



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring the PAETEC Dynamic IP SIP Trunk Service (BroadSoft Platform) with Avaya Aura® Solution for Midsize Enterprise 6.1 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the PAETEC Dynamic IP SIP Trunk Service and an Avaya SIP-enabled enterprise solution. PAETEC can offer the Dynamic IP SIP Trunk Service using several different platform technologies in the PAETEC network. These Application Notes correspond to the Dynamic IP SIP Trunk Service offered using a Broadsoft platform in the network. The Avaya solution consists of Avaya Aura® Solution for Midsize Enterprise, and various Avaya endpoints.

PAETEC 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.

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the PAETEC Dynamic IP SIP Trunk Service and an Avaya SIP-enabled enterprise solution. PAETEC can offer the Dynamic IP SIP Trunk Service using several different platform technologies in the PAETEC network. These Application Notes correspond to the Dynamic IP SIP Trunk Service offered using a Broadsoft platform in the network. The Avaya solution consists of Avaya Aura® Solution for Midsize Enterprise using the Avaya Aura® Session Border Controller, Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server along with various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with the PAETEC Dynamic IP SIP Trunk Service 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 ISDN-PRI.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Midsize Enterprise's Communication Manager, Session Manager and the Session Border Controller to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to the Dynamic IP SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

The Dynamic IP SIP Trunk Service passed compliance testing.

### 2.1. Interoperability Compliance Testing

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 PSTN calls 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 PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls and local directory assistance (411).
- Codecs G.729A, G.711MU and G.711A.

- DTMF transmission using 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.
- Network Call Redirection using the SIP REFER method or a 302 response.
- Off-net call forwarding and mobility (extension to cellular).

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- T.38 Fax not supported.

## 2.2. Test Results

Interoperability testing of the Dynamic IP SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party.
- **Network Call Redirection:** When PAETEC's Enterprise Trunking feature is active and Communication Manager is programmed to redirect an inbound call to a PSTN number before answering the call in a vector, PAETEC will send an ACK to the "302 Moved Temporarily" SIP message from the enterprise but will not redirect the call to the new party in the Contact header of the 302 message. The inbound call initiator hears a recording from PAETEC in this failure scenario. A workaround is to use the REFER method to redirect the call by having Communication Manager answer the call first with an announcement in the vector. When PAETEC's Enterprise Trunking feature is NOT active, Network Call Redirection works as expected.

## 2.3. Support

For technical support on the Dynamic IP SIP Trunk Service, contact PAETEC using the Customer Care links at [www.paetec.com](http://www.paetec.com).

## 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to the Dynamic IP SIP Trunk Service. This is the configuration used for compliance testing.

Avaya Aura® Solution for Midsize Enterprise packages several Avaya Aura® applications onto one server using System Platform technology. The following applications are included in the Midsize Enterprise template:

- Communication Manager
- Application Enablement Services
- Communication Manager Messaging

