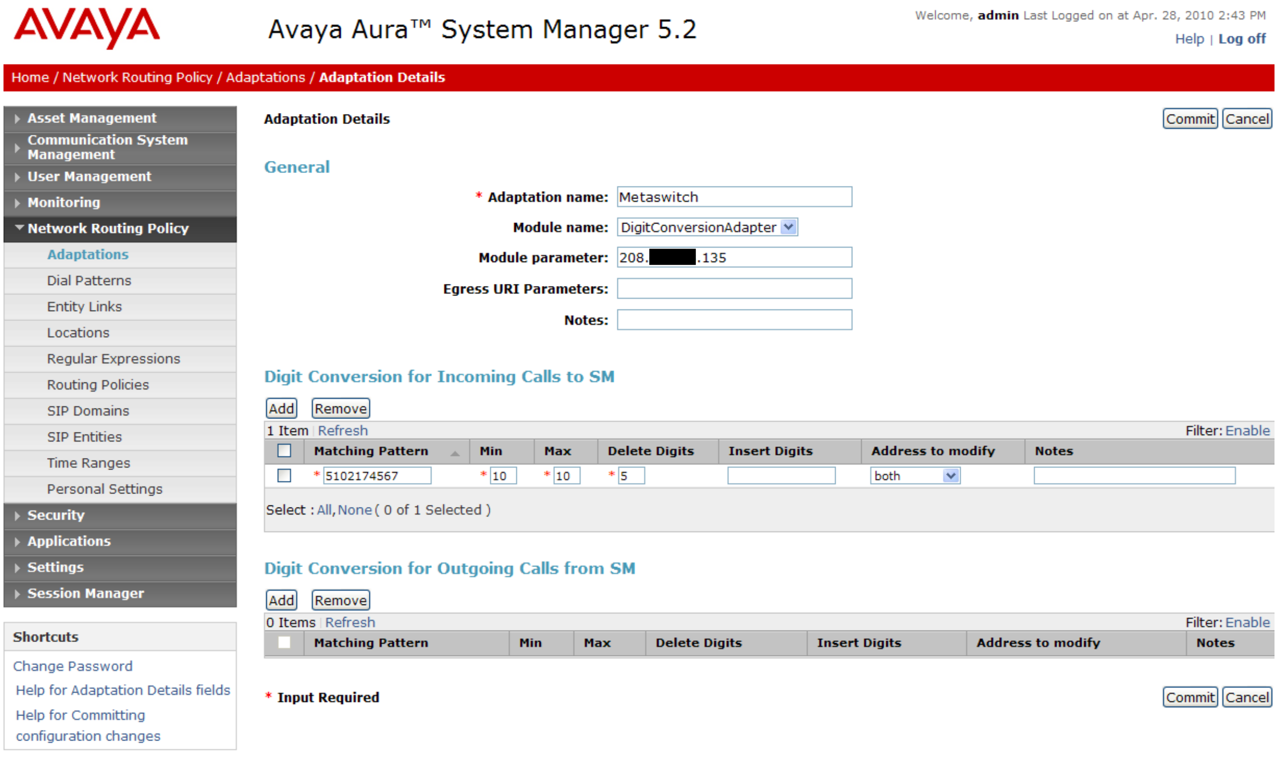

Figure 51: DigitConversionAdapter Adaptation

6.3.3 Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required. In the reference configuration, only the Avaya CPE site was defined as a Location.

To add a Location, select **Locations** in the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown below will open.

1. Enter a descriptive Location name in the Name field (e.g. **10.64.20/21.0**).
2. Enter a description in the **Notes** field if desired.
3. Under the **Location Pattern** heading, click on **Add**.
4. Enter the IP address information for the Location (e.g. **10.64.20.***)
5. Enter a description in the **Notes** field if desired.
6. Repeat steps 3 through 5 if the Location has multiple IP segments.
7. Modify the remaining values on the form, if necessary; otherwise, use all the default values.
8. Click on the **Commit** button.
9. Repeat all the steps for each new Location.

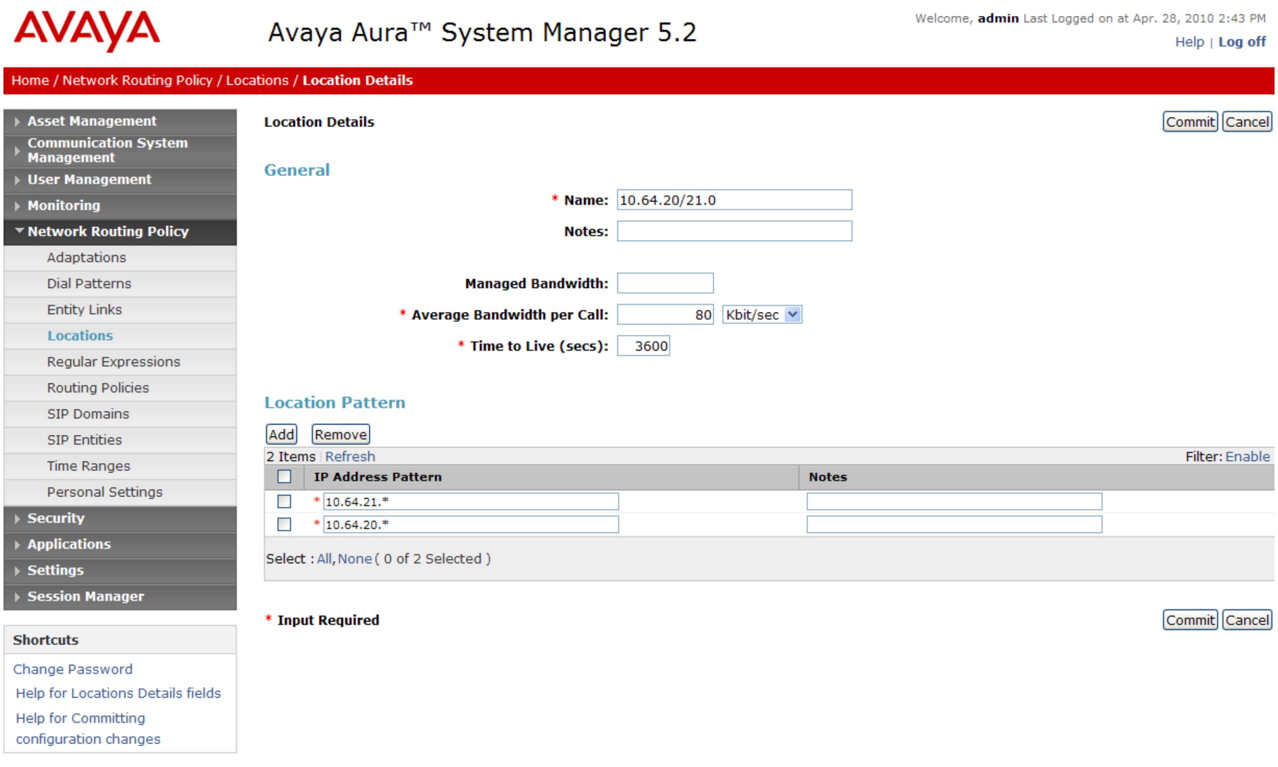

Figure 52: Locations Menu

6.3.4 SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. In the reference configuration the SIP Entities are provisioned for:

- Communication Manager
- Communication Manager (Feature Server)
- Acme Packet
- Session Manager itself.

To add a SIP Entity, select **SIP Entities** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown below is displayed.

1. **General** Section
   a. Enter a descriptive Location name in the **Name** field.
   b. Enter the IP address for the SIP Entity.
   c. From the **Type** drop down menu select a type that best matches the SIP Entity (e.g. **CM**).
   d. Enter a description in the **Notes** field if desired.
   e. From the **Adaptations** drop down menu, select the adaptation required for this Entity (see **Section 6.3.2**).

        - For the Acme Packet Entity, the **Metaswitch** adaptation is selected. This function is applied to convert the Metaswitch DID to a Communication Manager extension. It also converts the outbound call (Session Manager to Acme) request URI domain from the Avaya CPE domain, used by Communication Manager, to the Metaswitch domain.
    f. From the Locations drop down menu, select **10.64.20/21.0**.
    g. Select the appropriate time zone.
    h. Accept the other default values.
2. **SIP Link Monitoring** section
    a. Select the desired option.
3. **Port** section
    a. When defining a SIP Entity for Session Manager itself and **SM** is selected from the **Type** drop down menu, an additional section called **Ports** will appear. Click **Add**, then edit the fields in the resulting new row:
        - Enter the **Port** number on which the system listens for SIP requests.
        - Select the transport **Protocol** to be used.
        - Select the SIP Domain configured in **Section 6.3.1** for the **Default Domain**.
    b. Repeat step 3 for each Port to be configured.
4. Click on **Commit**.
5. Repeat these steps for each SIP Entity.

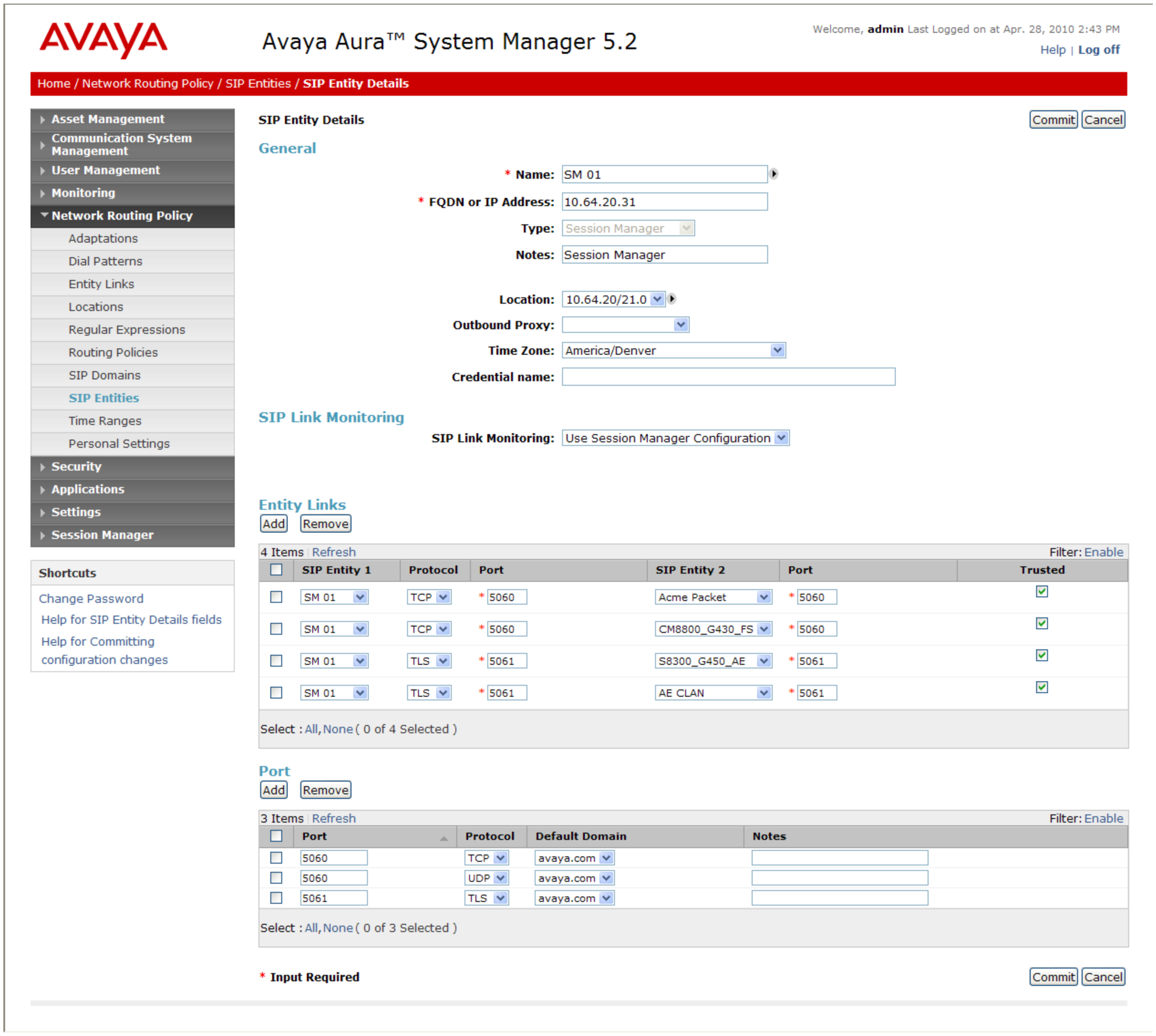

Figure 53: Session Manager SIP Entity Details

The following SIP Entity values were specified in the reference configuration.

Name	IP Address	Type	Adaptation	Location	Port	Protocol	Default Domain
S8300_G450_AE	10.64.21.41	CM	-	10.64.20/21.0	-	-	-
CM8800_G430_FS	10.64.20.25	CM	-	10.64.20/21.0	-	-	-
Acme Packet	10.64.20.106	Other	Metaswitch	10.64.20/21.0	-	-	-
SM 01	10.64.20.31	SM	-	10.64.20/21.0	5060 5060 5061	TCP UDP TLS	avaya.com

Table 2: SIP Entities Provisioning

6.3.5 Entity Links

Entity Links defined the connections between the SIP Entities and Session Manager. In the reference configuration, Entity Links are defined between Session Manager and:

- The Communication Manager
- The Communication Manager (Feature Server)
- Acme Packet

To add an Entity Link, select **Entity Links** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown below is displayed.

