



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Evolution Server, Avaya Aura® Session Manager, and Avaya Aura® Session Border Controller with AT&T Mobility SIP Trunk Services in Puerto Rico – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider AT&T Mobility in Puerto Rico and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller 6.0, Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager Evolution Server 6.0.1, and various Avaya endpoints.

The AT&T Mobility SIP Trunk Service in Puerto Rico provides PSTN access via a SIP trunk between the enterprise and the AT&T network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

AT&T Mobility in Puerto Rico is a member of the Avaya DevConnect Service Provider Program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1. Introduction	4
2. Test Scope and Results.....	4
2.1. Interoperability Compliance Testing.....	4
2.2. Test Results	5
2.3. Support.....	6
3. Reference Configuration.....	6
4. Equipment and Software Validated	8
5. Configure Communication Manager.....	9
5.1. Licensing and Capacity.....	9
5.2. System Features.....	10
5.3. IP Node Names.....	11
5.4. Codecs.....	11
5.5. IP Network Region	12
5.6. Signaling Group.....	13
5.7. Trunk Group.....	15
5.8. Calling Party Information.....	17
5.9. Inbound Routing.....	18
5.10. Outbound Routing.....	19
6. Configure Avaya Aura® Session Manager.....	22
6.1. System Manager Login and Navigation	23
6.2. Specify SIP Domain	24
6.3. Add Location	25
6.4. Add Adaptation Module	27
6.5. Add SIP Entities	28
6.6. Add Entity Links	32
6.7. Add Routing Policies	34
6.8. Add Dial Patterns.....	35
6.9. Add/View Session Manager	37
7. Configure Avaya Aura® Session Border Controller	38
7.1. Installation Wizard.....	38
7.1.1. Network Settings	39
7.1.2. VPN Access.....	40
7.1.3. SBC	41
7.1.4. Confirm Installation.....	43
7.2. Post Installation Configuration	44
7.2.1. Service Provider Domain and Options Frequency	45
7.2.2. Media Ports	46
7.2.3. Blocked Headers.....	47
7.2.4. Diversion Header Domain.....	49

7.2.5. Request URI	53
7.2.6. Save the Configuration	54
8. AT&T Mobility SIP Trunk Service Configuration	54
9. Verification and Troubleshooting	55
10. Conclusion.....	56
11. References.....	57
Appendix A: Avaya Aura® SBC Configuration File	58

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between AT&T Mobility SIP Trunk Service in Puerto Rico and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Border Controller or Avaya Aura® Session Manager.

The AT&T Mobility in Puerto Rico SIP Trunk service referenced within these Application Notes is designed for enterprise business customers. Customers using this service with the Avaya SIP-enabled enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

During the next pages and for brevity in these Application Notes, the service provider's name "AT&T Mobility in Puerto Rico" will be abbreviated and referred as "AT&T Mobility" or just as "AT&T".

2. Test Scope and Results

2.1. Interoperability Compliance Testing

A simulated enterprise site comprised of Communication Manager, Session Manager and the Session Border Controller was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to the AT&T Mobility SIP Trunk service.

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

- Incoming PSTN calls to various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
- Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phones.
- Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two signaling protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types, including: local, long distance, international, outbound toll-free, emergency (911) and local directory assistance (411, 611).
- Codecs G729A and G.711MU and proper codec negotiation.

- DTMF tone transmissions passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection using SIP REFER for transfer of inbound call back to PSTN.

Items not supported or not tested included the following:

- Operator services such as dialing 0 or 0 + 10 digits are not supported in this offer by AT&T in Puerto Rico.
- Inbound toll-free are supported but were not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of the AT&T Mobility SIP Trunk Service with the Avaya SIP-enabled enterprise solution was completed with successful results with the exception of the observations and limitations described below:

- **Call Display on PSTN transferred calls:** Call display was not properly updated on the PSTN phone to reflect the true connected party on calls that are transferred to the PSTN from the enterprise. After the call transfer was completed, the PSTN phone showed the party that initiated the transfer instead of the actual connected party.
- **Network Call Redirection:** When a Communication Manager vector is programmed to redirect an inbound call to a PSTN number before answering the call in the vector, AT&T will send an ACK to the “302 Moved Temporarily” SIP message from the enterprise, but it will not redirect the call to the new party in the Contact header of the 302 message. The initiator of the inbound call hears silence. Network call redirection works successfully when the Communication Manager vector is programmed to redirect the inbound call to a PSTN number after answering the call first in the vector (using SIP REFER message for network call redirection instead of the 302 message).
- **Network Call Redirection using REFER with redirected party Busy:** In the testing environment, when an inbound call was made to the enterprise, to a vector redirecting the call to another PSTN endpoint that was busy, the caller will hear a busy tone, but AT&T will not return a “486 Busy Here”, preventing any additional processing of the call by Communication Manager, like the routing of the call to a local agent on the enterprise.
- **SIP User to User Information:** When a Communication Manager vector is programmed to send “User-to-User Information” (UUI) to a remote party, the information is generated and included in the REFER header sent to AT&T, but the UUI is not passed to the destination SIP endpoint.
- **T.38 Fax:** T.38 fax calls did not complete reliably. Thus, it is recommended that T.38 Fax is not used with this solution.

2.3. Support

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

For technical support on the AT&T Mobility SIP Trunk Services offer, call the AT&T Mobility Network Operations Center at 787-717-9900.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the AT&T Mobility SIP Trunk Service through a public Internet WAN connection, which is the configuration used for the Compliance Testing.

For security purposes, private addresses are shown in these Application Notes for the SBC and the ITSP network interfaces, instead of the real public IP addresses used during the tests. Also PSTN routable phone numbers used in the compliance test have been changed to non-routable ones.

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

- Avaya Common Server HP Proliant DL360 running Avaya Aura® Communication Manager and Communication Manager Messaging.
- Avaya Common Server HP Proliant DL360 running Avaya Aura® Session Manager.
- Avaya Common Server HP Proliant DL360 running Avaya Aura® System Manager.
- Avaya Common Server HP Proliant DL360 running Avaya Aura® Session Border Controller.
- Avaya G450 Media Gateway
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Session Border Controller. 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. The transport protocol between the SBC and AT&T Mobility across the public IP network is UDP. The transport protocol between the SBC and the enterprise Session Manager across the enterprise IP network is TCP.

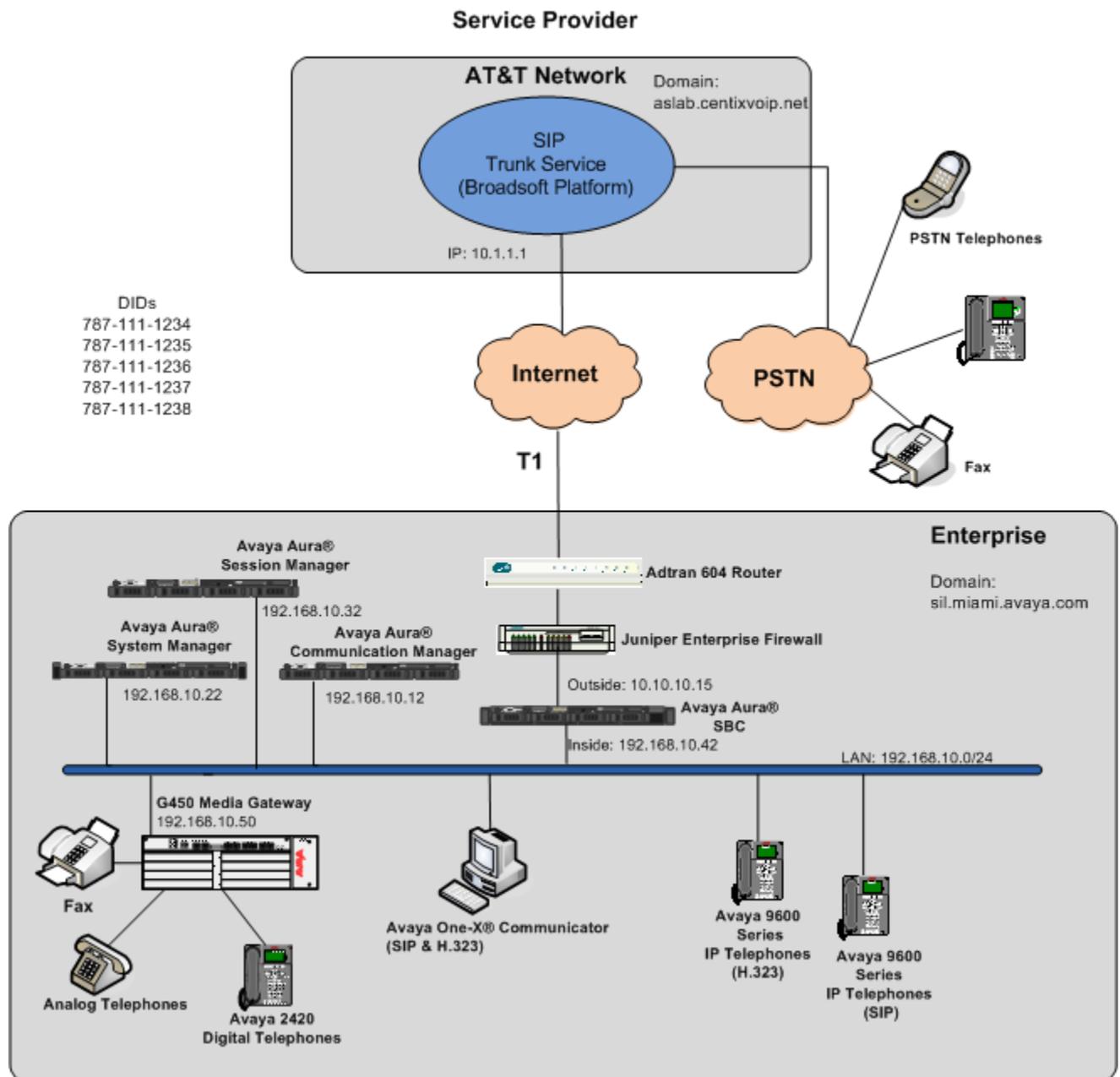


Figure 1: Avaya SIP Enterprise Solution connecting to AT&T Mobility SIP Trunk Service.