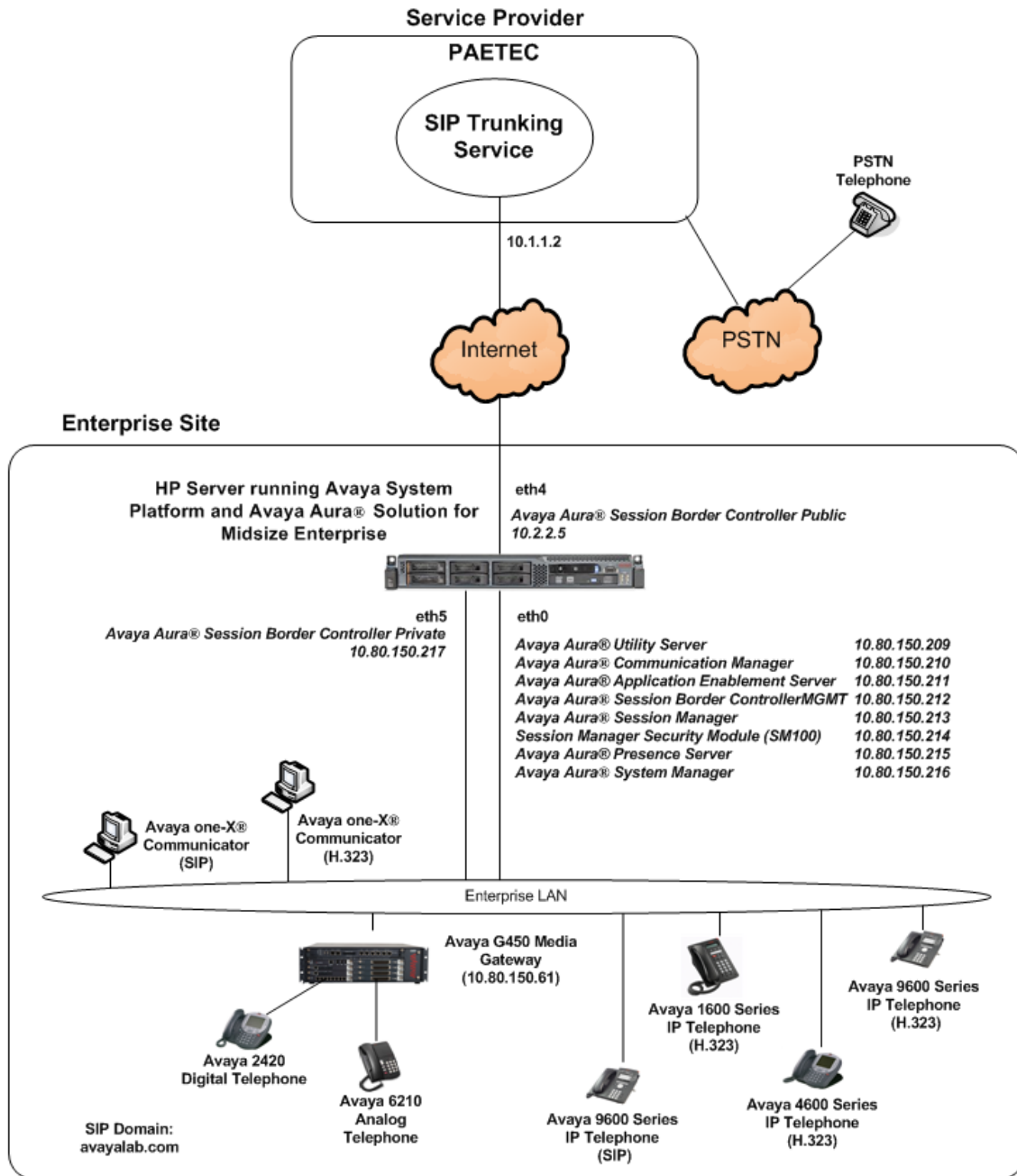
- Presence Services
- Avaya Aura® Session Border Controller
- Session Manager
- System Manager
- Utility Services

Along with the Midsize Enterprise the other Avaya components used to create the simulated customer site included:

- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X Communicator (H.323 and SIP)
- Avaya digital and analog telephones

**Note: Application Enablement Services and Presence Services were installed as part of the Midsize Enterprise solution but were not used during compliance testing. Configuration of these services is not covered in these Application Notes.**

Located at the edge of the enterprise is the Session Border Controller (SBC). It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.



**Figure 1: Avaya IP Telephony Network using the Dynamic IP 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 setting 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 are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to the Dynamic IP SIP Trunk Service.

PAETEC allows all North American Numbering Plan (NANP) numbers to be dialed with either 10 digits or 11 digits (1 + 10).

## 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Solution for Midsize Enterprise.	6.1.0.0.2580
Avaya Aura® Communication Manger	R016x.00.1.510.1
Avaya Aura® Communication Manger Messaging	vcm-016-00.1.510.1
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.112
Avaya Aura® Session Manager	6.1.1.0.611023
Avaya 1608 IP Telephone (H.323)	Avaya one-X Deskphone Value Edition 1.2.2
Avaya Aura® Session Border Controller	E362P4
Avaya G450	31.18.1
Avaya 4625SW IP Telephone (H.323)	2.9010
Avaya 9641 IP Telephone (H.323)	Avaya one-X Deskphone Edition 6.0
Avaya 9621 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 6.0
Avaya one-X Communicator (H.323 and SIP)	6.1.0.12
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
PAETEC SIP Trunking Solution Components	
Component	Release
BroadSoft Platform	14sp9

**Table 1: Equipment and Software Tested**

The specific configuration above was used for the compatibility 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 Dynamic IP SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from PAETEC. 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 the service provider. The example shows that **12000** licenses are available and **259** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	4
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	128	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	18000	0
Maximum Video Capable IP Softphones:	18000	0
<b>Maximum Administered SIP Trunks:</b>		<b>12000 259</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0