1. Enter a descriptive name in the **Name** field.
2. In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 6.3.4** (e.g. **SM 01**).
3. In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
4. In the **SIP Entity 2** drop down menu, select the one of the three entities in the bullet list above (which were created in **Section 6.3.4**).
5. In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
6. Check the **Trusted** box.
7. In the **Protocol** drop down menu, select the protocol to be used.
8. Enter a description in the **Notes** field if desired (not shown).
9. Click on the **Commit** button.
10. Repeat steps 1 – 9 for each Entity Link.

The following Entity Links were specified in the reference configuration.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
SM 01_S8300_G450_AE_5061_TLS	SM 01	TLS	5061	S8300_G450_AE	5061
SM 01_CM8800_FS_5060_TCP	SM 01	TCP	5060	CM8800_G430_FS	5060
SM 01_Acme_Packet_5060_TCP	SM 01	TCP	5060	Acme Packet	5060

Table 3: Entity Link Provisioning

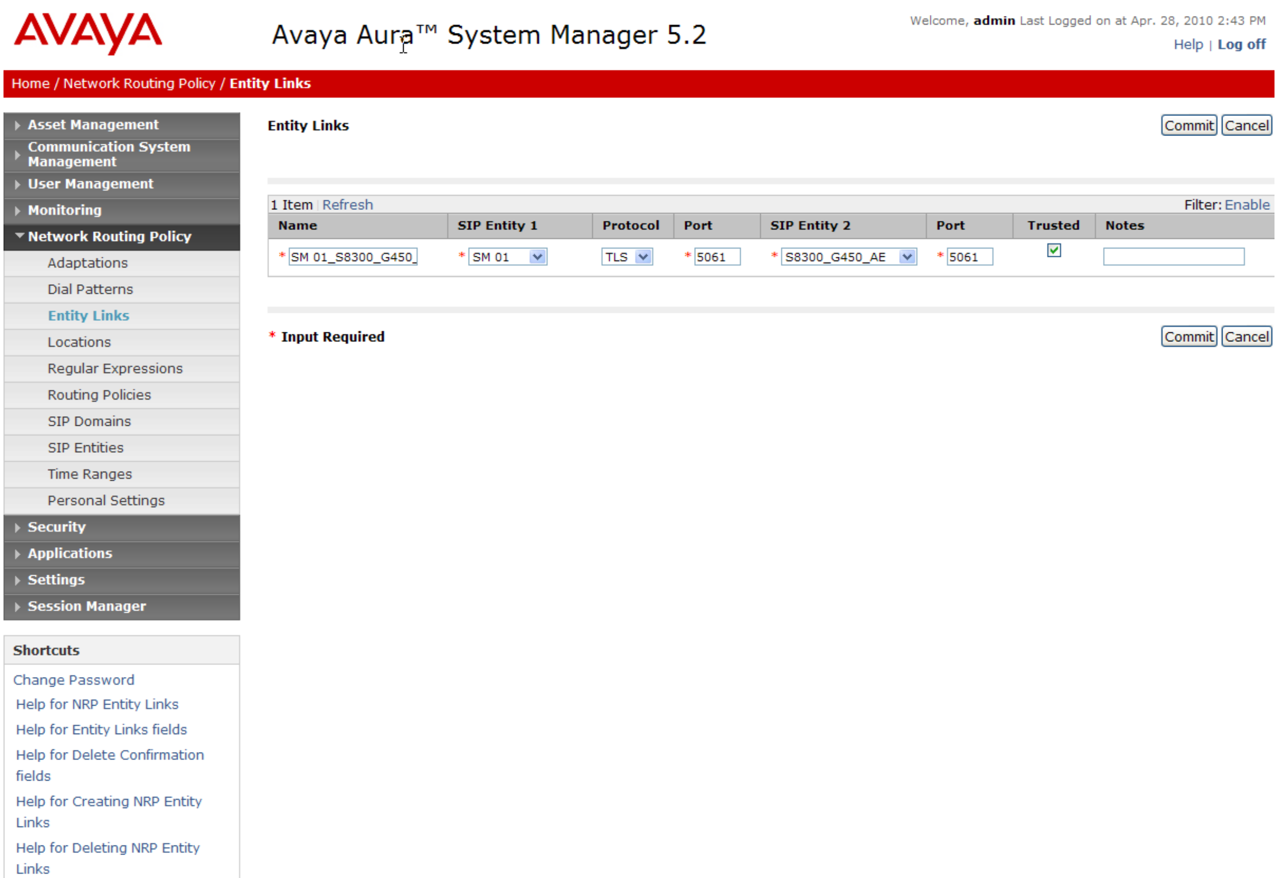

Figure 54: Entity Link – Communication Manager

6.3.6 Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 6.3.7**). In the reference configuration, no restrictions were used.

To add a Time Range, select **Time Ranges** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown below is displayed.

1. Enter a descriptive Location name in the **Name** field (e.g. **Anytime**).
2. Check each day of the week.
3. In the **Start Time** field, enter **00:00**.
4. In the **End Time** field, enter **23:59**.
5. Enter a description in the **Notes** field if desired.
6. Click the **Commit** button.

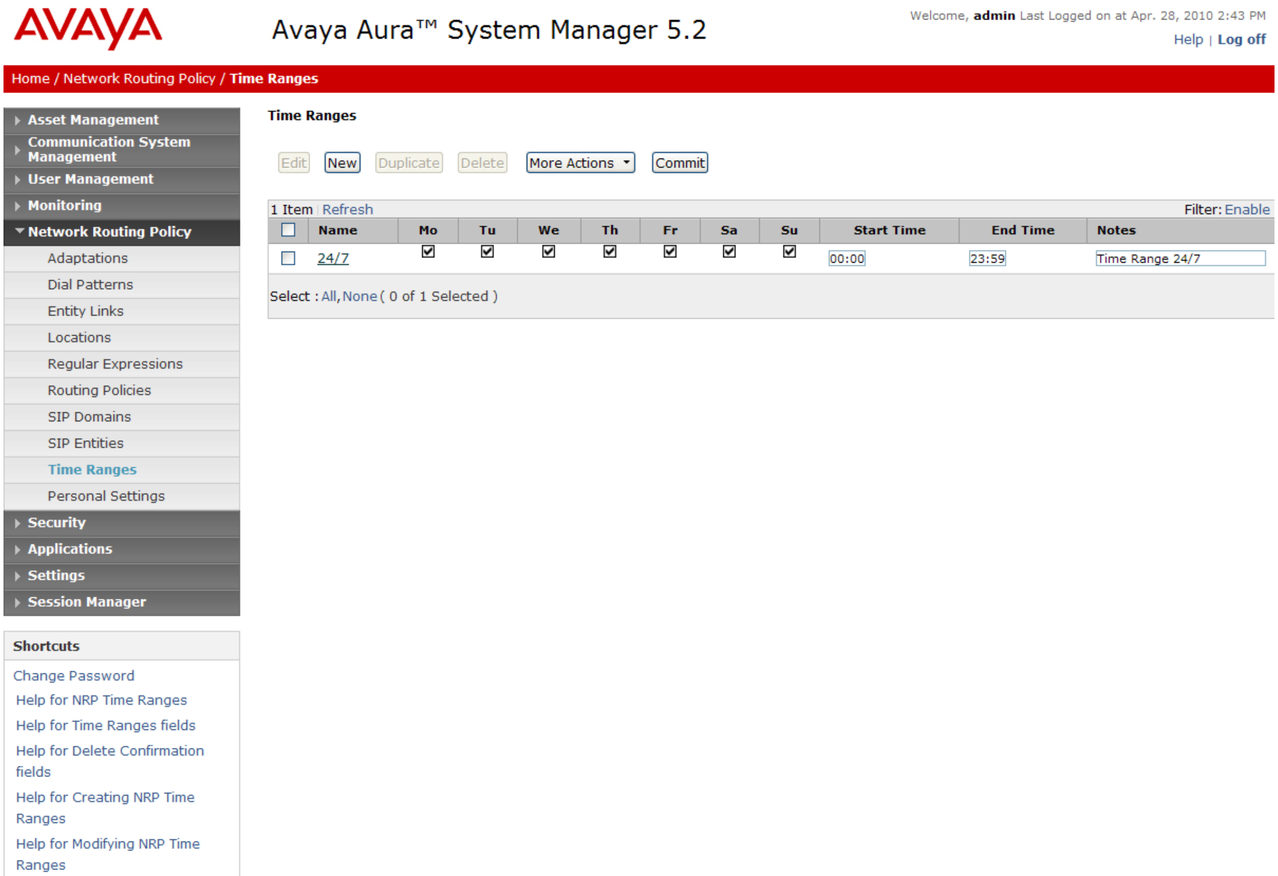

Figure 55: Time Ranges

6.3.7 Routing Policies

Routing Policies associate destination SIP Entities (**Section 6.3.4**) with Time of Day admission control parameters (**Section 6.3.6**) and Dial Patterns (**Section 6.3.8**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager
- Outbound calls to the Metaswitch network

Note – Since the SIP endpoints in the reference configuration register with Session Manager, Session Manager knows how to route calls to those extensions and it is not necessary to create a routing policy for Communication Manager (Feature Server).

Note – In the reference configuration the **Regular Expressions** parameters was not used.

Name	SIP Entity as Destination	Time Of Day	Dial Pattern(s)	Notes
to S8300_G450_AE	S8300_G450_AE	Anytime	7xxxx	Any call to a 5 digit extension beginning with 7 will be routed to Communication Manager
to Acme_Packet	Acme Packet	Anytime	303xxxxxxx 732xxxxxxx	Any call to a 10 digit number beginning with 303 or 732 will be routed to Acme Packet

Table 4: Routing Policy Provisioning

To add a Routing Policy, select **Routing Policies** on the left **Network Routing Policy** menu and click on the **New** button on the right. The Routing Policy Details window will open.

1. **General** section
   a. Enter a descriptive name in the **Name** field.
   b. Enter a description in the **Notes** field if desired.
2. **SIP Entity as Destination** section
   a. Click the **Select** button.
   b. Select the SIP Entity that will be the destination for this call.
   c. Click the **Select** button and return to the Routing Policy Details form.
3. **Time of Day** section
   a. Leave default values.

   Note – Multiple time ranges may be selected and a Ranking value applied (0 is the highest).
4. **Dial Pattern** section

   Note – Step 4 may be skipped. Dial Patterns will be mapped to Routing Policies in the **Section 6.3.8**.

   a. Click the **Add** button and select the **Dial Pattern** for this Routing Policy.
   b. Click on **Select** and return to the Routing Policy Details form.

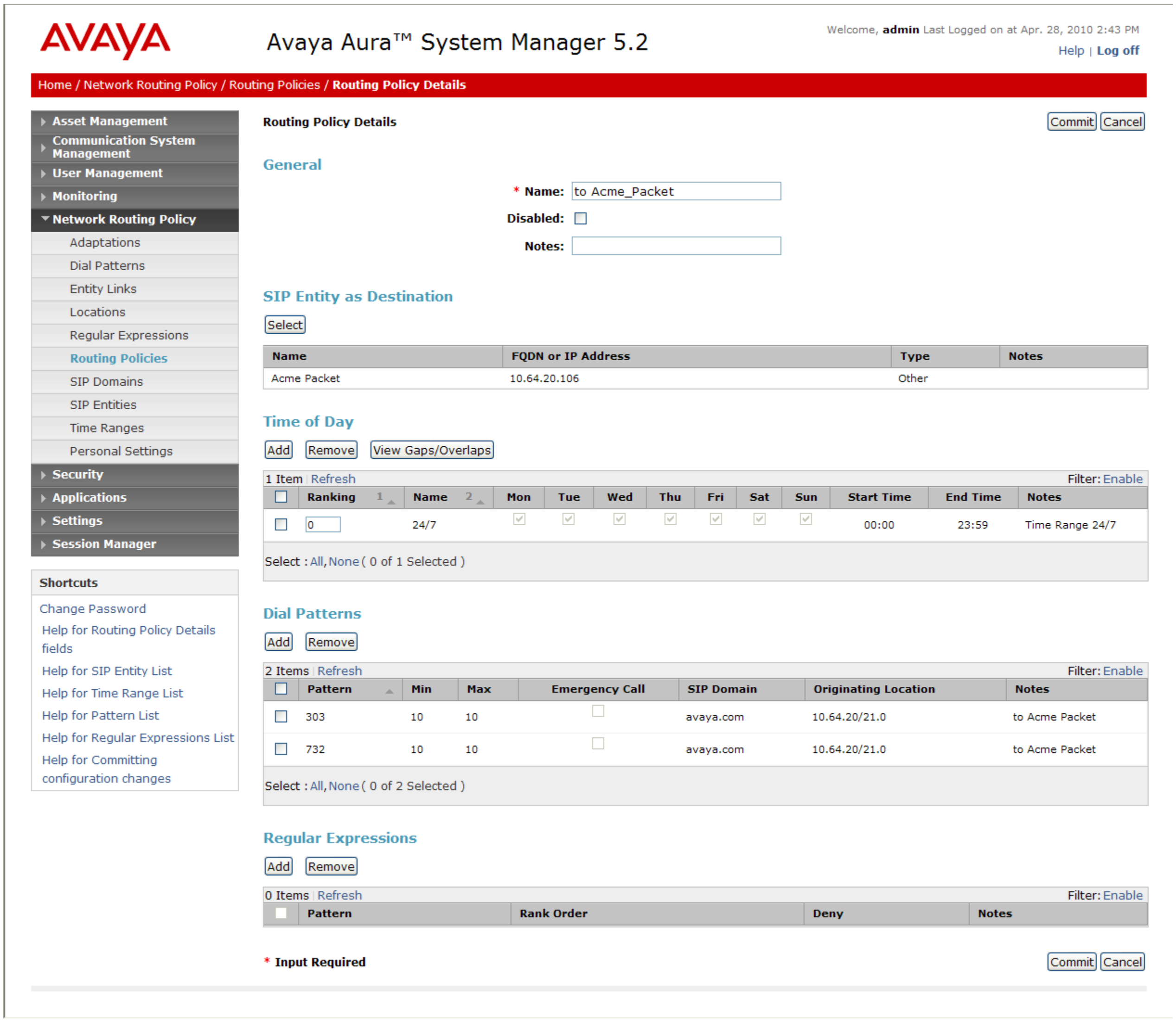

Figure 56: Routing Policy Details

5. Click the **Commit** button.
6. Repeat steps 1 through 5 for each Routing Policy.
7. Click the **Commit** button.

6.3.8 Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined.