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk, and not affect 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 the 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 were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Session Border Controller for egress to the AT&T network.

Since Puerto Rico is a country member of the North American Numbering Plan (NANP), the user dialed 10 digits for local calls, and 11 (1 + 10) digits for other calls between the NANP.

4. Equipment and Software Validated

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

Component	Release
Avaya	
Avaya Aura® Communication Manager on a HP® Proliant DL360 G7 Server.	6.0.1 SP3 (R016x.00.1.510.1)
Avaya Aura® Session Manager on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 3 (ASM 6.1.3.0.613006)
Avaya Aura® System Manager on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 3 Build No. 6.1.0.0.7345-6.1.5.112
Avaya Aura® Session Border Controller on a HP® Proliant DL360 G7 Server.	SBCT 6.0.2.0.3 (sbc E362P4)
Avaya G450 Media Gateway	31.19.2
Avaya 96xx Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.1
Avaya 96xx Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.6.4
Avaya one-X Communicator (H.323, SIP)	6.1.1.02-SP1-32858
AT&T Puerto Rico SIP Trunking	
Acme-Packet Net-Net 4250 SBC	SC6.1.0 MR-9 GA (Build 938)
BroadWorks Soft Switch	R17
Nortel CS2K PSTN Gateway	CVM11

The specific equipment and software above were used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Communication Manager.

This section describes the procedure for configuring Communication Manager for the AT&T Mobility SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from AT&T. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and 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 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 and from the service provider. The example shows that **24000** licenses are available and **26** 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 10
Maximum Concurrently Registered IP Stations: 18000 2
Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
Maximum Concurrently Registered IP eCons: 414 0
Max Concur Registered Unauthenticated H.323 Stations: 100 0
Maximum Video Capable Stations: 18000 0
Maximum Video Capable IP Softphones: 18000 1
Maximum Administered SIP Trunks: 24000 26
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
Maximum Number of DS1 Boards with Echo Cancellation: 522 0
Maximum TN2501 UAL Boards: 128 0
Maximum Media Gateway UAL 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: 100 0
(NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

Use the **change system-parameters features** 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? n
      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

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

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.

```
display 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:
      International Access Code:
```

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 DL360 Server running Communication Manager (procr) and Session Manager (asm). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

```
change node-names ip Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
asm	192.168.10.32
default	0.0.0.0
msgserver	192.168.10.12
procr	192.168.10.12
procr6	::
rselab	192.168.0.220

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 compliance test, ip-codec-set 2 was used for this purpose. The AT&T SIP Trunk Service supports codecs G.729A and G.711MU, in this order of preference. Enter *G.729A* and *G.711MU* in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

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

Since T.38 fax testing was not reliable, it is recommended to disable T.38 Fax by setting the **Fax Mode** field to *off* on **Page 2**. However, if T.38 fax is to be used, set the **Fax Mode** to *t.38-standard*.

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

IP Codec Set		
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
FAX	off	0
Modem	off	0
TDD/TTY	off	3
Clear-channel	n	0

5.5. IP Network Region

Create a separate IP network region for the service provider trunk group. 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 trunks. 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 **sil.miami.avaya.com** as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region. Note that a Session Manager adaptation (**Section 6.4**) is used to convert this shared domain name to the specific domain expected by AT&T.
- 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: sil.miami.avaya.com
Name: AT&T PR SIP Trunk
MEDIA PARAMETERS
Codec Set: 2          Intra-region IP-IP Direct Audio: yes
                    Inter-region IP-IP Direct Audio: yes
                    IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 65535
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
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
AUDIO RESOURCE RESERVATION PARAMETERS
RSUP Enabled? n
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). 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).

change ip-network-region 2										Page	4 of	20
Source Region: 2		Inter Network Region Connection Management							I	M		
dst rgn	codec set	direct WAN	WAN-BW-limits Units		Video Total Norm	Intervening Prio Shr Regions		Dyn CAC	G A R	A G L	t c e	
1	2	y	NoLimit					n			t	
2	2									all		
3												
4												

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the 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 2 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). 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). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For ease of troubleshooting, the compliance test was conducted with the **Transport Method** set to *tcp* and the **Near-end Listen Port** and **Far-end Listen Port** set to *5070*. (For TCP, the well-known port value is 5060).
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer is a Session Manager.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *asm*. 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.

```

change signaling-group 2                                     Page 1 of 1
                    SIGNALING GROUP

Group Number: 2                                           Group Type: sip
IMS Enabled? n                                           Transport Method: tcp
  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: asm
Near-end Listen Port: 5070                             Far-end Listen Port: 5070
                                                    Far-end Network Region: 2
                                                    Far-end Secondary Node Name:

Far-end Domain: sil.miami.avaya.com

Incoming Dialog Loopbacks: eliminate                    Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                               RFC 3389 Comfort Noise? n
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

```

- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- 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. If this value is set to *n*, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

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 2 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 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 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                         Group Type: sip
Group Name: AT&T PR SIP Trunk                          COR: 1      TN: 1      TAC: 602
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: 2
                                                         Number of Members: 6
```

On **Page 2**, 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 default value of **600** seconds was used.

```
change trunk-group 2                                     Page 2 of 21
Group Type: sip
TRUNK PARAMETERS
Unicode Name: auto
                                                         Redirect On OPTIM Failure: 5000
SCCAN? n                                             Digital Loss Group: 18
                                                         Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
```

On **Page 3**, set the **Numbering Format** field to **private**. 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 when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with AT&T Mobility. Thus, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.10**).

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

  Numbering Format: private
                                                    UII Treatment: service-provider

  Replace Restricted Numbers? y
  Replace Unavailable Numbers? y
```

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.

On **Page 4**, set the **Network Call Redirection** field to **y**. This enables the use of the SIP REFER method for calls transferred back to the PSTN. Set the **Send Diversion Header** field to **y**. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to **n**.

Set the **Telephone Event Payload Type** to **101**, and **Convert 180 to 183 for Early Media** to **y**, the values preferred by AT&T. Default values were used for all other fields.

```
change trunk-group 2                                     Page 4 of 21
PROTOCOL VARIATIONS
  Mark Users as Phone? n
  Prepend '+' to Calling Number? n
  Send Transferring Party Information? n
  Network Call Redirection? y
  Send Diversion Header? y
  Support Request History? n
  Telephone Event Payload Type: 101

  Convert 180 to 183 for Early Media? y
  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 private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs), and they are used to authenticate the caller with the Service Provider. In the sample configuration, 5 DID numbers were assigned for testing. These 5 numbers were mapped to 5 extensions, 3001 to 3005. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 5 extensions.

```
change private-numbering 3 Page 1 of 2
NUMBERING - PRIVATE FORMAT
```

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3			4	Total Administered: 11
4	3001	2	7871111234	10	Maximum Entries: 540
4	3002	2	7871111235	10	
4	3003	2	7871111236	10	
4	3004	2	7871111237	10	
4	3005	2	7871111238	10	

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension length, beginning with 3, will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 3 Page 1 of 2
NUMBERING - PRIVATE FORMAT
```

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3	2	787111	10	Total Administered: 11
					Maximum Entries: 540

5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by AT&T is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 2 Page 1 of 30
```

INCOMING CALL HANDLING TREATMENT				
Service/ Feature	Number Len	Number Digits	Del	Insert
public-ntwrk	10	7871111234	10	3001
public-ntwrk	10	7871111235	10	3002
public-ntwrk	10	7871111236	10	3003
public-ntwrk	10	7871111237	10	3004
public-ntwrk	10	7871111238	10	3005
public-ntwrk	—	—	—	—

In a real customer environment, where the DID number is normally comprised of the local extension plus a prefix, a single entry can be applied for all extensions, like in the example below.

```
change inc-call-handling-trmt trunk-group 2 Page 1 of 30
```

INCOMING CALL HANDLING TREATMENT				
Service/ Feature	Number Len	Number Digits	Del	Insert
public-ntwrk	10	787111	6	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—

5.10. Outbound 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 String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	ext						
2	4	ext						
3	4	ext						
4	4	ext						
5	4	ext						
6	3	dac						
7	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	2	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:	_____
Abbreviated Dialing List2	Access Code:	_____
Abbreviated Dialing List3	Access Code:	_____
Abbreviated Dial - Prgm Group List	Access Code:	_____
Announcement	Access Code:	#1
Answer Back	Access Code:	_____
Attendant	Access Code:	_____
Auto Alternate Routing (AAR)	Access Code:	8
Auto Route Selection (ARS) – Access Code 1:	9	Access Code 2: _____
Automatic Callback Activation:	_____	Deactivation: _____
Call Forwarding Activation Busy/DA:	_____ All: _____	Deactivation: _____
Call Forwarding Enhanced Status:	_____ Act: _____	Deactivation: _____

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk group to the service provider.

