Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SingTel Meg@POP SIP Trunking Service with Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Acme Packet 4250 Net-Net Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between SingTel Meg@POP SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Acme Packet 4250 Net-Net Session Border Controller and various Avaya endpoints.

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.

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between SingTel Meg@POP SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Acme Packet 4250 Net-Net Session Border Controller (SBC) and various Avaya endpoints.

SingTel Meg@POP SIP Trunking Service provides businesses with multiple location seamless access to Public Switched Telephone Network (PSTN). By converging voice and data services onto a single Meg@POP network, customers enjoy cost savings by simplifying their network infrastructure, and optimizing the existing network.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the SingTel Meg@POP SIP Trunking Service and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Acme Packet 4250 Net-Net SBC. Testing was done in the SingTel lab environment that simulated the actual SingTel Meg@POP SIP Trunking Service. Acme Packet 4250 Net-Net SBC was also provided and provisioned by Acme Packet engineers for the testing.

2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Both supported modes were tested. Both H.323 and SIP protocols were tested.
- Codecs G.711A and G.729A were tested.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Incoming PSTN calls to a Vector Directory Number (VDN) and delivered to agents.

Items not supported or not tested included the following:

- Long distance, international, outbound toll-free and operator assisted calls were not tested due to limitations in the test environment.
- T.38 Fax is not supported.
- Use of the REFER method and a 302 redirected response were not tested.

For the compliance test, the enterprise sent the dialed digits in non-E.164 format (e.g. 68591234, 00113035381234) in the destination headers (e.g., “Request-URI” and “To”) and sent 10 digits in E.164 format (e.g. +6568596789) in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). SingTel sent 10 digits in E.164 format in the destination headers and 8 digits in non-E.164 format in the source headers.

2.2. Test Results

Interoperability testing of SingTel Meg@POP SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **G.729A codec negotiation with Linksys SPA941 phone fails**. SingTel Meg@POP network contains other third-party SIP endpoints. Linksys phone sends “G729a” in the SDP description, instead of “G729” as defined in RFC4856. As such, Communication Manager does not accept the call.
- **G.729A definition in the SDP description not consistent for different third-party SIP endpoints in SingTel network**. As such, G.729A codec negotiation with some PSTN endpoints may fail. Work around: The IP Codec listed in **Section 5.4** has been tested to work successfully with all the SIP endpoints used in the testing.
- **Incoming call when all trunks are busy**. Communication Manager sends “404 Not Found”, which SingTel interprets as “Number not in service”. SingTel expects to receive “486 Busy Here”. Work around: Define the maximum number of trunk members in Communication Manager and allow SingTel to monitor the SIP trunk usage and plays network announcement/busytone to caller.

2.3. Support

For technical support on SingTel SIP Trunking Service on the SingTel Meg@POP IP VPN Network, contact the SingTel Account Manager assigned by SingTel or dial 1800-763-1111 for general enquiries.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to SingTel Meg@POP SIP Trunking Service. This is the configuration used for compliance testing.

The Avaya components used to create the simulated customer site included:

- Avaya S8800 Server running Avaya Aura® Solution for Midsize Enterprise
    - Avaya Aura® Session Manager
    - Avaya Aura® System Manager
    - Avaya Aura® Communication Manager
    - Avaya Aura® Communication Manager Messaging
- Avaya G430 Media Gateway
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 1600-Series IP telephones (H.323)
- Avaya 1400-Series Digital telephones
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya analog telephone

Located at the edge of the enterprise is the Acme Packet Net-Net 4250 SBC. This was provided and provisioned by Acme Packet engineers for the testing. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

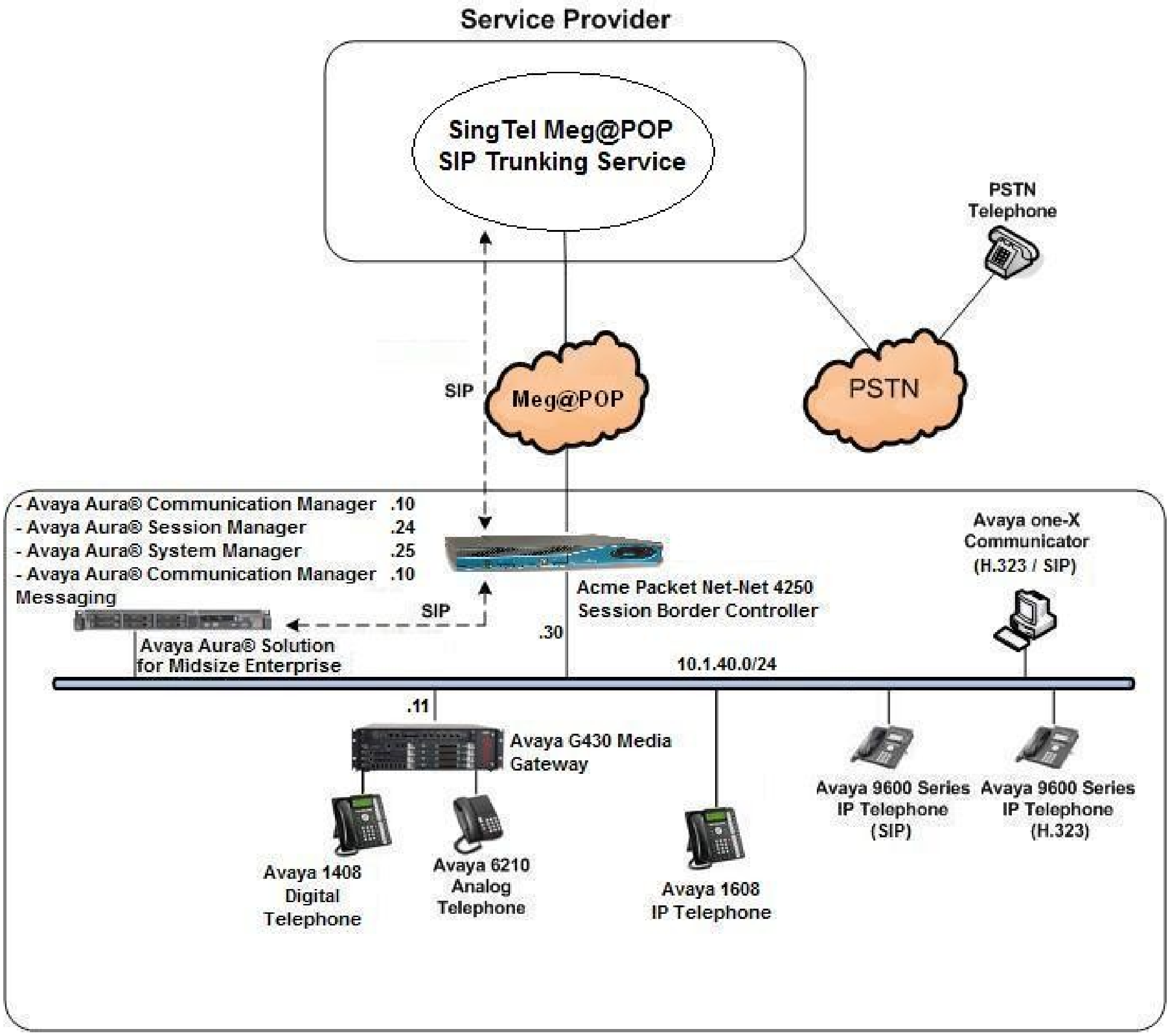


Figure 1: SingTel Meg@POP SIP Trunking Service Test Configuration

A separate trunk group was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk group or codec settings required by the service provider could be applied only to this trunk group without affecting other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the SBC, then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case, Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to SingTel Meg@POP SIP Trunking Service.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	**Release**
Avaya S8800 Server running Avaya Aura® Solution for Midsize Enterprise - Avaya Aura® Session Manager - Avaya Aura® System Manager - Avaya Aura® Communication Manager - Avaya Aura® Communication Manager Messaging	 6.1 Service Pack 2 6.1 Service Pack 2 6.0.1 Service Pack 3 6.0.1 Service Pack 1
Avaya G430 Media Gateway - MM711AP Analog MM - MM712AP DCP MM	31.19.2 HW31 FW095 HW07 FW011
Avaya 1608 IP Telephone (H.323)	1.300B
Avaya 9640G IP Telephone (H.323)	3.1 Service Pack 2
Avaya 9641G IP Telephone (SIP)	6.1 Service Pack 3
Avaya one-X® Communicator (H.323 and SIP)	6.1
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Acme Packet 4250 Net-Net Session Border Controller	6.1.0
SingTel Meg@POP SIP Trunking Service Solution Components	
Component	**Release**
Acme Packet Session Border Controller	Not provided
BroadSoft BroadWorks Softswitch	R17
Cisco Gateway	Not provided

Table 1: Equipment and Software Tested

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for SingTel Meg@POP SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from SingTel. It is assumed the general installation of Communication Manager, Avaya G430 Media Gateway and Session Manager has been previously completed and thus is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** 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 **12000** SIP trunks are available and **240** 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: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 250   1
                       Maximum Administered SIP Trunks: 12000 240
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 250   0
```

5.2. System Features

Use the **change system-parameters feature** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.