## 5.2. System Features

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

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

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

```
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: 1
      International Access Code: 011

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

### 5.3. IP Node Names

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

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
<b>SM</b>	<b>10.80.150.214</b>	
default	0.0.0.0	
mes-aes	10.80.150.211	
<b>procr</b>	<b>10.80.150.210</b>	
procr6	::	

### 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. The Dynamic IP SIP Trunk Service supports G.729A and G.711MU. Thus, these codecs were included in this set, in order of preference. The order of preference is defined by the end customer. 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
1: <b>G.729A</b>	n	2
2: <b>G.711MU</b>	n	2
3:		

Since T.38 fax is not supported, set the **Fax Mode** to **off**.

change ip-codec-set 2		Page 2 of 2
		IP Codec Set
		Allow Direct-IP Multimedia? n
<b>FAX</b>	Mode	Redundancy
	<b>off</b>	0
Modem	off	0
TDD/TTY	US	3

## 5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. 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 **avayalab.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                     Page 1 of 20

                                IP NETWORK REGION

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

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (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	
										G	A	t	
<b>dst</b>	<b>codec</b>	<b>direct</b>		WAN-BW-limits	Video	Intervening				Dyn	A	G	c
<b>rgn</b>	<b>set</b>	<b>WAN</b>	<b>Units</b>	Total	Norm	Prio	Shr	Regions		CAC	R	L	e
1	2	y	NoLimit							n			t
2	2												
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 1 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 **n**.
- Set the **Peer Server** to **Others**. When the Peer Server is detected or set to SM, Communication Manager precedes a + sign to the From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with PAETEC.
- 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 **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.

- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	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? n Peer Server: Others		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5070	Far-end Listen Port: 5060	
Far-end Network Region: 2		
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? y	
Enable Layer 3 Test? n	Alternate Route Timer(sec): 6	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

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

```
add trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1          Group Type: sip          CDR Reports: y
  Group Name: SIP trunk to PAETEC          COR: 1          TN: 1          TAC: *01
  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: 1
                                     Number of Members: 4
```

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 value of **600** seconds was used.

```
add trunk-group 1                                     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 **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

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

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
Maintenance Tests? y	
<b>Numbering Format: public</b>	UI Treatment: service-provider
	<b>Replace Restricted Numbers? y</b>
	<b>Replace Unavailable Numbers? y</b>
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

On **Page 4**, set the **Network Call Redirection** field to **y**. This allows inbound calls transferred back to the PSTN to use the SIP REFER method, see [17]. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is only needed when Enterprise Trunking from PAETEC is not being used to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. If Enterprise Trunking from PAETEC is used set this value to **n**. Set the **Support Request History** field to **n**.

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

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
<b>Network Call Redirection? y</b>	
<b>Send Diversion Header? y</b>	
<b>Support Request History? n</b>	
<b>Telephone Event Payload Type: 101</b>	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	

## 5.8. Inbound Routing

In general, the incoming call handling treatment 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 PAETEC 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 trunk-group** command to create an entry for each DID. As an example, the following screen illustrates a conversion of DID number **7135551234** to extension **12001**.

change inc-call-handling-trmt trunk-group 1					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	7135551234	10	12001	
public-ntwrk	10	7135551235	10	12002	
public-ntwrk	10	7135551236	10	12003	
public-ntwrk	10	7135551237	10	12004	
public-ntwrk					



## 5.9. Calling Party Information

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

In the sample configuration, four DID numbers were assigned for testing. These four numbers were assigned to the four extensions **12001**, **12002**, **12003** and **12004**. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these four extensions.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	1			5	Total Administered: 13
5	2			5	Maximum Entries: 9999
5	3			5	
5	4			5	Note: If an entry applies to
5	5			5	a SIP connection to Avaya
5	6			5	Aura(tm) Session Manager,
5	7			5	the resulting number must
5	8			5	be a complete E.164 number.
5	12001	1	7135551234	10	
5	12002	1	7135551235	10	
5	12003	1	7135551236	10	
5	12004	1	7135551237	10	

## 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. 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			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	attd							
1	5	ext							
2	5	ext							
3	5	ext							
4	5	ext							
5	5	ext							
6	5	ext							
7	5	ext							
8	5	ext							
<b>9</b>	<b>1</b>	<b>fac</b>							
*	3	dac							
#	3	dac							