Note – The Dial Pattern digit string with the most complete match will be selected. For example if the 5 digit string 700 is defined first in the list, and the 5 digit string 70001 is defined last, a call for 70001 will match on the 70001 string.

The following Dial Patterns were provisioned in the reference configuration.

Pattern	Min	Max	SIP Domain	Originating Location	Routing Policy Name
7	5	5	avaya.com	ALL	to S8300_G450_AE
303	10	10	avaya.com	10.64.20/21.0	to Acme_Packet
732	10	10	avaya.com	10.64.20/21.0	to Acme_Packet

Table 5: Routing Policy Provisioning

Note – The Metaswitch adaptation is provisioned on the Acme Packet SIP Entity. This means that the conversion from the Metaswitch DID to the Communication Manager extension is performed ***before*** the dial pattern match for inbound calls.

To add a Dial Pattern, select **Dial Patterns** on the left **Network Routing Policy** menu and click on the **New** button on the right. The screen shown below is displayed. In this example, a Request URI to a 10 digit number beginning with *732xxxxxxx*, and sent by *avaya.com*, is defined (this would be an outbound call from Communication Manager to Session Manager, destined for Metaswitch).

1. **General** section
    a. Enter a unique pattern in the **Pattern** field (e.g. **732**).
    b. In the **Min** column enter the minimum number of digits (e.g. **10**).
    c. In the **Max** column enter the maximum number of digits (e.g. **10**).
    d. In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
    e. Enter a description in the **Notes** field if desired.
2. **Originating Locations and Routing Policies** Section
    a. Click on the **Add** button and a window will open (not shown).
    b. Click on the boxes for the appropriate Originating Locations (see **Section 6.3.3**), and Routing Policies (see **Section 6.3.7**) that pertain to this Dial Pattern.
        i. Location **10.64.20/21.0**
        ii. Routing Policies **to Acme_Packet**.
    c. Click on the **Select** button and return to the Dial Pattern window.
3. Click the **Commit** button
4. Repeat steps 1 through 3 for the remaining Dial Patterns.

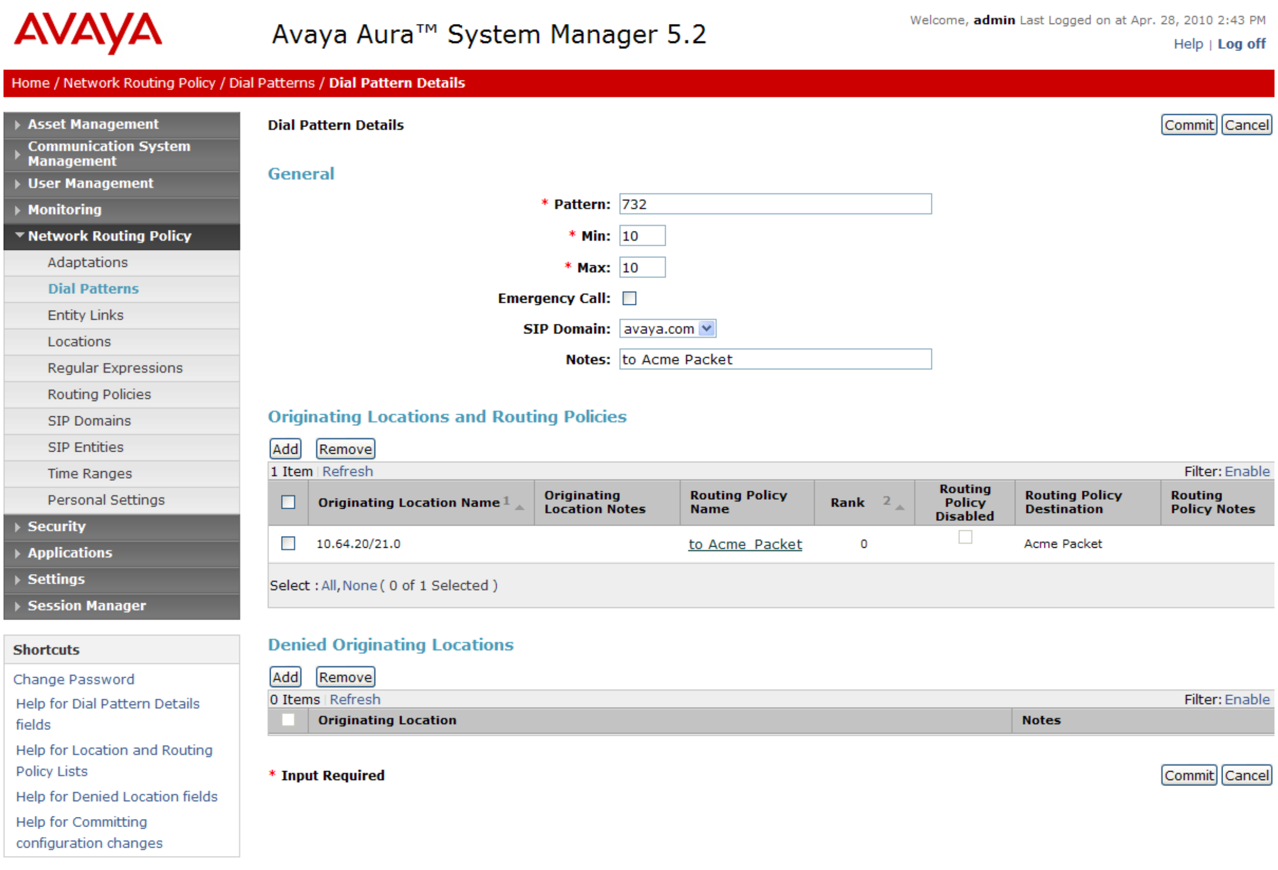

Figure 57: Dial Pattern Details

6.4. Avaya Aura™ Session Manager

To complete the Session Manager configuration, add a Session Manager instance. To add a Session Manager, select **Session Manager** on the left **Network Routing Policy** menu and click on the **New** button. The screen shown below is displayed.

1. **General** section
   a. Enter a name in the **SIP Entity Name** field (e.g. **SM 01**).
   b. Enter an optional description in the **Description** field.
   c. In the **Management Access Point Host Name/IP** field enter the IP address of the management interface of the Session Manager server. (e.g. **10.64.20.30**).
2. **Security Module** section

Note – The SIP Entity IP address is automatically populated with the IP address defined for this SIP Entity (**SM 01**) in **Section 6.3.4**.

   a. Enter the **Network Mask** (e.g. **255.255.255.0**)
   b. Enter the **Default Gateway** (e.g. **10.64.20.1**)
   c. In the **Speed & Duplex** drop down menu verify **Auto** is selected (default).
3. Use all other default parameters.

4. Click the **Save** button and the completed form will be displayed.

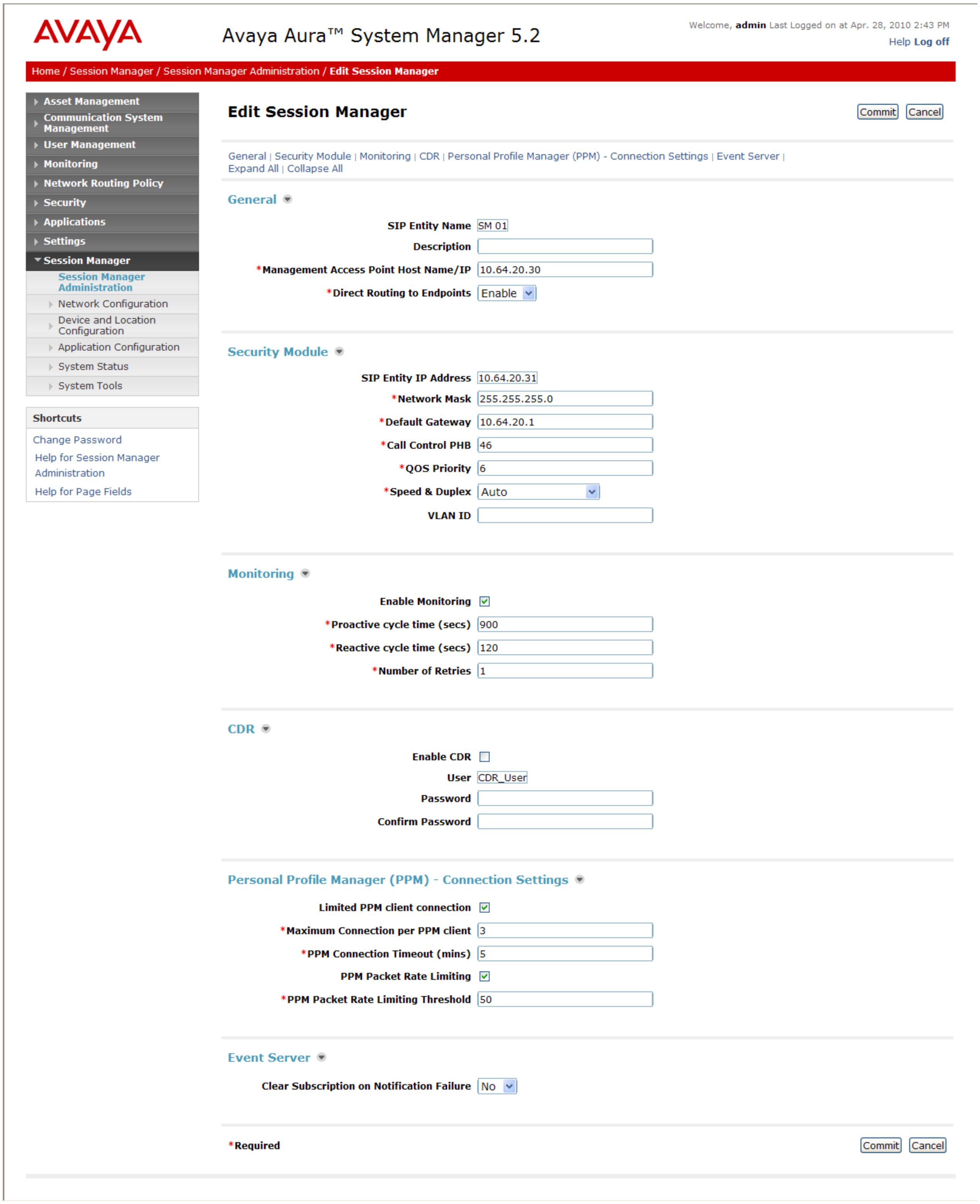

Figure 58: Completed Session Manager Form

6.5. Feature Server

In order for Communication Manager to provide configuration and Feature Server support to the Avaya 9600 Series SIP Telephones when they register to Session Manager, Communication Manager must be added as an application for Session Manager.

1. Select **Applications → Entities** on the left. Click on **New** (not shown). Select "CM" **Type** and in the displayed page, enter the following fields. Use defaults for the remaining fields:
    a. Enter a descriptive name in the **Name** field.
    b. Select **CM** for **Type**.
    c. In the **Node** field, Select IP address for Communication Manager SAT access.

    Under the *Attributes* section, enter the following fields, and use defaults for the remaining fields:

    d. Enter the login used for SAT access in the **Login** field.
    e. Enter the password used for SAT access in the **Password** field.
    f. Enter the password used for SAT access in the **Confirm Password** field.
2. Click the **Commit** button.