```
change system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
                Automatic Callback with Called Party Queuing? n
     Automatic Callback - No Answer Timeout Interval (rings): 3
                        Call Park Timeout Interval (minutes): 10
         Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

On **Page 9,** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.

```
change system-parameters features                              Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: 65
          International Access Code: 011

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8800 Server running Communication Manager **(procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM                   10.1.40.24
default              0.0.0.0
procr                10.1.40.10
procr6               ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the SingTel SIP Trunking Service, the preferred codec is G.729A. However, due to a difference in the way Avaya handles the G.729 MIME Type in the Session Description Protocol (SDP) parameters, Avaya recommends that the G.729AB codec is listed before the G.729A codec. To use these codecs, enter **G.729AB, G.729A, G.711A** and **G.711MU** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 1

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

On **Page 2**, set the **Fax Mode** to **off** since T.38 fax is not supported.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  2048:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  2048:Kbits

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

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com**. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name: SingTel SIP Trunk
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 2 will automatically create a complementary table entry on the ip network region 1 form for destination region 2. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

```
change ip-network-region 2                                      Page   4 of  20

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    2     y    NoLimit                                             n       t
 2    2                                                                all
 3
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 4 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). The transport method specified here is used between the Communication Manager and Session Manager.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5062**.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and can not be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager running on the Avaya S8800 Server as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds the that Communication Manager will wait for a response (other than 100 Trying) to an outbound

INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.

- Default values may be used for all other fields.

```
change signaling-group 4                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 4              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
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 2
                                   Far-end Secondary Node Name:
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
                                                   Alternate Route Timer(sec): 6
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 4 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
change trunk-group 4                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 4                    Group Type: sip           CDR Reports: y
  Group Name: SingTel SIP Trunk           COR: 1        TN: 1        TAC: #04
   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: 4
                                                     Number of Members: 255
```

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
change trunk-group 4                                           Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y

             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 format) when passed in the SIP "From", "Contact" and "P-Asserted Identity" headers. The addition of the + sign does not impact interoperability with SingTel.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
change trunk-group 4                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y


                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? n

 DSN Term? n
```

On **Page 4**, set the **Network Call Redirection** field to **n**. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**, the value preferred by SingTel.

```
change trunk-group 4                                               Page   4 of  21
                              PROTOCOL VARIATIONS

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


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 40001, 40010 and 40022. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
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: 9
 5  1                                      5        Maximum Entries: 9999
 5  4                                      5
 5  40001          4         6568596345    10    Note: If an entry applies to
 5  40010          4         6568596346    10    a SIP connection to Avaya
 5  40022          4         6568596343    10    Aura(tm) Session Manager,
                                                 the resulting number must
                                                 be a complete E.164 number.
```

5.9. Outbound Call Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1** as a feature access code (**fac**).

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

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   0            1   attd
   4            5   ext
   9            1   fac
   *            3   fac
   #            3   dac
```

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern **4** which contains the SIP trunk to the service provider (as defined next).

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

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    001                   11   23    4         intl         n
    3                     8    8     4         pubu         n
    6                     8    8     4         pubu         n
    8                     8    8     4         pubu         n
    9                     8    8     4         pubu         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 4 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.

```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4   Pattern Name: SingTelSIPTrunk
                             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: 4    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

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

5.10. Inbound Call Routing

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from SingTel can be manipulated as necessary to route calls to the desired extension. In general, the DID numbers should correlate with the internal extensions, so that only some of the leading digits need to be deleted. However, for this testing, all the DID digits were deleted and replaced by the internal extension as illustrated below.