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)						Page 1 of 10
Abbreviated Dialing List1 Access Code: *10									
Abbreviated Dialing List2 Access Code: *12									
Abbreviated Dialing List3 Access Code: *13									
Abbreviated Dial - Prgm Group List Access Code: *14									
Announcement Access Code: *19									
Answer Back Access Code:									
Auto Alternate Routing (AAR) Access Code: *00									
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>						Access Code 2:			
Automatic Callback Activation: *33						Deactivation: #33			
Call Forwarding Activation Busy/DA: *30 All: *31						Deactivation: #30			
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 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 1					Page 1 of 2		
ARS DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
1303		11	11	1	fnpa		n
1502		11	11	1	fnpa		n
1720		11	11	1	fnpa		n
1800		11	11	1	fnpa		n
1866		11	11	1	fnpa		n
1877		11	11	1	fnpa		n
1888		11	11	1	fnpa		n
1908		11	11	1	fnpa		n
2		10	10	1	hnpa		n
3		10	10	1	hnpa		n
4		10	10	1	hnpa		n
411		3	3	1	svcl		n
5		10	10	1	hnpa		n
555		7	7	deny	hnpa		n
6		10	10	1	hnpa		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 1 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **1** 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 long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

change route-pattern 1												Page 1 of 3	
Pattern Number: 1												Pattern Name: PAETEC SIP TRK	
SCCAN? n												Secure SIP? n	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC
No			Mrk	Lmt	List	Del	Digits					QSIG	
												Intw	
1:	1	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				Dgts	Format		
												Subaddress	
1:	y	y	y	y	y	n	n	rest				none	
2:	y	y	y	y	y	n	n	rest				none	
3:	y	y	y	y	y	n	n	rest				none	
4:	y	y	y	y	y	n	n	rest				none	
5:	y	y	y	y	y	n	n	rest				none	
6:	y	y	y	y	y	n	n	rest				none	

## 6. Configure Avaya Aura® Session Manager

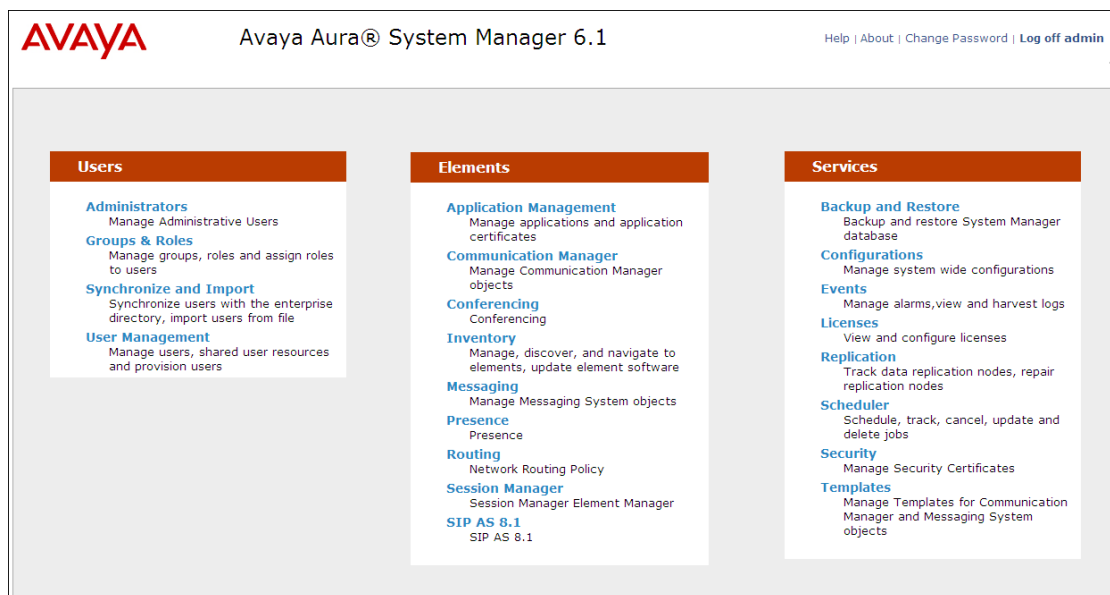
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