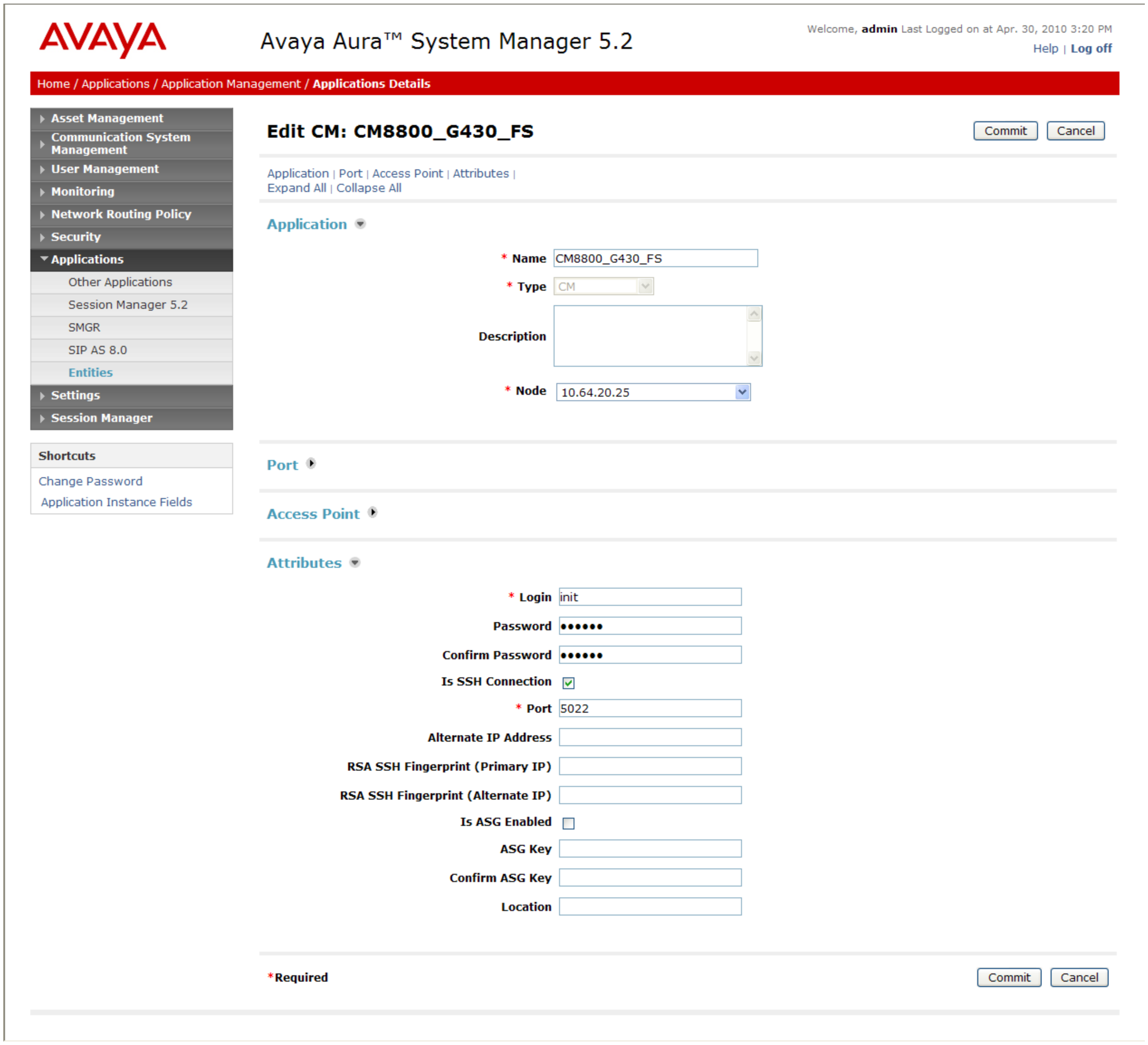

Figure 59: Application Entities Form

3. Select **Session Manager → Application Configuration → Applications** on the left. Click on **New** (not shown). Enter the following fields, and use defaults for the remaining fields:
    a. Enter a descriptive name in the **Name** field.
    b. Select the Communication Manager SIP Entity (see **Section 6.3.4**) for **SIP Entity**.
4. Click the **Commit** button.

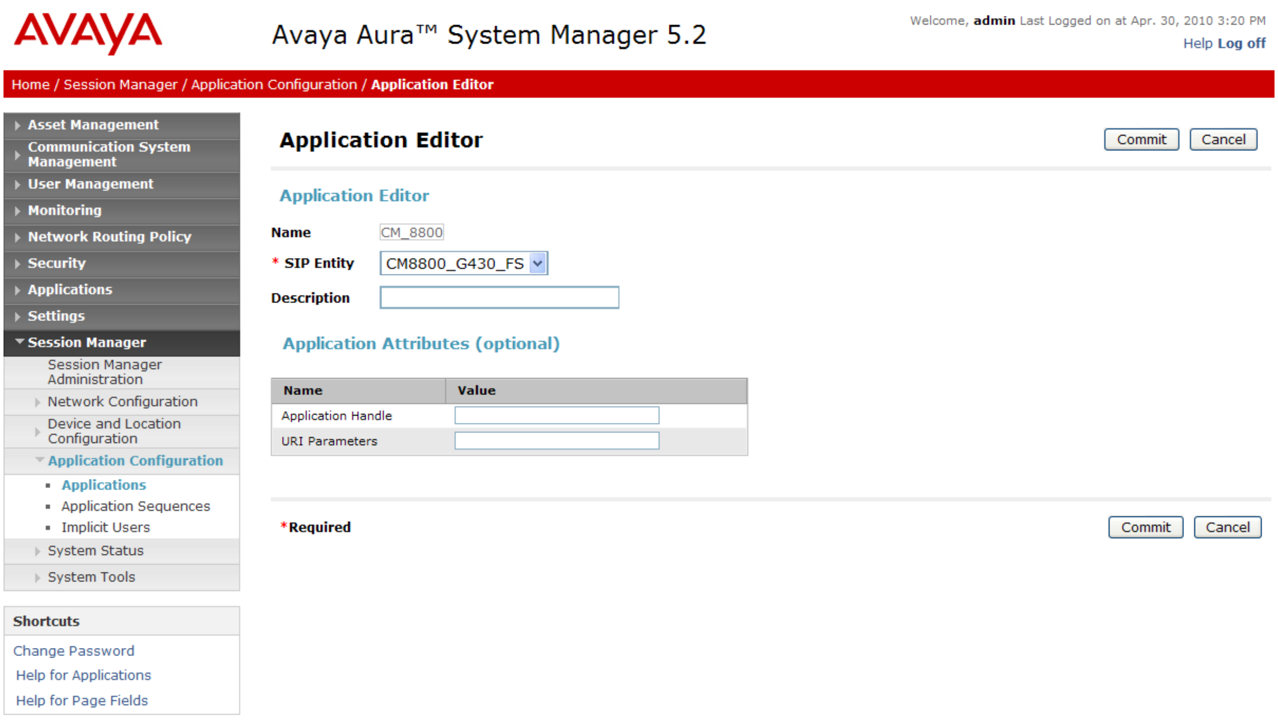

Figure 60: Application Editor Form

5. Select **Session Manager → Application Configuration → Application Sequences** on the left. Click on **New** (not shown).
   a. Enter a descriptive name in the **Name** field.
   b. Click on the "+" sign next to the appropriate Available Applications, and the selected available application will be moved up to the Applications in this Sequence section.
6. Click the **Commit** button.

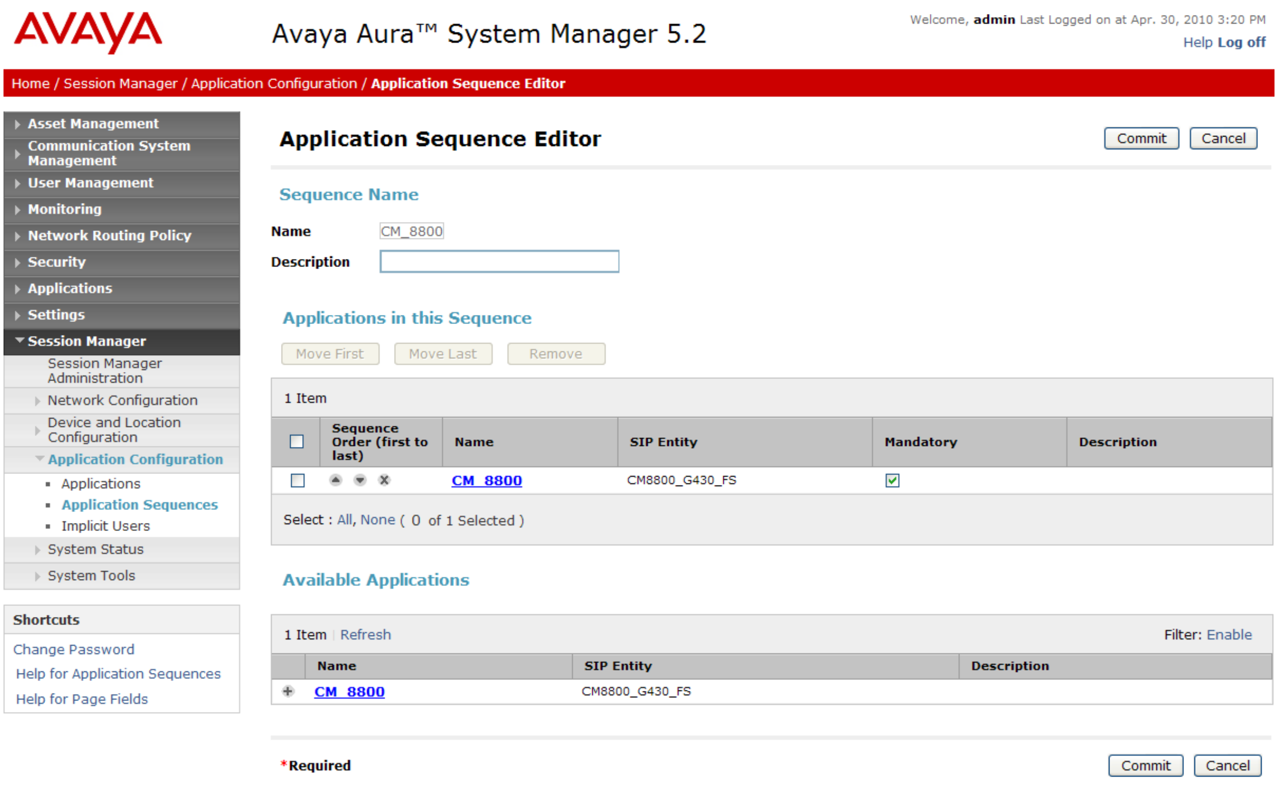

Figure 61: Application Sequence Editor Form

7. Select **Communication System Management → Telephony** on the left.
   a. Select the appropriate **Element Name**.
   b. Select **Initialize data for selected devices** radio button.
   c. Click the **Now** button. This will cause a data synchronization task to start. This may take some time to complete.

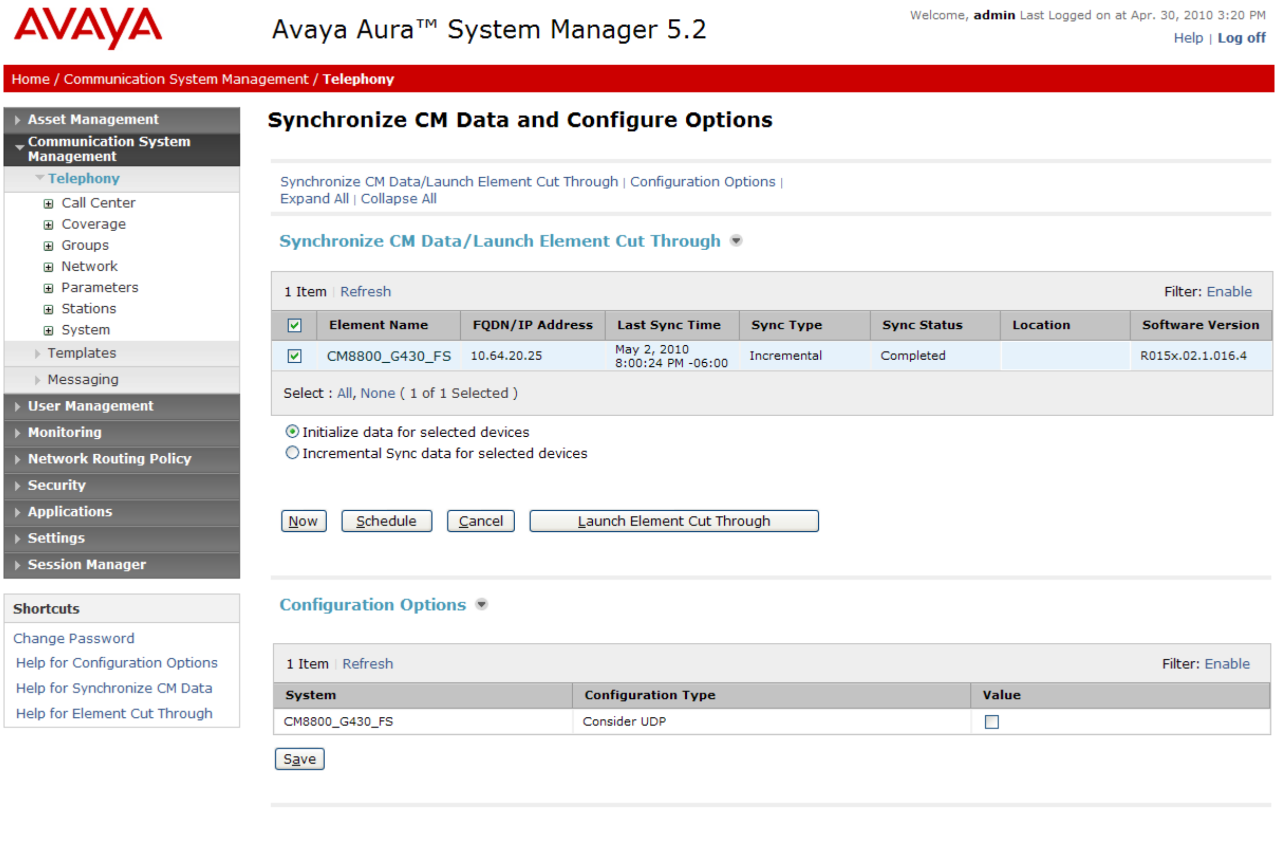

Figure 62: Synchronize CM Data and Configure Options Form

6.6. User Management for Adding SIP Telephone Users

SIP users must be added to Session Manager.