```
change inc-call-handling-trmt trunk-group 4                     Page   1 of   1
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert            Per Call Night
 Feature        Len      Digits                           CPN/BN   Serv
 public-ntwrk    11 +6568596343      11  40001
 public-ntwrk    11 +6568596345      11  40022
 public-ntwrk    11 +6568596346      11  40010
```

6. Configure Avaya Aura® Session Manager

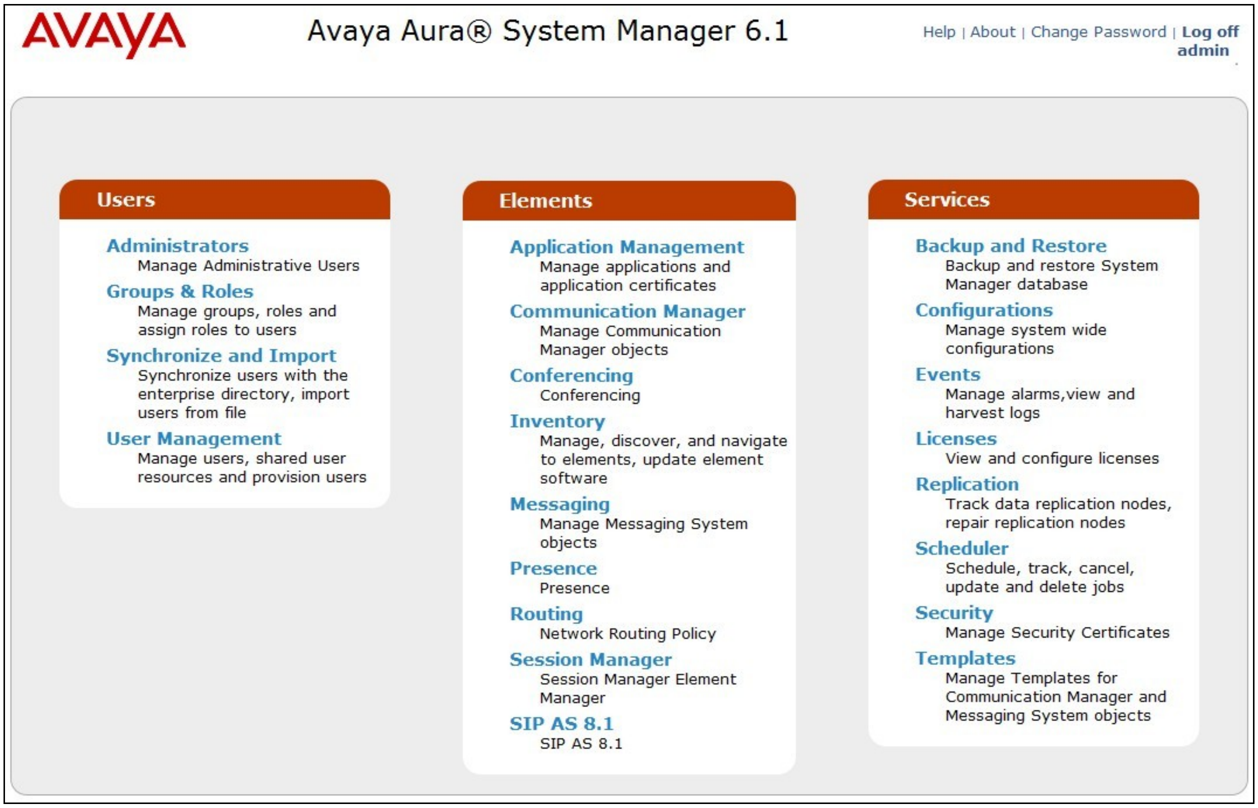
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the SBC and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, to be managed by System Manager.

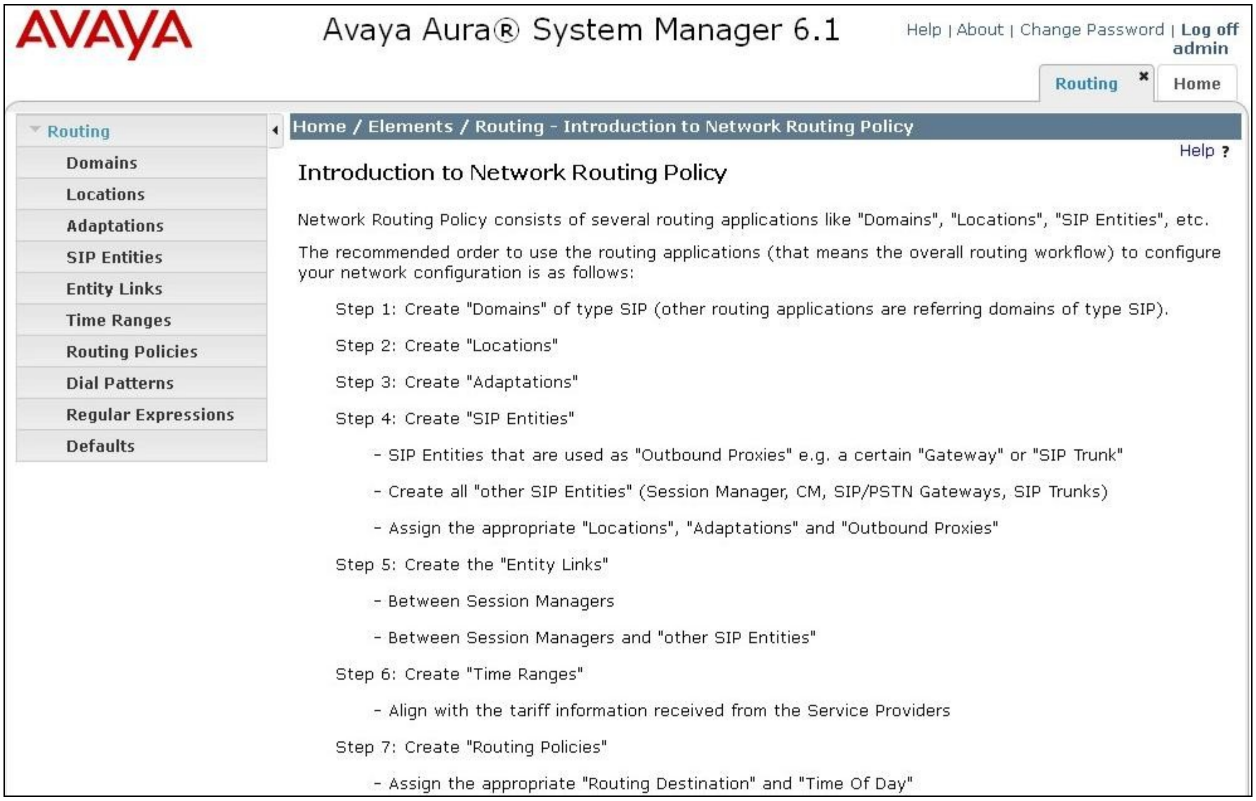
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The **Home Screen** as shown below is then displayed. Select **Routing** under Elements Section.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration.

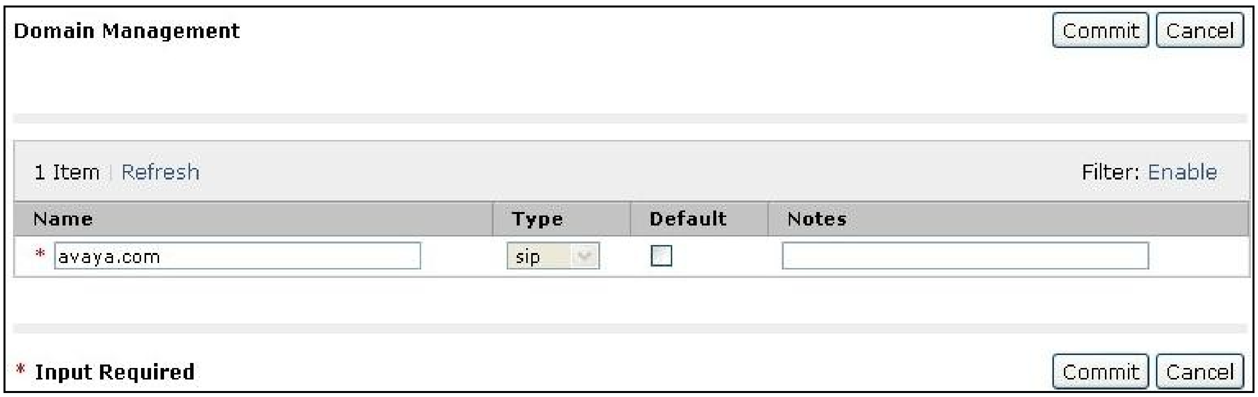


6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.com**). Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the enterprise domain.



6.3. Configure Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. For the compliance test, one location was defined based on the enterprise IP subnet shown in **Figure 1**. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

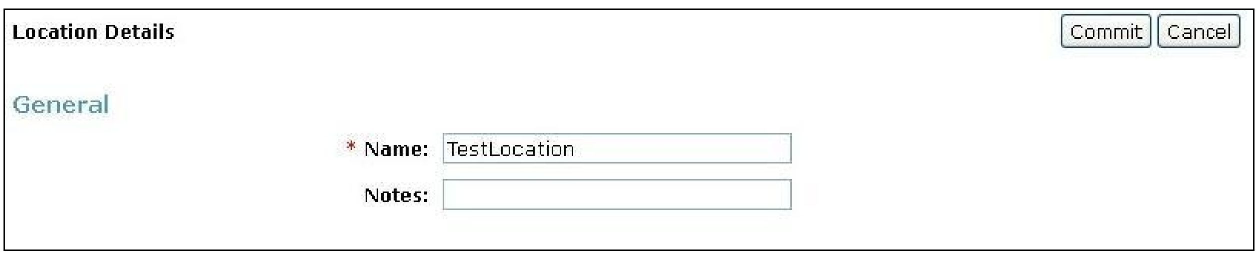
In the **General** section, enter the following values. Use default values for all remaining fields.

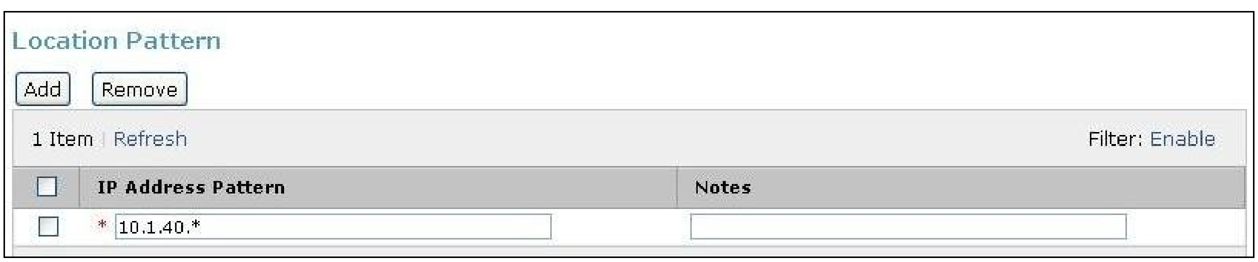
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

In the **Location Pattern** section, click **Add** and enter the following values. Use default values for all remaining fields.

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of the location named **TestLocation**, which includes all equipment on the **10.1.40.x** IP subnet including Communication Manager, and the SBC. Click **Commit** to save.





6.4. Add Adaptation Module

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

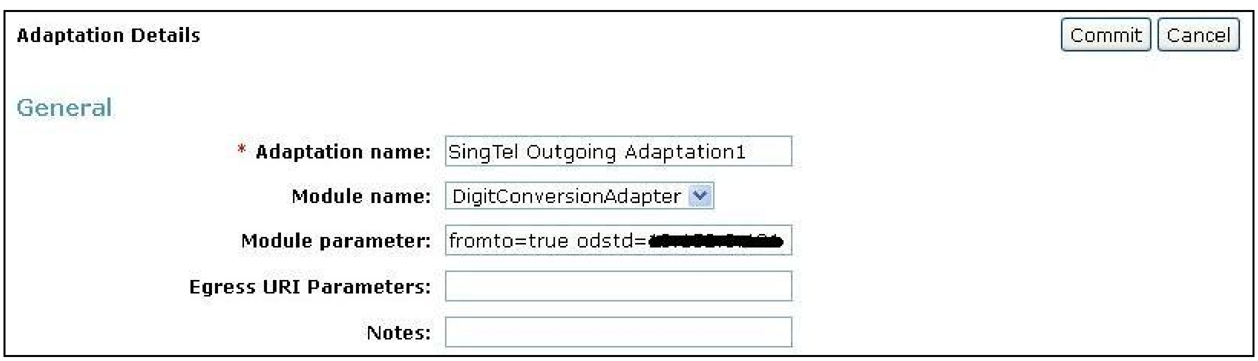
For SingTel interoperability, one adaptation is needed. The adaptation is applied to the Acme Packet SBC SIP entity and converts the domain part of the outbound Request URI header from Session Manager containing the enterprise domain to the SingTel SIP proxy IP address.

To create the adaptation, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter **DigitConversionAdapter**.
- **Module parameter:** Enter **fromto=true odstd=<ipaddr>**, where <ipaddr> is the IP address of the SBC located on SingTel network. This value is provided by SingTel. This parameter replaces the domain in the Request URI header with the given value for outbound only.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



6.5. Add SIP Entities

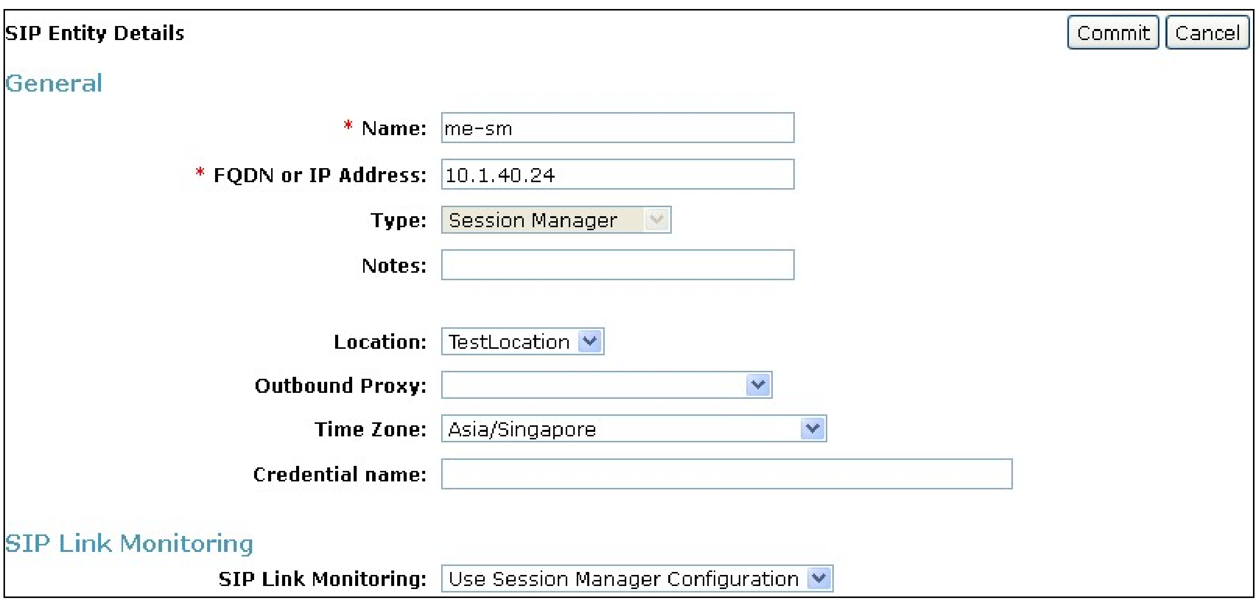
A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the SBC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the SBC.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all SIP Entites are located in **TestLocation**.

  Time Zone: Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.



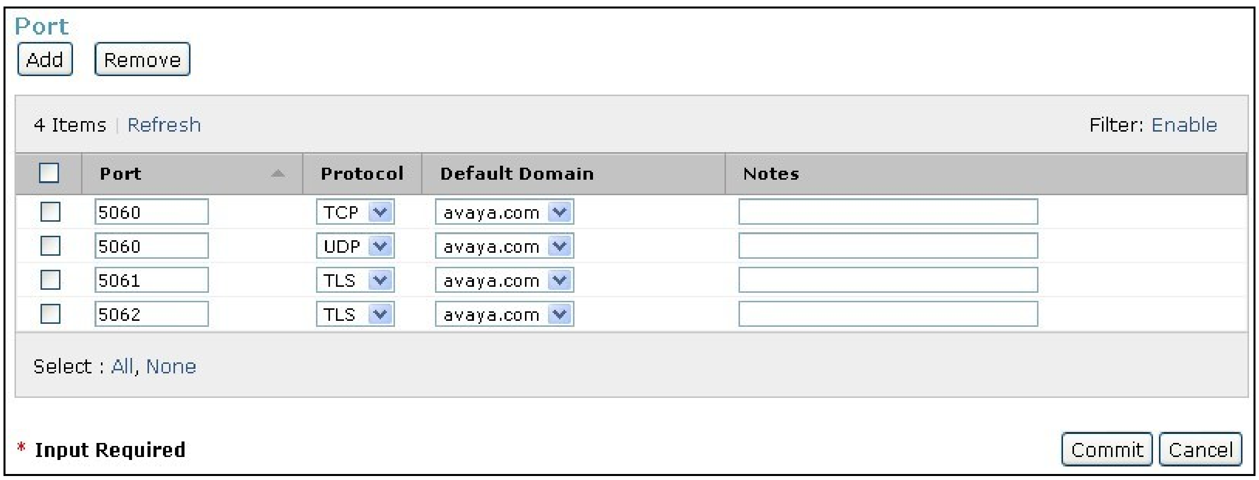
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

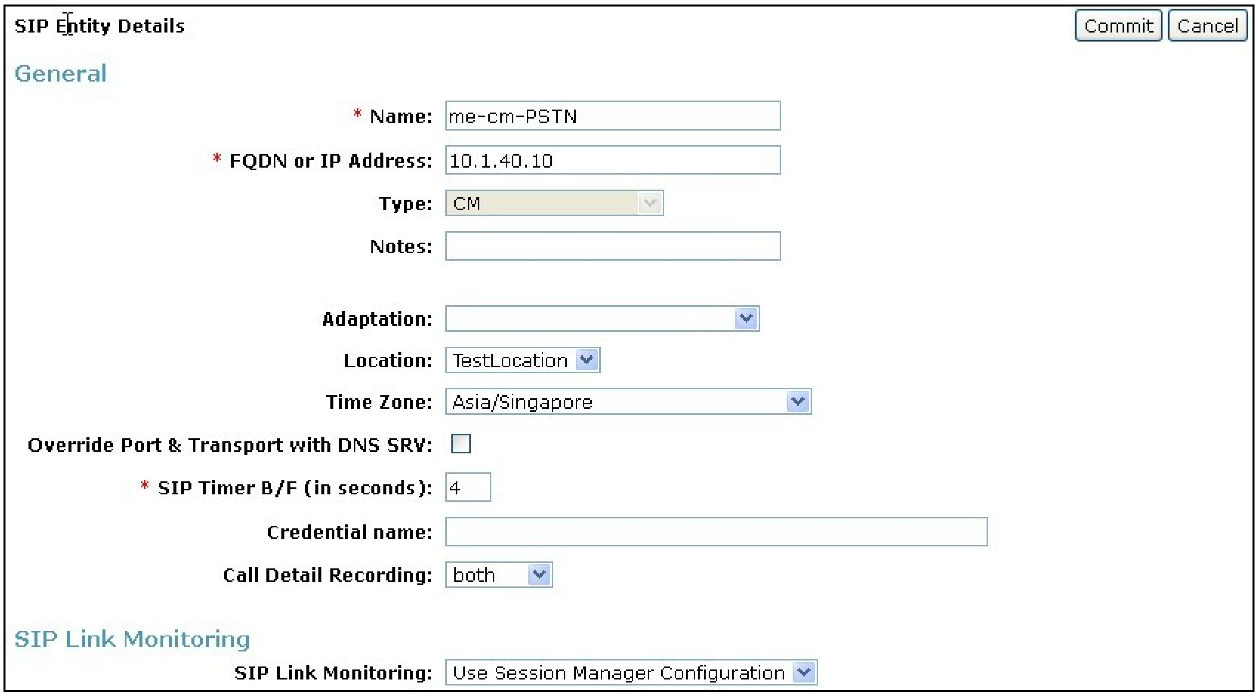
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

Defaults can be used for the remaining fields. Click **Commit** to save.

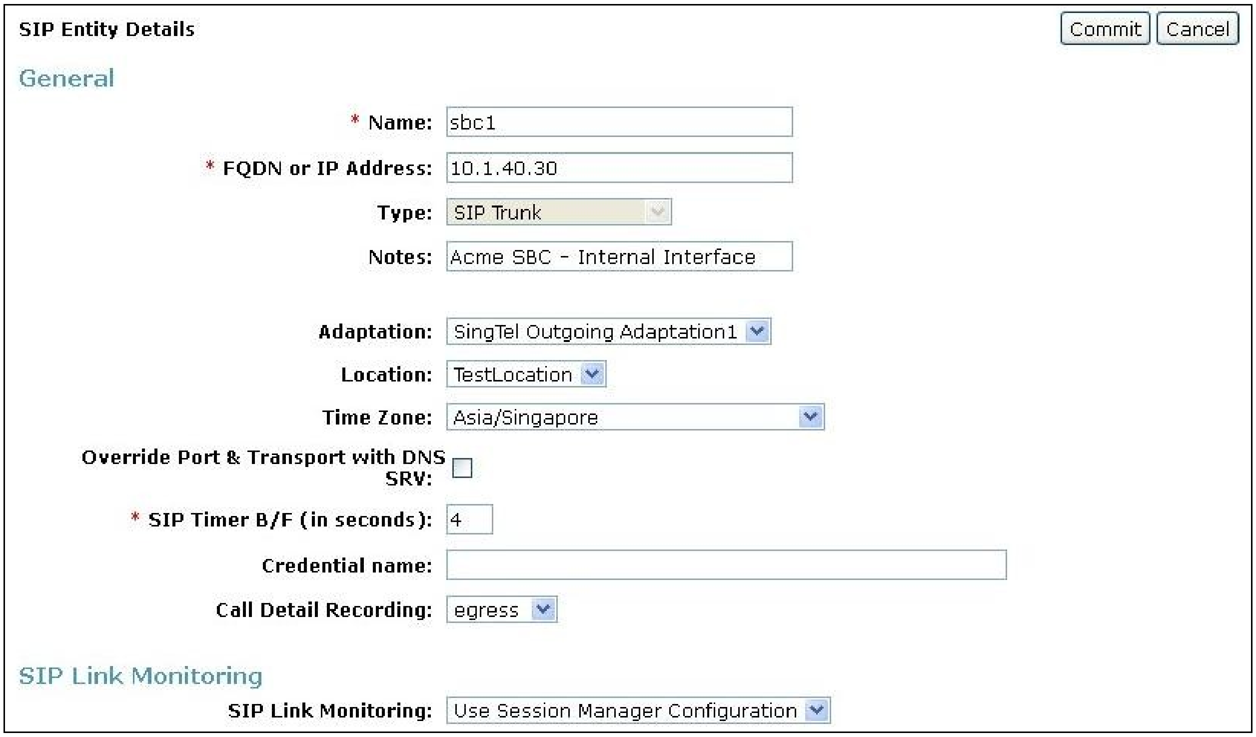
For the compliance test, four **Port** entries were added as shown below.