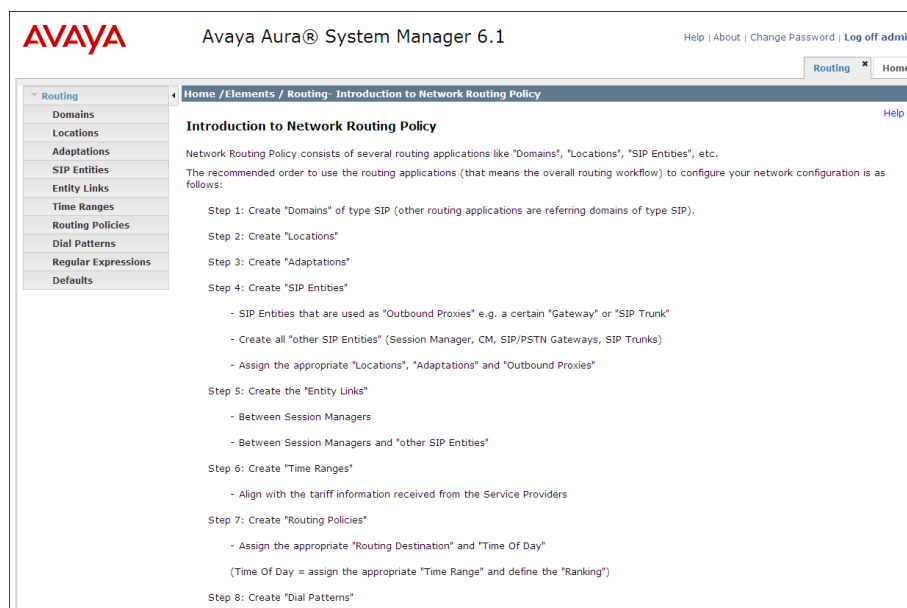
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session 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 shown above 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 (**avayalab.com**).

Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, 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 **avayalab.com** domain.

The screenshot shows a web interface for "Domain Management". 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 "Commit" and "Cancel" buttons are on the right, along with a "Help ?" link. A horizontal line separates the header from the main content area. The main content area has a light gray background and contains a table with one item. Above the table, it says "1 Item | Refresh" on the left and "Filter: Enable" on the right. The table has four columns: "Name", "Type", "Default", and "Notes". The first row of the table contains the following data: "Name" is "\* avayalab.com" (with an asterisk in a red box), "Type" is "sip" (in a dropdown menu), "Default" is an unchecked checkbox, and "Notes" is an empty text box.

Name	Type	Default	Notes
* avayalab.com	sip	<input type="checkbox"/>	

### 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 **Westminster**, which includes all equipment on the **10.80.x.x** subnet including Communication Manager, Session Manager and SIP clients. Click **Commit** to save.

Home / Elements / Routing / Locations- Location Details

Location Details [Help ?](#)

**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:  Kbit/sec

**Location Pattern**

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.80.*	Enterprise

Select : All, None



**Note: that call bandwidth management parameters should be set per customer requirement.**

Repeat the preceding procedure to create a separate Location for the SBC. Displayed below is the screen for addition of the **SP-SIP-TRUNK-SBC** Location, which specifies the specific IP address for the AA-SBC. Click **Commit** to save.

Home / Elements / Routing / Locations- Location Details

Location Details

CommitCancelHelp ?

General

\* Name:

SP-SIP-Trunk-SBC

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

Minimum Multimedia Bandwidth:

64

Kbit/Sec

\* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

AddRemove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.80.150.217	AASBC

Select : All, None

## 6.4. 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 SBC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the SBC.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** 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 Session Manager. The IP address of the virtual Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. The page title is 'SIP Entity Details' with a 'Help ?' link. There are 'Commit' and 'Cancel' buttons in the top right. The 'General' section contains the following fields: 'Name' (required, value: SessionManager1), 'FQDN or IP Address' (required, value: 10.80.150.214), 'Type' (dropdown, value: Session Manager), 'Notes' (text area), 'Location' (dropdown, value: Westminster), 'Outbound Proxy' (dropdown), 'Time Zone' (dropdown, value: America/Denver), and 'Credential name' (text field). The 'SIP Link Monitoring' section contains a 'SIP Link Monitoring' dropdown with the value 'Use Session Manager Configuration'.

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

SIP Entity Details [Help ?](#)

[Commit](#) [Cancel](#)

**General**

\* **Name:** SessionManager1

\* **FQDN or IP Address:** 10.80.150.214

**Type:** Session Manager

**Notes:**

**Location:** Westminster

**Outbound Proxy:**

**Time Zone:** America/Denver

**Credential name:**

**SIP Link Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

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. This section defines a default set of ports that the Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. The Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

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.

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

**Port**

4 Items
Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	avayalab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	avayalab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS	avayalab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5070"/>	TCP	avayalab.com	<input type="text"/>

Select : All, None

\* Input Required

The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, a new SIP entity is created separate from the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the Communication Manager.

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities- SIP Entity Details](#)

[Help ?](#)

SIP Entity Details

CommitCancel

General

\* Name: CommunicationManagerTG1

\* FQDN or IP Address: 10.80.150.210

Type: CM

Notes: CM Trunk Group 1 (PEATEC SP)

Adaptation:

Location: Westminster

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

The following screen shows the addition of the SBC SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for the SBC in **Section 6.3**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.