change ars analysis 0							Page 2 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							
Percent Full: 1							
Dialed String	Total		Route	Call	Node	ANI	
	Min	Max	Pattern	Type	Num	Reqd	
011	10	18	2	intl	---	n	
787	10	10	2	hnpa	---	n	
1305	11	11	2	fnpa	---	n	
1786	11	11	2	fnpa	---	n	
1800	11	11	2	fnpa	---	n	
411	3	3	2	svcl	---	n	
611	3	3	2	svcl	---	n	
	---	---	---	---	---	n	
	---	---	---	---	---	n	
	---	---	---	---	---	n	
	---	---	---	---	---	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 2 for 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 2 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.
- **Pfx Mrk: 1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format: unk-unk** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR: next.**

```
change route-pattern 2                                     Page 1 of 3
                Pattern Number: 2   Pattern Name: AT&T SIP Trunk
                SCCAN? n           Secure SIP? n
  Grp FRL  NPA Pfx Hop Toll No.  Inserted          DCS/  IXC
  No   No   Mrk Lmt List Del  Digits          QSIG
                Dgts                               Intw
1:  2   0   1   -   -   -   -   -   -   -   -   -   -   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      rest      Subaddress
1:  y y y y y n  n      rest      unk-unk  next
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
```

6. Configure Avaya Aura® Session Manager

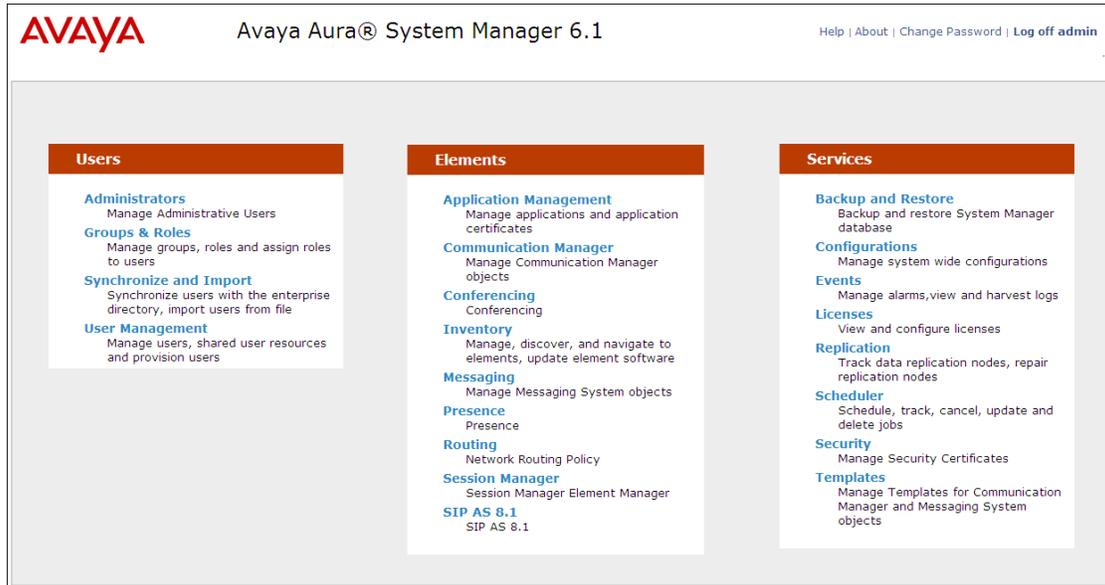
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform URI manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Session Border Controller.
- 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, corresponding to the Session Manager Server to be managed by System Manager.

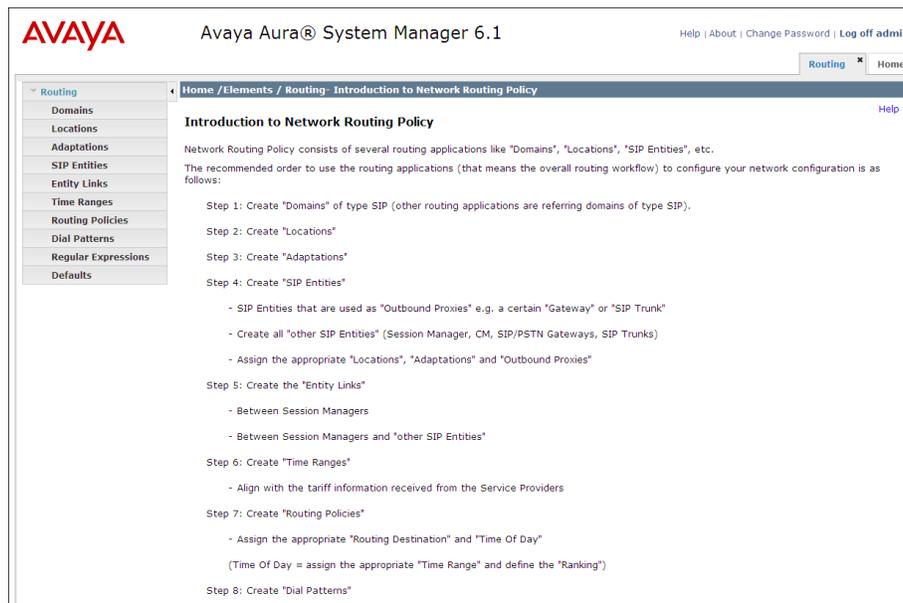
It may not be necessary to create all the items above when creating a connection to the service provider, since some of them would have already been defined as part of the initial Session Manager installation. This includes entries such as certain SIP domains, locations, SIP entities, and Session Manager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

6.1. 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 **Log On** (not shown). The screen shown below is then displayed.



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column to bring up the Introduction to Network Routing Policy screen.

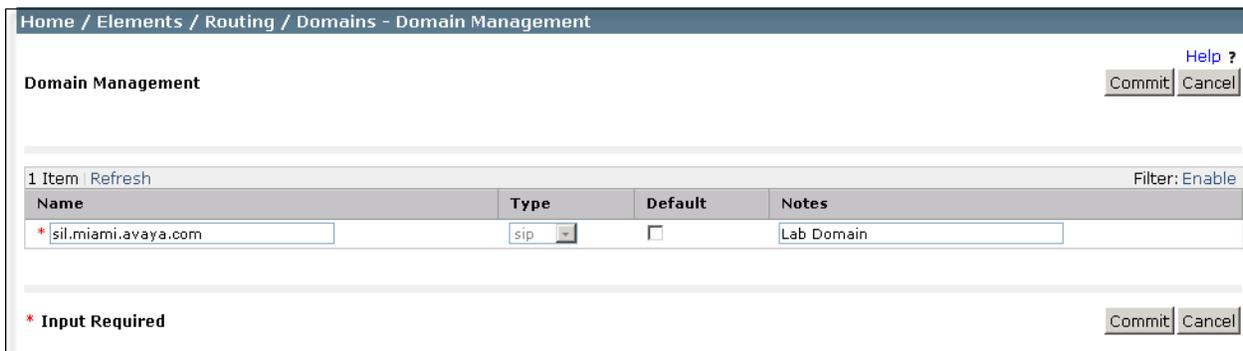


6.2. Specify SIP Domain

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, **sil.miami.avaya.com**, and the AT&T domain, **aslab.centixvoip.net**. 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.

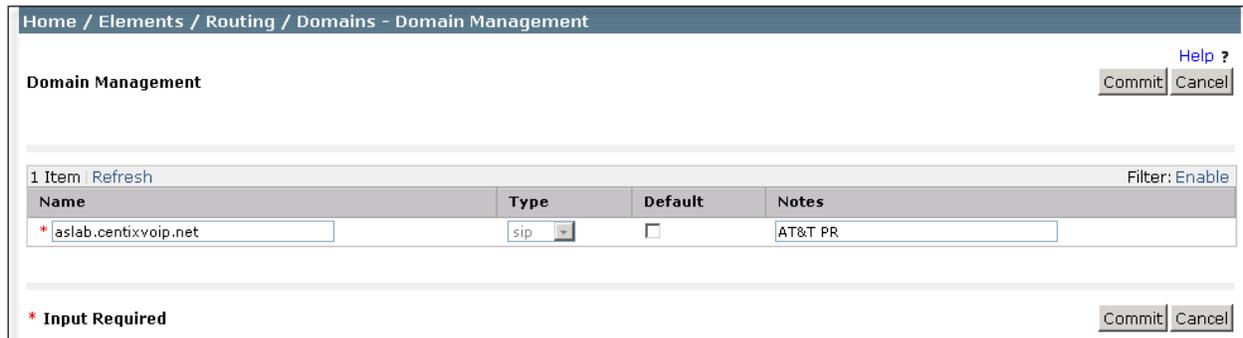


The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains - Domain Management'. Below this, the title 'Domain Management' is displayed on the left, and 'Help ?', 'Commit', and 'Cancel' buttons are on the right. A table below shows one item with the following details:

Name	Type	Default	Notes
* sil.miami.avaya.com	sip	<input type="checkbox"/>	Lab Domain

At the bottom of the table, there is a 'Filter: Enable' link. Below the table, there is a red asterisk and the text '* Input Required', followed by 'Commit' and 'Cancel' buttons.

The screen below shows the entry for the AT&T test domain.



The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains - Domain Management'. Below this, the title 'Domain Management' is displayed on the left, and 'Help ?', 'Commit', and 'Cancel' buttons are on the right. A table below shows one item with the following details:

Name	Type	Default	Notes
* aslab.centixvoip.net	sip	<input type="checkbox"/>	AT&T PR

At the bottom of the table, there is a 'Filter: Enable' link. Below the table, there is a red asterisk and the text '* Input Required', followed by 'Commit' and 'Cancel' buttons.

6.3. Add 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. 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 **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 **SIL Lab**, which includes all equipment in the Avaya Interoperability Lab, including Communication Manager and Session Manager itself, and resides in the 192.168.10.0 subnet. Click **Commit** to save.

Home / Elements / Routing / Locations - Location Details

Location Details Help ?
Commit Cancel

General

* Name:
Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec
Minimum Multimedia Bandwidth: Kbit/Sec
* Default Audio Bandwidth:

Location Pattern

1 Item Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*192.168.10.*	

Note that call bandwidth management parameters should be set per customer requirements.

