Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Metaswitch MetaSphere CFS 7.3 and Metaswitch Perimeta Session Border Controller 3.1.0 with Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet 3800 Net-Net Session Director 6.2 – Issue 1.0

Abstract

These application notes describe the steps required to configure Session Initiation Protocol (SIP) trunking between a Metaswitch MetaSphere Call Feature Server (CFS) and Metaswitch Perimeta Session Border Controller (SBC) solution connecting to Avaya telephony solution using Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Acme Packet 3800 Session Border Controller.

This is not a replacement of Service Provider SIP Trunk service compliance test. To verify the SIP Trunk service for a particular Service Provider, a test needs to be requested by the Service Provider.

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

©2012 Avaya Inc. All Rights Reserved.

Table of Contents

.

©2012 Avaya Inc. All Rights Reserved.

©2012 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) trunking between a Metaswitch MetaSphere Call Feature Server (CFS) with a Metaswitch Perimeta Session Border Controller (SBC) solution connecting to an Avaya telephony solution using Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and the Acme Packet 3800 Session Border Controller. Various Avaya analog, digital, H.323, and SIP stations are also included in the configuration

The Acme Packet 3800 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 Perimeta Session Border Controller is used at the edge between public network and Metaswitch CFS.

MetaSphere is a broad suite of telephony applications. MetaSphere applications may be deployed individually or in combination to deliver the full spectrum of legacy and next-generation voice services.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site consisting of Communication Manager, Session Manager, System Manager and an ACME Packet 4500 Net-Net Session Director supporting SIP Trunking connecting to a Metaswitch solution consisting of MetaSphere CFS and Perimeta SBC. This configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify SIP trunking interoperability between the Metaswitch solution and the Avaya solution.

©2012 Avaya Inc. All Rights Reserved.

The following areas are covered in the test:

- Response to SIP OPTIONS queries
- Incoming calls to various phone types from Metaswitch CommPortal softclient registered to Metaswitch CFS. Phone types included SIP, H.323, digital, and analog telephones at the enterprise.
- Outgoing DID calls from various phone types. Phone types included SIP, H.323, digital, and analog telephones at the enterprise. All outbound DID calls were routed from the enterprise across the SIP trunk to Metaswitch CFS
- Inbound and outbound calls to/from the Avaya one-X Communicator softclient
- Inbound and outbound long hold time call stability
- Codec G.711 A-LAW, G.711 U-LAW and G.729 (a)
- Caller number/ID presentation
- Privacy requests (e.g., caller anonymous) and Caller ID restriction for inbound and outbound calls
- DTMF transmission using RFC 2833
- Voicemail navigation for inbound and outbound calls
- EC500 Features
- T.38 Fax Support
- Telephony features such as hold and resume, transfer, and conference.
- Call forwarding

The following areas are not covered in the test:

- Various PSTN call types including: local, long distance, international, outbound toll-free, operator service and directory assistance could not be tested due to limitation of Metaswitch lab environment

2.2. Test Results

Interoperability testing of Metaswitch SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below:

- Inbound/Outbound PSTN calls were not tested as part of this compliance test. The Metaswitch lab environment did not support PSTN testing.
- Metaswitch CommPortal does not support G.729. Only G.711 could be tested with it. G.711 and G.729 were tested from Avaya DID to Avaya DID traversing the SIP trunk to Metaswitch CFS.
- In Communication Manager, when 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 endpoint, one way audio is experienced. This issue is being investigated.

©2012 Avaya Inc. All Rights Reserved.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

For technical support on Metaswitch SIP Trunking contact Metaswitch at www.metaswitch.com.

3. 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. For security purposes, the real public IP addresses used in the compliance test are masked (at least partially) in these Application Notes.

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 sbc-whistler.metaswitch.com. The Avaya CPE environment was assigned the domain avaya.com.

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

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Acme Packet 3800 Net-Net Session Director
- Avaya 96x0 IP Telephone (H.323 protocol)
- Avaya 96x1 IP Telephone (H.323 protocol)
- Avaya 96x0 IP Telephone (SIP protocol)
- Avaya 96x1 IP Telephone (SIP protocol)
- Avaya 1416 Digital Telephone
- Avaya one-X Communicator (H.323 softphone)
- Generic Analog Telephone
- Generic Fax Machine
- Metaswitch MetaSphere CFS
- MetaswitchPerimeta Session Border Controller
- Metaswitch CommPortal (softclient)

©2012 Avaya Inc. All Rights Reserved.

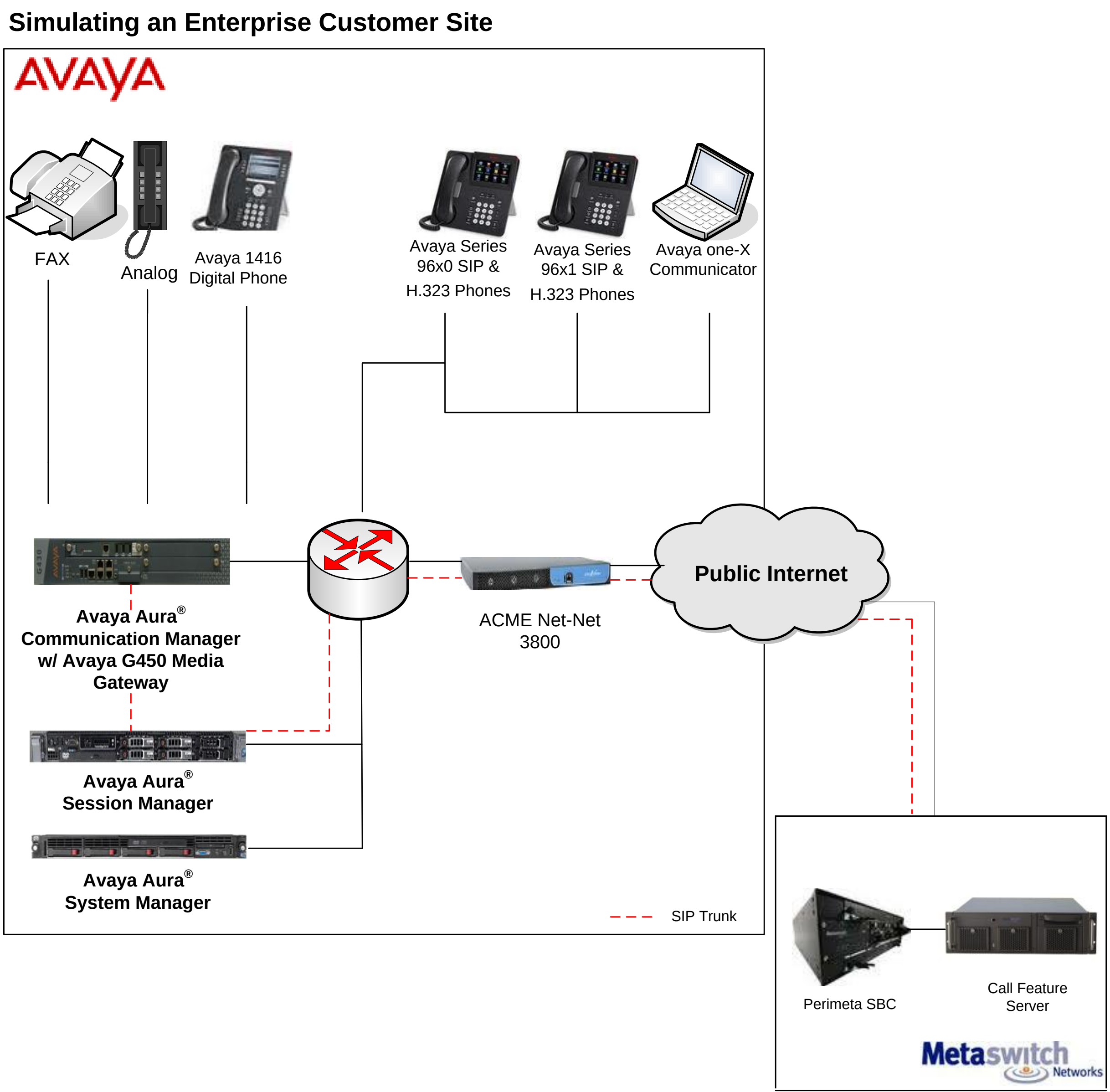

Figure 1: Avaya IP Telephony Network connected to Metaswitch

©2012 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment/Software	**Release/Version**
Avaya Aura® Session Manager – HP ProLiant DL360 G7 Server	6.1 SP6
Avaya Aura® System Manager – HP ProLiant DL360 G7 Server	6.1 SP6
Avaya Aura® Communication Manager – Avaya S8300D Server	6.0.1 SP7 With Avaya Aura® Communication Manager Messaging
Avaya G450 Media Gateway	-
Avaya 96x0 Series (H.323)	3.1-SP3
Avaya 96x1 Series (H.323)	6.2
Avaya 96x0 Series (SIP)	2.6-SP7
Avaya 96x1 Series (SIP)	6.0-SP3
Avaya 1416 Digital Telephone	N/A
Generic Analog Phone	N/A
Generic Fax Machines	N/A
Avaya one-X Communicator	6.1.3.09-SP3
Metaswitch Solution Components	
Metaswitch MetaSphere CFS	7.3
Metaswitch Perimeta SBC	3.1.0
CommPortal Communicator	1.2.2

Table 1: Equipment and Software

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager with the necessary signaling and media characteristics for the SIP trunk connection with Session Manager and the Metaswitch solution. The procedures include the following areas:

- Verify Capacity and Features
- Configure IP Node Names
- Configure IP Codec Set
- Configure IP Network Region
- Administer SIP Trunks with Session Manager
- Configure Route Pattern
- Configure Dial Plan
- Configure Uniform Dial Plan
- Configure Public Unknown Numbering
- Configure Feature Access Codes

©2012 Avaya Inc. All Rights Reserved.

- Administer ARS Analysis
- Administer AAR Analysis
- Administer Stations (non-SIP)
- EC500 Provisioning
- Saving Translations

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.

Throughout this section, the administration of Communication Manager is performed using a System Access Terminal (SAT) via SSH with the appropriate administrative permissions.

5.1. Verify Capacity and Features

Use the **display system-parameters customer-options** command and on **Page 2 to** verify that the **Maximum Administered SIP Trunks** value is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **4000** licenses are available and **30** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  30
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    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: 300   0

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

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

©2012 Avaya Inc. All Rights Reserved.

On **Page 3**, verify that **ARS** is set to **y.**

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

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



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

Figure 3: System-Parameters Customer-Options Form – Page 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? y                     ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                         ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                ISDN-PRI? y
              ESS Administration? y             Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? n        Multimedia Call Handling (Basic)? n
             Hospitality (Basic)? y     Multimedia Call Handling (Enhanced)? n
 Hospitality (G3V3 Enhancements)? y             Multimedia IP SIP Trunking? n
                       IP Trunks? y

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

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

©2012 Avaya Inc. All Rights Reserved.

5.2. Configure IP Node Names

The node names are mappings of names to IP addresses that can be used in various screens. The following command **change node-names ip** output shows the node-names used in this test configuration. The node name for Session Manager is **sm_60_19** with IP Address **10.64.60.19**. The node name and IP Address for the Processor Ethernet (procr) are **procr** and **10.64.60.13**. The procr is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
ipo_60_70           10.64.60.70
ipo_meta            198.147.226.94
msgserver           10.64.60.13
procr               10.64.60.13
procr6              ::
sm_60_19            10.64.60.19
```

Figure 5: IP Node Names – Page 1

5.3. IP-Network-Regions

Use the **list ip-interface all** command and note the **PROCR** interface address to be used for SIP trunks between the Communication Manager and the Session Manager.

```
list ip-interface all

                                IP INTERFACES


                                                                               Net
ON Type   Slot  Code/Sfx      Node Name/       Mask                        Rgn  VLAN
                              IP-Address/
                              Gateway Node
-- ------ ----- --------      ---------------  ----                        ---  ----
 y PROCR                      procr            /24                         1
                              10.64.60.13
                              10.64.60.1
```

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

©2012 Avaya Inc. All Rights Reserved.

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   2
                                  IP INTERFACES


                 Type: PROCR
                                                     Target socket load: 4800

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


                                 IPV4 PARAMETERS
             Node Name: procr                    IP Address: 10.64.60.13


           Subnet Mask: /24
```

Figure 9: IP-Interface IP-Network-Region Assignments – Page 1

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.

5.3.1. IP-Network-Region 1

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** if supported. This allows audio traffic to be sent directly between IP endpoints to reduce the use of media resources. During this compliance test they were set to **no**.
- 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  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: Compliance Testing
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 1              Inter-region IP-IP Direct Audio: no
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 10: IP Network Region 1 – Page 1

©2012 Avaya Inc. All Rights Reserved.