The screenshot displays the 'SIP Entity Details' configuration page for an entity named 'SBC1'. The page has a breadcrumb trail at the top: 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. In the top right corner, there is a 'Help ?' link and two buttons: 'Commit' and 'Cancel'. The main section is titled 'SIP Entity Details' and contains a 'General' subsection. Under 'General', the following fields are visible: 'Name' (SBC1), 'FQDN or IP Address' (10.80.150.217), 'Type' (SIP Trunk), 'Notes' (AASBC), 'Adaptation' (dropdown), 'Location' (SP-SIP-Trunk-SBC), and 'Time Zone' (America/Fortaleza). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV:'. Below this, 'SIP Timer B/F (in seconds)' is set to 4, 'Credential name' is an empty field, and 'Call Detail Recording' is set to 'egress'. A second subsection, 'SIP Link Monitoring', is also present. It includes a dropdown for 'SIP Link Monitoring' set to 'Link Monitoring Enabled', a 'Proactive Monitoring Interval (in seconds)' of 900, a 'Reactive Monitoring Interval (in seconds)' of 120, and a 'Number of Retries' of 1.

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

SIP Entity Details [Help ?](#)

**General**

\* Name: SBC1

\* FQDN or IP Address: 10.80.150.217

Type: SIP Trunk

Notes: AASBC

Adaptation:

Location: SP-SIP-Trunk-SBC

Time Zone: America/Fortaleza

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

**SIP Link Monitoring**

SIP Link Monitoring: Link Monitoring Enabled

\* Proactive Monitoring Interval (in seconds): 900

\* Reactive Monitoring Interval (in seconds): 120

\* Number of Retries: 1

## 6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** 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 aid in 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
* SessionManager1	* SessionManager1	TCP	* 5070	* CommunicationManagerTG1	* 5070	<input checked="" type="checkbox"/>	

Entity Link to the SBC:

Home /Elements / Routing / Entity Links- Entity Links

Entity Links [Help ?](#)

---

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SessionManager1	* SessionManager1	UDP	* 5060	* SBC1	* 5060	<input checked="" type="checkbox"/>	

\* Input Required

The following screen shows the complete list of Entity Links.

Home /Elements / Routing / Entity Links- Entity Links

Entity Links [Help ?](#)

---

5 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	<a href="#">cm-sm</a>	SessionManager1	TLS	<a href="#">5061</a>	CommunicationManagerTG3	<a href="#">5061</a>
<input type="checkbox"/>	<a href="#">ps-sm</a>	SessionManager1	TLS	<a href="#">5061</a>	Presence1	<a href="#">5061</a>
<input type="checkbox"/>	<a href="#">SessionManager1_CommunicationManagerTG1_5070_TCP</a>	SessionManager1	TCP	<a href="#">5070</a>	CommunicationManagerTG1	<a href="#">5070</a>
<input type="checkbox"/>	<a href="#">SessionManager1_SBC1_5060_UDP</a>	SessionManager1	UDP	<a href="#">5060</a>	SBC1	<a href="#">5060</a>
<input type="checkbox"/>	<a href="#">sm-cmm</a>	SessionManager1	TCP	<a href="#">6060</a>	Messaging	<a href="#">6060</a>

Select : All, None

## 6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added: one for Communication Manager and one for the SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

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

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

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

The following screens show the Routing Policies for Communication Manager and the SBC.

The screenshot shows the 'Routing Policy Details' form. In the 'General' section, the 'Name' field is filled with 'To-CommunicationManagerTG1', the 'Disabled' checkbox is unchecked, and the 'Notes' field is filled with 'To CM Trunk Group 1'. In the 'SIP Entity as Destination' section, the 'Select' button is visible. Below it is a table with the following data:

Name	FQDN or IP Address	Type	Notes
CommunicationManagerTG1	10.80.150.210	CM	CM Trunk Group 1 (PEATEC SP)

The screenshot shows the 'Routing Policy Details' form. In the 'General' section, the 'Name' field is filled with 'To-SBC1', the 'Disabled' checkbox is unchecked, and the 'Notes' field is filled with 'AASBC'. In the 'SIP Entity as Destination' section, the 'Select' button is visible. Below it is a table with the following data:

Name	FQDN or IP Address	Type	Notes
SBC1	10.80.150.217	SIP Trunk	AASBC



## 6.7. Add Dial Patterns

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

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

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

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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that **11** digit dialed numbers that begin with **1** uses route policy **To-SBC1**.