1. Select **User Management → User Management** on the left. Then click on **New** (not shown) to open the New User Profile page.
   a. Enter a **First Name** and **Last Name** for the user.

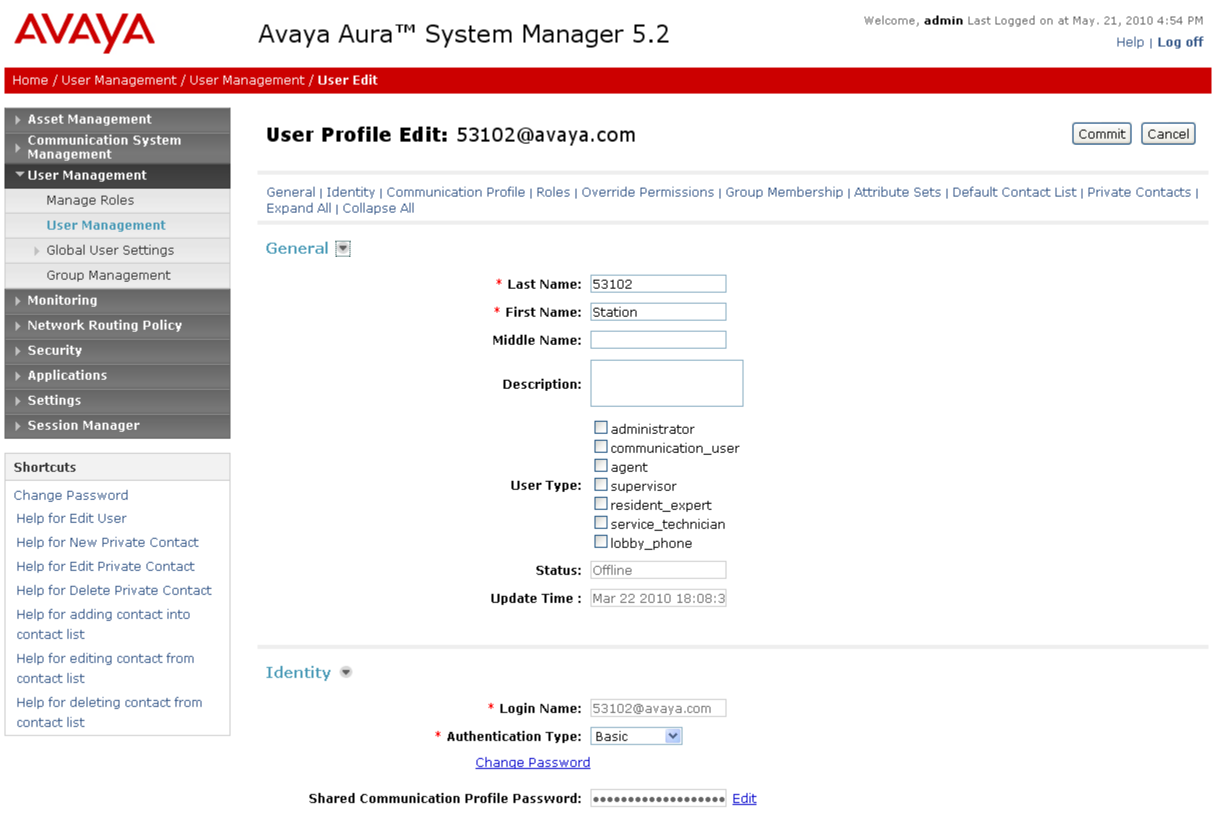

Figure 63: New User Profile Form

2. Click on **Identity** to expand that section. Enter the following fields, and use defaults for the remaining fields:
   a. **Login Name:** <extension>@avaya.com
   b. **SMGR Login Password:** Password to log into System Manager
   c. **Confirm Password:** Password to log into System Manager
   d. **Shared Communication**
   e. **Profile Password:** Password to be entered by the user when logging onto the telephone
   f. **Confirm Password:** Password to be entered by the user when logging onto the telephone
   g. **Localized Display Name:** Name to be used as calling party
   h. **Endpoint Display Name:** Full name of user
   i. **Language Preference:** Select the appropriate language preference
   j. **Time Zone:** Select the appropriate time zone

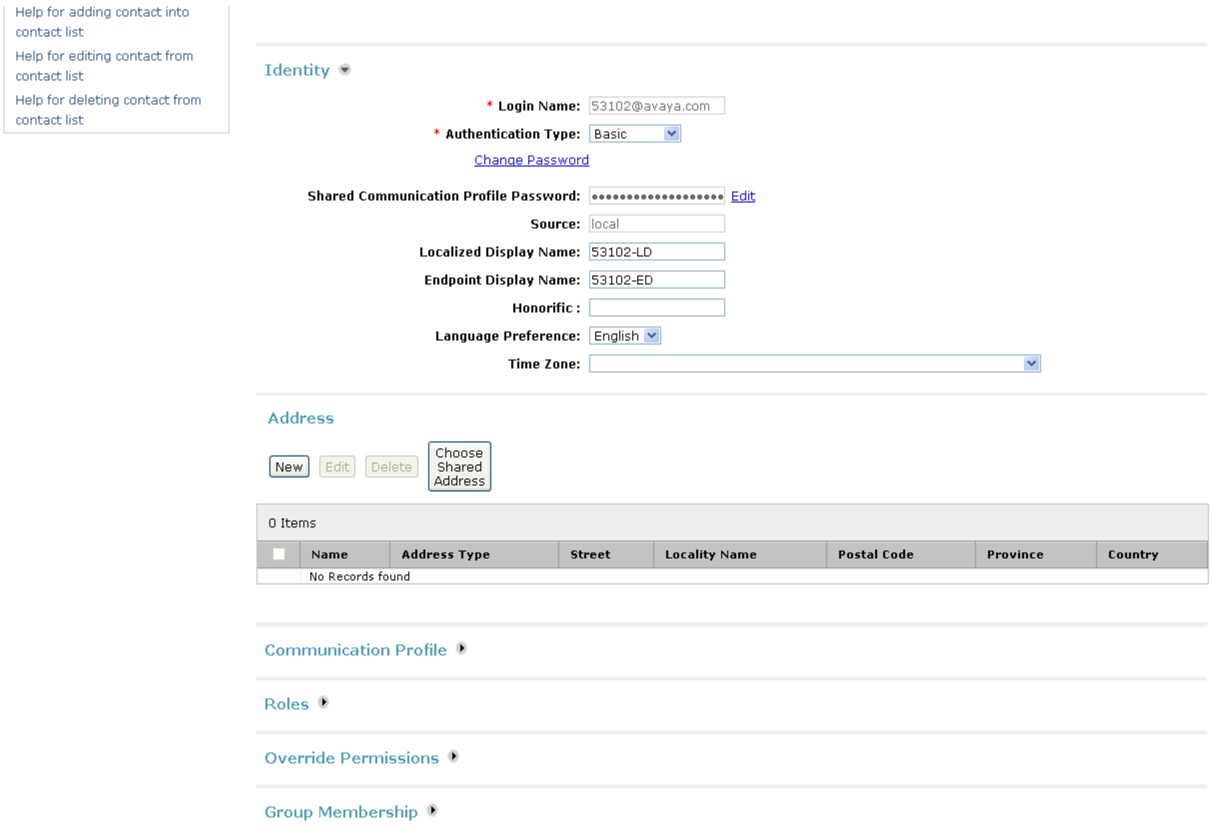

Figure 64: New User Profile Form – continued

3. Click on **Communication Profile** to expand that section in the above screen. Then click on **Communication Address** to expand that section. Enter the following fields and use defaults for the remaining fields:
   a. **Type:** Select "sip"
   b. **SubType:** Select "username"
   c. **Fully Qualified Address:** Enter the extension and select the domain as specified in **Section 6.3.1**
   d. Click on **Add** to add the record with the above information.

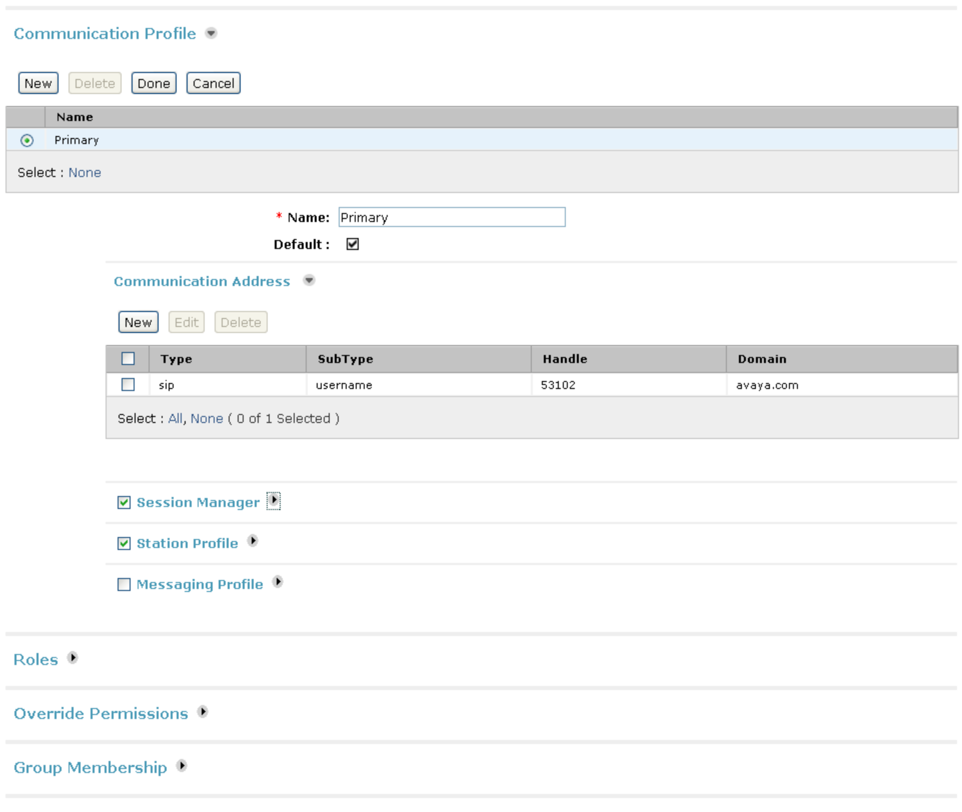

Figure 65: New User Profile Form – continued

4. Click on **Session Manager** in the above screen to expand that section. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence**, select the Application Sequence configured in **Section 6.5**.
5. Click on **Station Profile** in the above screen to expand that section. Enter the following fields and use defaults for the remaining fields:
   a. **System:** Select the Communication Manager entity.
   b. **Use Existing Stations:** Check this box.
   c. **Extension:** Enter the extension.
   d. **Template:** Select an appropriate template matching the telephone type.
   e. **Port:** Click on the Search icon to pick a port (in this case ("IP")
6. Click on **Commit** (not shown).

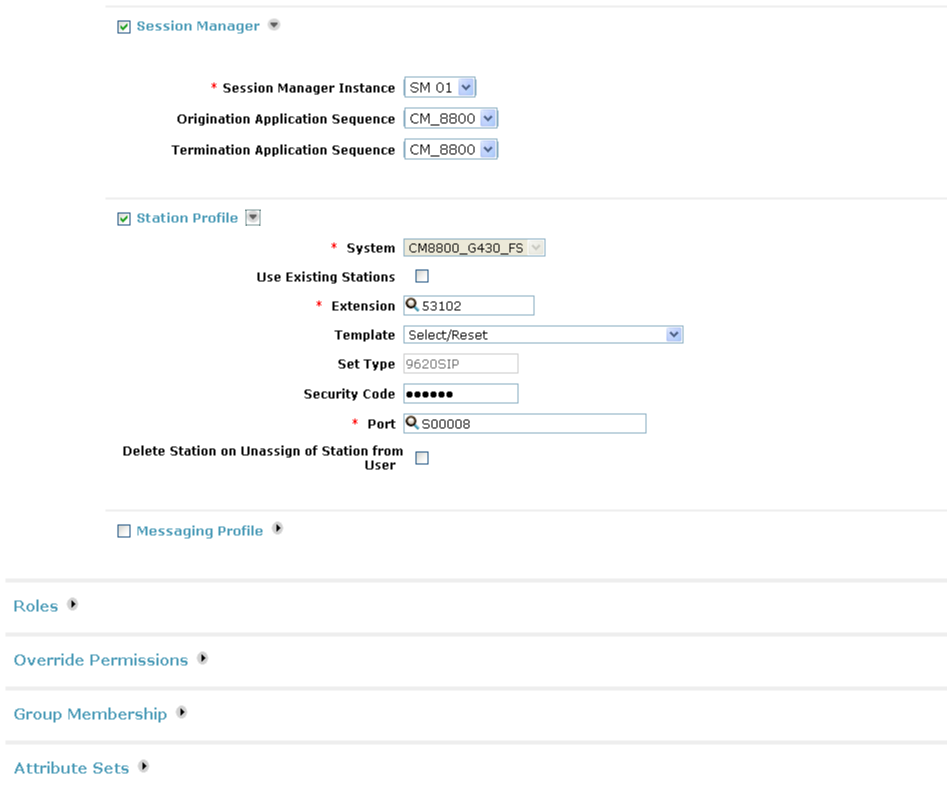

Figure 66: New User Profile Form – continued

7. Repeat the above procedures to add each SIP user.

7. Acme Packet 3800 Net-Net Session Director

In the reference configuration, an Acme Packet Session Border Controller (SBC) was used to provide access to the Metaswitch network.