The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager running on the Avaya S8800 Server. The **Location** field is set to **TestLocation** which is the location defined for the subnet where Communication Manager resides.



The following screen shows the addition of the Acme Packet SBC. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). For the **Adaptation** field, select the adaptation module previously defined for this SIP entity in **Section 6.4**. The **Location** field is set to **TestLocation** which is the location defined for the subnet where the SBC resides.

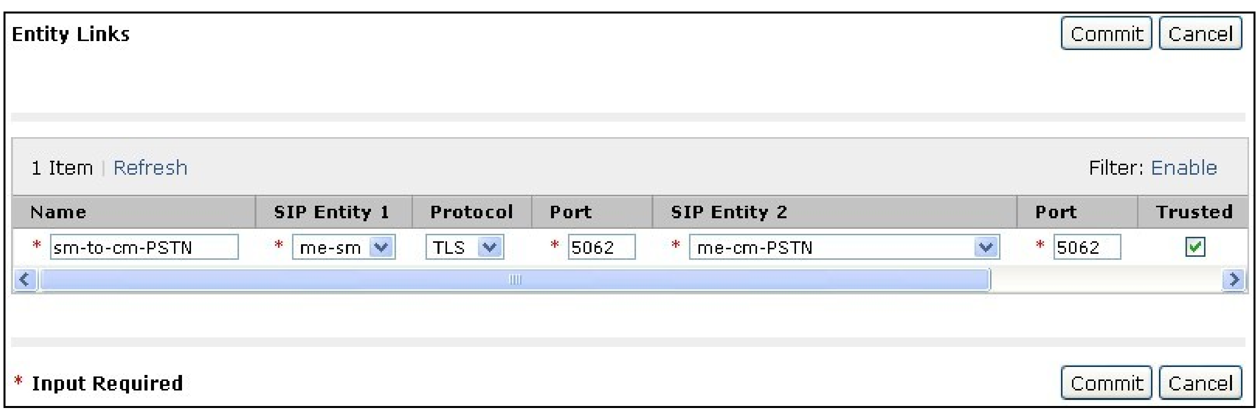


6.6. Add Entity Links

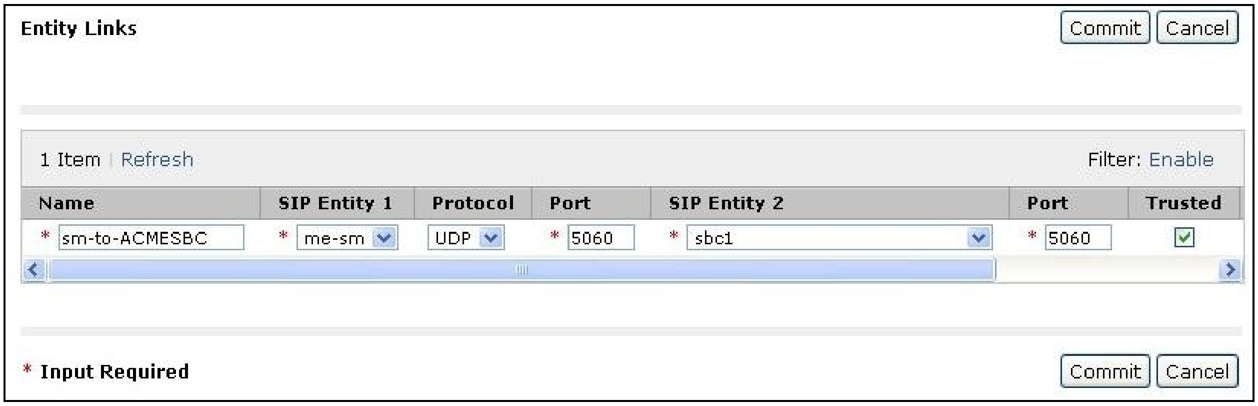
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager and one to the SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the 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 the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.*

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.



The following screen illustrates the Entity Link between Session Manager and the Acme Packet SBC.



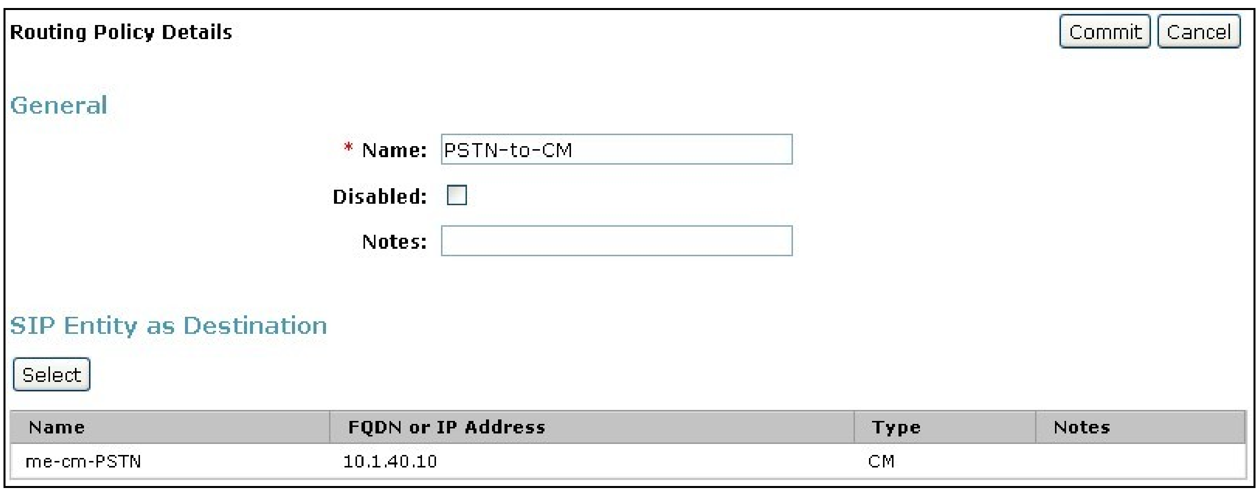
6.7. Add Routing Policies

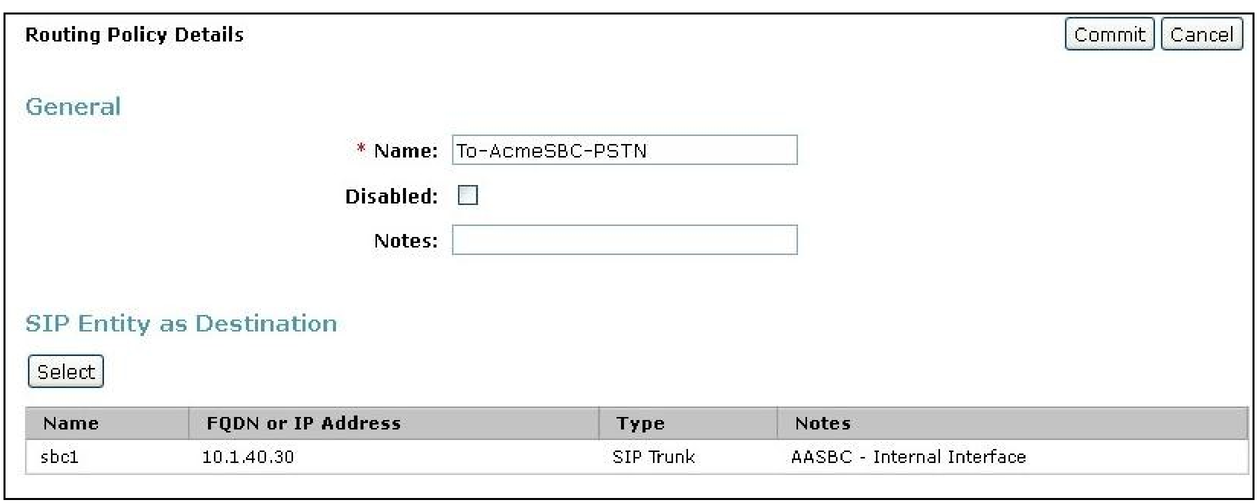
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the SBC. To add a routing policy, navigate to **Routing →Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields. Click **Commit** to save. The following screens show the Routing Policies for Communication Manager and the SBC.





6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to SingTel and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing →Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

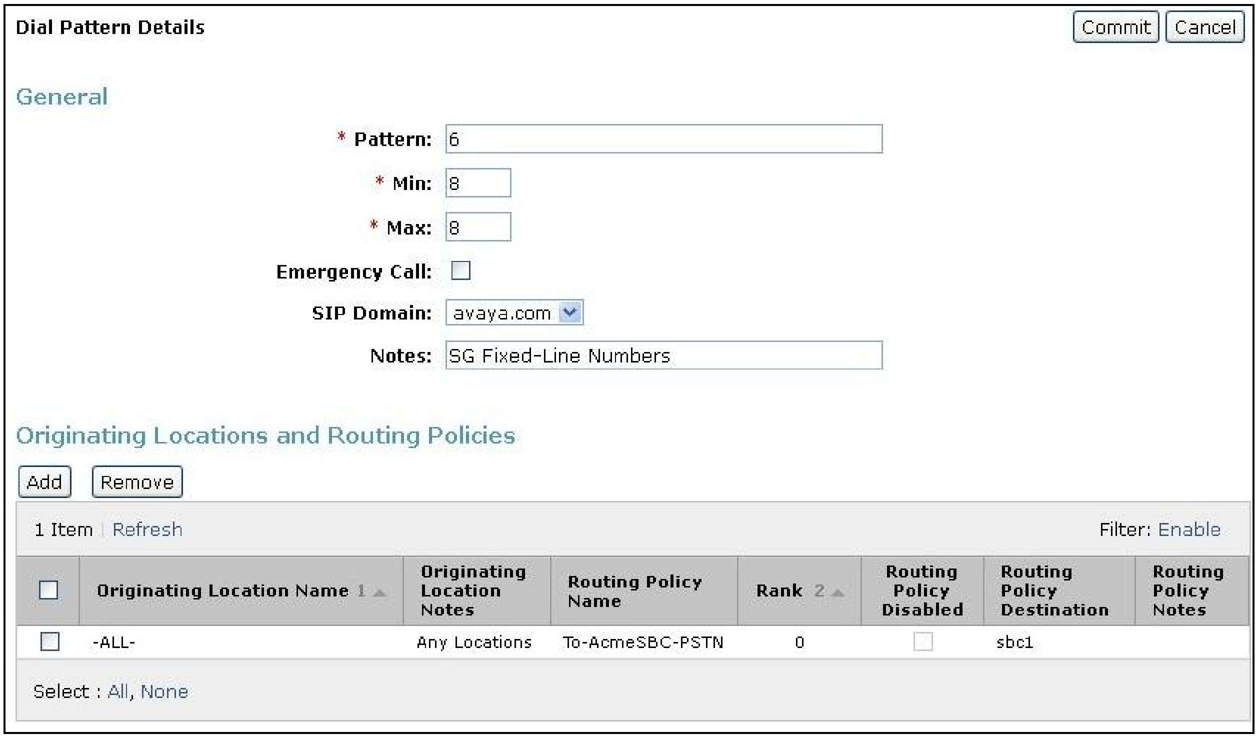
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 8-digit numbers that begin with a 6 and have a destination domain of **avaya.com** from **Any Locations** uses route policy **To-AcmeSBC-PSTN**.


Dial Pattern Details

Commit Cancel

General

* Pattern: 6

* Min: 8

* Max: 8

Emergency Call:

SIP Domain: avaya.com

Notes: SG Fixed-Line Numbers

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh

Filter: Enable

	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
	-ALL-	Any Locations	To-AcmeSBC-PSTN	0		sbc1	

Select : All, None

The second example shows that 11-digit numbers (including the + sign) that start with **+656859634** to domain **avaya.com** and originating from A**ny Locations** uses route policy **To-CM**. These are the DID numbers assigned to the enterprise from SingTel.

Dial Pattern Details

Commit Cancel

General

* Pattern: +656859634

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes: DID call to CM

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

☐	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	PSTN-to-CM	0	☐	me-cm-PSTN	

Select : All, None

The complete list of dial patterns defined for the compliance test is shown below.

Dial Patterns

Edit New Duplicate Delete More Actions

12 Items | Refresh Filter: Enable

☐	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
☐	001	11	24	☐	avaya.com	
☐	1	4	4	☐	avaya.com	SG Service Numbers
☐	+656859634	11	11	☐	avaya.com	DID call to CM
☐	3	8	8	☐	avaya.com	SG VoIP Numbers
☐	4	5	5	☐	avaya.com	CM 4xxxx Extensions
☐	49999	5	5	☐	avaya.com	To CMM
☐	6	8	8	☐	avaya.com	SG Fixed-Line Numbers
☐	8	8	8	☐	avaya.com	SG Mobile Numbers
☐	9	8	8	☐	avaya.com	SG Mobile Numbers