[Home](#) / [Elements](#) / [Routing](#) / [Dial Patterns- Dial Pattern Details](#)

[Help ?](#)

Commit

Cancel

Dial Pattern Details

General

\* Pattern:

1

\* Min:

11

\* Max:

11

Emergency Call:

☐

SIP Domain:

avayalab.com

Notes:

OUTBOUND 1+

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-SBC1	0	<input type="checkbox"/>	SBC1	AASBC

Select : All, None

The second example shows that a 10 digit number **7135551234** to domain **avayalab.com** and originating from **SP-SIP-TRUNK-SBC** uses route policy **To-CommunicationManagerTG1**. This is a DID number assigned to the enterprise from PAETEC. SP-SIP-TRUNK-SBC is selected because these calls come from the SBC which resides in that location.

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

Dial Pattern Details
Commit Cancel

General

\* Pattern: 7135551234

\* Min: 10

\* Max: 10

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: DID to x12001

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 Destination
<input type="checkbox"/>	SP-SIP-Trunk-SBC		To-CommunicationManagerTG1	0	<input type="checkbox"/>	CommunicationManagerTG1

Select : All, None

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

Dial Patterns

[Help ?](#)

Edit

New

Duplicate

Delete

More Actions ▾

10 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	<u>0</u>	1	36	<input type="checkbox"/>	avayalab.com	OUTBOUND 0+
<input type="checkbox"/>	<u>1</u>	11	11	<input type="checkbox"/>	avayalab.com	OUTBOUND 1+
<input type="checkbox"/>	<u>1200</u>	5	5	<input type="checkbox"/>	avayalab.com	CM EXT
<input type="checkbox"/>	<u>1300</u>	5	5	<input type="checkbox"/>	avayalab.com	CM EXT
<input type="checkbox"/>	<u>19</u>	5	5	<input type="checkbox"/>	avayalab.com	CM EXT
<input type="checkbox"/>	<u>411</u>	3	3	<input type="checkbox"/>	avayalab.com	OUTBOUND 411
<input type="checkbox"/>	<u>7135551234</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12001
<input type="checkbox"/>	<u>7135551235</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12002
<input type="checkbox"/>	<u>7135551236</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12003
<input type="checkbox"/>	<u>7135551237</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12004

Select : All, None

## 6.8. Add/View Session Manager Instance

The creation of a Session Manager Instance 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 screen below:

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.

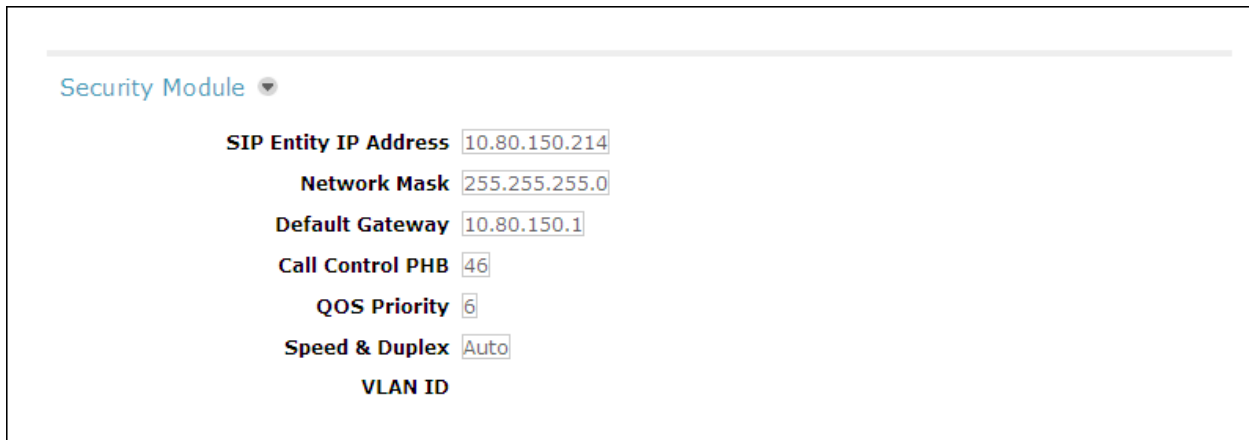
The screen below shows the Session Manager values used for the compliance test.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows the navigation path: 'Home / Elements / Session Manager / Session Manager Administration- Session Manager Administration'. The left-hand navigation pane lists various system components, with 'Session Manager Administration' selected. The main content area is titled 'View Session Manager' and contains a 'General' tab. Under the 'General' tab, the following configuration details are visible: 'SIP Entity Name' is 'SessionManager1', 'Description' is 'Session Manager', 'Management Access Point Host Name/IP' is '10.80.150.213', and 'Direct Routing to Endpoints' is set to 'Enable'. A 'Return' button is located in the top right corner of the configuration area.