5.4. Configure IP Codec Set

The following screen shows the configuration for codec set to be used for local and external calls. In general, an **IP codec** set is a list of allowable codecs in priority order.
Use the **change ip-codec-set** command for the codec set specified in the **IP Network Region 1** form above. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability testing G.711MU, G.711A and various G.729 codes were used.

```
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: G.711A            n         2        20
 3: G.729A            n         2        20
 4: G.729B            n         2        20
```

Figure 6: IP Codec Set – Page 1

```
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 7: IP Codec Set – Page 2

©2012 Avaya Inc. All Rights Reserved.

5.5. Administer SIP Trunks with Avaya Aura® Session Manager

To administer a SIP Trunk on Communication Manager, three intermediate steps are required, creation of a signaling group, a trunk group for calls within the enterprise and a trunk group for calls to Metaswitch.

5.5.1. Add SIP Signaling Group for calls within the Enterprise

Use the **add signaling-group n** command, where **n** is an available **signaling group number**, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type**: **sip**
- **Transport Method**: **tls**
- **Near-end Node Name**: **procr**
- **Far-end Node Name**: **sm_60_19**
- **Near-end Listen Port**: **5061**
- **Far-end Listen Port**: **5061**
- **Far-end Domain**: **avaya.com** (The SIP domain in use within the enterprise)
- **DTMF over IP**: **rtp-payload** (This value enables Communication Manager to send DTMF transmissions using RFC 2833)

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

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



   Near-end Node Name: procr                 Far-end Node Name: sm_60_19
 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                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Figure 11: Internal calls SIP Trunk - Signaling Group 1

©2012 Avaya Inc. All Rights Reserved.

5.5.2. Add a SIP Trunk Group for calls within the Enterprise

Add the corresponding trunk group controlled by signaling group 1 via the add **trunk-group n command**, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type**: **sip**
- **Group Name**: **sm_60_19**
- **TAC**: ***001**
- **Service Type**: **tie**
- **Signaling Group**: **1 (**Signaling group added in **Section 5.5.1**)
- **Number of Members**: **10**
- **Numbering Format:** **private**

Note: The number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: sm_60_19                   COR: 1        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

Figure 12: Internal calls Trunk Group 1 – Page 1

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



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n



                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Figure 13: Internal calls Trunk Group 1 – Page 3

©2012 Avaya Inc. All Rights Reserved.

5.5.3. Add Signaling group for off-network calls

Use the **add signaling-group n command**, where **n** is an available **signaling group number**, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields

- **Group Type**: **sip**
- **Transport Method**: **tls**
- **Near-end Node Name**: **procr**
- **Far-end Node Name**: **sm_60_19**
- **Near-end Listen Port**: **5061**
- **Far-end Listen Port**: **5061**
- **Far-end Domain**: **blank**
- **DTMF over IP**: **rtp-payload** (This value enables Communication Manager to send DTMF transmissions using RFC 2833)

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

 Group Number: 9             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: sm_60_19
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

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

Figure 14: External calls SIP Trunk - Signaling Group 9

©2012 Avaya Inc. All Rights Reserved.

5.5.4. Add a SIP Trunk Group for off-network calls

Add the corresponding trunk group controlled by signaling group 9 via the add **trunk-group n** command, where **n** is an available **trunk group number** and fill in the indicated fields.

- **Group Type**: **sip**
- **Group Name**: **To Metaswitch**
- **TAC**: ***109**
- **Service Type**: **public-ntwrk**
- **Signaling Group**: **9** (Signaling group added in **Section 5.5.3)**
- **Number of Members**: **10**
- **Numbering Format** **public**

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

Group Number: 9                    Group Type: sip          CDR Reports: y
  Group Name: To Metaswitch              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
                                              Member Assignment Method: auto
                                                       Signaling Group: 9
                                                     Number of Members: 10
```

Figure 15: External calls Trunk 9 - Page 1

```
add trunk-group 9                                                   Page   3 of  21
TRUNK FEATURES
          ACA Assignment?              Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Figure 16: External calls Trunk 9 - Page 3

©2012 Avaya Inc. All Rights Reserved.

5.6. Configure Route Patterns

Configure two route patterns to correspond to the newly added SIP trunk groups Use **change route pattern n** command, where **n** is an available **route pattern**.

5.6.1. Route Pattern for Enterprise calls

- **Pattern Name -** A descriptive name (e.g., **to sip stations**)
- Set the **Grp No** field **- 1**. (The trunk group number from **Section 5.5.2**)
- Set the **FRL** field **- 0**.
- The default values for the other fields may be used.

```
change route-pattern 1                                           Page   1 of   3
                    Pattern Number: 1   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: 1    0                                                               n   usr
 2:                                                                      n   usr
```

Figure 17: Route Pattern for Enterprise calls – Page 1

5.6.2. Route Pattern for External calls to Metaswitch

- **Pattern Name -** A descriptive name (e.g., **Outbound-SM6019**)
- Set the **Grp No** field **- 9**. (The trunk group number from **Section 5.5.4**)
- Set the **FRL** field **- 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-SM6019
                             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   usr
 2:                                                                      n   usr
```

Figure 18: Route Pattern for External calls – Page 1

©2012 Avaya Inc. All Rights Reserved.

5.7. Configure Dial Plan

In the configuration below, the Avaya environment uses 5 digits to dial the local extensions. For outbound calls via SIP trunk to Metaswitch, the feature access code (fac) 9 is used to access the Automatic Route Selection (ARS) table. Use command **change dialplan analysis.**

- **Dial String** set to **9**
- **Total length** set to **1**
- **Call Type** set to f**ac**

```
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
   2           3   aar
   5           5   ext
   7           5   ext
   8           1   fac
   9           1   fac
   *           4   dac
```

Figure 19: Dial Plan – Page 1

5.8. Configure Uniform Dial Plan

Configure the uniform dial plan for **5** digit extensions to route using **aar**. Use command **change uniform-dialplan 0**.

- **Matching Pattern** set to **531**
- **Len** field set to **5**
- **Del** field, set to **0**
- **Net** field, enter **aar**
- **Conv** field set to **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
 5                5   0                  aar  n
```

Figure 20: Uniform Dial Plan – Page 1

©2012 Avaya Inc. All Rights Reserved.

5.9. Public Unknown Numbering

Use the **change public-unknown-numbering 0** command to assign number presented by Communication Manager when call is leaving to Session Manager to reach to Metaswitch.

Add an entry each extensions. Enter the following values for the specified fields.

- **Ext Len -** Number of digits of the station (e.g., **5**).
- **Ext. Code -** Digits in the station number (e.g., **50001**).
- **Trk Group -** Trunk number configured to reach Metaswitch as in **Section 5.5.4** (e.g., **9**).
- **CPN Prefix -** Configure according to the DIDs provided by Metaswitch
- **Total CPN Len -** Number of digits (e.g., **10**).

```
change public-unknown-numbering 0                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 11
 5  5                                       5        Maximum Entries: 240
 5  7             1                         5
 5  599                                     5     Note: If an entry applies to
 5  50001         9         6049020173      10    a SIP connection to Avaya
 5  50002         9         6049020177      10    Aura(tm) Session Manager,
 5  50101         9         6049020170      10    the resulting number must
 5  52101         9         6049020174      10    be a complete E.164 number.
 5  53102         9         6049020175      10
 5  53202         9         6049020176      10
 5  54000         9         6049020178      10
 5  54101         9         6049020179      10
```

Figure 21: Public Unknown Numbering – Page 1

©2012 Avaya Inc. All Rights Reserved.

5.10. Change Feature Access Codes

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  10
                              FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *108   All: *107   Deactivation: *106
   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 22: Feature Access Codes – Page 1

©2012 Avaya Inc. All Rights Reserved.

5.11. Administer ARS Analysis

The Automatic Route Selection feature is used to route calls via a SIP trunk, configured in **Section 5.5.4**, to Session Manager, which in turn completes the calls to the Metaswitch. In the reference configuration, ARS is triggered by dialing a 9 in feature access code or FAC (from **Section 5.10**) and then dialing the called number. ARS matches on the called number and sends the call to a specified route pattern. Enter the following values for the specified fields. Use the command **change ars analysis**.

- **Dialed String** field to **1604**.
- **Total Min** field to **11**.
- **Total Max** field to **11**.
- **Route Pattern** field to **9** (will direct to off network calls trunk).
- **Type** field to **fnpa**.

```
change ars analysis 1604                                       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
    1604                  11   11     9        fnpa         n
```

Figure 23: ARS Analysis – Page 1

5.12. Administer AAR Analysis

The Automatic Alternate Routing feature is used to route calls to the SIP trunk, configured in **Section 5.5.2**, 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. Use the command **change aar analysis**.

- **Dialed String** field to **501**, **521** and 5**31** (added for local extensions)
- **Total Min** field to **5**.
- **Total Max** field to **5**.
- **Route Pattern** field to **1**
- **Call Type** field to **aar**.

```
change aar analysis 5                                          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
    501                   5    5      1        aar          n
    521                   5    5      1        aar          n
    531                   5    5      1        aar          n
    59997                 5    5      99       aar          n
```

Figure 24: AAR Analysis – Page 1

©2012 Avaya Inc. All Rights Reserved.

5.13. Avaya Aura® Communication Manager Stations (non-SIP)

The figures below show an example of an extension (Avaya H.323 IP phone). Since the phone is an IP device, a virtual port is automatically assigned by the system. Use the command **add station n**, where **n** is 50001 in the example below.

- Set the **Type** field to match the station type (e.g., **9640**)
- Set the **Name** field to a desired value
- Set the **Security Code** (optional) to a desired value

```
add station 50001                                            Page   1 of   5
                                     STATION

Extension: 50001                         Lock Messages? n             BCC: 0
     Type: 9640                          Security Code: 123456         TN: 1
     Port: S00003                      Coverage Path 1: 99            COR: 1
     Name: 50001, station              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: 50001
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                         IP Video? n
                              Short/Prefixed Registration Allowed: default

                                               Customizable Labels? y
```

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

©2012 Avaya Inc. All Rights Reserved.

By default, three call appearances are defined 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.

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

```
add station 50001                                          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                       5:
 2: call-appr                       6:
 3: ec500      Timer? n             7:
 4: extnd-call                      8:

    voice-mail
```

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

©2012 Avaya Inc. All Rights Reserved.

5.14. 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. 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.

- Station Extension: **This field will automatically populate.**
- Application: **EC500**.
- Phone Number: **16049020162 (**phone number that will also be called)
- Trunk Selection: **9 (**to route the call over trunk 9).
- Config Set: **1**
- Use the default values for all other fields.