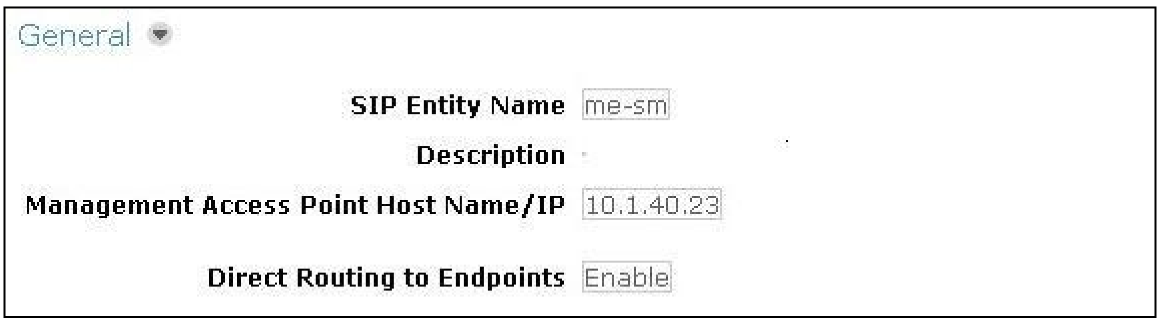
6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager →Session Manager Administration** from the Home Screen and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

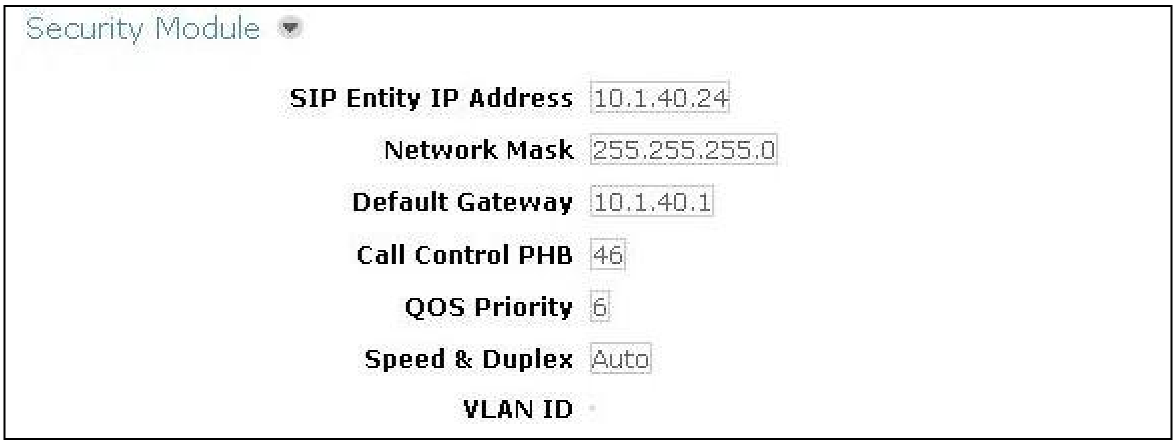
The screen below shows the Session Manager values used for the compliance test.



In the **Security Module** section, enter the following values:

- **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.



7. Configure Acme Packet 4250 Net-Net Session Border Controller

The Acme Packet 4250 Net-Net SBC was installed and provisioned by Acme Packet engineers for this testing. As such, the step-by-step provisioning of the SBC is not discussed in these Application Notes. The SBC configuration file is shown in **Appendix A** for reference.

8. SingTel Meg@POP SIP Trunking Service Configuration

In order to use SingTel SIP Trunking Service on the Meg@POP IP VPN Network, a customer must order the service from SingTel. For further information on SingTel Meg@POP as well as its network and access services, contact a SingTel Account Manager or call 1800-763-1111 (local toll-free).

SingTel will provide the IP address of the SingTel SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to configure Communication Manager, Session Manager, and Acme Packet SBC discussed in the previous sections.

The configuration between SingTel Meg@POP SIP Trunking Service and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the SingTel network.

9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

1. Communication Manager:
   - **list trace station** <extension number> - Traces calls to and from a specific station.
   - **list trace tac** <trunk access code> - Traces calls over a specific trunk group.
   - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk-group number> - Displays trunk group information.
   - **status trunk** <trunk-group number/member-number> - Displays signaling and media information for an active trunk member.
2. Session Manager:
   - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements > Session Manager > System Tools > Call Routing Test**. Enter the requested data to run the test.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet 4250 Net-Net Session Border Controller to SingTel Meg@POP SIP Trunking Service. SingTel Meg@POP SIP Trunking Service passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

11. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509, Issue 6.0.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.0, June 2010, Document Number 555-245-205, Issue 8.0.

[3] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010.

[4] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Document Number 03-603324, Issue 1.

[5] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x,* May 2010, Document Number 16-601443.

[6] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-603838, Issue 1.

[7] *Avaya one-X™ Deskphone SIP Administrator Guide,* December 2010, Document Number 16-300698.

[8] *Using Avaya one-X® Communicator Release 6.1,* April 2011.

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

[10] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

[11] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

[12] RFC 4856, Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences, http://www.ietf.org/

12. Appendix A: Acme Packet 4250 Net-Net Session Border Controller Configuration File