7.1. Acme Packet Service States

Acme Packet requests and provides service states by sending out and responding to SIP *OPTIONS* messages. Acme Packet sends the OPTIONS message with the hop count (SIP Max-Forwards) set to zero.

- Acme Packet/Session Manager
  - Acme Packet sends OPTIONS → Session Manager responds with 200 OK
  - Session Manager sends OPTIONS → Acme Packet responds with 200 OK
- Acme Packet/Metaswitch
  - Acme Packet sends OPTIONS → Metaswitch responds with 200 OK
  - Metaswitch sends OPTIONS → Acme Packet responds with 200 OK

7.2. Acme Packet Network Interfaces

The physical and network interface provisioning for the "OUTSIDE" (to Metaswitch) and "INSIDE" (to Avaya CPE) interfaces is described in **Sections 7.3.3 and 7.3.4**.

7.3. Acme Packet Provisioning

Note – Only the Acme Packet provisioning required for the reference configuration is described in these Application Notes.

The Acme Packet SBC was configured using the Acme Packet CLI via a serial console port connection. An IP remote connection to a management port is also supported. The following are the generic steps for configuring various elements.

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** command and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (*configure)#*.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4-8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until returned to the Superuser prompt.
10. Type **save-configuration** to save the configuration.
11. Type **activate-configuration** to activate the configuration.

Once the provisioning is complete, the configuration may be verified by entering the ***show running-config*** command.

7.3.1 Acme Packet Management

Initial Acme Packet provisioning is performed via the console serial port (115200, 8/None/1/None). Network management is enabled by provisioning interface "Wancom0". In the reference configuration, the management IP address 169.254.1.1 is assigned.

From the *configure* prompt (steps 1 through 3 in **Section 7.3**):

1. Enter **bootparam**

> **Note** - This command will prompt one line at a time showing the existing value. Enter the new value next to the existing value. If there is no change to a value, hit the enter key and the next line will be presented. Be careful not to modify any values other than those listed below, or the Acme Packet may not recover after a reboot.

Console output will appear as follows:

```
acmesbc-pri(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

boot device          : wancom0
```

2. Press Enter at the **boot device : wancom0** line, and the next 4 lines until the following is displayed:

```
inet on ethernet (e)   :
```

3. Enter the IP address and mask (in hex) to be used for network management (e.g. **169.254.1.1:ffffff00**) and press Enter 3 more times until the following is displayed:

```
gateway inet (g)       :
```

4. Enter the management network gateway IP address (e.g. **169.254.1.1**) and press Enter.
5. Continue to press Enter until returned to the "configure" prompt. After the last bootparam line, the following message is displayed:

```
NOTE: These changed parameters will not go into effect until reboot.  Also, be aware
that some boot parameters may also be changed through PHY and Network Interface
Configurations.
```

6. At the "configure" prompt enter **exit**
7. Reboot the Acme Packet by entering **reboot** at the Superuser "#" prompt.

7.3.2 Local Policies

Allows any SIP requests from the **INSIDE** realm to be routed to the SERV_PROVIDER Session Agent Group in the OUTSIDE realm (and vice-versa).

7.3.2.1 INSIDE to OUTSIDE

From the *configure* prompt (steps 1 through 3 in **Section 5.3**):

1. Configure **session-router → local-policy** to create a local-policy for the INSIDE realm with the following settings:
   a. **from-address → ***
   b. **to-address → ***
   c. **source-realm → INSIDE**
   d. **state → enabled**
   e. **policy-attributes**
      i. **next-hop → SAG:SERV_PROVIDER**
      ii. **realm → OUTSIDE**
      iii. **start-time → 0000**
      iv. **end-time → 2400**
      v. **days-of-week → U-S**
      vi. **app-protocol → SIP**
      vii. **state → enabled**

7.3.2.2 OUTSIDE to INSIDE

1. Configure **session-router → local-policy** to create a local-policy for the **OUTSIDE** realm with the following settings:
   a. **from-address → ***
   b. **to-address → ***
   c. **source-realm → OUTSIDE**
   d. **state → enabled**
   e. **policy-attributes**
      i. **next-hop → SAG:ENTERPRISE**
      ii. **realm → INSIDE**
      iii. **start-time → 0000**
      iv. **end-time → 2400**
      v. **days-of-week → U-S**
      vi. **app-protocol → SIP**
      vii. **state → enabled**

7.3.3 Network Interfaces

This Section defines the network interfaces to the private (Avaya CPE) and public (Metaswitch) IP networks.

7.3.3.1 Public Network Interface

1. Configure **system → network-interface** to create a network-interface to the public (Internet/Metaswtich) side of the Acme Packet with the following settings:
   a. **name → Public**
   b. **ip-address → 205.xxx.xxx.106**
   c. **netmask → 255.255.255.128**
   d. **gateway → 205.xxx.xxx.1**

7.3.3.2 Private Network Interface

1. Configure **system → network-interface** to create a network-interface to the private (Avaya CPE) side of the Acme Packet with the following settings:
   a. **name → Private**
   b. **ip-address → 10.64.20.106**
   c. **netmask → 255.255.255.0**
   d. **gateway → 10.64.20.1**

7.3.4 Physical Interfaces

This Section defines the physical interfaces to the private (Avaya CPE) and public (Metaswitch) networks.

7.3.4.1 Public Physical Interface

1. Configure **system → phy-interface** to create a network-interface to the public (Internet/Metaswitch) side of the Acme Packet with the following settings:
   a. **name → Public**
   b. **operation-type → media**
   c. **port → 0**
   d. **slot → 0**
   e. **virtual-mac → 00:08:25:A0:E2:28**
      i. Virtual MAC addresses are assigned based on the MAC address assigned to the Acme. This MAC address is found by entering the command → *show prom-info mainboard* (e.g. **00:08:25:A0:E2:20**). To define a virtual MAC address, replace the last digit with **8** through **f**.
   f. **duplex-mode → FULL**
   g. **speed → 100**

7.3.4.2 Private Physical Interface

1. Configure **system → phy-interface** to create a phy-interface to the private (Avaya CPE) side of the Acme Packet with the following settings:
   a. **name → Private**
   b. **operation-type → media**
   c. **port → 0**
   d. **slot → 1**
   e. **virtual-mac → 00:08:25:A0:E2:2e**
   f. **duplex-mode → FULL**
   g. **speed → 100**

7.3.5 Realms

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces as well as applying header manipulation such as NAT.

7.3.5.1 Outside Realm

1. Configure **media-manager → realm-config** to create a realm for the outside network with the following settings:
    a. **identifier → OUTSIDE**
    b. **addr-prefix → 0.0.0.0**
    c. **network-interfaces → Public:0**
    d. **out-manipulationid → NAT_IP**
    e. **mm-in-realm → enabled**
    f. **mm-in-network → enabled**
    g. **mm-same-ip → enabled**
    h. **mm-in-system → enabled**
    i. **access-control-trust-level → medium**
    j. **invalid-signal-threshold → 1**
    k. **maximum-signal-threshold → 1**
    l. **untrusted-signal-threshold → 1**

7.3.5.2 Inside Realm

1. Configure **media-manager → realm-config** to create a realm for the inside network with the following settings:
    a. **identifier → INSIDE**
    b. **addr-prefix → 0.0.0.0**
    c. **network-interfaces → Private:0**
    d. **out-manipulationid → NAT_IP**
    e. **mm-in-realm → enabled**
    f. **mm-in-network → enabled**
    g. **mm-same-ip → enabled**
    h. **mm-in-system → enabled**
    i. **access-control-trust-level → high**
    j. **invalid-signal-threshold → 0**
    k. **maximum-signal-threshold → 0**
    l. **untrusted-signal-threshold → 0**

7.3.6 Steering-Pools

Steering pools define sets of ports that are used for steering media flows through the Acme.

7.3.6.1 Outside Steering-Pool

1. Configure **media-manager → steering-pool** to create a steering-pool for the outside network with the following settings:
    a. **ip-address → 205.xxx.xxx.106**
    b. **start-port → 49152**
    c. **end-port → 65535**
    d. **realm-id → OUTSIDE**

7.3.6.2 Inside Steering-Pool

1. Configure **media-manager → steering-pool** to create a steering-pool for the inside network with the following settings:
   a. **ip-address → 10.64.20.106**
   b. **start-port → 49152**
   c. **end-port → 65535**
   d. **realm-id → INSIDE**

7.3.7 Session-Agents

A session-agent defines an internal "next hop" signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for the Metaswitch service node (outside) and for the Session Manager (inside).

7.3.7.1 Outside Session-Agent

1. Configure **session-router → session-agent** to create a session-agent for the outside network with the following settings:
   a. **hostname → 208.xxx.xxx.135**
   b. **ip-address → 208.xxx.xxx.135**
   c. **port → 5060**
   d. **state → enabled**
   e. **app-protocol → SIP**
   f. **transport-method → UDP**
   g. **realm-id → OUTSIDE**
   h. **description → To_Metaswitch**
   i. **ping-method → Options;hops=0**
   j. **ping-interval → 60**
   k. **ping-send-mode → keep-alive**

7.3.7.2 Inside Session-Agent

1. Configure **session-router → session-agent** to create a session-agent for the inside network with the following settings:
   a. **hostname → 10.64.20.31**
   b. **ip-address → 10.64.20.31**
   c. **port → 5060**
   d. **state → enabled**
   e. **app-protocol → SIP**
   f. **transport-method → staticTCP**
   g. **realm-id → INSIDE**
   h. **description → To_Session Manager**
   i. **ping-method → Options;hops=0**
   j. **ping-interval → 60**
   k. **ping-send-mode → keep-alive**
   l. **tcp-keepalive → enabled**
   m. **tcp-reconn-interval → 10**

7.3.8 Session Groups

Session-groups (SAG) define single or multiple destinations that are referenced in provisioning session-agents.

7.3.8.1 Metaswitch Session-group

1. Configure **session-router → session-group** to create a session-group for the Metaswitch network with the following settings:
   a. **groupname → SERV_PROVIDER**
   b. **state → enabled**
   c. **app-protocol → SIP**
   d. **strategy → Hunt**
   e. **dest → 208.xxx.xxx.135**

7.3.8.2 Avaya CPE Session-group

1. Configure **session-router → session-group** to create a session-group for the Avaya CPE network with the following settings:
   a. **groupname → ENTERPRISE**
   b. **state → enabled**
   c. **app-protocol → SIP**
   d. **strategy → Hunt**
   e. dest → 10.64.20.31

7.3.9 SIP Configuration

This command sets the values for the Acme Packet SIP operating parameters. The home-realm defines the SIP daemon location, and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere.

1. Configure **session-router → sip-config** with the following settings:
   a. **state → enabled**
   b. **operation-mode → dialog**
   c. **home-realm-id → INSIDE**
   d. **egress-realm-id → OUTSIDE**

7.3.10 SIP Interfaces

The SIP interface defines the signaling interface (IP address and port) to which the Acme Packet sends and receives SIP messages.

7.3.10.1 Outside SIP- interface

1. Configure **session-router → sip-interface** to create a sip-interface for the outside network with the following settings:
   a. **state → enabled**
   b. **realm-id → OUTSIDE**
   c. **sip-port →**
      i. **address → 205.xxx.xxx.106**
      ii. **port → 5060**
      iii. **transport-protocol → UDP**

7.3.10.2 Inside SIP- interface

1. Configure **session-router → sip-interface** to create a sip-interface for the inside network with the following settings:
   a. **state → enabled**
   b. **realm-id → INSIDE**
   c. **sip-port**
      i. **address → 10.64.20.106**
      ii. **port → 5060**
      iii. **transport-protocol → TCP**

7.3.11 SIP Manipulation

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. In the reference configuration the following header manipulations are performed:

- NAT IP addresses in the From header of SIP requests.
- NAT IP addresses in the To header of SIP requests.
- NAT IP addresses in the Remote-Party-ID header of SIP requests.
- NAT IP addresses in the History-Info header of SIP requests.
- NAT IP addresses in the Alert-Info header of SIP requests. This is different from other rules because it will NAT CID (caller ID) URIs in addition to SIP URIs.