```
change off-pbx-telephone station-mapping 50001                  Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 50001            EC500        -     16049020162       ars        1
```

Figure 27: EC500 Station Mapping- Page 1

5.15. Saving Avaya Aura® Communication Manager Translations

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

©2012 Avaya Inc. All Rights Reserved.

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

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

- **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.

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

©2012 Avaya Inc. All Rights Reserved.

6.1. Logging into System Manager

Session Manager is managed via System Manager. Using a web browser, access https://<ip-addr of System Manager>/SMGR. In the Log On screen, enter appropriate User ID and Password and press the Log On button

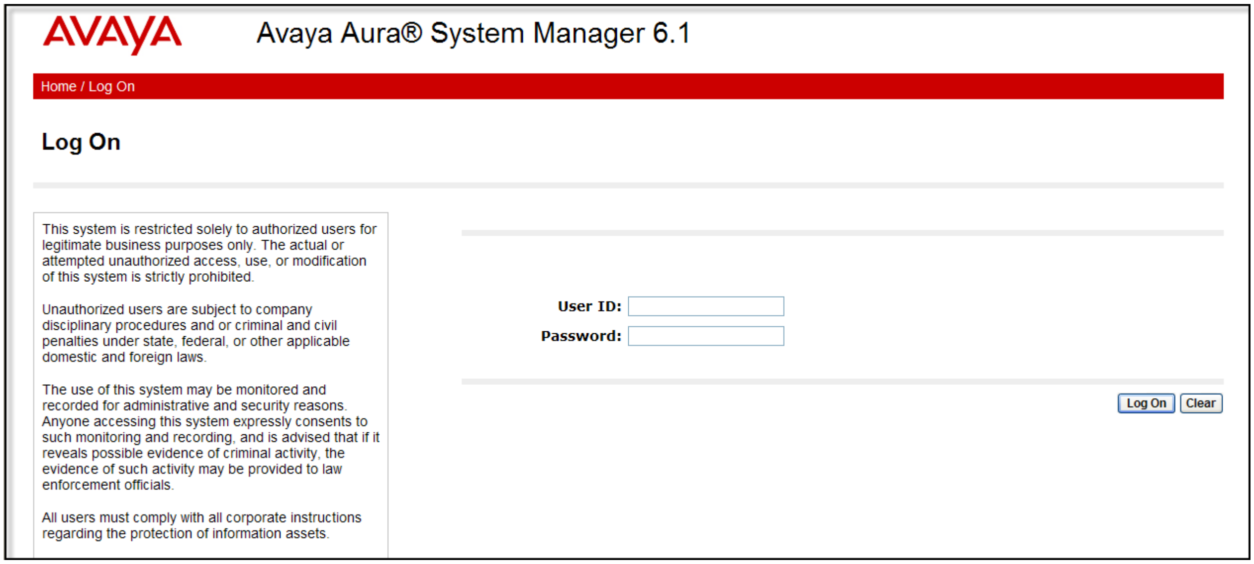

Figure 28: System Manager GUI Log On Screen

Once logged in, the Home Screen will display as shown below.

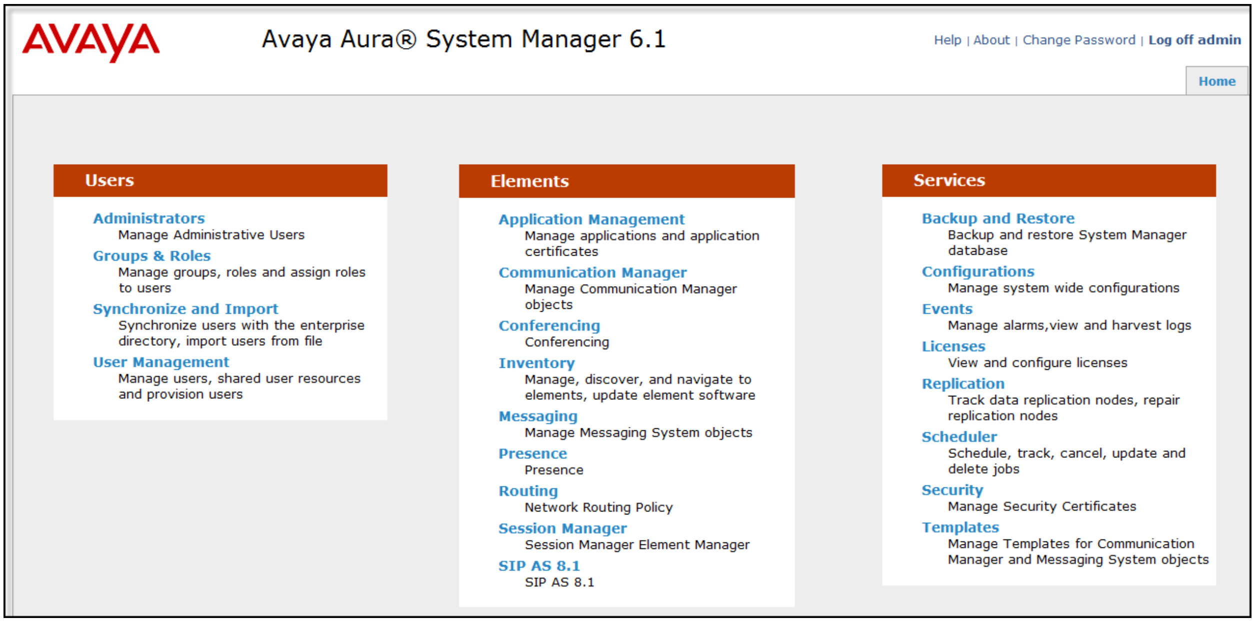

Figure 29: System Manger Home Screen

©2012 Avaya Inc. All Rights Reserved.

6.2. Network Routing Policy

Select **Routing** from the Home Screen. This will take you into **Network Routing Policy** which consists of several different routing applications.

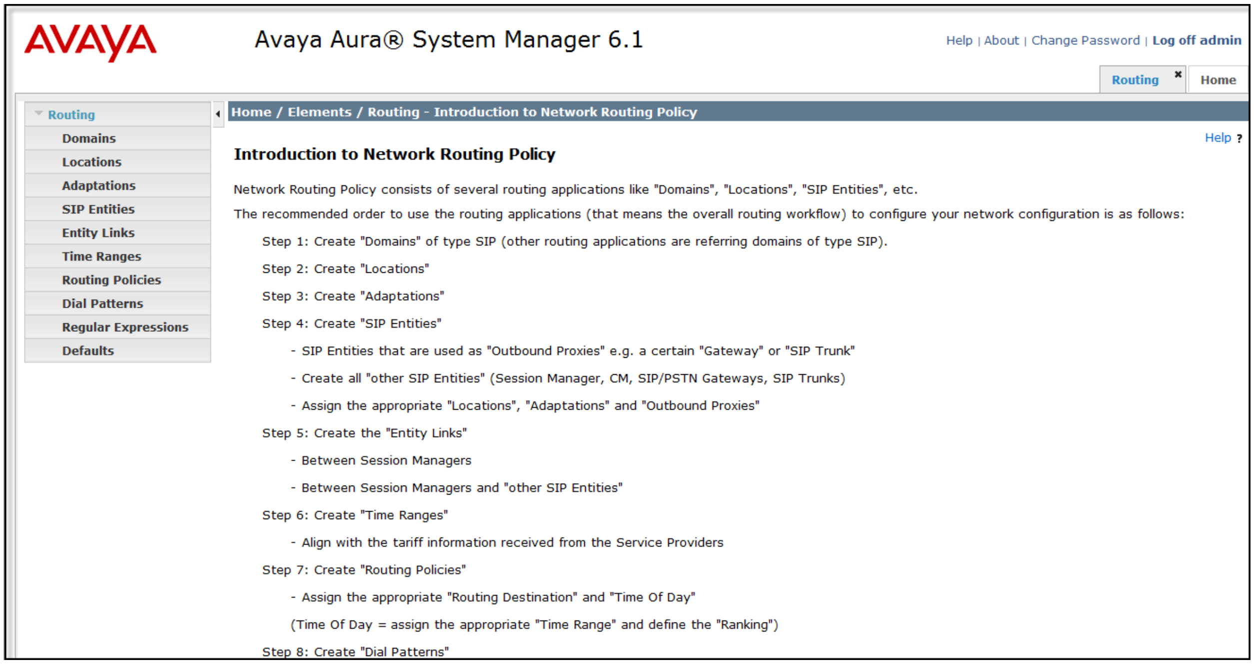

Figure 30: Network Routing Policy Menu

6.2.1. SIP Domains

In the reference configuration, one SIP domain was used; **avaya.com**.
To add SIP domains that will be used with Session Manager, select **Domains** →**New** to add a new SIP domain entry

- Enter the SIP Domain (**avaya.com**) in the **Name** field.
- Enter a description in the **Notes** field if desired.
- Click on the **Commit** button.

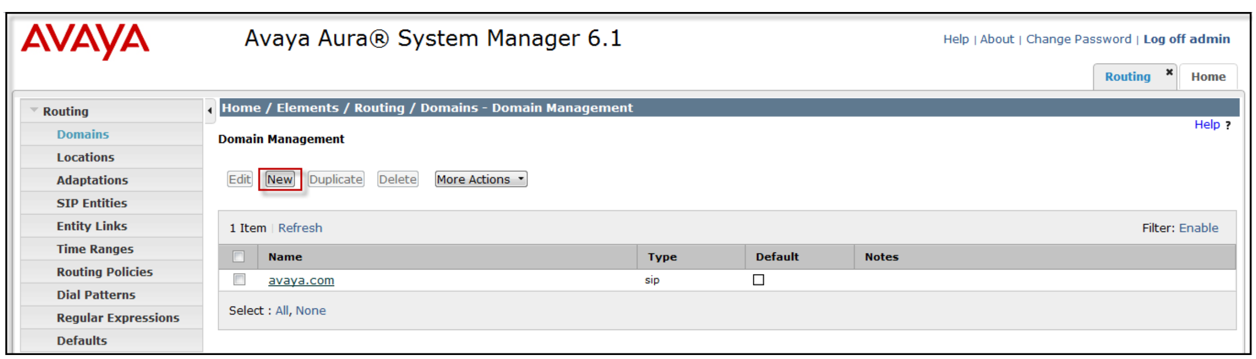

Figure 31: SIP Domain Menu

©2012 Avaya Inc. All Rights Reserved.

6.2.2. 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, menu and click on the **New** button on the right.

- Enter a descriptive Location name in the **Name** field (ie. **sub_60**).
- Enter a description in the **Notes** field if desired.
- Under the **Location Pattern** heading, click on **Add.**
- Enter the IP address information for the Location (e.g., **10.64.60.***)
- Enter a description in the **Notes** field if desired.
- Repeat steps 3 through 5 if the Location has multiple IP segments.
- Modify the remaining values on the form, if necessary; otherwise, use all the default values.
- Click on the **Commit** button.
- Repeat all the steps for each new Location.

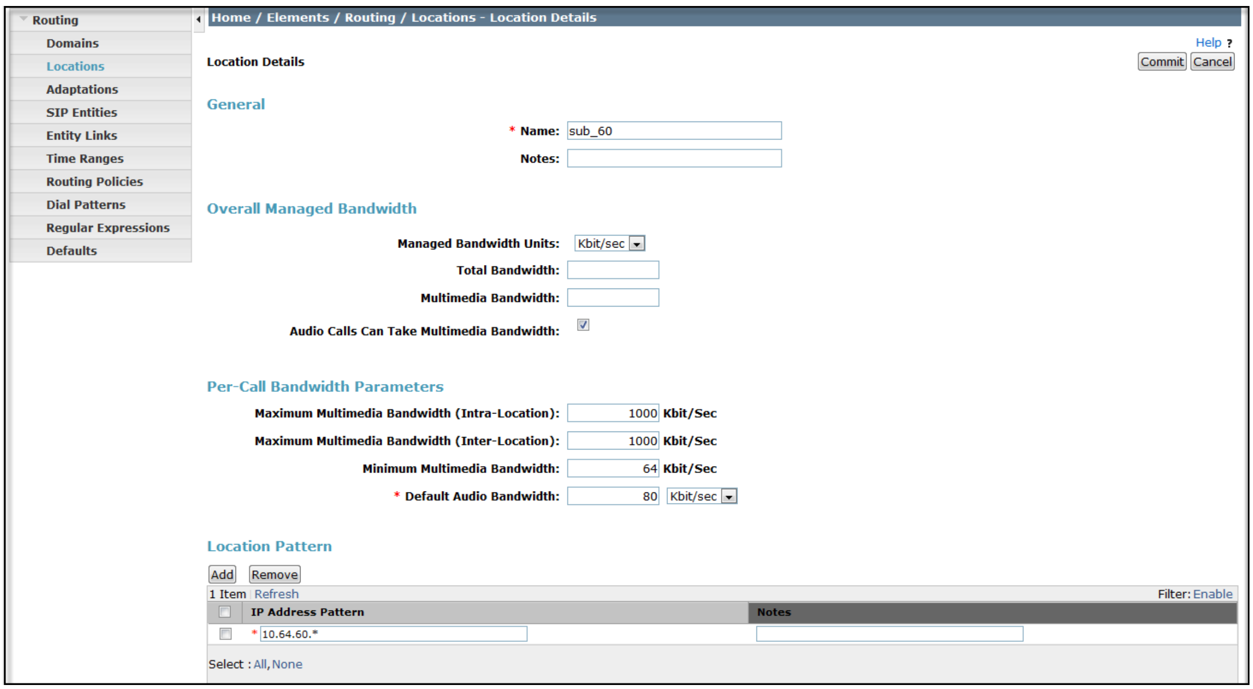

Figure 32: Locations Menu

©2012 Avaya Inc. All Rights Reserved.

6.2.3. 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

6.2.3.1 Digit Conversion

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

Select **Adaptation** on the left, then **New** on the right.

- Enter a descriptive name (e.g., **Metaswitch**).
- Specify **DigitConversionAdapte**r in the **Adaptation Module** field.
- **Set Module parameter** to the domain of **sbc-whistler.metaswitch.com** (provided by Metaswitch). The reference configuration required that domain contained in the Request URI to be replaced with sbc-whistler.metaswitch.com before being sent out to Metaswitch via the Acme Packet.
- 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 incoming calls, the Metaswitch DIDs are converted to Communication Manager to extensions via this adaptor in the **Digit Conversion for Incoming Calls to SM** section. Click the **Add** button.

- **Matching Pattern –** The digit string to match DID provided by Metaswitch (e.g., **6049020170**)
- **Min –** The minimum number of digits set to **10**
- **Max –** The maximum number of digits set to **10**
- **Delete Digits –** The number of digits to delete set to **10**
- **Insert Digits –** The 5 digit extension (e.g., **50101**)
- **Address to Modify** - Associated headers to be monitored for matching digits set to **destination**.
- **Notes -** Enter a description in the Notes field if desired
- Click the **Commit** button.

©2012 Avaya Inc. All Rights Reserved.

For outgoing calls to Metaswitch, the calls were going out +10-digit DID. Metaswitch wanted the + removed. This was accomplished in the **Digit Conversion for Outgoing calls from SM** section. Click the **Add** button.

- **Matching Pattern** – The digit string to match (e.g., **+6049020170**)
- **Min** – The minimum number of digits set to **11**
- **Max** – The maximum number of digits set to **11**
- **Delete Digits** – The number of digits to delete set to **1**
- **Insert Digits** – The DID provided by Metaswitch (e.g., **6049020170**)
- **Address to Modify -** Associated headers to be monitored for matching digits set to **both**.
- **Notes -** Enter a description in the Notes field if desired