```
local-policy
      from-address
                               *
      to-address
                               *
      source-realm
                               access
      description
      activate-time            N/A
      deactivate-time          N/A
      state                    enabled
      policy-priority          none
      last-modified-by         admin@console
      last-modified-date       2008-09-24 17:07:15
      policy-attribute
            next-hop                 10.1.40.24
            realm                    core
            action                   none
            terminate-recursion      disabled
            carrier
            start-time               0000
            end-time                 2400
            days-of-week             U-S
            cost                     0
            app-protocol             SIP
            state                    enabled
            methods
            media-profiles
local-policy
      from-address
                               *
      to-address
                               *
      source-realm
                               core
      description
      activate-time            N/A
      deactivate-time          N/A
      state                    enabled
      policy-priority          none
      last-modified-by         admin@console
      last-modified-date       2008-10-04 15:46:15
      policy-attribute
            next-hop                 x.x.x.x          (SingTel SBC)
            realm
            action                   none
            terminate-recursion      disabled
            carrier
            start-time               0000
            end-time                 2400
            days-of-week             U-S
```

```
            cost                              0
            app-protocol                      SIP
            state                             enabled
            methods
            media-profiles
media-manager
      state                             enabled
      latching                          enabled
      flow-time-limit                   86400
      initial-guard-timer               300
      subsq-guard-timer                 300
      tcp-flow-time-limit               86400
      tcp-initial-guard-timer           300
      tcp-subsq-guard-timer             300
      tcp-number-of-ports-per-flow      2
      hnt-rtcp                          disabled
      algd-log-level                    NOTICE
      mbcd-log-level                    NOTICE
      red-flow-port                     1985
      red-mgcp-port                     1986
      red-max-trans                     10000
      red-sync-start-time               5000
      red-sync-comp-time                1000
      media-policing                    enabled
      max-signaling-bandwidth           10000000
      max-untrusted-signaling           100
      min-untrusted-signaling           30
      app-signaling-bandwidth           0
      tolerance-window                  30
      rtcp-rate-limit                   0
      min-media-allocation              32000
      min-trusted-allocation            1000
      deny-allocation                   1000
      anonymous-sdp                     disabled
      arp-msg-bandwidth                 32000
      fragment-msg-bandwidth            0
      rfc2833-timestamp                 disabled
      default-2833-duration             100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event       disabled
      dnsalg-server-failover            disabled
      last-modified-by                  admin@console
      last-modified-date                2007-09-22 10:08:00
network-interface
      name                              M10
      sub-port-id                       0
      description
      hostname
      ip-address                        10.1.40.30
      pri-utility-addr
      sec-utility-addr
      netmask                           255.255.255.0
      gateway                           10.1.40.24
      sec-gateway
      gw-heartbeat
            state                             disabled
```