Repeat the preceding procedure to create a separate Location for the AT&T SIP Trunk. Displayed below is the screen for addition of the *AT&T PR SIP Trunk* Location, which specifies the inside IP address for the Session Border Controller. Click **Commit** to save.

Home / Elements / Routing / Locations - Location Details Help ?

Location Details Commit Cancel

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): Kbit/Sec

Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth:

Location Pattern

1 Item Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* <input type="text" value="192.168.10.42"/>	<input type="text" value="Inside IP Address of AA-SBC"/>

6.4. Add Adaptation Module

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

For the compliance test, the adaptation “Outbound to AT&T” was created. It will be assigned to the SIP Entity for the Avaya Aura® Session Border Controller, later in these Application Notes. This adaptation uses the “DigitConversionAdapter” generic module and specifies two parameters that are used to adapt the FQDN to the domains expected by the AT&T network in the sample configuration.

- “**osrcd=aslab.centixvoip.net**”. This parameter enables the outbound source domain to be overwritten with “aslab.centixvoip.net”. For outbound PSTN calls from the enterprise to AT&T, the domain portion of the PAI header will now contain “aslab.centixvoip.net”, as expected by AT&T.
- “**odstd=aslab.centixvoip.net**”. This parameter enables the outbound destination domain to be overwritten with “aslab.centixvoip.net”. For outbound PSTN calls from the enterprise to AT&T, the domain portion of the Request-URI will contain “aslab.centixvoip.net”, as expected by AT&T.

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domains in this fashion. In the sample configuration, where “sil.miami.avaya.com” was already in use in the shared Avaya Lab environment, it was necessary for Session Manager to adapt the domain in the headers discussed above from “sil.miami.avaya.com” to the domain known to AT&T “aslab.centixvoip.net”.

The screen below shows the adaptation “Outbound to AT&T” created for the compliance test. All other fields were left with their default values.

The screenshot shows a web interface for configuring an adaptation. The breadcrumb trail is "Home / Elements / Routing / Adaptations - Adaptation Details". The page title is "Adaptation Details". There are "Commit" and "Cancel" buttons in the top right, along with a "Help ?" link. The "General" section contains the following fields:

- * Adaptation name:** Outbound to AT&T
- Module name:** DigitConversionAdapter (selected from a dropdown menu)
- Module parameter:** odstd=aslab.centixvoip.net osrcd=
- Egress URI Parameters:** (empty text box)
- Notes:** (empty text box)

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya Aura® Session Border Controller. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). 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:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the Avaya Aura® Session Border Controller.
- **Adaptation:** This field is only present if **Type** is not set to *Session Manager*. If applicable, select the **Adaptation** name created in **Section 6.4** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager signaling interface (virtual SM-100) is entered for **FQDN or IP Address**.

The screenshot shows a web browser window with the URL `Home / Elements / Routing / SIP Entities - SIP Entity Details`. The page title is "SIP Entity Details" and there are "Commit" and "Cancel" buttons in the top right corner. The "General" section contains the following fields:

- Name:** MA_Session Manager
- FQDN or IP Address:** 192.168.10.32
- Type:** Session Manager (dropdown menu)
- Notes:** SM100
- Location:** SIL Lab (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/New_York (dropdown menu)
- Credential name:** (empty text field)

The "SIP Link Monitoring" section contains the following field:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

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 to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	sil.miami.avaya.com	
<input type="checkbox"/>	5060	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	5061	TLS	sil.miami.avaya.com	
<input type="checkbox"/>	5070	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	5080	TCP	sil.miami.avaya.com	

Select : All, None

* Input Required

Commit Cancel

The compliance test used 2 **Port** entries:

- **5060** with **TCP** for connecting to Avaya Aura® Session Border Controller
- **5070** with **TCP** for connecting to Communication Manager

Port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. In addition, port 5080 with TCP was used in a separate link between Session Manager and a different Trunk Group in Communication manager. These two SIP Links were part of the previous configuration on Session Manager in the shared Lab environment, and were not directly relevant to the interoperability with AT&T.

In order for Session Manager to route SIP service provider traffic on a defined trunk group in Communication Manager, a separate entity link to Communication Manager is required.

The following screen shows the addition of this SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager.

The screenshot shows a web-based configuration interface for SIP Entity Details. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities - SIP Entity Details". In the top right corner, there are "Commit" and "Cancel" buttons, and a "Help ?" link. The main section is titled "SIP Entity Details" and has a "General" sub-section. The configuration fields are as follows:

- Name:** C.M. Trunk 2 AT&T PR
- FQDN or IP Address:** 192.168.10.12
- Type:** CM
- Notes:** (empty text box)
- Adaptation:** (empty dropdown menu)
- Location:** SIL Lab
- Time Zone:** America/New_York
- Override Port & Transport with DNS SRV:**
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text box)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

The following screen shows the addition of the SBC Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). For **Adaptation** field, select the adaptation module “**Outbound to AT&T**” previously defined in **Section 6.4**.

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details [Help ?](#)
Commit Cancel

General

* Name: MA_AA-SBC

* FQDN or IP Address: 192.168.10.42

Type: Other

Notes:

Adaptation: Outbound to AT&T

Location: AT&T PR SIP Trunk

Time Zone: America/Fortaleza

Override Port & Transport with DNS SRV:

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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 the Communication Manager for use only by service provider traffic and one to the Avaya Aura® Session Border Controller. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **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 screens illustrate the Entity Links to Communication Manager and the SBC. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. For the compliance test, TCP was used to facilitate troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM to CM Trunk 2	* MA_Session Manager	TCP	* 5070	* C.M. Trunk 2 AT&T PR	* 5070	<input checked="" type="checkbox"/>	

Entity Link to the SBC:

Home / Elements / Routing / Entity Links - Entity Links Help ?

Entity Links Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM to AA-SBC	* MA_Session Manager	TCP	* 5060	* MA_AA-SBC	* 5060	<input checked="" type="checkbox"/>	

* Input Required Commit Cancel

The following screen shows the complete list of Entity Links. Note that only the highlighted links were created for the compliance test, and are the ones relevant to these Application Notes.

Home / Elements / Routing / Entity Links - Entity Links Help ?

Entity Links

Edit New Duplicate Delete More Actions

8 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	Lab-HG SM to Lab-HG AA-SBC	Lab-HG SM	TCP	5060	Lab-HG AA-SBC	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Lab-HG SM to Lab-HG CM	Lab-HG SM	TCP	5080	Lab-HG CM	5080	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM to AA-SBC	MA_Session Manager	TCP	5060	MA_AA-SBC	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM to Acme s1p0	MA_Session Manager	TCP	5060	Acme Packet s1p0	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM to Acme s1p1	Lab-HG SM	TCP	5060	Acme Packet s1p1	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM to CM trunk 1	MA_Session Manager	TCP	5060	C.M. Trunk 1 SIP Phones.	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM to CM Trunk 10	MA_Session Manager	TCP	5080	C.M. Trunk 10 S8300D	5080	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM to CM Trunk 2	MA_Session Manager	TCP	5070	C.M. Trunk 2 AT&T PR	5070	<input checked="" type="checkbox"/>	

Select : All, None

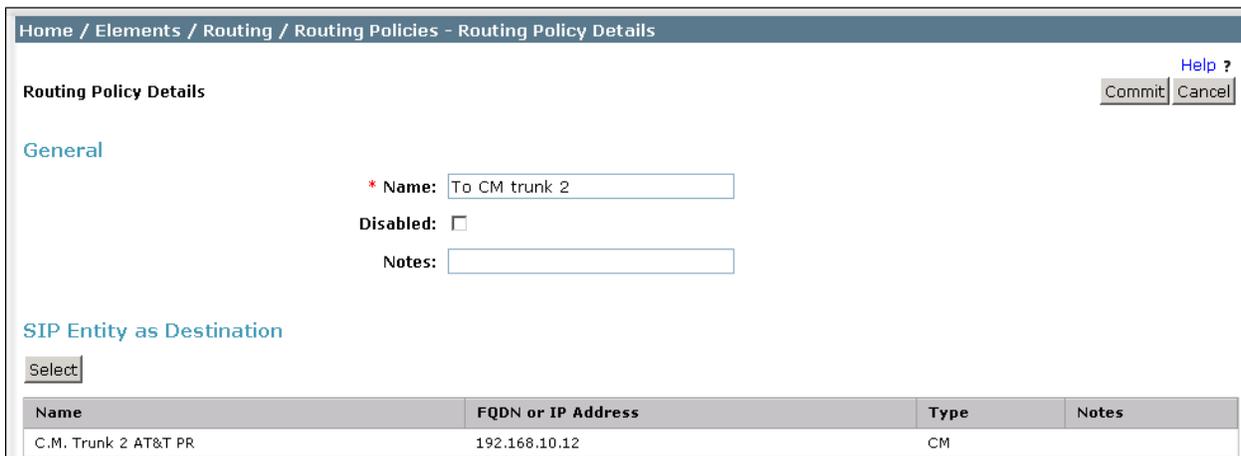
6.7. Add Routing Policies

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 Avaya Aura® Session Border Controller. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter the following values:

- **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 Session Border Controller.



Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details Help ?
Commit Cancel

General

* Name:

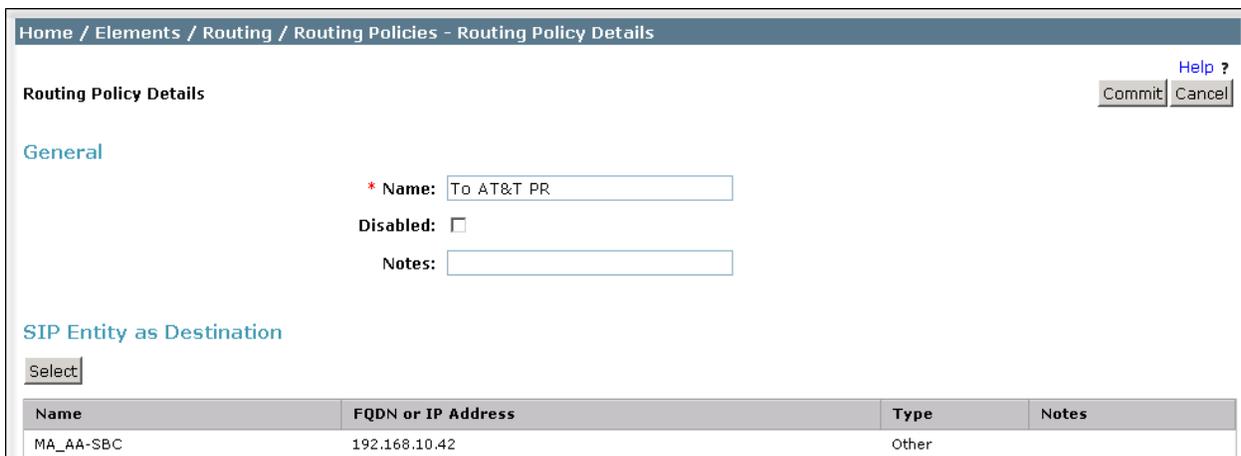
Disabled:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
C.M. Trunk 2 AT&T PR	192.168.10.12	CM	



Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details Help ?
Commit Cancel

General

* Name:

Disabled:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
MA_AA-SBC	192.168.10.42	Other	

6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to AT&T 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 navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **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 11 digit dialed numbers that begin with 1 uses route policy “**To AT&T PR**”.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Commit Cancel Help ?

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹ ▲	Originating Location Notes	Routing Policy Name	Rank ² ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To AT&T PR	0	<input type="checkbox"/>	MA_AA-SBC	

The second example shows that a 10 digit number starting with **787111**, to domain **sil.miami.avaya.com** and originating from the **AT&T PR SIP Trunk** location, will use route policy **To CM Trunk 2**. This number falls in the DID range assigned to the enterprise by AT&T. **AT&T PR SIP Trunk** is selected for the **Originating Location** because these calls come from the SBC, which resides in that location.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ?
Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹ ▲	Originating Location Notes	Routing Policy Name	Rank ² ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AT&T PR SIP Trunk		To CM trunk 2	0	<input type="checkbox"/>	C.M. Trunk 2 AT&T PR	

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** 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:

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.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura® System Manager 6.1", and utility links for "Help", "About", "Change Password", and "Log off admin". A breadcrumb trail shows the current location: "Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration". The left-hand navigation pane is expanded to "Session Manager Administration". The main content area is titled "View Session Manager" and features a "Return" button. Below the title, there are tabs for "General", "Security Module", "NIC Bonding", "Monitoring", "CDR", and "Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All". The "General" tab is selected, showing the following configuration fields:

- SIP Entity Name:** MA_Session Manager
- Description:** SIL_MA SM
- Management Access Point Host Name/IP:** 192.168.10.31
- Direct Routing to Endpoints:** Enable

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.



The screenshot shows a configuration window titled "Security Module" with a dropdown arrow. It contains several input fields with the following values:

Field	Value
SIP Entity IP Address	192.168.10.32
Network Mask	255.255.255.0
Default Gateway	192.168.10.254
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controller. This configuration is done in two parts. The first part is done during the SBC installation via the installation wizard. These Application Notes will not cover the SBC installation in its entirety but will include the use of the installation wizard (invoked during the loading of the SBC template). For information on installing the Avaya Aura® System Platform and the loading of the Avaya Aura® Session Border Controller template see [1].

The second part of the configuration is done after the installation is complete using the SBC web interface. The resulting SBC configuration file is shown in **Appendix A**.

7.1. Installation Wizard

During the installation of the Session Border Controller template, the installation wizard will prompt the installer for information that will be used to create the SBC initial configuration.

7.1.1. Network Settings

The first screen of the installation wizard is the **Network Settings** screen. Fill in the fields as described below and shown in the following screen:

- **IP Address:** Enter the IP address of the private side of the SBC.
- **Hostname:** Enter a host name for the SBC.
- **Domain:** Enter the domain used for the enterprise.
- **Default Domain:** Enter the domain used for the enterprise.

Click **Next Step** to continue

AVAYA

Home

Configuration

Installation

- Load
- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Save

Network Settings

Enter network settings

Domain-0 IP Address: 192.168.10.40

CDom IP Address: 192.168.10.41

Gateway IP Address: 192.168.10.254

Network Mask: 255.255.255.0

Primary DNS: 192.168.10.100

Secondary DNS (Optional):

Default Search List (Optional):

HTTPS Proxy (Optional) [IP Address:Port Number]:

Virtual Machine	IP Address	Hostname	Domain
SBC	192.168.10.42	aa-sbc	sil.miami.avaya.com (Optional)

Default Domain: sil.miami.avaya.com (Optional)

Apply to all VMs

[Previous Step](#) [Next Step](#)

7.1.2. VPN Access

VPN remote access to the Session Border Controller was not part of the compliance test. Thus, on the **VPN Access** screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?** Click **Next Step** to continue.

AVAYA

Home

Configuration

Installation

- Load
- Network Settings
- Logins
- VPN Access**
- SBC
- Summary
- Save

VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

Yes No

VPN Access Configuration

VPN Router IP Address (Optional)

Remote Access Network

Remote Access Network Subnet Mask

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

[Previous Step](#) [Next Step](#)

7.1.3. SBC

On the **SBC** screen, fill in the fields as described below and shown in the following screen:

In the **SIP Service Provider Data** section:

- **Service Provider:** From the pull-down menu, select the name of the service provider to which the SBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for AT&T Mobility in Puerto Rico. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was complete.
- **Port:** Enter the port number that the service provider uses to listen for SIP traffic.
- **IP Address1:** Enter the AT&T provided IP address of the service provider SIP Proxy. If the service provider has multiple proxies, enter the primary and secondary proxy on this screen and additional proxies can be added after installation.
- **Signaling/Media Network1:** Enter the AT&T provided subnet where signaling/media traffic will originate. If signaling/media traffic can originate from multiple networks, two network addresses can be entered on this screen and additional networks can be added after installation.
- **Signaling/Media Netmask1:** Enter the netmask corresponding to **Signaling/Media Network1**.

The screenshot shows the Avaya SBC configuration interface. The top left features the Avaya logo and a navigation menu with options like Configuration, Installation, Load, Network Settings, Logins, VPN Access, SBC, Summary, and Save. The main content area is titled 'SBC Session Border Controller Data' and contains a 'SIP Service Provider Data' section. This section includes fields for Service Provider (set to 'Generic'), Port (5060), IP Address1 (10.1.1.1), Signalling/Media Network1 (10.1.1.0), Signalling/Media Netmask1 (255.255.255.0), and optional fields for IP Address2, Signalling/Media Network2, Signalling/Media Netmask2, and Hunting.

SIP Service Provider Data			
Service Provider	Port		
Generic	5060		
IP Address1	Signalling/Media Network1	Signalling/Media Netmask1	
10.1.1.1	10.1.1.0	255.255.255.0	
IP Address2 (Optional)	Signalling/Media Network2 (Optional)	Signalling/Media Netmask2 (Optional)	Hunting (Optional)

Further down on the same **SBC** screen, fill in the fields as described below:

In the **SBC Network Data** section:

- **Public IP Address:** Enter the IP address of the public side of the SBC.
- **Public Net Mask:** Enter the netmask associated with the public network to which the SBC connects.
- **Public Gateway:** Enter the default gateway of the public network.

In the **Enterprise SIP Server** section:

- **SIP Domain:** Enter the enterprise SIP domain.
- **IP Address1:** Enter the IP address of the Enterprise SIP Server to which the SBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface.
- **Transport1:** From the pull-down menu, select the transport protocol to be used for SIP traffic between the SBC and Session Manager.

Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to continue to the final step.

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	192.168.10.42	255.255.255.0	192.168.10.254
Public	<input type="text" value="10.10.10.15"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="10.10.10.254"/>

Enterprise SIP Server		
SIP Domain <input type="text" value="sil.miami.avaya.c"/>		
IP Address1 <input type="text" value="192.168.10.32"/>	Transport1 <input type="text" value="TCP"/>	
IP Address2 (Optional) <input type="text"/>	Transport2 (Optional) <input type="text"/>	Hunting (Optional) <input type="text"/>

[◀ Previous Step](#) [Next Step ▶](#)

7.1.4. Confirm Installation

The **Confirm Installation** screen will indicate if any required or optional fields have not been set. The list of required fields that have not been set should be empty. If not, click **Previous Step** to navigate to the relevant screen to set the required fields. Otherwise, click **Accept** to finish the wizard and to continue the overall template installation.

AVAYA

Home

- Configuration
- Installation
 - Load
 - Network Settings
 - Logins
 - VPN Access
 - SBC
 - Summary
 - Save

Save

The following optional fields have not been set

- [Default Search List](#)
- [Secondary DNS](#)
- [HTTPS Proxy](#)
- [SBC Service Provider IP Address 2](#)
- [SBC Service Provider Hunting](#)
- [SBC Service Provider Media Netmask2](#)
- [SBC Service Provider Media Network2](#)
- [SBC Enterprise SIP Server IP2](#)
- [SBC Enterprise SIP Server Transport2](#)
- [SBC Enterprise SIP Server Hunting](#)

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook, 555-025-600*.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

[◀ Previous Step](#)

7.2. Post Installation Configuration

The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 7.1.3**. Since a **Generic** provider was selected in the installation wizard, additional manual changes must also be performed. These changes are performed by accessing the browser-based GUI of the Session Border Controller, using the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured in **Section 7.1.1**. Log in with the proper credentials.

Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

Username:

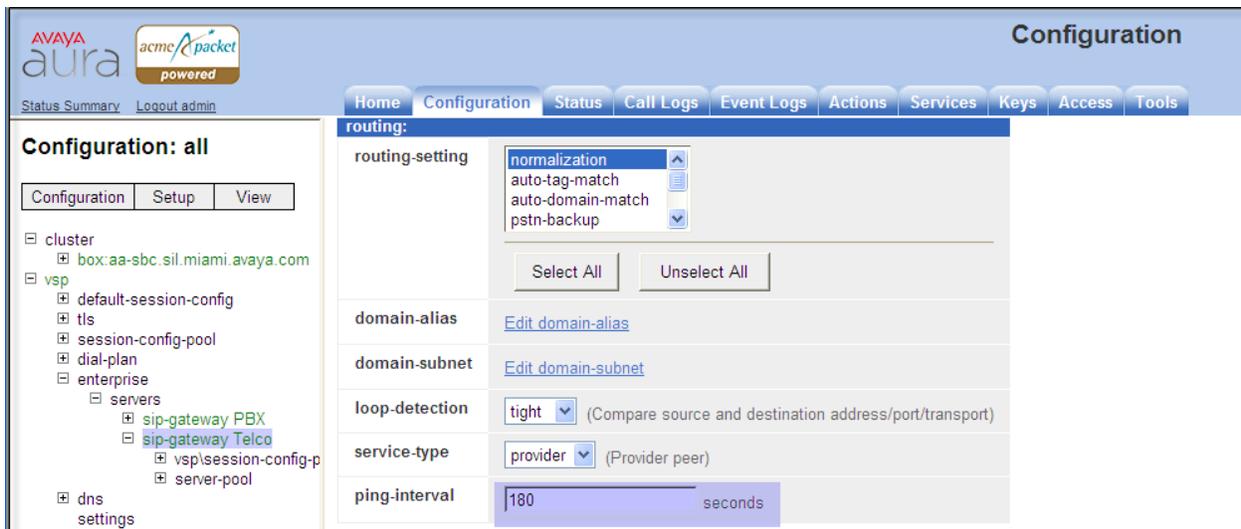
Password:

7.2.1. Service Provider Domain and Options Frequency

To enter the domain for the AT&T Mobility network, on the **Configuration** tab, navigate to **vsp** → **enterprise** → **servers** → **sig-gateway Telco**. In the **domain** field, enter the service provider's domain. For the compliance test, the domain **aslab.centixvoip.net** was used.



To set the frequency of the OPTIONS messages sent from the SBC to the service provider, click **Show Advanced** in the previous figure and scroll down to the **Routing** section of the form. Enter the desired interval in the **ping-interval** field. For the compliance test, 180 seconds was used. Click **Set** at the top of the form (shown in previous figure).



7.2.2. Media Ports

To adjust the port range assigned to media streams leaving the outside interface of the SBC, to match the range specified by AT&T for the compliance test of 50000 to 54999, navigate to **cluster → box → interface eth2 → ip outside**. On the right pane, navigate to **media-ports** and click **Configure**.

The screenshot shows the Avaya Aura Configuration interface. The breadcrumb path is **Configure cluster\box:aa-sbc.sil.miami.avaya.com\interface eth2\ip outside**. The left sidebar shows a tree view with 'ip outside' selected. The main panel displays configuration options for the 'ip outside' resource. The 'media-ports' section is highlighted with a blue bar and a 'Configure' button.

general:	
* name	outside
admin	enabled (Resource is active)
* ip-address	* type: static (static IP address)
	* address/mask: 10.10.10.15/24 (n.n.n.n/n)
geolocation	0
security-domain	enter [] or select from <Not configured>
address-scope	enter [] or select from <Not configured>
filter-intf	disabled (Resource is inactive)
media-ports	Configure

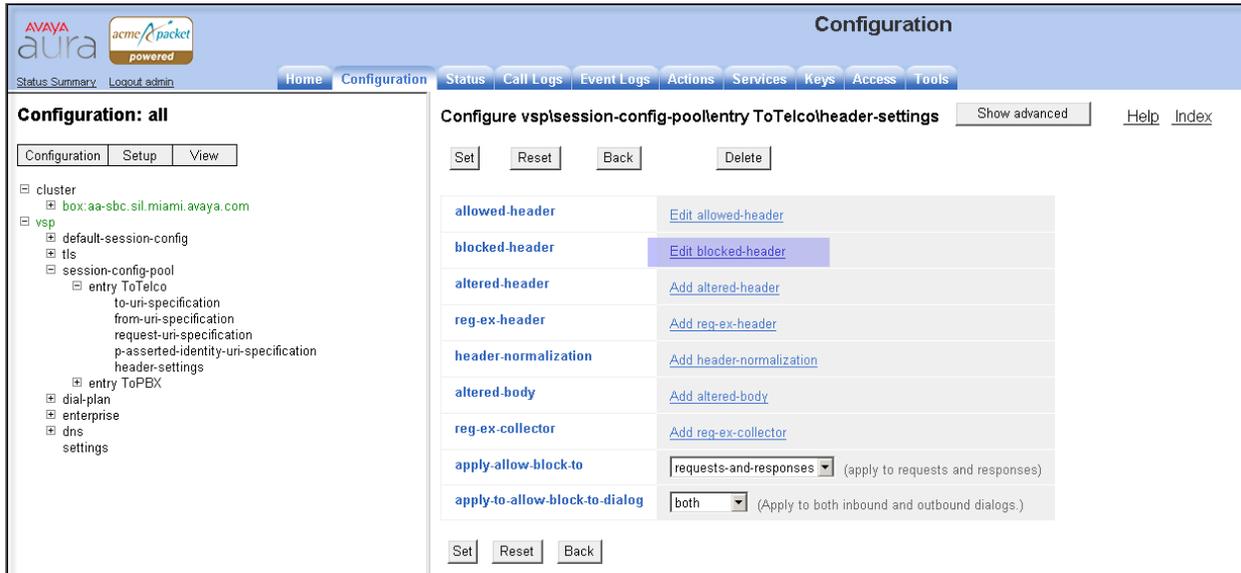
On the next screen, set the value for **base-port** to **50000**, and the **count** to **4999**. Click **Set** to complete the configuration.

The screenshot shows the Avaya Aura Configuration interface for the 'media-ports' resource. The breadcrumb path is **Configure cluster\box:aa-sbc.sil.miami.avaya.com\interface eth2\ip outside\media-ports**. The main panel displays configuration options for the 'media-ports' resource. The 'base-port' and 'count' fields are highlighted with blue bars.

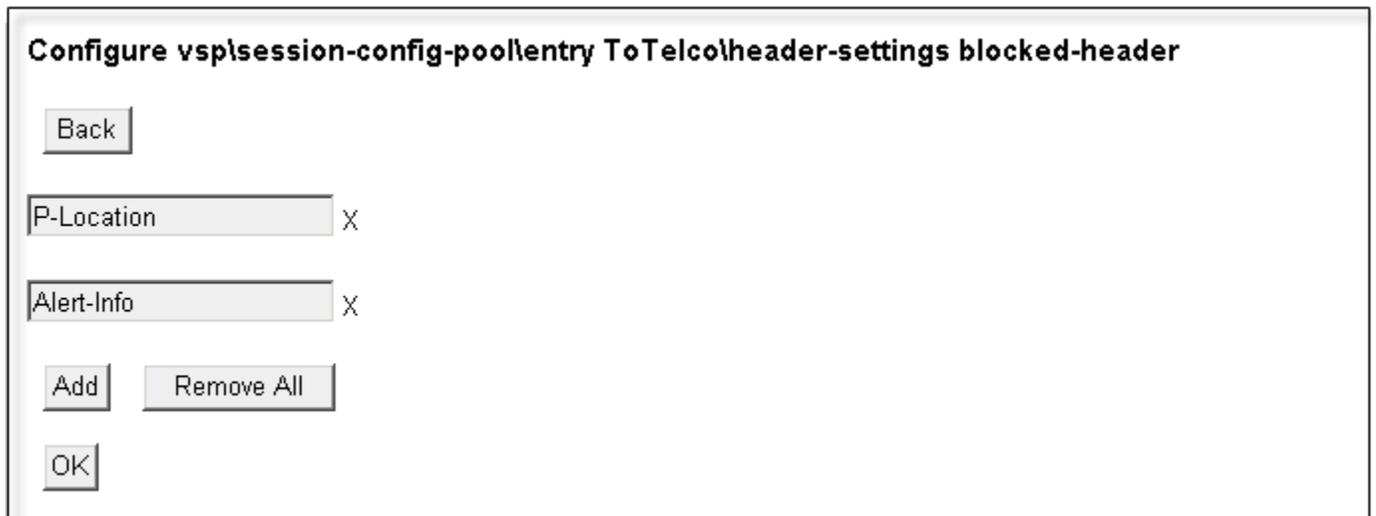
admin	enabled (Resource is active)
base-port	50000 (at minimum 1, default=20000)
count	4999 (from 0 to 65,535)
idle-monitor	enabled (Resource is active)

7.2.3. Blocked Headers

The P-Location and Alert-Info headers are sent in SIP messages from the Session Manager to the AT&T network. These headers contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries. These headers were simply removed (blocked) from both requests and responses for outbound calls. To create a rule for blocking a header on an outbound call, first navigate to **vsp** → **session-config-pool** → **entry ToTelco** → **header-settings**. Click **Edit blocked-header**.