- Click the **Commit** button.

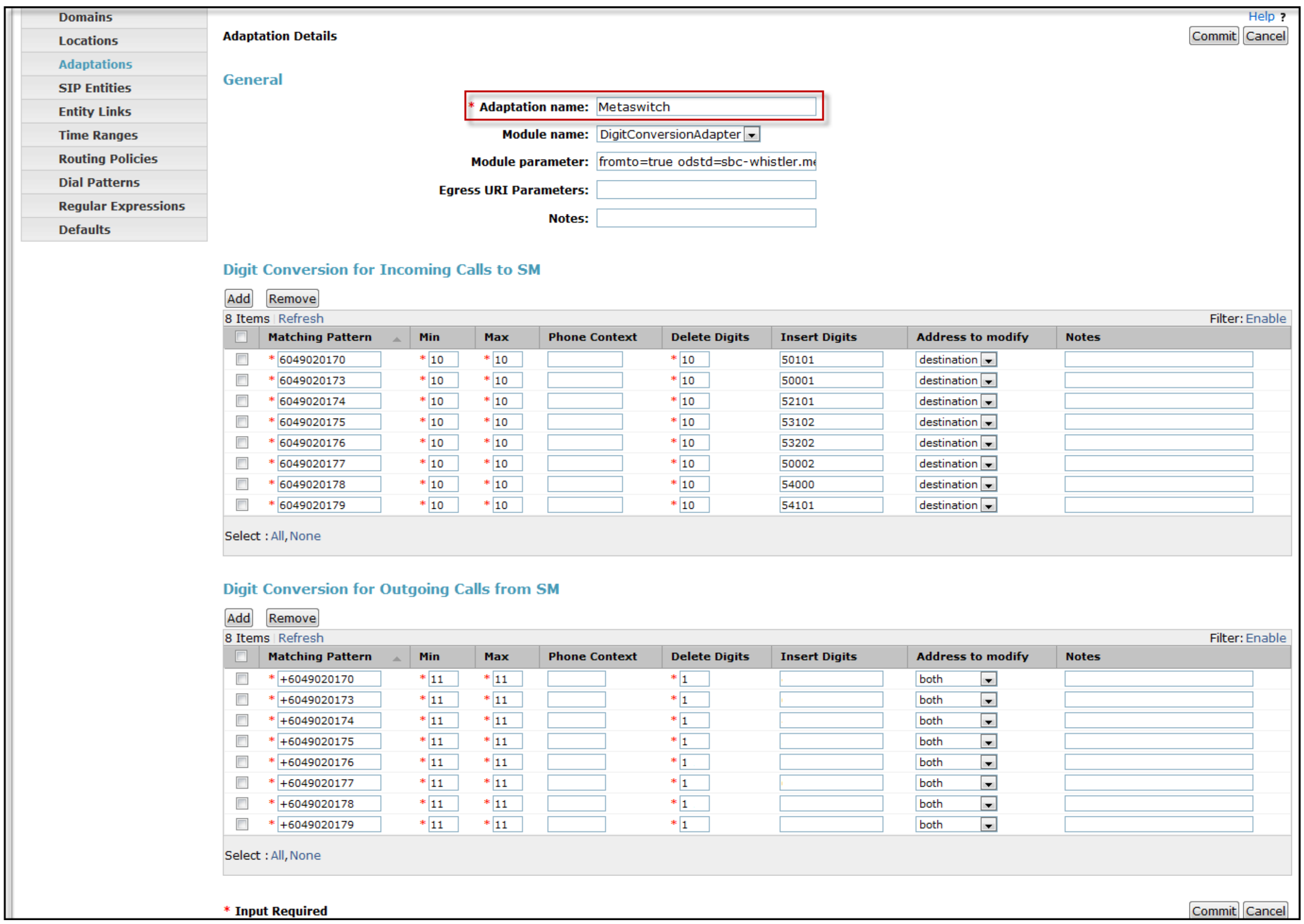

Figure 33: Adapation/Digit Conversion

©2012 Avaya Inc. All Rights Reserved.

6.2.4. 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 there are three SIP Entities:

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

To add a SIP Entity, select **SIP Entities** on the left and **New** button on the right.

Section **General**:

- **Name** field- Enter an descriptive name
- **FQDN or IP Address** field - Enter the IP address of the SIP Entity
- **Type -** Select best match for the SIP entity (e.g., Session Manager)
- **Location -** Select the appropriate location (Configured in **Section 6.2.2**) from the drop down menu (e.g., **sub_60)**
- **Time Zone** field - Enter the time zone for the SIP Entity
- **Adaptation** – Select adaptation if one is required for the SIP Entity. (For the ACME SIP Entity select Metaswitch configured in Section **6.2.3**)

Section **SIP Link Monitoring**:

- Select desired option

Section **Ports**:

When defining a SIP Entity for Session Manager 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 6.2.1** for the **Default Domain**.
- Repeat step 3 for each Port to be configured.

©2012 Avaya Inc. All Rights Reserved.

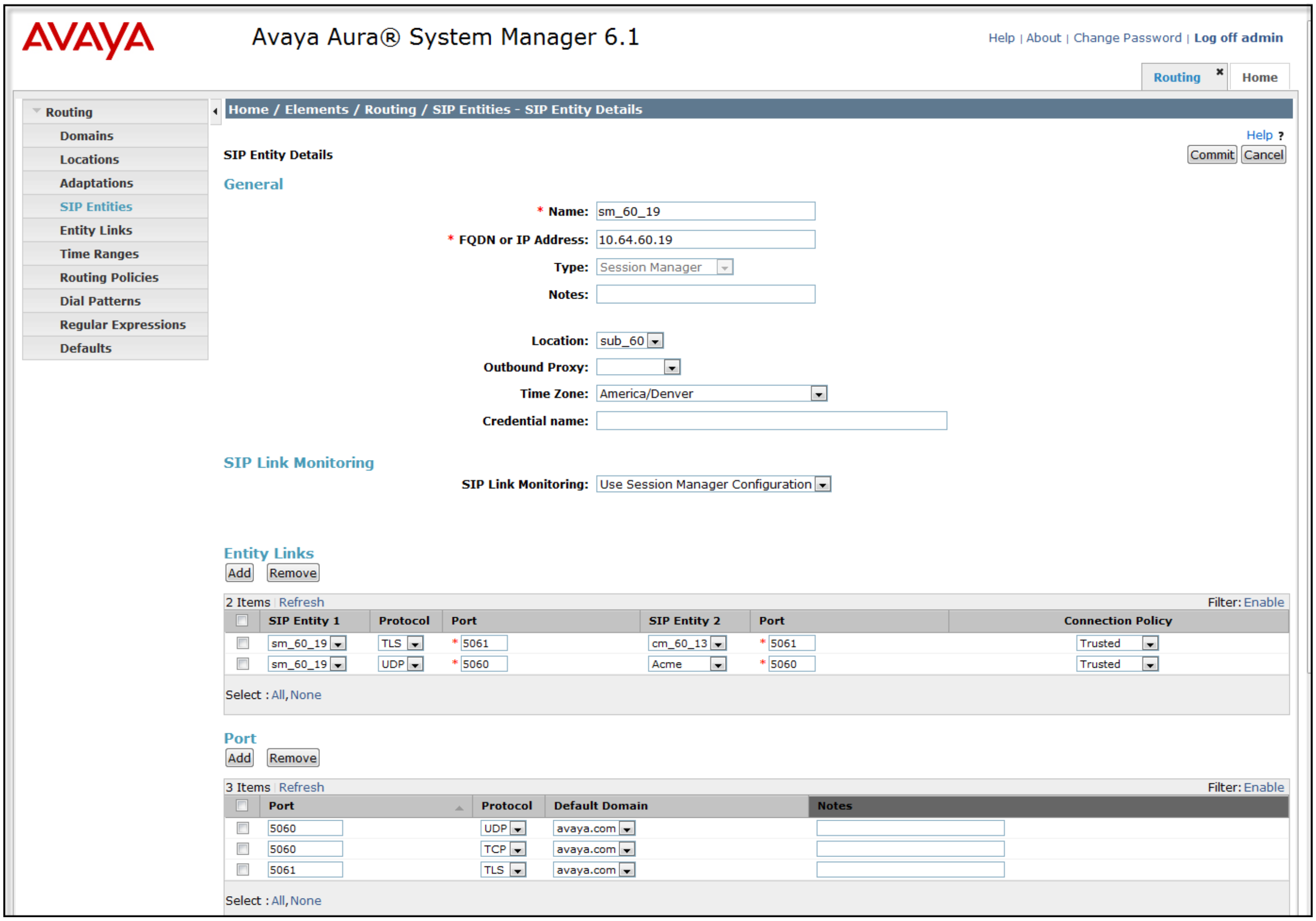

Figure 34: Session Manager SIP Entity Details

The following SIP Entity values were specified in the reference configuration

Name	IP Address	Type	Adaptation	Location	Port	Protocol	Default Domain
Communication Manager (cm_60_13)	10.64.60.13	CM	_	sub_60	-	-	-
ACME Packet (Acme)	10.64.60.205	Other	Metaswitch	sub_60	-	-	-
Session Manager (sm_60_19)	10.64.60.19	Session Manager	_	sub_60	5060 5060 5061	UDP TCP TLS	avaya.com

Table 2: SIP Entities Provisioning

©2012 Avaya Inc. All Rights Reserved.

6.2.5. Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Routing** → **Entity Links**. Click the **New** button to add a link for:

- Communication Manager
- ACME Packet

Fill the following fields out:

- **Name -** Enter an descriptive name
- **SIP Entity 1 -** Select the SIP Entity for Session Manager.
- **Protocol -** Select the transport protocol used for this link.
- **Port -** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the Far-end Listen Port defined on the Communication Manager signaling group.
- **SIP Entity 2**: Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined.
- **Port -** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the Near-end Listen Port defined on the Communication Manager signaling group.
- **Trusted -** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity will be denied.
- Click the **Commit** button

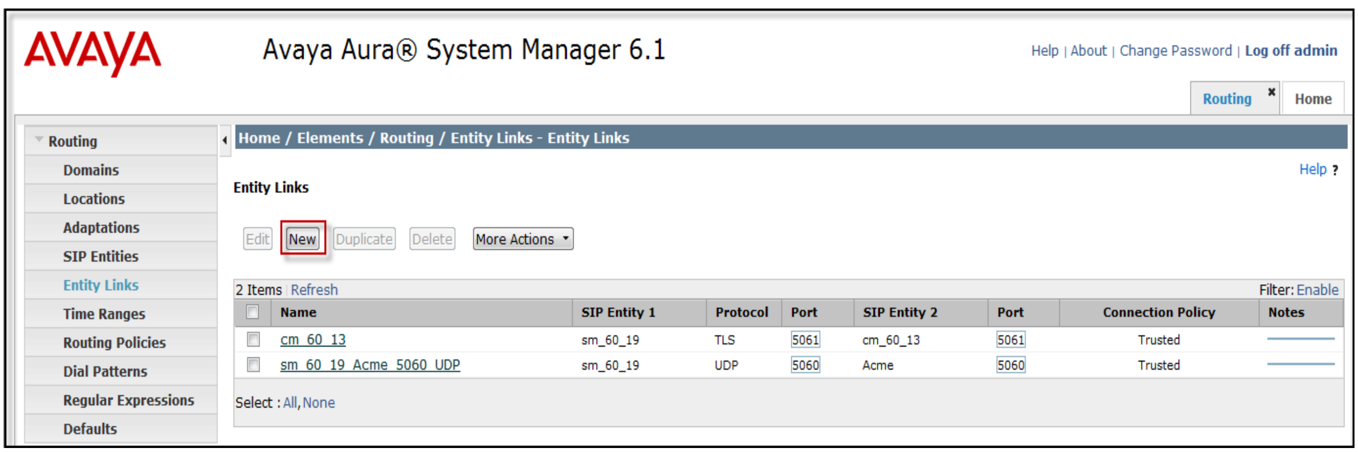

Figure 35: Entity Links

©2012 Avaya Inc. All Rights Reserved.

6.2.6. Time Ranges

The **Time Ranges** form allows admission control criteria to be specified for **Routing Policies** (**Section 6.2.7**). In the reference configuration, no restrictions were used.

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

- **Name -** Enter an descriptive name
- Check each day of the week.
- **Start Time -** enter 00:00.
- **End Time -** enter 23:59.
- **Notes** - Enter a description if desired.
- Click the **Commit** button.

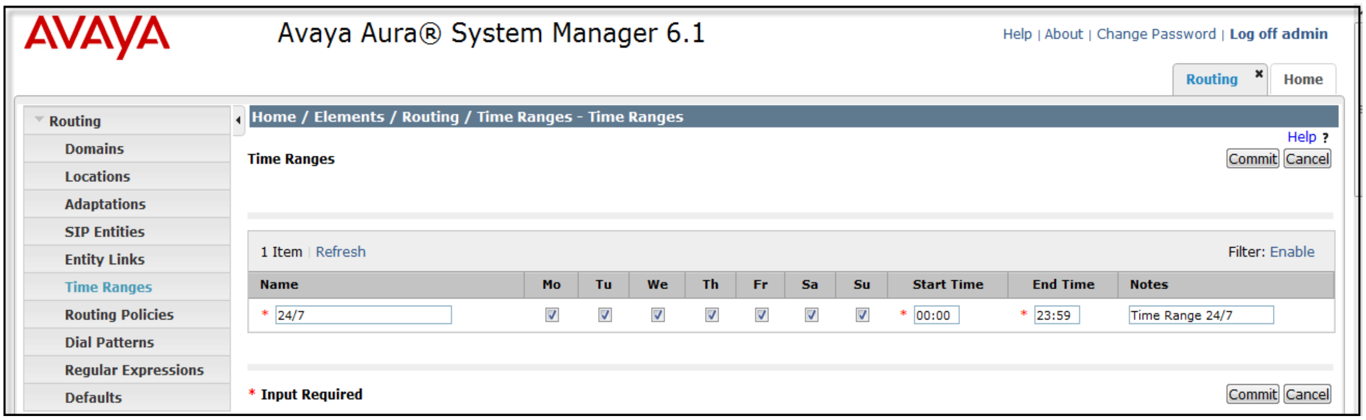

Figure 36: Time Ranges

6.2.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.2.4**. To add a routing policy, navigate **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

Two routing policies must be added:

- Inbound calls to Communication Manager
- Outbound calls to the Metaswitch network (ACME Packet)

Name	SIP Entity as Destination	Time Of Day	Dial Pattern(s)	Notes
Communication Manager (cm_60_13)	cm_60_13	24/7	5xxxx	Any call to a 5 digit extension beginning with 5 will be routed to Communication

©2012 Avaya Inc. All Rights Reserved.

				Manager
ACME Packet (To_Acme)	Acme	24/7	604xxxxxxx	Any call to a 10 digit number beginning with 604 will be routed to Acme Packet

Table 3: Routing Policies

Section **General:**

- **Name** field- Enter an descriptive name
- **Notes** field – Add a brief description (optional)

Section **SIP Entity as Destination:**

- Click Select, and then select the appropriate **SIP Entity** to which this routing policy applies

Section **Time of Day:**

- Click **Add**, and select the time range configured from **Section 6.2.6**.

Defaults can be used for the remaining fields. Click **Commit** to save each **Routing Policy** definition.

The following screens show the Routing Policy for Communication Manager and ACME.

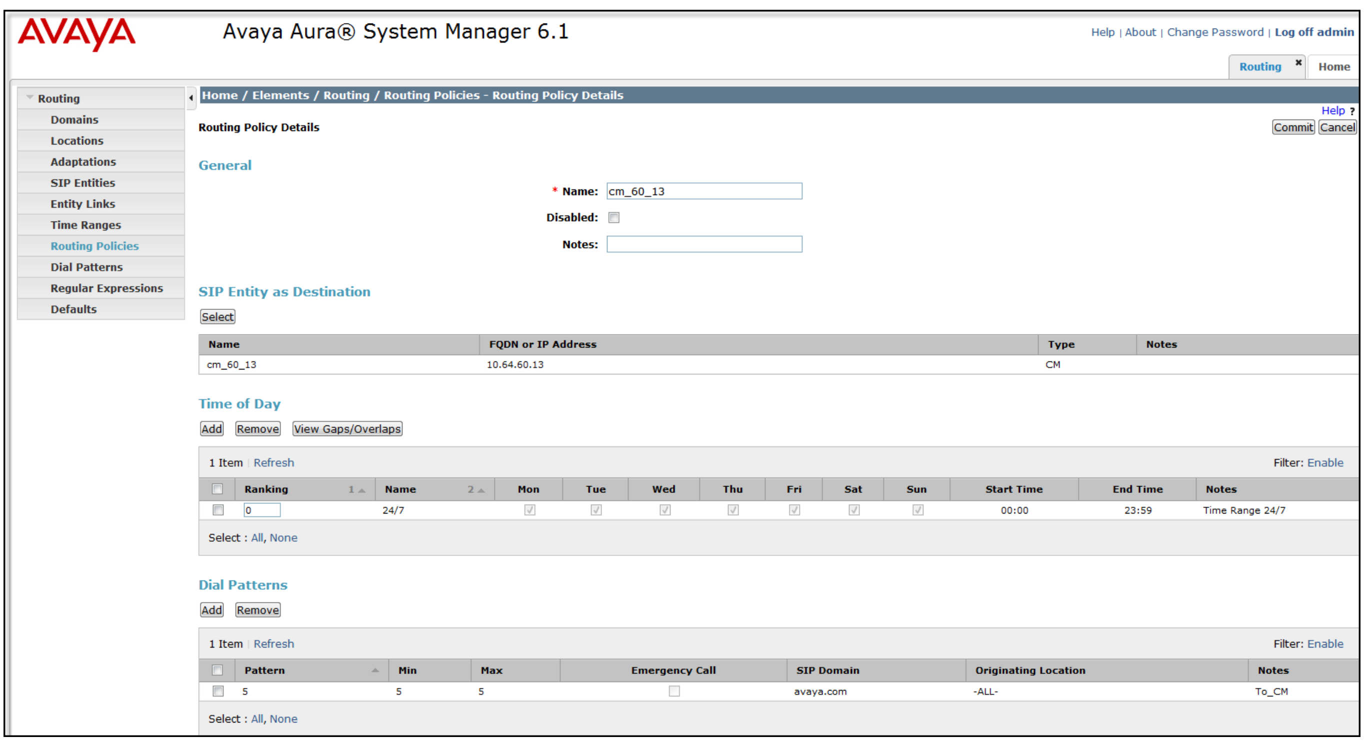

Figure 37: Routing Policy for Communication Manager

©2012 Avaya Inc. All Rights Reserved.

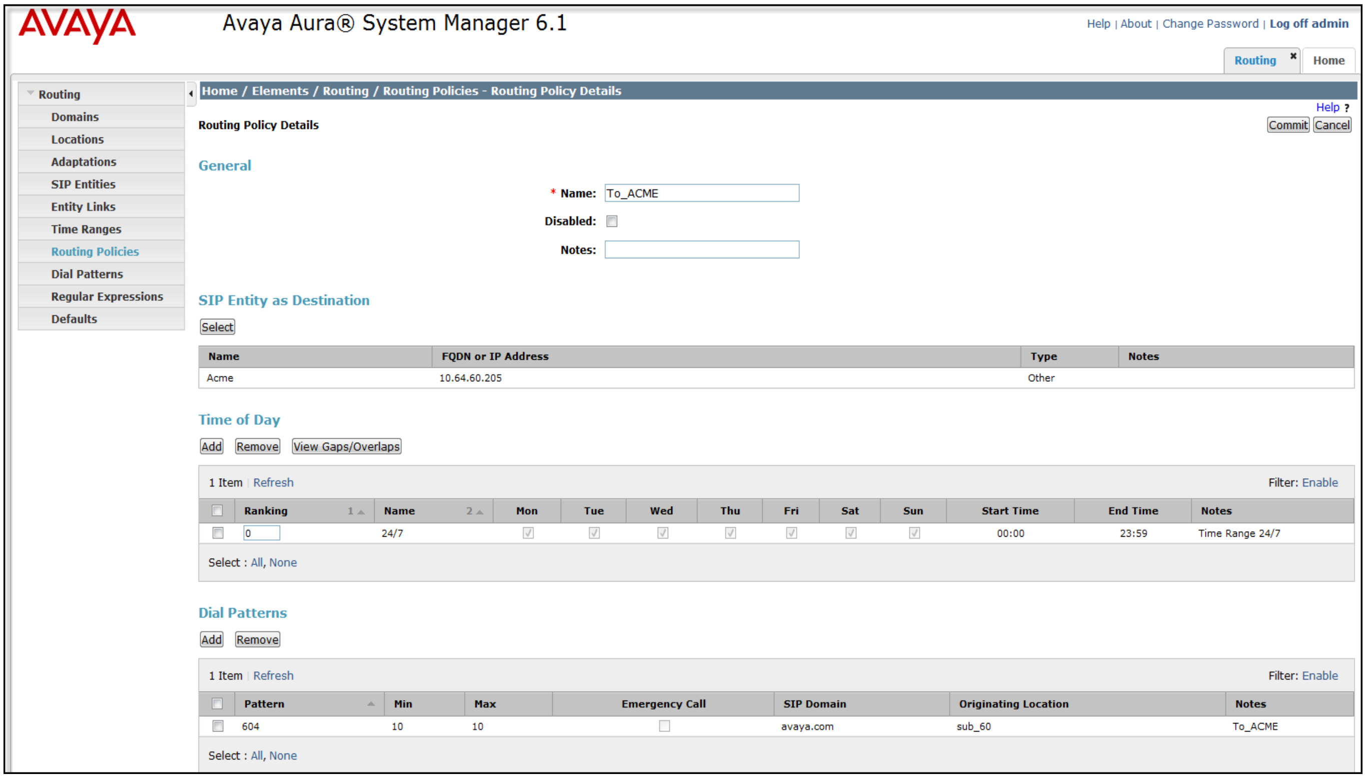

Figure 38: Routing Policy for ACME (Metaswitch)