```
            heartbeat                       0
            retry-count                     0
            retry-timeout                   1
            health-score                    0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                     11
        hip-ip-list                     10.1.40.30
      ftp-address
        icmp-address                    10.1.40.30
      snmp-address
      telnet-address
      last-modified-by                admin@console
      last-modified-date              2008-09-24 16:45:01
network-interface
      name                            M00
      sub-port-id                     0
      description
      hostname
      ip-address                      192.168.3.2
      pri-utility-addr
      sec-utility-addr
      netmask                         255.255.255.0
      gateway                         192.168.3.11
      sec-gateway
      gw-heartbeat
            state                           disabled
            heartbeat                       0
            retry-count                     0
            retry-timeout                   1
            health-score                    0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                     11
        hip-ip-list                     192.168.3.2
      ftp-address                     192.168.3.2
        icmp-address                    192.168.3.2
      snmp-address
      telnet-address                  192.168.3.2
      last-modified-by                admin@10.1.1.188
      last-modified-date              2008-09-24 18:05:45
phy-interface
      name                            M00
      operation-type                  Media
      port                            0
      slot                            0
      virtual-mac
      admin-state                     enabled
      auto-negotiation                enabled
      duplex-mode                     FULL
      speed                           100
      last-modified-by                admin@console
```

```
        last-modified-date             2007-09-22 10:04:09
phy-interface
        name                           M10
        operation-type                 Media
        port                           0
        slot                           1
        virtual-mac
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100
        last-modified-by               admin@console
        last-modified-date             2007-09-22 10:04:31
realm-config
        identifier                     core
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M10:0
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        qos-enable                     disabled
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        fallback-bandwidth             0
        max-priority-bandwidth         0
        max-latency                    0
        max-jitter                     0
        max-packet-loss                0
        observ-window-size             0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
```

```
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        last-modified-by                admin@console
        last-modified-date              2007-09-22 10:11:43
realm-config
        identifier                      access
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M00:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              NAT_IP
        manipulation-string
```

```
      class-profile
      average-rate-limit             0
      access-control-trust-level     none
      invalid-signal-threshold       0
      maximum-signal-threshold       0
      untrusted-signal-threshold     0
      nat-trust-threshold            0
      deny-period                    30
      ext-policy-svr
      symmetric-latching             disabled
      pai-strip                      disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching            none
      restriction-mask               32
      accounting-enable              enabled
      user-cac-mode                  none
      user-cac-bandwidth             0
      user-cac-sessions              0
      icmp-detect-multiplier         0
      icmp-advertisement-interval    0
      icmp-target-ip
      monthly-minutes                0
      net-management-control         disabled
      delay-media-update             disabled
      refer-call-transfer            disabled
      codec-policy
      codec-manip-in-realm           disabled
      constraint-name
      call-recording-server-id
      stun-enable                    disabled
      stun-server-ip                 0.0.0.0
      stun-server-port               3478
      stun-changed-ip                0.0.0.0
      stun-changed-port              3479
      match-media-profiles
      qos-constraint
      last-modified-by               admin@console
      last-modified-date             2008-09-22 16:58:57
session-agent
      hostname                       x.x.x.x          (SingTel SBC)
      ip-address                     x.x.x.x          (SingTel SBC)
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       access
      egress-realm-id
      description
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
```