1. Configure **session-router → sip-manipulation** with the following settings :
   a. **name → NAT_IP**
   b. **description → Topology hiding for SIP headers**
2. Proceed to the following sections.

7.3.11.1 From Header

1. Configure **session-router → sip-manipulation → header-rule** with the following settings:
   a. **name → manipFrom**
   b. **action → manipulate**
   c. **comparison-type → case-sensitive**
   d. **msg-type → request**
   e. **element-rule**
      i. **name → FROM**
      ii. **type → uri-host**
      iii. **action → replace**
      iv. **match-val-type → ip**
      v. **comparison-type → case-sensitive**
      vi. **new-value → $LOCAL_IP**

7.3.11.2 To Header

1. Configure **session-router → sip-manipulation → header-rule** with the following settings:
    a. **name → manipTo**
    b. **action → manipulate**
    c. **comparison-type → case-sensitive**
    d. **msg-type → request**
    e. **element-rule**
        i. **name → TO**
        ii. **type → uri-host**
        iii. **action → replace**
        iv. **match-val-type → ip**
        v. **comparison-type → case-sensitive**
        vi. **new-value → $REMOTE_IP**

7.3.11.3 Remote Party ID Header

1. Configure **session-router → sip-manipulation → header-rule** with the following settings:
    a. **name → manipRpid**
    b. **header-name → Remote-Party-ID**
    c. **action → manipulate**
    d. **comparison-type → case-sensitive**
    e. **msg-type → request**
    f. **element-rule**
        i. **name → RPID**
        ii. **type → uri-host**
        iii. **action → replace**
        iv. **match-val-type → ip**
        v. **comparison-type → case-sensitive**
        vi. **new-value → $LOCAL_IP**

7.3.11.4 History Info Header

1. Configure **session-router → sip-manipulation → header-rule** with the following settings:
    a. **name → manipHistInfo**
    b. **header-name → History-Info**
    c. **action → manipulate**
    d. **comparison-type → case-sensitive**
    e. **msg-type → request**
    f. **element-rule**
        i. **name → HISTORYINFO**
        ii. **type → uri-host**
        iii. **action → replace**
        iv. **match-val-type → ip**
        v. **comparison-type → case-sensitive**
        vi. **new-value → $REMOTE_IP**

7.3.11.5 Alert-info Header

1. Configure **session-router → sip-manipulation → header-rule** with the following settings:
   a. **name → storeAlertInfo**
   b. **header-name → Alert-Info**
   c. **action → store**
   d. **comparison-type → pattern-rule**
   e. **match-value → (.+@) ([0-9.]+) (.+)**
   f. **msg-type → request**
2. Configure **session-router → sip-manipulation → header-rule** with the following settings:
   a. **name → manipAlertInfo**
   b. **header-name → Alert-Info**
   c. **action → manipulate**
   d. **comparison-type → boolean**
   e. **match-value → $storeAlertInfo**
   f. **msg-type → request**
   g. **new-value → $storeAlertInfo.$1+$REMOTE_IP+$storeAlertInfo.$3**

7.3.12 Other Acme Packet provisioning

7.3.12.1 Access-control

This is a static Access Control List that is used to limit SIP access to only known devices.

1. Configure **session-router → access-control** with the following settings:
   a. **realm-id → OUTSIDE**
   b. **source-address → 208.xxx.xxx.135:5060**
   c. **application-protocol → SIP**
   d. **transport-protocol → UDP**
   e. **access → permit**

7.3.12.2 Media-Manager

Verify that the media-manager process is enabled.

1. Navigate to **media-manager → media-manager**
2. Enter **select → show →** Verify that the media-manager state is enabled. If not, configure the following settings:
   a. **state → enabled**

7.3.12.3 System-config

In the system-config, specify a hostname and the default gateway of the management interface.

1. Configure **system → system-config** with the following settings:
   a. **hostname → acmesbc**
   b. **default-gateway → 10.64.20.1**

8. Metaswitch Configuration

During the test effort, the Metaswitch network was protected by a pair of Acme Packet Net-Net SD 3820 session border controllers. The session border controllers are not required as part of the solution. For brevity, only the configuration of the MetaSphere CFS is discussed below. If a session border controller is used between the MetaSphere CFS solution and the Avaya solution, contact a Metaswitch Networks support representative for additional configuration details.

8.1. Media Gateway Model

A truncated text dump of the Remote Media Gateway Model used for the testing is shown below. For an importable version, contact a Metaswitch customer service representative.

```
begin MediaGatewayModel MediaGatewayModel.176 // Remote Media Gateway Model "Avaya
CM/SM"
  Category                                          SIP
  ModelName                                         Avaya CM/SM
  ControlProtocol                                   SIP
  DefaultModel                                      False
  SupportedHighBandwidthMediaFormats                {G.711 u-law,G.711 A-law}
  SupportedLowBandwidthMediaFormats                 {G.729 AB}
  PreferredLowBandwidthMediaFormats                 {G.729 AB}
  AdvancedVoiceCodecsPermitted                      Any codecs
  VideoCodecsPermitted                              Any codecs
  PacketizationInterval                             0
  SilenceSuppressionAllowed                         False
  MaximumSimultaneousTransactionsOutstanding        100
  DigitOverhangTime                                 250
  FixBitsMGCPMeGaCoSIP                              {Cannot be hub,Simple contexts,Cannot
                                                     control endpoint connectivity,Cannot
                                                     move contexts,Connections always
                                                     receive,Cannot report detection of
                                                     call-type discrimination tones,T.38
                                                     supported}
  DynamicFixBitsMGCPMeGaCoSIP                       {}
  FixBitsSIP                                        {Supports SDP connectivity
                                                     requests,Supports receiving INVITEs
                                                     with no SDP,Supports receiving SIP
                                                     Reason header over tandem trunk
                                                     calls}
  FixBitsSIP2                                       {}
  ReferenceCount                                    1
  UpToDateCount                                     1
  ExportHeading                                     Export
  StatusHeading                                     Status
  RequestedStatus                                   Enabled
end //MediaGatewayModel
```

8.2. Configured SIP Binding

The connection to the Avaya solution is modeled as a configured SIP binding. During compliance testing, the configured SIP binding was configured as follows.

Name	Value
Name	Avaya CM/SM
Customer information	
Customer information 2	
Customer information 3	
Customer information 4	
Customer information 5	
Customer information 6	
Usage	Subscriber
Use DN for identification	True
SIP authentication required	False
SIP domain name	208.[redacted].135
IP address match required	False
Contact IP address (Format: w.x.y.z)	205.[redacted].106
Contact IP port (0 - 65535)	5060
Supported incoming trunk group parameter type	None
Trunk group parameter type on outgoing messages	None
Proxy IP address (Format: w.x.y.z)	10.220.20.25
Proxy IP port (0 - 65535)	5060
Transport protocol	UDP
Media Gateway model	Media Gateway Model "Avaya CM/SM"
Network Node ☐ Override	None [Default]
Preferred location of Trunk Gateway	None
ESA Protection Domain	None
Trusted	True
Use caller name provided by SIP device	False
Play announcements when error conditions occur	True
Use static NAT mapping	False
Maximum call appearances (1 - 2147483647)	1024
Maximum concurrent high bandwidth call appearanc...	0
Poll peer device	True
Polling interval (1 - 3600 seconds)	30
Current number of call appearances in use	0

8.3. PBX object configuration

The Avaya solution is modeled in MetaView as a PBX. The settings used during testing are shown below.

8.3.1 PBX Object

Settings

Setting	Override	Value
Subscriber Group		(604-698) Remote Subscribers, Whistler, BC
Number status		Normal
Recently moved from old number		False
Signaling type		SIP
Fix bits		☐ 10 digit max ANI ☐ Always 10 digit ANI
Send DID sequence for Listed Directory Number		True
DNIS used in DID sequence for Listed Directory Num…		6046982010
Calling number / connected line ID screening	☐ Override	Owned DN [Default]
Default maximum call appearances for PBX lines (1 - …	☐ Override	64 [Default]
Long distance carrier	☑ Override	0001
IntraLATA carrier	☑ Override	0001
International carrier	☑ Override	0001
PIN		0000
Locale		English (US)
Second locale		None
Billing type	☐ Override	Flat rate [Default]
Number Validation and routing attributes	☐ Override	☐ Pre-paid / off-switch calling card sub… ☐ Fax / Modem subscriber ☐ Nomadic subscriber
Deny all usage sensitive features	☐ Override	False [Default]
Service suspended		None
Force LNP lookup	☐ Override	False [Default]
Subscriber timezone	☐ Override	US/Pacific [Default]
Line Traffic Study		False
Enabled date (PDT)		4/14/10 11:50:04 AM
Charge indication	☐ Override	None [Default]
Category	☐ Override	Ordinary calling subscriber [Default]

8.3.2 PBX Line Object

Settings		
Configured SIP Binding		Avaya CM/SM
Maximum call appearances (1 - 2147483647)	Override	20
Line usage		Voice and fax
PBX plays ringback		True

8.3.3 DID objects

Two DID ranges were configured during compliance testing due to the setup in Metaswitch's test lab. Two DID ranges are not required.

Name	Value
Type	DID range
Description	normal
Range size (1 - 1000000000)	9
(First) Directory number	6046982011
Last Directory number	6046982019
First code	6046982011
Last code	6046982019

Type	DID range
Description	PSTN
Range size (1 - 1000000000)	1
(First) Directory number	5102174567
Last Directory number	5102174567
First code	5102174567
Last code	5102174567

9. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between Metaswitch and the Avaya CPE. This section covers the general test approach and the test results.

The Avaya CPE was connected using SIP trunking to the Metaswitch network. The general test approach included the following:

- Inbound Calls – Verify that calls placed from a PSTN telephone to a DID number are properly routed via the SIP trunk to the expected extension on Communication Manager. Verify the talk-path exists in both directions, that calls remain stable for several minutes and disconnect properly.

- Outbound Calls – Verify that calls placed to a PSTN telephone are properly routed via the SIP trunk. Verify that the talk-path exists in both directions and that calls remain stable and disconnect properly.

- Inbound DTMF Digit Navigation – Verify inbound DID calls can properly navigate voice mail menus.

2. Outbound DTMF Digit Navigation – Verify outbound calls can properly navigate a voice mail or interactive response system reached via a PSTN number.

Interoperability testing of the reference configuration was completed with successful results.

The following observations were noted:

1. The Metaswitch test lab did not support x11 calls (e.g 411, 911, international, etc.).

2. Due to limitations of the Metaswitch test lab configuration, the caller-id did not always display the proper calling party number for calls to and from the PSTN (rather, an administered 10 digit number was display).

10. Verification Steps

This Section provides the verification steps that may be performed to verify basic operation of the Avaya Aura™ SIP trunk solution with Metaswitch.

10.1. Verify Avaya Aura™ Communication Manager 5.2

Verify the status of the SIP trunk group by using the ***status trunk n*** command, where "n" is the administered trunk group number. Verify that all trunks are in the "in-service/idle" state as shown below.

```
status trunk 9

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0009/001 T00334   in-service/idle    no
0009/002 T00335   in-service/idle    no
0009/003 T00336   in-service/idle    no
0009/004 T00337   in-service/idle    no
0009/005 T00338   in-service/idle    no
0009/006 T00339   in-service/idle    no
0009/007 T00340   in-service/idle    no
0009/008 T00341   in-service/idle    no
0009/009 T00342   in-service/idle    no
0009/010 T00343   in-service/idle    no
```

Figure 67: Status Trunk

Verify the status of the SIP signaling groups by using the ***status signaling-group n*** command, where "n" is the administered signaling group number. Verify the signaling group is "in-service" as indicated in the **Group State** field shown below.

```
status signaling-group 9
                         STATUS SIGNALING GROUP

        Group ID: 9                               Active NCA-TSC Count: 0
      Group Type: sip                              Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

Figure 68: Status Signaling Group

Make a call between a Communication Manager H.323 station and the PSTN. Verify the status of connected SIP trunk by using the ***status trunk x/y*** command, where "x" is the number of the SIP trunk group, and "y" is the active member number of a connected trunk. Verify on Page 1 that the **Service State** is "**in-service/active**". On Page 2, verify that the IP addresses of the procr or C-LAN and Session Manager are shown in the **Signaling** section. In addition, the **Audio** section shows the G.711 codec and the IP address of the Avaya H.323 endpoint and the Acme Packet SBC. The **Audio Connection Type** displays "**ip-direct**", indicating direct media between the two endpoints.

```
status trunk 9/7                                                Page   1 of   3
                              TRUNK STATUS

 Trunk Group/Member: 0009/007             Service State: in-service/active
               Port: T00340           Maintenance Busy? no
 Signaling Group ID: 9

   IGAR Connection? no

    Connected Ports: S00027
```

Figure 69: Status Trunk – Active Call – Page 1

```
status trunk 9/7                                                Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: 01A0017
  Signaling   IP Address                              Port
   Near-end:  10.64.21.41                           : 5061
    Far-end:  10.64.20.31                           : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.711MU
   Audio      IP Address                              Port
   Near-end:  10.64.21.71                           : 2662
    Far-end:  10.64.20.106                          : 50248

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

Figure 70: Status Trunk – Active Call – Page 2

10.2. Verify Avaya Aura™ Session Manager

Monitoring of Session Manager is performed via System Manager.