6.2.8. Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the configuration below, 5-digit extensions beginning with **5** reside on Communication Manager and numbers beginning with **604** with 10-digits reside on Metaswitch.

.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown). Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Acme that in turn will be forwarded to Metaswitch's CFS:

Section **General**:

- **Pattern -** Dialed number or prefix
- **Min -** Minimum length of dialed number
- **Max -** Maximum length of dialed number
- **SIP Domain -** Select **avaya.com**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.

This example shows example shows that 5-digit dialed numbers that begin with **5** originating from location **Any Location** uses routing policy **cm_60_13**.

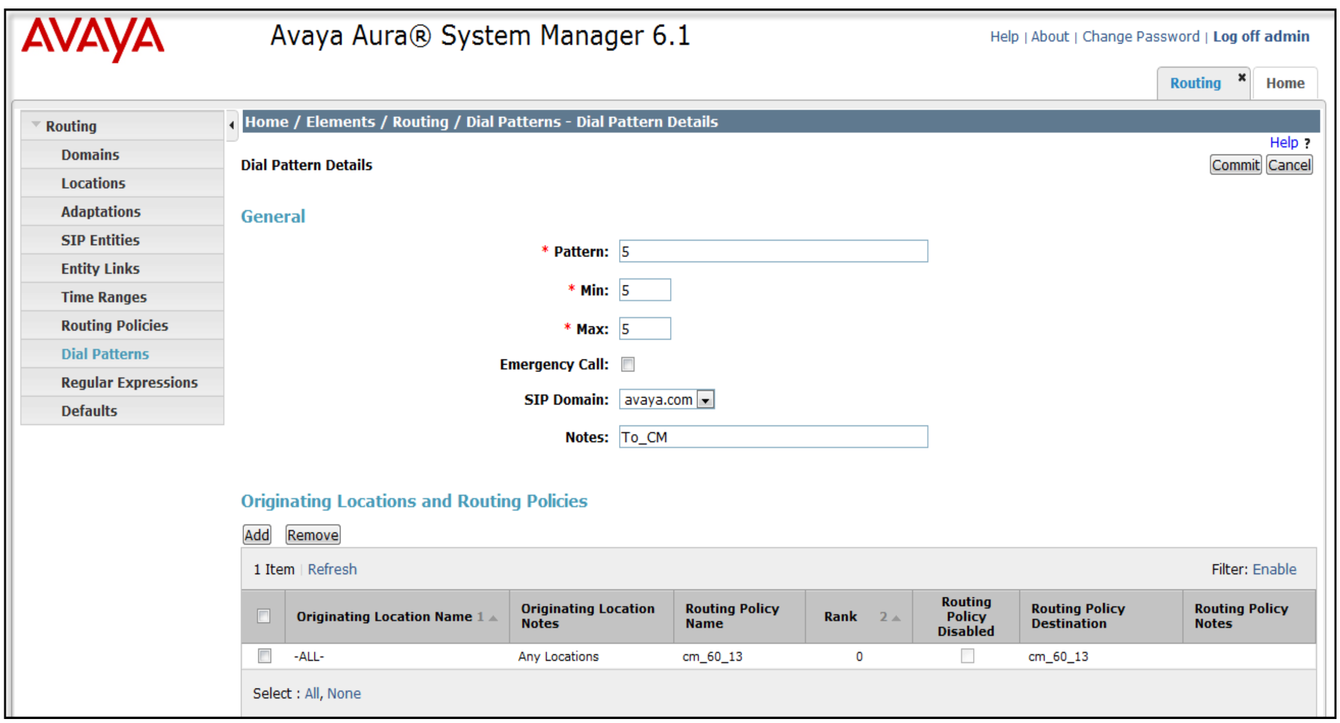

Figure 39: Dial Pattern 5-digit extentions

©2012 Avaya Inc. All Rights Reserved.

This example shows example shows that 10-digit dialed numbers that begin with **604** originating from location **sub_60,** uses routing policy **To_ACME**.

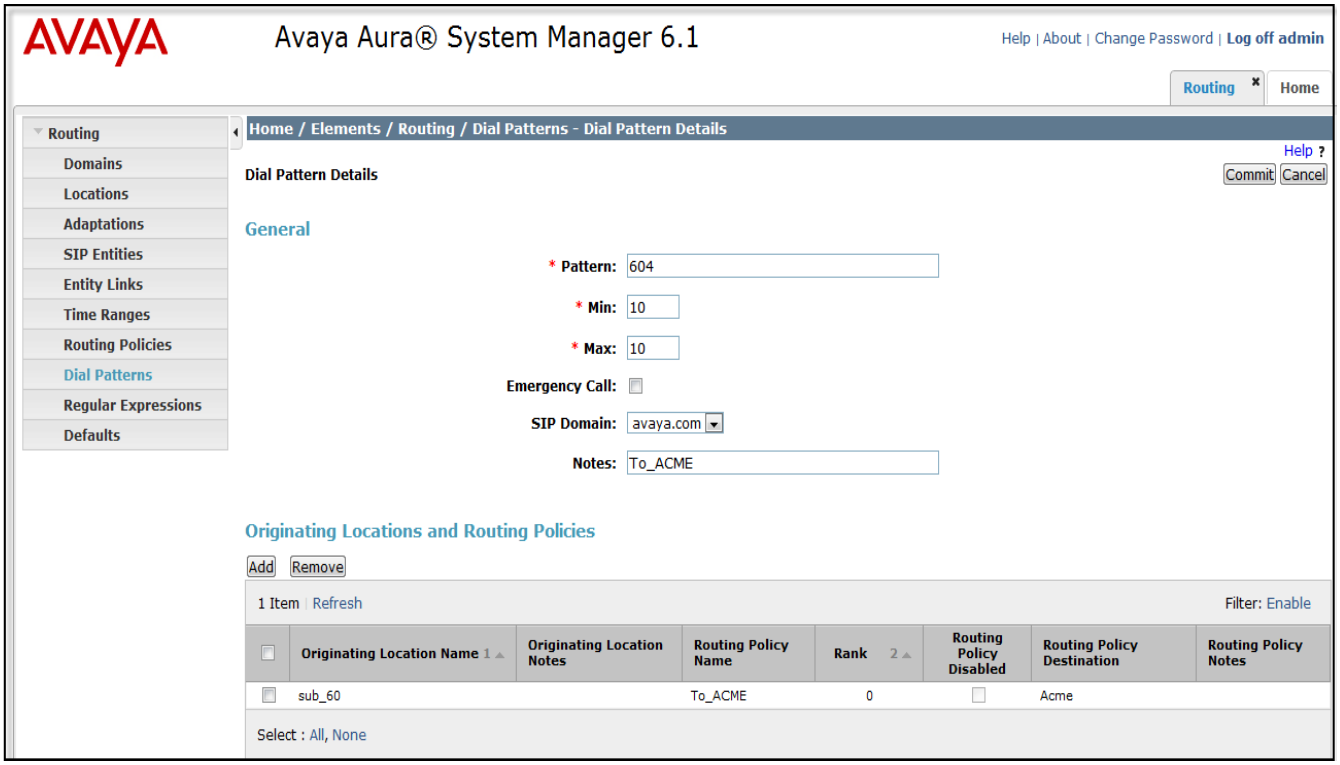

Figure 40: Dial Pattern 604 route to Metaswitch

6.3. Add/View Avaya Aura® Session Manager

To complete the Session Manager configuration, add a Session Manager instance. To add a Session Manager, navigate to **Elements** → **Session Manager** → **Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

Section **General:**

- **SIP Entity Name -** Select the name of the SIP Entity added for Session Manager
- **Description -** Descriptive comment (optional)
- **Management Access Point Host Name/IP -** Enter the IP address of the Session Manager management interface

©2012 Avaya Inc. All Rights Reserved.

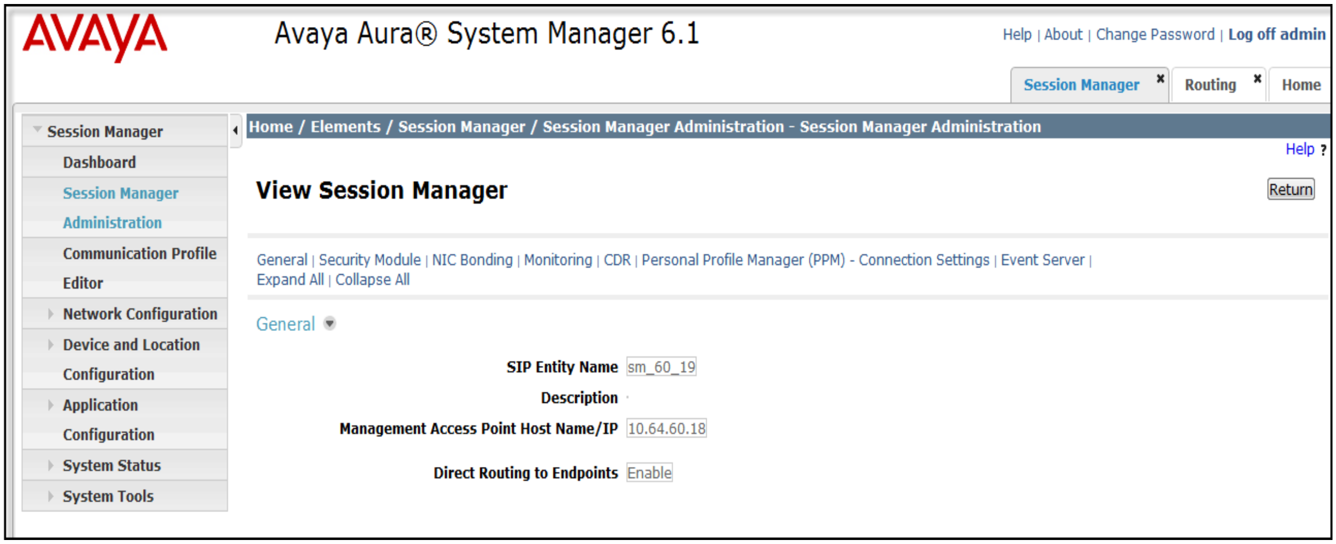

Figure 41: Session Manager Administration

Section **Security Module**

- **SIP Entity IP Address -** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask** - Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway -** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.

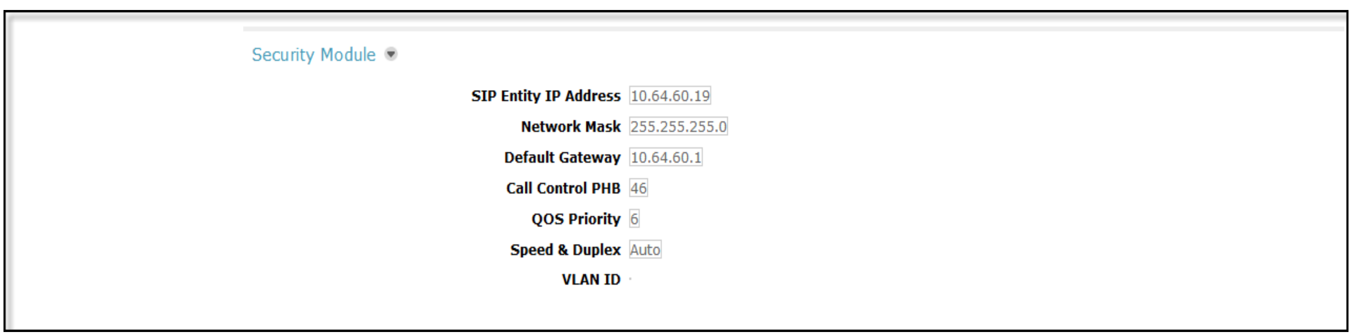

Figure 42: Session Manager Security Module

©2012 Avaya Inc. All Rights Reserved.

7. Acme Packet 3800 Net-Net Session Director

This section describes the configuration of the Acme Packet Net-Net 3800 necessary for interoperability with the Avaya Communication Manager and Metaswitch systems. The Net-Net 3800 was configured via the Acme Packet Command Line Interface (ACLI). In this testing, according to the configuration reference in **Figure 1**, the Avaya elements reside on the Private side and Metaswitch elements reside on the Public side of the network

7.1. Acme Packet Provisioning

The Acme Packet Session Director is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements

.

1. Access the console port of the Acme Packet Session Director using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the Session Director for cable connection). Use the following settings for the serial port on the PC.
   - Bits per second: 115200
   - Data bits: 8
   - Parity : None
   - Stop bits: 1
   - Flow control: None
2. Log in to the Acme Packet Session Director with appropriate credentials.
3. Enable the Superuser mode by entering the **enable** command and then the superuser password. The command prompt will change to include a "#" instead of a ">" while in Superuser mode. This level of system access (e.g.,. at the "acmesystem#" prompt) will be referred to as the **main** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific elements and specific parameters of those elements.
4. In Superuser mode, enter command **configure terminal**. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the **configuration** level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., name **s0p0**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all the elements.
11. Enter exit to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration

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

7.1.1. System Configuration

The system configuration defines system-wide parameters for the Acme Packet Session Director. Configure **system → system-config.** The key system configuration (**system-config**) fields are:

- **hostname -** Set the primary hostname used to identify the system. This parameter is used for information purposes.
- **description -** Enter a textual description of the system. This parameter is used for informational purposes. (e.g., **acmesbc**)
- **location -**Set a location description field for your system. This parameter is used for informational purposes. For example, you could include the site name and address of the location where the Net-Net system chassis is located.
- **default-gateway** -Set the default gateway for this SBC. This is the egress gateway for traffic without an explicit destination. The application of your Net-Net SBC determines the configuration of this parameter. (e.g.,192.168.62.1)