```
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method
ping-interval                  0
ping-send-mode                 keep-alive
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
last-modified-by               admin@console
last-modified-date             2008-10-04 15:47:19
```

```
session-agent
      hostname                       10.1.40.24
      ip-address                     10.1.40.24
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               StaticTCP
      realm-id                       core
      egress-realm-id
      description
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method
      ping-interval                  0
      ping-send-mode                 keep-alive
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                       disabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                    disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
      p-asserted-id
      trunk-group
```

```
      max-register-sustain-rate      0
      early-media-allow
      invalidate-registrations       disabled
      rfc2833-mode                   none
      rfc2833-payload                0
      codec-policy
      enforcement-profile
      refer-call-transfer            disabled
      reuse-connections              NONE
      tcp-keepalive                  none
      tcp-reconn-interval            0
      max-register-burst-rate        0
      register-burst-window          0
      last-modified-by               admin@10.1.1.12
      last-modified-date             2008-09-27 14:51:16
sip-config
      state                          enabled
      operation-mode                 dialog
      dialog-transparency            enabled
      home-realm-id                  core
      egress-realm-id
      nat-mode                       None
      registrar-domain               *
      registrar-host                 *
      registrar-port                 5060
      register-service-route         always
      init-timer                     500
      max-timer                      4000
      trans-expire                   32
      invite-expire                  180
      inactive-dynamic-conn          32
      enforcement-profile
      pac-method
      pac-interval                   10
      pac-strategy                   PropDist
      pac-load-weight                1
      pac-session-weight             1
      pac-route-weight               1
      pac-callid-lifetime            600
      pac-user-lifetime              3600
      red-sip-port                   1988
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      add-reason-header              disabled
      sip-message-len                4096
      enum-sag-match                 disabled
      extra-method-stats             disabled
      registration-cache-limit       0
      register-use-to-for-lp         disabled
      options                        max-udp-length=0
      add-ucid-header                disabled
      proxy-sub-events
      last-modified-by               admin@10.1.1.12
      last-modified-date             2008-09-27 18:05:58
sip-feature
```

```
      name                          avayaoption
      realm                         option-1
      support-mode-inbound          Pass
      require-mode-inbound          Reject
      proxy-require-mode-inbound    Pass
      support-mode-outbound         Pass
      require-mode-outbound         Reject
      proxy-require-mode-outbound   Pass
      last-modified-by              admin@10.1.1.12
      last-modified-date            2008-09-27 17:21:01
sip-interface
      state                         enabled
      realm-id                      core
      description
      sip-port
            address                       10.1.40.30
            port                          5060
            transport-protocol            TCP
            tls-profile
            allow-anonymous               agents-only
            ims-aka-profile
      carriers
      trans-expire                  0
      invite-expire                 0
      max-redirect-contacts         0
      proxy-mode
      redirect-action
      contact-mode                  none
      nat-traversal                 none
      nat-interval                  30
      tcp-nat-interval              90
      registration-caching          enabled
      min-reg-expire                300
      registration-interval         3600
      route-to-registrar            disabled
      secured-network               disabled
      teluri-scheme                 disabled
      uri-fqdn-domain
      trust-mode                    all
      max-nat-interval              3600
      nat-int-increment             10
      nat-test-increment            30
      sip-dynamic-hnt               disabled
      stop-recurse                  401,407
      port-map-start                0
      port-map-end                  0
      in-manipulationid
      out-manipulationid
      manipulation-string
      sip-ims-feature               disabled
      operator-identifier
      anonymous-priority            none
      max-incoming-conns            0
      per-src-ip-max-incoming-conns 0
      inactive-conn-timeout         0
      untrusted-conn-timeout        0
```

```
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode           pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                 none
      implicit-service-route         disabled
      rfc2833-payload                101
      rfc2833-mode                   transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                disabled
      enforcement-profile
      refer-call-transfer            disabled
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      last-modified-by               admin@10.1.1.12
      last-modified-date             2008-09-27 18:11:51
sip-interface
      state                          enabled
      realm-id                       access
      description
      sip-port
            address                        192.168.3.2
            port                           5060
            transport-protocol             UDP
            tls-profile
            allow-anonymous                agents-only
            ims-aka-profile
      carriers
      trans-expire                   0
      invite-expire                  0
      max-redirect-contacts          0
      proxy-mode
      redirect-action
      contact-mode                   none
      nat-traversal                  none
      nat-interval                   30
      tcp-nat-interval               90
      registration-caching           enabled
      min-reg-expire                 300
      registration-interval          3600
      route-to-registrar             disabled
      secured-network                disabled
      teluri-scheme                  disabled
      uri-fqdn-domain
      trust-mode                     all
      max-nat-interval               3600
      nat-int-increment              10
      nat-test-increment             30
      sip-dynamic-hnt                disabled
```

```
      stop-recurse                   401,407
      port-map-start                 0
      port-map-end                   0
      in-manipulationid
      out-manipulationid
      manipulation-string
      sip-ims-feature                disabled
      operator-identifier
      anonymous-priority             none
      max-incoming-conns             0
      per-src-ip-max-incoming-conns  0
      inactive-conn-timeout          0
      untrusted-conn-timeout         0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode           pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                 none
      implicit-service-route         disabled
      rfc2833-payload                101
      rfc2833-mode                   transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                disabled
      enforcement-profile
      refer-call-transfer            disabled
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      last-modified-by               admin@console
      last-modified-date             2008-09-24 16:49:46
sip-manipulation
      name                           NAT_IP
      description
      header-rule
            name                           From
            header-name                    From
            action                         manipulate
            comparison-type                case-sensitive
            match-value
            msg-type                       request
            new-value
            methods
            element-rule
                  name                           From
                  parameter-name                 From
                  type                           uri-host
                  action                         replace
                  match-val-type                 ip
                  comparison-type                case-sensitive
                  match-value
```

```
                new-value                       $LOCAL_IP
      header-rule
            name                          To
            header-name                   To
            action                        manipulate
            comparison-type               case-sensitive
            match-value
            msg-type                      request
            new-value
            methods
            element-rule
                  name                          To
                  parameter-name                To
                  type                          uri-host
                  action                        replace
                  match-val-type                ip
                  comparison-type               case-sensitive
                  match-value
                  new-value                     $REMOTE_IP
      last-modified-by              admin@console
      last-modified-date            2008-09-22 16:56:32
steering-pool
      ip-address                    192.168.3.2
      start-port                    20000
      end-port                      20099
      realm-id                      access
      network-interface             M00:0
      last-modified-by              admin@console
      last-modified-date            2008-09-24 16:54:48
steering-pool
      ip-address                    10.1.40.30
      start-port                    20000
      end-port                      20099
      realm-id                      core
      network-interface             M10:0
      last-modified-by              admin@console
      last-modified-date            2008-09-24 16:55:05
system-config
      hostname                      sd1
      description
      location
      mib-system-contact
      mib-system-name
      mib-system-location
      snmp-enabled                  enabled
      enable-snmp-auth-traps        disabled
      enable-snmp-syslog-notify     disabled
      enable-snmp-monitor-traps     disabled
      enable-env-monitor-traps      disabled
      snmp-syslog-his-table-length  1
      snmp-syslog-level             WARNING
      system-log-level              WARNING
      process-log-level             NOTICE
      process-log-ip-address        0.0.0.0
      process-log-port              0
      collect
```

```
            sample-interval                5
            push-interval                  15
            boot-state                     disabled
            start-time                     now
            end-time                       never
            red-collect-state              disabled
            red-max-trans                  1000
            red-sync-start-time            5000
            red-sync-comp-time             1000
            push-success-trap-state        disabled
      call-trace                     disabled
      internal-trace                 disabled
      log-filter                     all
      default-gateway                192.168.3.11
      restart                        enabled
      exceptions
      telnet-timeout                 0
      console-timeout                0
      remote-control                 enabled
      cli-audit-trail                enabled
      link-redundancy-state          disabled
      source-routing                 enabled
      cli-more                       disabled
      terminal-height                24
      debug-timeout                  0
      trap-event-lifetime            0
      cleanup-time-of-day            00:00
      last-modified-by               admin@console
      last-modified-date             2008-09-24 17:09:04
task done
```

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.