10.2.1 Verify SIP Entity Link Status

Expand the **Session Manager** menu and click SIP Monitoring. Verify that none of the links to the defined SIP entities are down (as indicated by **0/4** in the figure below), indicating that they are all reachable for call routing.

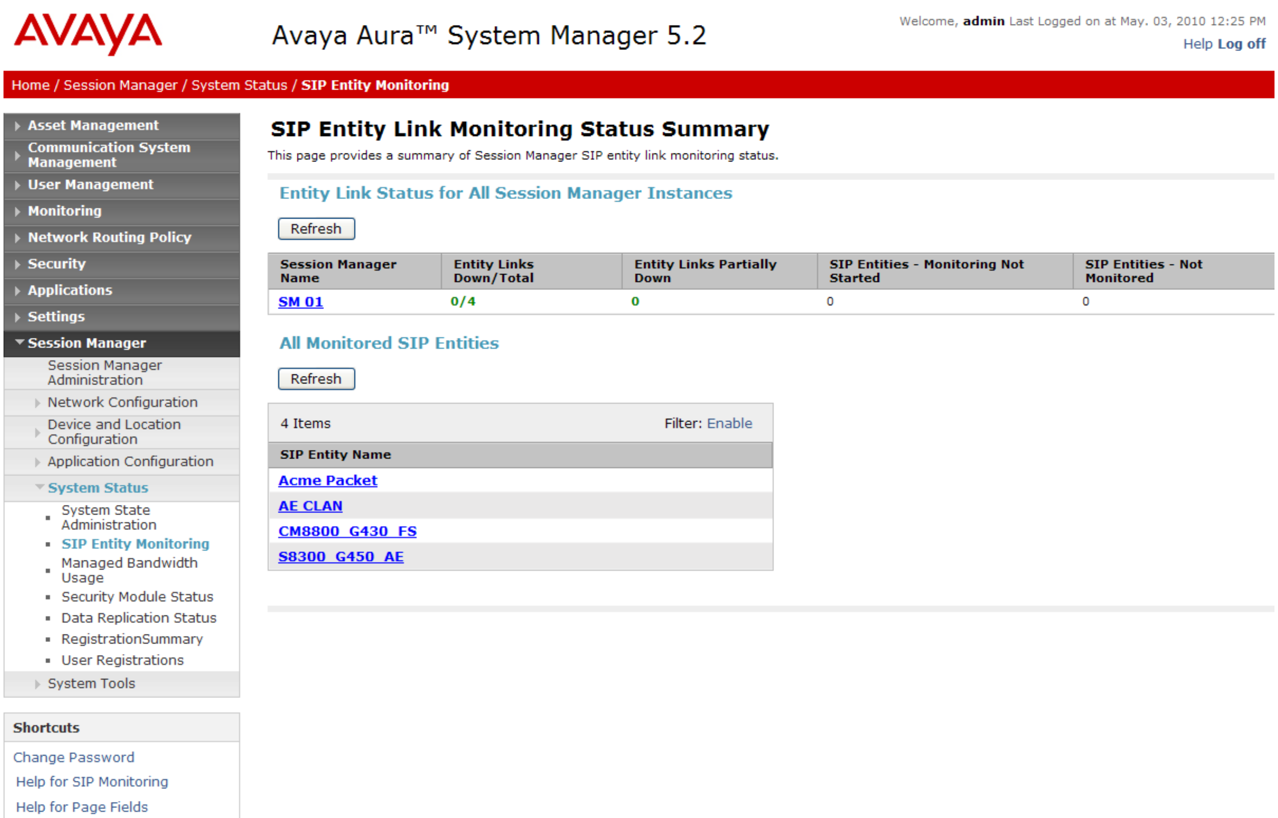

Figure 71: SIP Entity Link Monitoring - Summary

Selecting a monitored SIP Entity from the list will display its status (e.g. **S8300_G450_AE**).

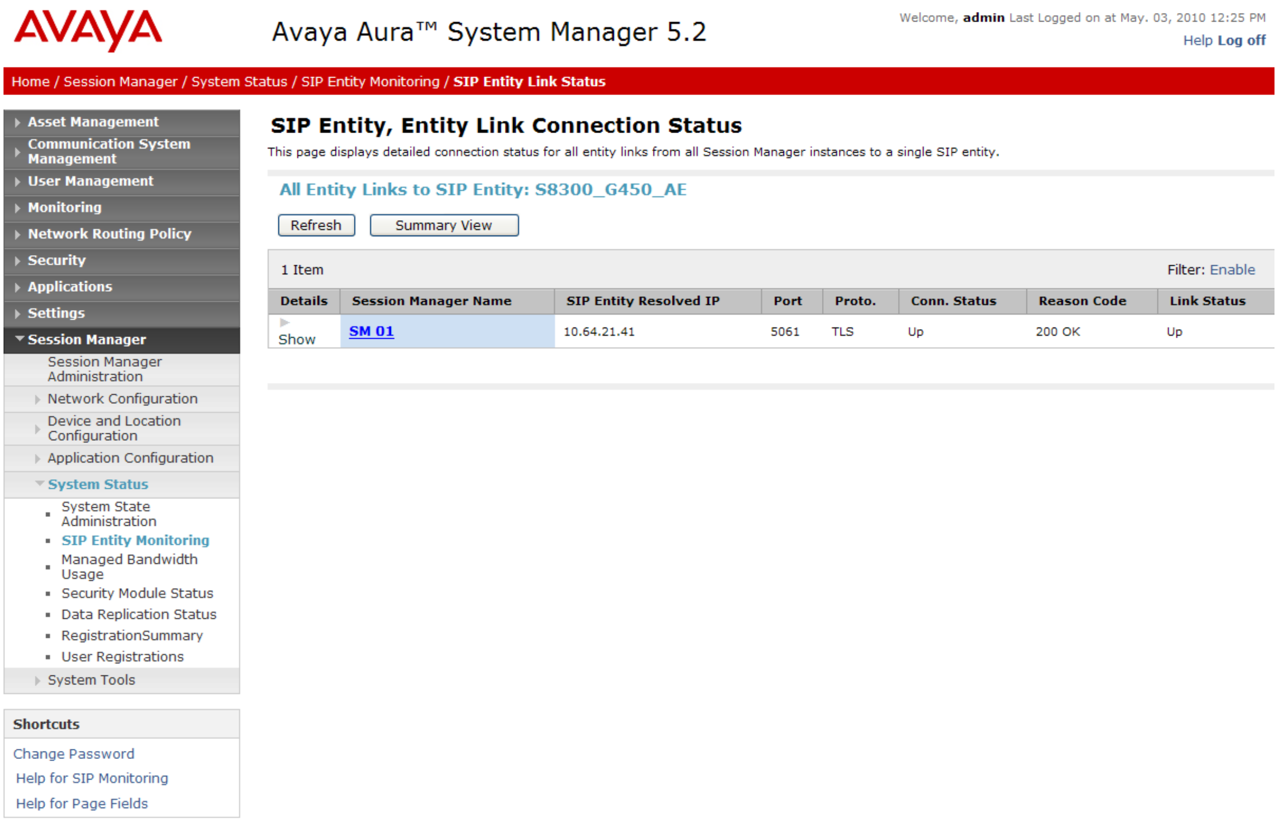

Figure 72: SIP Entity Link Connection Status

10.2.2 Verify System State

Expand the **Session Manager** menu and click **System State Administration**. Verify that the Management State is Management Enabled and the Service State is Accept New Service.

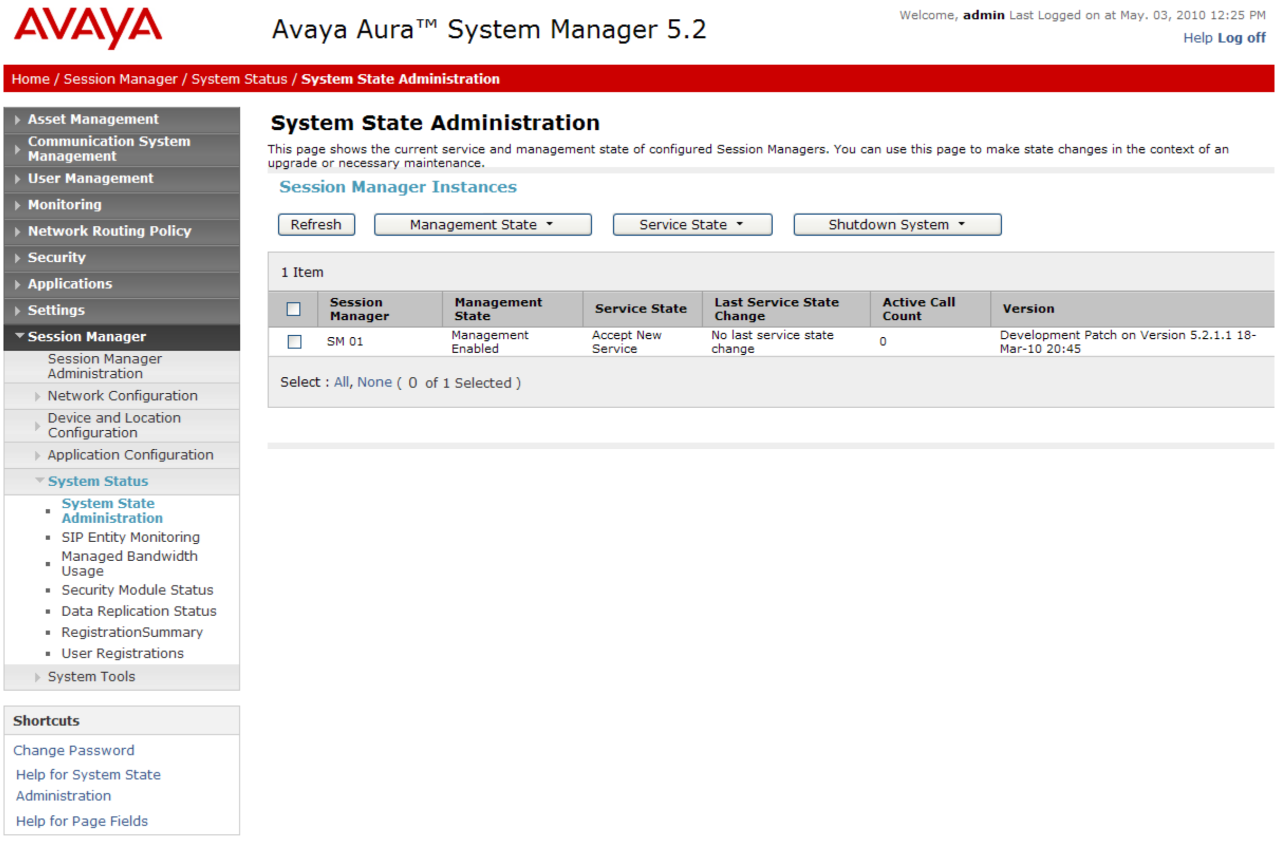

Figure 73: System State

10.3. Verification Call Scenarios

Verification scenarios for the configuration described in these Application Notes included:

- Inbound and outbound basic voice calls between various telephones on the Communication Manager and PSTN can be made in both directions.
  - Avaya One-X Communicator (H.323 Softphone), as well as traditional analog, digital, and SIP phones.
- Inbound and outbound fax calls between Communication Manager and PSTN can be made in both directions.
- Direct IP-to-IP Media (also known as "Shuffling") when applicable.
- DTMF Tone Support.
- Additional PSTN numbering plans.
- Supplementary calling features were verified. The supplementary calling features verified are:
  - Hold, Call transfer, Conference.
  - Voicemail Coverage and Retrieval.
  - Call Forwarding.
  - Call Coverage.
  - Extend Call.
  - EC500 (call forking).

10.4. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 5.2.1, Avaya Aura™ Session Manager 5.2.1.1, and Acme Packet Session Border Controller 6.1.0 can be configured to interoperate successfully with Metaswitch MetaSphere CFS. This solution provides users of Communication Manager the ability to support inbound and outbound as well as on-net and off-net calling over a SIP trunk.

11. References

11.1. Avaya

The following Avaya product documentation is available at http://support.avaya.com.

[1] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May 2009.
[2] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009.
[3] *Avaya Aura™ Session Manager Overview*, Doc ID 03-603323, Issue 2, Release 5.2, March 2010.
[4] *Installing Avaya Aura™ Session Manager*, Doc ID 03-603473, Issue 1.3, Release 5.2, January 2010.
[5] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Issue 2, Release 5.2, November 2009.
[6] *Administering Avaya Aura™ Communication Manager as a Feature Server*, Doc ID 03-603479, Issue 1.3, Release 5.2, March 2010
[7] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325.
[8] *Feature Description and Implementation for Avaya Communication Manage*r, Doc ID555-245-205, Issue 7, Release 5.2, May 2009

11.2. Metaswitch

Metaswitch product documentation is available at http://www.metaswitch.com/support/.

11.3. Acme Packet

The following Acme Packet product documentation is available at:
https://support.acmepacket.com/

[9] *Net-Net® 4000, ACLI Reference Guide, Release Version S-C6.1.0*
[10] *Net-Net® 4000 ACLI, Configuration Guide, Release Version S-C6.1.0*

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.