```
system-config
        hostname                        acmesbc
        description
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                    enabled
        enable-snmp-auth-traps          disabled
        enable-snmp-syslog-notify       disabled


        < text removed for brevity >

        call-trace                      enabled
        internal-trace                  enabled
        log-filter                      all
        default-gateway                 192.168.62.1
        restart                         enabled
        exceptions
        telnet-timeout                  0
        console-timeout                 0
        remote-control                  enabled
```

Figure 43: Acme System Config

7.1.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface **slot 0 / port 0** of the SBC was connected to the external un-trusted network. Ethernet **slot 0 / port 1** was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.
Configure **system → phy-interface.** The key physical interface (phy-interface) fields are:

- **name -** A descriptive string used to reference the Ethernet interface.
- **operation-type -** Media indicates both signaling and media packets are sent on this
- interface.

©2012 Avaya Inc. All Rights Reserved.

- **slot / port -** The identifier of the specific Ethernet interface used.

```
phy-interface
        name                           s0p0
        operation-type                 Media
        port                           0
        slot                           0
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        overload-protection            disabled

phy-interface
        name                           s0p1
        operation-type                 Media
        port                           1
        slot                           0
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        overload-protection            disabled
```

Figure 44: Acme Physical Interface

Configure **system → network-interface.** The key network interface (**network-interface**) fields are:

- **name -** Set the name for the network interface. This must be the same name as
- the physical interface (defined previously) to which it corresponds.
- **ip-address -** The IP address on the interface connected to the network on which the Metaswitch SIP trunk service resides. In the compliance test, the IP address **192.168.62.25** was assigned to the **public interface** and **10.64.60.205** was assigned to the private interface
- **netmask -** Subnet mask for the IP subnet
- **gateway -** Set the gateway that this network interface uses to communicate with the next hop
- **hip-ip-list -** Set all possible address on which you want the Net-Net SBC to accept administrative traffic. For compliance testing hip-ip was added only on the private network-interface.
- **icmp-address -** The list of IP addresses to which the Acme Packet Session Director will answer ICMP requests on this interface
- **ssh-address –** Set the address where port 22 is open for access. Only the private network-interface was configured for ssh access for the compliance test.

©2012 Avaya Inc. All Rights Reserved.

```
network-interface
        name                          s0p0
        sub-port-id                   0
        description
        hostname
        ip-address                    192.168.62.25
        pri-utility-addr
        sec-utility-addr
        netmask                       255.255.255.128
        gateway                       192.168.62.1
        sec-gateway

      < text removed for brevity >

        dns-domain
        dns-timeout                   11
        hip-ip-list
        ftp-address
        icmp-address                  192.168.62.25        snmp-address
        telnet-address
        ssh-address
```

Figure 45: Network Interface – Public

```
network-interface
        name                          s0p1
        sub-port-id                   0
        description
        hostname
        ip-address                    10.64.60.205
        pri-utility-addr
        sec-utility-addr
        netmask                       255.255.255.0
        gateway                       10.64.60.1
        sec-gateway

      < text removed for brevity >

        dns-domain
        dns-timeout                   11
        hip-ip-list                   10.64.60.205
        ftp-address                   10.64.60.205
        icmp-address                  10.64.60.205
        snmp-address
        telnet-address
        ssh-address                   10.64.60.205
```

Figure 46: Network Interface - Private

©2012 Avaya Inc. All Rights Reserved.

7.1.3. Realm

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces as well as applying header manipulation. Two realms were defined for the compliance test. The **EXTERNAL** realm was defined for the external network and the **INTERNAL** realm was defined for the internal network.

Configure **media-manager → realm-config**. The key realm (**realm-config**) fields are:

- **identifier -** A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces -** The network interfaces located in this realm.
- **out-manipulationid -** NAT_IP This name refers to a set of sip-manipulations that are performed on outbound traffic from the Acme Packet Session Director. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side of the Acme Packet Session Director as well as to outbound traffic from the private side of the Acme Packet Session Director.