In the right pane that appears, click **Add**. In the blank fields, enter the name of the header to be blocked. After all the blocked headers are added, click **OK**. The screen below shows the **P-Location** and the **Alert-Info** headers configured to be blocked for the compliance test.



The list of blocked headers for outbound calls will appear in the right pane as shown below. Click **Set** to complete the configuration.

Configure vsp|session-config-poolentry ToTelco|header-settings [Show advanced](#) [Help](#) [Index](#)

allowed-header	Edit allowed-header
blocked-header	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 2px;">P-Location</div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 2px;">Alert-Info</div> Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization
altered-body	Add altered-body
reg-ex-collector	Add reg-ex-collector
apply-allow-block-to	<input type="text" value="requests-and-responses"/> (apply to requests and responses)
apply-to-allow-block-to-dialog	<input type="text" value="both"/> (Apply to both inbound and outbound dialogs.)

7.2.4. Diversion Header Domain

Avaya Aura® Session Manager can adapt the domain in various SIP headers such as the Request-URI and P-Asserted-Identity. As described in these Application Notes, the Session Manager capability to adapt the domain in various headers allowed a shared Avaya Interoperability Lab configuration already configured for the enterprise domain “sil.miami.avaya.com” to be used for the AT&T Mobility SIP Trunk testing, even though the AT&T SIP Trunk Service understood the domain to be “aslab.centixvoip.net”.

To allow diverted calls to be processed properly in the shared configuration, the SBC was used to convert the domain in the Diversion header to the AT&T expected “aslab.centixvoip.net”.

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** → **header-settings**. The screen below shows the configuration before making changes for the Diversion header. Click **Add altered-header**.

The screenshot displays the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The main content area is titled 'Configure vspsession-config-poolentry ToTelcoheader-settings' and features a 'Show advanced' button and 'Help' and 'Index' links. Below the title are 'Set', 'Reset', 'Back', and 'Delete' buttons. The configuration area is divided into several sections: 'allowed-header' (with an 'Edit allowed-header' link), 'blocked-header' (with input fields for 'P-Location' and 'Alert-Info' and an 'Edit blocked-header' link), 'altered-header' (with an 'Add altered-header' button), 'reg-ex-header' (with an 'Add reg-ex-header' link), 'header-normalization' (with an 'Add header-normalization' link), 'altered-body' (with an 'Add altered-body' link), 'reg-ex-collector' (with an 'Add reg-ex-collector' link), 'apply-allow-block-to' (with a dropdown menu set to 'requests-and-responses' and a note '(apply to requests and responses)'), and 'apply-to-allow-block-to-dialog' (with a dropdown menu set to 'both' and a note '(Apply to both inbound and outbound dialogs)'). At the bottom of the configuration area are 'Set', 'Reset', and 'Back' buttons. On the left side, a sidebar shows a tree view of the configuration hierarchy under 'Configuration: all', with 'session-config-pool' expanded to show 'entry ToTelco' and 'header-settings' selected.

In the **number** field, enter an appropriate unused number. Since this is the first altered-header rule, number 1 was used. For the **source-header** field, select “**Diversion**” from the drop-down menu.

In the source-field area enter the following:

- **type:** Choose “**selection**” from the drop-down menu
- **value:** Either enter a value to match directly, or click the **regular expression** link for assistance in creating the proper **value**. In the sample configuration, the rule will match on “sil.miami.avaya.com” appearing in the Diversion header.
- **replacement:** Enter the domain to appear in the host portion of the Diversion header, in place of “sil.miami.avaya.com”. For the compliance test, AT&T expected “aslab.centixvoip.net”.

In the **destination** area, select “**Diversion**” from the drop-down menu. Select “**host**” from the **type** drop-down menu, since it is the host portion of the Diversion header that the rule should replace. Click the **Create** button.

Create vsp|session-config-pool|entry ToTelco|header-settings|altered-header 0 - Step 1 of 1: Edit altered-header 0 [Help](#) [Index](#)

Please provide some basic information for altered-header 0. Then press "Create".

* number	<input type="text" value="1"/>						
* source-header	enter <input type="text" value="Diversion"/> or select from <input type="text" value="Diversion"/>						
* source-field	<table><tr><td>* type</td><td><input type="text" value="selection"/> (Regular expression based selection of portion of the URI.)</td></tr><tr><td>* value</td><td><input type="text" value="*sil.miami.avaya.com"/> (regular expression)</td></tr><tr><td>* replacement</td><td><input type="text" value="aslab.centixvoip.net"/></td></tr></table>	* type	<input type="text" value="selection"/> (Regular expression based selection of portion of the URI.)	* value	<input type="text" value="*sil.miami.avaya.com"/> (regular expression)	* replacement	<input type="text" value="aslab.centixvoip.net"/>
* type	<input type="text" value="selection"/> (Regular expression based selection of portion of the URI.)						
* value	<input type="text" value="*sil.miami.avaya.com"/> (regular expression)						
* replacement	<input type="text" value="aslab.centixvoip.net"/>						
* destination	enter <input type="text" value="Diversion"/> or select from <input type="text" value="Diversion"/>						
* destination-field	* type <input type="text" value="host"/> (Host portion of the URI.)						

If the **regular expression** link is clicked on the previous screen, the screen shown below is presented for assistance in generating the regular expression. Enter the string to match in the **Enter String Pattern** field, select the appropriate **Match option**, and press **OK**.

You can set the match option so that the system matches the entire string, the beginning or end of the string, or any part of the string.

Enter String Pattern

Match option Exact Match Match Beginning Match End Match Any

Additional configuration can be applied to the altered-header rule using the screen shown below. In the sample configuration, the defaults were retained. Click the **Set** button.

Configure vsp|session-config-pool|entry ToTelco|header-settings|altered-header 1

admin	<input type="text" value="enabled"/> (Resource is active)
* number	<input type="text" value="1"/>
* source-header	enter <input type="text" value="Diversion"/> or select from <input type="text" value="Diversion"/>
* source-field	<p>* type <input type="text" value="selection"/> (Regular expression based selection of portion of the URI.)</p> <p>* value <input type="text" value=".*sil\.miami\.avaya\.com"/> (regular expression)</p> <p>* replacement <input type="text" value="aslab.centixvoip.net"/></p>
* destination	enter <input type="text" value="Diversion"/> or select from <input type="text" value="Diversion"/>
* destination-field	* type <input type="text" value="host"/> (Host portion of the URI.)
apply-to-methods	<input type="text" value="INVITE"/> <input type="text" value="REFER"/> <input type="text" value="MESSAGE"/> <input type="text" value="INFO"/> <p><input type="button" value="Select All"/> <input type="button" value="Unselect All"/></p>
apply-to-responses	* type <input type="text" value="no"/> (Do not apply to responses (requests only))
apply-to-dialog	<input type="text" value="both"/> (Apply to both inbound and outbound dialogs.)
session-persistent	<input type="text" value="disabled"/> (Resource is inactive)

The following screen shows a summary of the altered-header rule configured in this section. It also shows the blocked-header rule configured in **Section 7.2.3**.

Configure vspisession-config-poolentry ToTelcolheader-settings [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

allowed-header [Edit allowed-header](#)

blocked-header

P-Location
Alert-Info

[Edit blocked-header](#)

altered-header

	altered-header	admin	source-header	source-field	destination	destination-field	apply-to-methods	apply-to-responses	apply-to-dialog	session-persistent
Edit Delete	altered-header.1	enabled	Diversion	selection.*sil.miami\avaya\com aslab.centixvoip.net	Diversion	host	INVITE	no	both	disabled

[Add altered-header](#)

reg-ex-header [Add reg-ex-header](#)

header-normalization [Add header-normalization](#)

altered-body [Add altered-body](#)

reg-ex-collector [Add reg-ex-collector](#)

apply-allow-block-to [requests-and-responses](#) (apply to requests and responses)

apply-to-allow-block-to-dialog [both](#) (Apply to both inbound and outbound dialogs.)

[Set](#) [Reset](#) [Back](#)

7.2.5.Request URI

On incoming calls to the enterprise, AT&T will always send the same “pilot” DID number on the user portion of the request-line of any incoming INVITE, and the actual number dialed in the user portion of the “To” header. Since Session Manager routes the calls based on the number contained in the request-uri, it is necessary to modify the user portion of the request-uri sent to Session Manager, to replace the “pilot” number with the actual number being called. Navigate to **vsp → session-config-pool → entry ToPBX**. Click on **request-uri-specification**.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view under 'Configuration: all' with 'entry ToPBX' selected, and 'request-uri-specification' highlighted. The main content area displays a table of configuration options under the 'uri:' section:

uri:	
to-uri-specification	
Delete	
from-uri-specification	Configure
request-uri-specification	
Delete	
p-asserted-identity-uri-specification	Configure
contact-uri-settings-in-leg	Configure
contact-uri-settings-out-leg	Configure
inbound-request-uri-specification	Configure
contact-uri-settings-3xx-response	Configure
remote-party-id-specification	Configure

On the next screen, on the **user** field, select “**to-uri**” from the drop-down menu, instead of the default “**request-uri**”. By making this change, the call is allowed to be routed to the correct destination by Session Manager, and ultimately by Communication Manager. Click **Set** to complete the configuration.

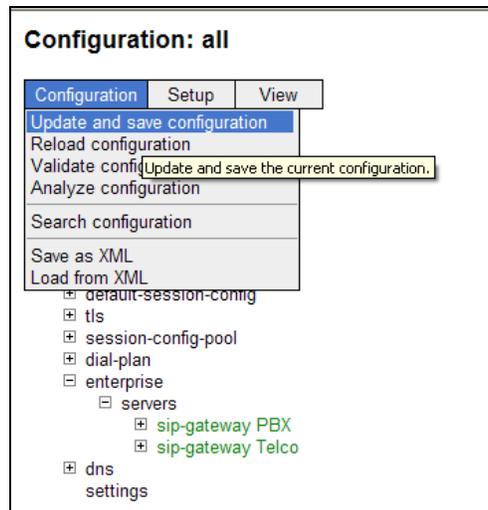
The screenshot shows the configuration page for 'vsp/session-config-pool/entry ToPBX/request-uri-specification'. The page title is 'Configure vsp/session-config-pool/entry ToPBX/request-uri-specification' with 'Help' and 'Index' links. Below the title are buttons for 'Set', 'Reset', 'Back', and 'Delete'. The configuration fields are as follows:

user	enter <input type="text" value="to-uri"/> or select from <input type="text" value="to-uri"/> (Net-Net OS-E uses the value from the incoming TO URI.)
host	enter <input type="text" value="next-hop-domain"/> or select from <input type="text" value="next-hop-domain"/> (Net-Net OS-E uses the domain of the next-hop server.)
port	enter <input type="text" value="request-uri"/> or select from <input type="text" value="request-uri"/> (Net-Net OS-E uses the value from the incoming REQUEST URI.)
transport	<input type="text" value="request-uri"/> (Net-Net OS-E uses the value from the incoming REQUEST URI.)
user-param	<input type="text" value="omit"/>
user-truncate-non-digits	<input type="text" value="disabled"/> (Resource is inactive)
uri-parameter	Add uri-parameter
apply-to-routing	<input type="text" value="false"/>
use-location-cache-contact-uri	<input type="text" value="true"/>

At the bottom of the page are buttons for 'Set', 'Reset', and 'Back'.

7.2.6. Save the Configuration

To save the configuration, begin by clicking on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.



8. AT&T Mobility SIP Trunk Service Configuration

Information about how to establish the AT&T Mobility SIP Trunk Service in Puerto Rico can be obtained by contacting an AT&T Mobility sales representative.

AT&T Mobility is responsible for the configuration of the AT&T Mobility SIP Trunk service in their network. To establish service, the customer will need to provide AT&T with the IP address used to reach the SBC at the enterprise. AT&T will provide the customer with the necessary information to configure the SIP connection from the enterprise site to the AT&T network, including:

- IP address of the AT&T SIP proxy.
- AT&T SIP domain.
- CPE SIP domain.
- Supported codecs.
- DID numbers
- Port numbers used for signaling and media.

This information is used to complete the Communication Manager, Session Manager, and the Session Border Controller configuration discussed in the previous sections.

9. Verification and Troubleshooting

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. Session Border Controller:
 - **Call Logs** - On the web user interface of the Avaya Aura® Session Border Controller, the **Call Logs** tab can provide useful diagnostic or troubleshooting information.
2. Communication Manager:
 - **list trace station** <extension number>
Traces calls to and from a specific station.
 - **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
 - **status signaling-group** <signaling group number>
Displays signaling group service state.
 - **status trunk** <trunk group number>
Displays trunk group service state.
 - **status station** <extension number>
Displays signaling and media information for an active call on a specific station.
3. Session Manager:
 - **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.
 - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Home** → **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.

10. Conclusion

AT&T Mobility SIP Trunk Service in Puerto Rico passed compliance testing.

These Application Notes describe the configuration necessary to connect the above service to Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0.

The AT&T Mobility SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. AT&T Mobility SIP Trunk Service provides a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, February 2011.
- [2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
- [3] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.0, June 2010, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.
- [7] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Document Number 03-603324.
- [8] *Avaya Aura® Session Border Controller System Administration Guide*, V.6.0, September 2010
- [9] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [10] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [11] *Administering Avaya one-X® Communicator*, April 2011.
- [12] *Using Avaya one-X® Communicator*, April 2011.
- [13] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Appendix A: Avaya Aura® SBC Configuration File

```
#
# Copyright (c) 2004-2011 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 22:21:29 Tue 2011-09-13
#
config cluster
config box 1
  set hostname aa-sbc.sil.miami.avaya.com
  set timezone America/New_York
  set name aa-sbc.sil.miami.avaya.com
  set identifier 00:ca:fe:80:25:99
config interface eth0
  config ip inside
    set ip-address static 192.168.10.42/24
  config ssh
  return
  config snmp
    set trap-target 192.168.10.41 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
  return
  config icmp
  return
  config media-ports
  return
  config routing
    config route Default
      set gateway 192.168.10.254
    return
    config route Static0
      set destination network 192.11.13.4/30
      set gateway 192.168.10.40
    return
    config route Static1
      set admin disabled
    return
```

```

config route Static2
  set admin disabled
return
config route Static3
  set admin disabled
return
config route Static4
  set admin disabled
return
config route Static5
  set admin disabled
return
config route Static6
  set admin disabled
return
config route Static7
  set admin disabled
return
return
return
return
config interface eth2
config ip outside
  set ip-address static 10.10.10.15/24
config sip
  set udp-port 5060 "" "" any 0
return
config media-ports
  set base-port 50000
  set count 4999
return
config routing
  config route Default
    set admin disabled
  return
  config route external-sip-media-1
    set destination network 10.1.1.0/24
    set gateway 10.10.10.254
  return
return
config kernel-filter
  config allow-rule allow-sip-udp-from-peer-1
    set destination-port 5060
    set source-address/mask 10.1.1.0/24
    set protocol udp
  return
  config deny-rule deny-all-sip
    set destination-port 5060
  return
return
return
return
config cli
  set prompt aa-sbc.sil.miami.avaya.com
return
return

```

```

return

config services
config event-log
  config file access
    set filter access info
    set count 3
  return
config file system
  set filter system info
  set count 3
return
config file errorlog
  set filter all error
  set count 3
return
config file db
  set filter db debug
  set filter dosDatabase info
  set count 3
return
config file management
  set filter management info
  set count 3
return
config file peer
  set filter sipSvr info
  set count 3
return
config file dos
  set filter dos alert
  set filter dosSip alert
  set filter dosTransport alert
  set filter dosUrl alert
  set count 3
return
config file krnlsys
  set filter krnlsys debug
  set count 3
return
return
return

config master-services
config database
  set media enabled
return
return

config vsp
set admin enabled
config default-session-config
  config media
    set anchor enabled
    set rtp-stats enabled
return

```

```

config sip-directive
  set directive allow
return
config log-alert
  set apply-to-methods-for-filtered-logs
return
config third-party-call-control
  set handle-refer-locally disabled
return
return
config tls
config default-ca
  set ca-file /cxc/certs/sipca.pem
return
config certificate ws-cert
  set certificate-file /cxc/certs/ws.cert
return
config certificate aasbc.p12
  set certificate-file /cxc/certs/aasbc.p12
  set passphrase-tag aasbc-cert-tag
return
return
config session-config-pool
config entry ToTelco
  config to-uri-specification
    set host next-hop
  return
  config from-uri-specification
    set host local-ip
  return
  config request-uri-specification
    set host next-hop
  return
  config p-asserted-identity-uri-specification
  return
  config header-settings
    set blocked-header P-Location
    set blocked-header Alert-Info
  config altered-header 1
    set source-header Diversion
    set source-field selection ".*sil\.miami\.avaya\.com"
aslab.centixvoip.net
  set destination Diversion
  set destination-field host
  return
  return
return
config entry ToPBX
  config to-uri-specification
    set host next-hop-domain
  return
  config request-uri-specification
    set user to-uri
    set host next-hop-domain
  return
return

```

```

return
config dial-plan
  config route Default
    set priority 500
    set location-match-preferred exclusive
  return
  config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
return
config enterprise
  config servers
    config sip-gateway PBX
      set domain sil.miami.avaya.com
      set failover-detection ping
      set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
      config server PBX1
        set host 192.168.10.32
        set transport TCP
      return
    return
  config sip-gateway Telco
    set domain aslab.centixvoip.net
    set routing-setting normalization
    set failover-detection ping
    set ping-interval 180
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
      config server Telco1
        set host 10.1.1.1
      return
    return
  return
return
config dns
  config resolver
    config server 192.168.10.100
  return
return
config settings
  set read-header-max 8191
return
return

config external-services

```

```
return

config preferences
  config gui-preferences
    set enum-strings SecurityDomain aslab.centixvoip.net
    set enum-strings SecurityDomain sbclab.centixvoip.net
    set enum-strings SIPSourceHeader History-Info
    set enum-strings SIPSourceHeader Diversion
  return
return

config access
  config permissions superuser
    set cli advanced
  return
  config permissions read-only
    set config view
    set actions disabled
  return
  config users
    config user admin
      set password 0x00ea4c38120e5596d177c171d6ee31cb2cab4f30ca4e833ff82f221527
      set permissions access\permissions superuser
    return
    config user cust
      set password 0x00c718e10fc1cdcae12da12bcb7987663e1464ce037a59b6982ee99bb8
      set permissions access\permissions read-only
    return
    config user init
      set password 0x00f9fbdf4bee98a74b779c3ce0b3fc53d9b0c800929e8e91edce08fe32
      set permissions access\permissions superuser
    return
    config user craft
      set password 0x003ac1a725ba1b66d4ac676ac6f090648d9009740aba1527de00ec8a8d
      set permissions access\permissions superuser
    return
    config user dadmin
      set password 0x008a6b4a14c6be023541b3ce7ae257820ea41fed755031f6549ff65c1b
      set permissions access\permissions read-only
    return
  return
return

config features
return
```

©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.