```
realm-config
        identifier                     EXTERNAL
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s0p0:0
        < text removed for brevity >
        out-translationid
        in-manipulationid
        out-manipulationid             NAT_IP

        < text removed for brevity >

realm-config
        identifier                     INTERNAL
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s0p1:0
        < text removed for brevity>
        out-translationid
        in-manipulationid
        out-manipulationid             NAT_IP

       < text removed for brevity >
```

Figure 47: Realm Configuration

©2012 Avaya Inc. All Rights Reserved.

7.1.4. SIP Configuration

The SIP configuration (**sip-config**) defines the global system-wide SIP parameters.
Configure **session-router → sip-config.** The key SIP configuration (**sip-config**) fields are:

- **home-realm-id -** The name of the realm on the private side of the Acme SBC.
- **egress-realm-id – (**Optional) Enter the egress realm ID to define the default route for SIP requests addressed to destinations outside the home realm's address prefix
- **nat-mode – None** (other options are public and private)
- **registrar-domain -** An asterisk (*****) is specified to allow any domain.
- **registrar-host -** An asterisk (*****) is specified to allow any host.
- **registrar-port -** port used for registration. Default is 0.
- **options -** max-udp-length=0. Option required to process long udp invites.

```
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INTERNAL
        egress-realm-id                EXTERNAL
        nat-mode                       None
        registrar-domain               *
        registrar-host                 *
        registrar-port                 0

       < text removed for brevity >

       options                        max-udp-length=0
```

Figure 48: SIP Configuration

©2012 Avaya Inc. All Rights Reserved.

7.1.5. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet SBC such as Session Manager or Metaswitch's Perimeta SBC.
Configure **session-router → session-agent.** The key session agent (**session-agent**) fields are:

- **Hostname -** Fully qualified domain name or IP address of this SIP peer. (Metaswitch Perimeta SBC required FQDN)
- **ip-address -** The IP address of this SIP peer.
- **Port -** The port used by the peer for SIP traffic. (e.g**.**, **5060**)
- **app-protocol - SIP**
- **transport-method - UDP**
- **realm-id -** The realm id where this peer resides.
- **Description -**A descriptive name for the peer.
- **ping-method:** OPTIONS;hops=0 defines that the SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Acme Packet SBC to set the SIP "Max-Forward" field to 0 in outbound SIP OPTIONS pings generated by the Acme Packet SBC to this session agent.
- **ping-interval**: Specifies the interval (in seconds) between each ping attempt

The settings for the session agent on the private side are shown below.

```
session-agent
        hostname                       10.64.60.19
        ip-address                     10.64.60.19
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       INTERNAL
        egress-realm-id
        description                    To_Session_Manager
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0

       < text removed for brevity >

        response-map
        ping-method                    OPTIONS;hops=0
        ping-interval                  60
        ping-send-mode                 keep-alive

       < text removed for brevity >
```

Figure 49: Session Agent for Avaya Session Manager

©2012 Avaya Inc. All Rights Reserved.

The settings for the session agent on the public side are shown below

```
session-agent
        hostname                       sbc-whistler.metaswitch.com
        ip-address                     198.147.226.94
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       EXTERNAL
        egress-realm-id
        description                    To_Metaswitch
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0

       < text removed for brevity >

        response-map
        ping-method                    OPTIONS;hops=0
        ping-interval                  60
        ping-send-mode                 keep-alive

       < text removed for brevity >
```

Figure 50: Session Agent for Metaswitch

©2012 Avaya Inc. All Rights Reserved.

7.1.6. SIP Interface

The SIP interface (**sip-interface**) defines the receiving characteristics of the SIP interfaces on the Acme Packet SBC. Two SIP interfaces were defined; one for each realm.
Configure **session-router → sip-interface.** The key SIP interface (**sip-interface**) fields are:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sip-port**
  - **address -** The IP address assigned to this sip-interface.
  - **port -** The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
  - **transport-protocol -** The transport method used for this interface.
  - **allow-anonymous -** Defines from whom SIP requests will be allowed. On the peer side, the value of agents-only is used. Thus, SIP requests will only be accepted from session agents on this interface. On the core side, the value of **all** is used. Thus, SIP requests will be accepted from anyone on this interface.

```
sip-interface
        state                           enabled
        realm-id                        INTERNAL
        description
        sip-port
                address                         10.64.60.205
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0


      < text removed for brevity >

sip-interface
        state                           enabled
        realm-id                        EXTERNAL
        description
        sip-port
                address                         192.168.62.25
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 agents-only
                ims-aka-profile
        carriers
        trans-expire                    0

        < text removed for brevity >
```

Figure 51: SIP Interfaces

7.1.7. Session Agent Group

Session-groups (**SAG)** define single or multiple destinations for fail-over or load balancing purposes that are referenced in provisioning session-agents.

Configure **session-router → session-group.** The key session agent group (**session-group**) fields are:

- **group-name -** A descriptive string used to reference the session agent group.
- **state - enabled**
- **app-protocol - SIP**
- **strategy -** Hunt This strategy will route to the secondary session agent only if the primary fails.
- **Dest** - The list of session agents to be added to the group. (Add multiple destinations for redundancy.)
- **sag-recursion -** Enable this parameter if you want to use SIP SAG recursion for this SAG. The default value is **disabled**

```
session-group
        group-name                     ENTERPRISE
        description
        state                          enabled
        app-protocol                   SIP
        strategy                       Hunt
        dest
                                       10.64.60.19
        trunk-group
        sag-recursion                  disabled

session-group
        group-name                     METASWITCH
        description
        state                          enabled
        app-protocol                   SIP
        strategy                       Hunt
        dest
                                       sbc-whistler.metaswitch.com
        trunk-group
        sag-recursion                  disabled
```

Figure 52: Session Agent Group

7.1.8. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. 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.

©2012 Avaya Inc. All Rights Reserved.

Configure **session-router → sip-manipulation.** The key SIP manipulation (**sip-manipulation**) fields are:

- **name -** The name of this set of SIP header rules.
- **header-rule**
  - **name-** The name of this individual header rule.
  - **header-name-** The SIP header to be modified.
  - **Action-** The action to be performed on the header.
  - **comparison-type-** The type of comparison performed when determining a match.
  - **msg-type-** The type of message to which this rule applies.
  - **element-rule**
    - **name -** The name of this individual element rule.
    - **Type -** Defines the particular element in the header to be modified.
    - **Action -** The action to be performed on the element.
    - **match-val-type** - Element matching criteria on the data type (if any) in order to perform the defined action.
    - **comparison-type -** The type of comparison performed when determining a match.
    - **match-value-** Element matching criteria on the data value (if any) in order to perform the defined action.
    - **new-value**- New value for the element (if any).

```
sip-manipulation
        name                           NAT_IP
        description                    Topology-hiding-SIP-headers
        split-headers
        join-headers
        header-rule
                name                           manipFrom
                header-name                    From
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           From
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 ip
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $LOCAL_IP
        header-rule
                name                           manipTo
                header-name                    To
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           To
```


©2012 Avaya Inc. All Rights Reserved.

```
                parameter-name
                type                                uri-host
                action                              replace
                match-val-type                      ip
                comparison-type                     case-sensitive
                match-value                         any
                new-value                           $REMOTE_IP
        header-rule
            name                                manipRpid
            header-name                         Remote-Party-ID
            action                              manipulate
            comparison-type                     case-sensitive
            msg-type                            request
            methods
            match-value
            new-value
            element-rule
                name                                rpid
                parameter-name
                type                                uri-host
                action                              replace
                match-val-type                      ip
                comparison-type                     case-sensitive
                match-value
                new-value                           $LOCAL_IP
        header-rule
            name                                manipHistInfo
            header-name                         History-Info
            action                              manipulate
            comparison-type                     case-sensitive
            msg-type                            request
            methods
            match-value
            new-value
            element-rule
                name                                HistoryInfo
                parameter-name
                type                                uri-host
                action                              replace
                match-val-type                      ip
                comparison-type                     case-sensitive
                match-value
                new-value                           $REMOTE_IP
        header-rule
            name                                storeAlertInfo
            header-name                         Alert-Info
            action                              store
            comparison-type                     pattern-rule
            msg-type                            request
            methods
            match-value                         (.+@)([0-9.]+)(.+)
            new-value
        header-rule
            name                                manipAlertInfo
            header-name                         Alert-Info
            action                              manipulate
            comparison-type                     boolean
            msg-type                            request
            methods
            match-value                         $storeAlertInfo
            new-value
$storeAlertInfo.$1+$REMOTE_IP+$storeAlertInfo.$3
```


©2012 Avaya Inc. All Rights Reserved.

Figure 53: SIP Manipulation NAT_IP

7.1.9. Local Policy

Local policy controls the routing of SIP calls from one realm to another.
Configure **session-router → local-policy.** The key local policy (**local-policy**) fields are:

- **from-address -** A policy filter indicating the originating IP address to which this policy applies. An asterisk (*****) indicates any IP address.
- **to-address -** A policy filter indicating the terminating IP address to which this policy applies. An asterisk (*****) indicates any IP address.
- **source-realm -** A policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute**
  - **next-hop -** The location where the message should be sent when the policy rules match.
  - **Realm -** The realm associated with the next-hop location.

The first policy provides a simple routing rule indicating that messages originating from the INTERNAL realm are to be sent to the EXTERNAL realm via SAG:METASWITCH (Metaswitch Perimeta SBC). The second indicates that messages originating from the EXTERNAL realm are to be sent to the INTERNAL realm via SAG:ENTERPRISE.

```
local-policy
        from-address
                                *
        to-address
                                *
        source-realm
                                INTERNAL
        description
        activate-time           N/A
        deactivate-time         N/A
        state                   enabled
        policy-priority         none
        policy-attribute
                next-hop                SAG:METASWITCH
                realm                   EXTERNAL
        < text removed for brevity >

 local-policy
        from-address
                                *
        to-address
                                *
        source-realm
                                EXTERNAL
        description
        activate-time           N/A
        deactivate-time         N/A
        state                   enabled
        policy-priority         none
        policy-attribute
```


©2012 Avaya Inc. All Rights Reserved.

```
                next-hop                        SAG:ENTERPRISE
                realm                           INTERNAL
        < text removed for brevity >
```

Figure 54: Local Policy

7.1.10. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.
Configure **media-manager→ steering-pool.** The key steering pool (**steering-pool**) fields are:

- **ip-address** - The address of the interface on the Acme Packet SBC.
- **start-port -** An even number of the port that begins the range.
- **end-port -** An odd number of the port that ends the range.
- **realm-id -** The realm to which this steering pool is assigned.

```
steering-pool
        ip-address                      192.168.62.25
        start-port                      49152
        end-port                        65535
        realm-id                        EXTERNAL
        network-interface

steering-pool
        ip-address                      10.64.60.205
        start-port                      49152
        end-port                        65535
        realm-id                        INTERNAL
        network-interface
```

Figure 55: Steering Pool

©2012 Avaya Inc. All Rights Reserved.

8. Configure Metaswitch

During the test effort, the Metaswitch network was protected by Metaswitch Perimeta Session Border Controller. The session border controller is not required as part of the solution. Basic configuration is provided below. If a Perimeta 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 Avaya Communication Manager and Session Manager testing is shown below. For an importable version, contact a Metaswitch customer service representative.

```
begin MediaGatewayModel  // Remote Media Gateway Model "AvayaCM/SM "
  Category                                SIP
  ModelName                                   AvayaCM/SM
  Description                              Aura ip pbx
  ControlProtocol                             SIP
  DefaultModel                               False
  AlertInfoStringsForDistinctiveRingingHeading    Alert-Info strings for Distinctive Ringing
  SignalingSettingsHeading                     Signaling settings
  SupportedHighBandwidthMediaFormats            {G.711 u-law,G.711 A-law}
  SupportedLowBandwidthMediaFormats             {G.726 32kbps,G.729 AB}
  PreferredLowBandwidthMediaFormats            {}
  AdvancedVoiceCodecsPermitted                 Any codecs
  VideoCodecsPermitted                       Any codecs
  PacketizationInterval                      0
  SilenceSuppressionAllowed                    False
  MaximumSimultaneousTransactionsOutstanding      100
  DigitOverhangTime                          250
  FixBitsMGCPMeGaCoSIPMSML                    {Cannot be hub,Simple contexts,Cannot play ringback,Cannot control endpoint connectivity,Cannot move contexts,Connections always receive,Cannot report detection of call-type discrimination tones,Requires out-of-band DTMF for all codecs,T.38 supported}
  DynamicFixBitsMGCPMeGaCoSIPMSML              {Supports RTCP,Trust packet loss statistics,Trust jitter statistics}
  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
```


©2012 Avaya Inc. All Rights Reserved.

8.2. Configured SIP Bindings

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/SM2
Customer information	
Customer information 2	
Customer information 3	
Customer information 4	
Customer information 5	
Customer information 6	
Usage	Subscriber
Delegated Management Group	default
Use DN for identification	True
SIP authentication required	False
SIP domain name	
IP address match required	False
Contact IP address (Format: IPv4)	192.168.62.25
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: IPv4)	10.220.21.30
Proxy IP port (0 - 65535)	5060
Transport protocol	UDP
Media Gateway model	mote Media Gateway Model "AvayaCM/SM "
Network Node ☐ Override	None [Default]
Preferred location of Trunk Gateway	None
ESA Protection Domain	None
Trusted	True

©2012 Avaya Inc. All Rights Reserved.

Use caller name provided by SIP device	True
Play announcements when error conditions occur	True
Use static NAT mapping	False
Maximum call appearances (1 - 2147483647)	1024
Maximum concurrent high bandwidth call appearances allowed	0
Poll peer device	True
Polling interval (1 - 3600 seconds)	30
Current number of call appearances in use	0
Current number of high bandwidth call appearances in use	0
Deactivation mode	Normal

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

Subscriber Group		Whisiter local numbers (604-902)
Number status		Normal
Recently moved from old number		False
Signaling type		SIP
Line selection method		Round robin ascending (ISDN/SIP only)
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 Number		6049020161
Calling number precedence for emergency calls	☐ Override	CPN - UPN - DN [Default]
Calling number / connected line ID screening	☐ Override	Owned DN [Default]
Additional calling number screening for emergency calls	☐ Override	No Screening [Default]
Default maximum call appearances for PBX lines (1 - 2147483...	☐ Override	64 [Default]
Long distance carrier	☑ Override	0001
IntraLATA carrier	☑ Override	0001
International carrier	☑ Override	0001
PIN		0000

©2012 Avaya Inc. All Rights Reserved.

Second locale		None
Billing type	Override	Flat rate [Default]
Number Validation and routing attributes	Override	Pre-paid / off-switch calling card subscriber 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)		3/26/12 5:47:16 PM
Charge indication	Override	None [Default]
Category	Override	Ordinary calling subscriber [Default]

8.3.2. PBX Line Object

Settings

Configured SIP Binding		Avaya CM/SM2
Maximum call appearances (1 - 2147483647)	Override	64 [Default]
Line usage		Voice and fax
PBX plays ringback		False

8.3.3. DID Objects

Type	DID range
Description	
Range size (1 - 1000000000)	10
(First) Directory number	6049020170
Last Directory number	6049020179
First code	6049020170
Last code	6049020179

©2012 Avaya Inc. All Rights Reserved.

8.3.4. Perimeta SBC Configuration

Adding a Trusted Device (e.g. PBX, Proxy, and Application Server) into the Perimeta SBC:

- Login into Perimeta and enter the defcraft menu as shown below

```
SUMMARY
-------
Tue Apr 10 00:24:09 BST 2012 = Mon Apr 9 23:24:09 UTC 2012
This is processor B.
Processor B is the primary processor

Process  RunningTime
ethmgr   14-03:10:07
vpcn      5-21:54:11
vpsi      5-21:54:07


CPU2:ITG-PerimetaB:~# su - defcraft

--------------------------------------------------------------------------------

                                                     10-Apr-2012 00:24:31 +0100
Perimeta ISC ITG-Perimeta is running
WARNING: System running on an unsupported hardware configuration for role.
This is processor-blade B; processor-blade A is contactable;
Session Controller is partnered; processor-blade B is primary
[Main] [=]
  Select a command group or command
  Press ENTER to refresh
0   Exit         < Log off the craft menu
1   CLI            Command Line Interface
2   Admin        > Administrator Function
3   Software     > Update Perimeta Session Controller Software
4   Diagnostics  > Retrieve Diagnostic Information
:
```

- Enter the CLI interface.

- Go into Configuration Mode and navigate to the trusted sources section as follows:
    - System -> ip-acces-control ->trusted-sources

©2012 Avaya Inc. All Rights Reserved.

```
------------------------------------------------------------------------------

% Warning: this system is not licensed.  Enter your license key using the
apply-license command or contact your sales representative to acquire a valid
license key.
ITG-Perimeta#config
ITG-Perimeta(config)#system
ITG-Perimeta(system)#ip-access
ITG-Perimeta(ip-access-ctrl)#trusted-sources
```

- Add in the appropriate ip addresses of the trusted devices as follows:
  - **Prompt>** permit-peer service-network 1 ipv4 <***ip-address***>

```
ITG-Perimeta(trusted-src)#?
  end                                    Return to top level mode
  exit                                   Exit the current CLI mode
  no                                     Remove object or set config to default
  permit-peer                            Configure a trusted IP device
ITG-Perimeta(trusted-src)#permit-peer service-network 1 ipv4 123456789012
```

- Type **exit** until out of the CLI command tree (e.g. system > ip-access-control > trusted-sources > permit-peer > service-network 1)

9. 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

9.1. Verify Avaya Aura® Communication Manager

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 T00046   in-service/idle    no
0009/002 T00047   in-service/idle    no
0009/003 T00048   in-service/idle    no
0009/004 T00049   in-service/idle    no
0009/005 T00050   in-service/idle    no
```

Figure 56: Trunk Status

©2012 Avaya Inc. All Rights Reserved.

Below is an example of an active call from Avaya SIP endpoint to Metaswitch CommPortal.

```
status trunk 9

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0009/001 T00046   in-service/idle    no
0009/002 T00047   in-service/idle    no
0009/003 T00048   in-service/idle    no
0009/004 T00049   in-service/idle    no
0009/005 T00050   in-service/idle    no
0009/006 T00051   in-service/idle    no
0009/007 T00052   in-service/idle    no
0009/008 T00053   in-service/active  no   T00001
0009/009 T00054   in-service/idle    no
0009/010 T00055   in-service/idle    no
```

Figure 57: Trunk Status/Active Call

From the active call, 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**".

```
status trunk 9/8                                                Page   1 of   4
                              TRUNK STATUS

 Trunk Group/Member: 0009/008             Service State: in-service/active
               Port: T00053            Maintenance Busy? no
 Signaling Group ID: 9

   IGAR Connection? no

    Connected Ports: T00001
```

Figure 58: Trunk Status/Active Call – Page 1

©2012 Avaya Inc. All Rights Reserved.

On **Page 2**, verify that **the IP addresses** of the **procr** and **Session Manager** are shown in the **Signaling** section. In addition, the **Audio** section shows the **G.711MU** codec and the IP address of the **Avaya endpoint** and the **Acme Packet SBC**.

```
status trunk 9/8                                               Page   2 of   4
                                 CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                              Port
   Near-end:  10.64.60.13                           : 5061
    Far-end:  10.64.60.19                           : 5061
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-tdm        Authentication Type: None
    Near-end Audio Loc: MG1                    Codec Type: G.711MU
   Audio      IP Address                              Port
   Near-end:  10.64.60.20                           : 2052
    Far-end:  10.64.60.205                          : 52272

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

Figure 59: Trunk Status/Active Call – Page 2

©2012 Avaya Inc. All Rights Reserved.

9.2. SIP Monitoring on Avaya Aura® Session Manager

Select **Session Manager** from the **Home Screen**. On the left navigation panel select **System Status** to expand it**,** and then select **SIP Entity Monitoring**. Verify that none of the links to the defined SIP entities are down (as indicated by **0/2** in the figure below), indicating that they are all reachable for call routing.

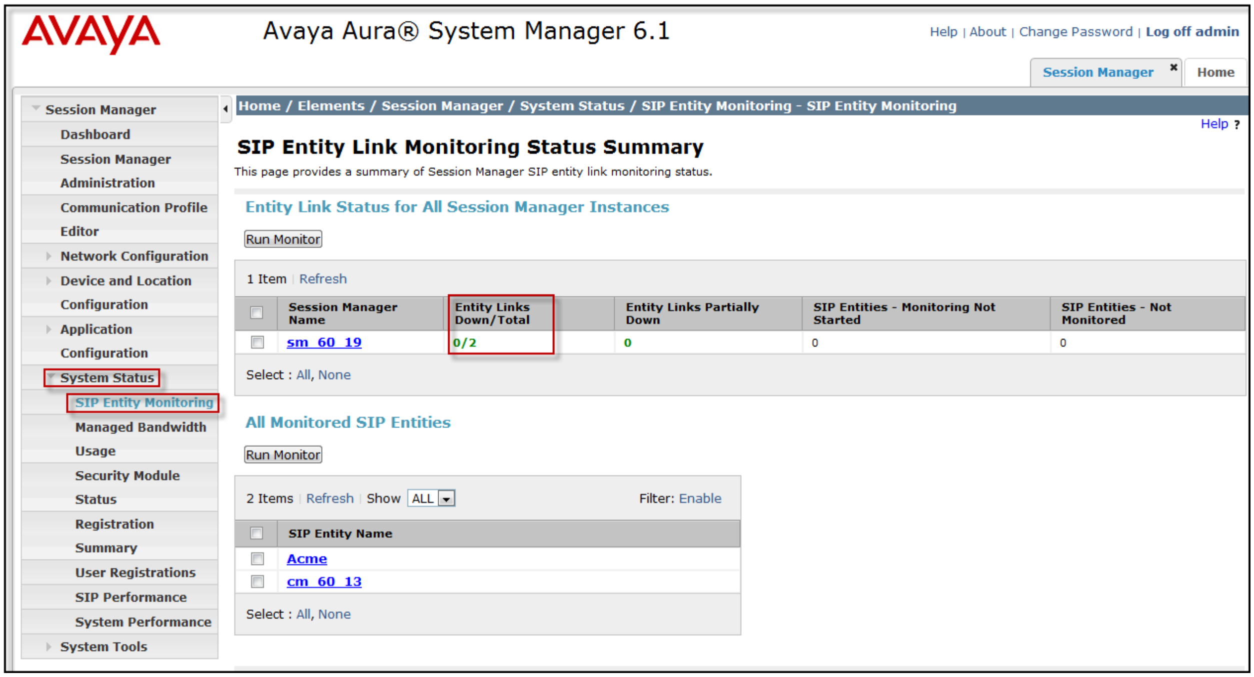

Figure 60: SIP Entity Link Monitoring - Summary

9.3. Verification Call Scenarios

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

- Inbound and outbound basic voice calls between various Analog, Digital, SIP and H.323 endpoints on the Communication Manager and Metaswitch CommPortal can be made in both directions.
- Verify that the H.323, SIP, Digital and Analog endpoints on the enterprise site can place calls terminating over the SIP trunk and the call can remain active for more than 35 seconds.
- Verify that the endpoints at the enterprise site can receive calls from the CommPortal registered to Metaswitch CFS and can remain active for more than 35 seconds.
- Verify that the CommPortal can terminate an active call by hanging up.
- Verify that an endpoint at the enterprise site can terminate an active call by hanging up.
- Verify fax calls between Communication Manager and Metaswitch can be made.
- DTMF Tone Support.
- Supplementary calling features were verified. The supplementary calling features verified are:

©2012 Avaya Inc. All Rights Reserved.

- o Hold, Call transfer, Conference.
- o Voicemail Coverage and Retrieval.
- o Call Forwarding.
- o Call Coverage.
- o Extend Call.
- o EC500 (call forking).

10. Conclusion

Metaswitch SIP Trunking passed compliance testing. As illustrated in these Application Notes, Avaya Aura® Communication Avaya Aura® Session Manager, and Acme Packet Session Border Controller can be configured to interoperate successfully with Metaswitch MetaSphere Call Feature Server and Metaswitch Perimeta Session Border Controller. 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. Please refer to **Section 2.2** above for Test Results and any limitations that were observed.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com . Acme Packet product documentation is available at http://www.acmepacket.com . A support account may be required to access the Acme Packet documentation. Product documentation for Metaswitch SIP Trunking is available from Metaswitch.

[1] *Installing and Configuring Avaya Aura® System Platform, Release 6.0.3 Issue 2.1 March 2012*

[2] *Administering Avaya Aura® Communication Manager, Release 6.0, 03-300509 Issue 6.0, June 2010*

[3] *Avaya Aura® Communication Manager Feature Description and Implementation, June 2010, Document Number 555-245-205.*

[4] *Avaya Aura® Communication Manager 6.0.1 SP7 Release Notes, February 13, 2012, Release 1.0.*

[5] *Avaya Aura® Session Manager Release 6.1 Service Pack 6 Release Notes*

[6] *Maintaining and Troubleshooting Avaya Aura® Session Manager, 03-603325, Release 6.1, Issue 4.2, November 2011.*

[7] *Administering Avaya Aura® Session Manager, November 2010, Document Number 03-03324.*

[8] *Installing and Configuring Avaya Aura® Session Manager Release 6.1, Issue 2.2, April 2011.*

[9] *Net-Net® 4000 Maintenance and Troubleshooting Guide Release Version S-C6.1.0.*

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

©2012 Avaya Inc. All Rights Reserved.

©2012 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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