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 displays the 'Security Module' configuration interface. It features a header 'Security Module' with a dropdown arrow. Below this, several configuration fields are listed, each with a label and a text input box containing a default value:

- SIP Entity IP Address:** 10.80.150.214
- Network Mask:** 255.255.255.0
- Default Gateway:** 10.80.150.1
- Call Control PHB:** 46
- QOS Priority:** 6
- Speed & Duplex:** Auto
- VLAN ID:** (empty field)

## 7. Configure Session Border Controller

This section describes the configuration of the Session Border Controller (SBC). This configuration is done in two parts. The first part is done during the Midsize Enterprise installation via the installation wizard. These Application Notes will not cover the Midsize Enterprise installation in its entirety but will include the SBC portion of the installation wizard. For information on installing the Avaya System Platform and the loading of the Solution for Midsize Enterprise template see [1] and [3].

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 Solution for Midsize Enterprise template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC.

### 7.1.1. Network Settings

The **Network Settings** screen is where IP Addresses, Hostnames and Domains are assigned to Virtual Machines. Fill in the fields as described below and shown in the following screen:

- **IP Address:** Enter the IP address of the management side of the SBC (eth0).
- **Hostname:** Enter a host name for the SBC
- **Domain:** Enter the Enterprise Domain

**Home**

Configuration

Installation

- Load
- Network Settings
- Logins
- Country
- DHCP
- VPN Access
- Gateways
- Stations and Voice Mail
- Trunks
- Session Border Controller
- Session Manager
- System Manager
- Presence
- Summary
- Save

## Network Settings

### Enter network settings

Domain-0 IP Address: 10.80.150.207

CDom IP Address: 10.80.150.208

Gateway IP Address: 10.80.150.1

Network Mask: 255.255.255.0

Primary DNS: 10.80.150.201

Secondary DNS (Optional):

Default Search List: avayalab.com

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

Virtual Machine	IP Address	Hostname	Domain
Communication Manager	10.80.150.210	mes-cm	avayalab.com (Optional)
Utility Server	10.80.150.209	mes-utility	avayalab.com (Optional)
Application Enablement Services	10.80.150.211	mes-aes	avayalab.com (Optional)
Session Border Controller	10.80.150.212	mes-sbc	avayalab.com (Optional)
Session Manager	10.80.150.213	mes-sm	avayalab.com
Session Manager SIP Entity IP:	10.80.150.214		
Presence	10.80.150.215	mes-presence	avayalab.com
System Manager	10.80.150.216	mes-smgr	avayalab.com

**Default Domain**

avayalab.com (Optional)

Apply to all VMs



### 7.1.2. Logins

The **Services Logins for SBC (optional)** screen is where passwords for the various applications are set. Assign passwords for the different accounts.

Login name	Password	Re-type password
craft	.....	.....
init	.....	.....
dadmin	.....	.....

### 7.1.3. SBC

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

In the **Configure** section check **Yes** for the question **Do you wish to configure Session Border Controller?**

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 create a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for PAETEC. Thus, **Generic** was chosen instead and further customization was done manually after the wizard was complete.
- **IP Address:** Enter the IP address of the SIP proxy of the service provider. If the service provider has multiple proxies, enter the primary proxy on this screen and additional proxies can be added after installation.
- **Port:** Enter the port number that the service provider uses to listen for SIP traffic.
- **Media Network:** Enter the network address of the network where media traffic will originate from the service provider. If media can originate from multiple networks, enter one network address on this screen and additional networks can be added after installation.
- **Media Netmask:** Enter the netmask corresponding to the **Media Network**.

In the **SBC Network Data** section:

- **Private IP Address:** Enter the IP address of the private side of the SBC (eth5).
- **Private Net Mask:** Enter the netmask associated with the private network to which the SBC connects.
- **Private Gateway:** Enter the default gateway of the private network.
- **Public IP Address:** Enter the IP address of the public side of the SBC (eth4).
- **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:

- **IP Address:** 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.
- **Transport:** From the pull-down menu, select the transport protocol to be used for SIP traffic between the SBC and Session Manager.

The screenshot displays the SBC configuration interface. On the left is a navigation menu with options like Configuration, Installation, Load, Network Settings, Logins, Country, DHCP, VPN Access, Gateways, Stations and Voice Mail, Trunks, Session Border Controller, Session Manager, System Manager, Presence, Summary, and Save. The main area is titled 'SBC' and contains three sections:

- Session Border Controller Data:** Includes a 'Configure' section asking 'Do you wish to configure Session Border Controller?' with 'Yes' selected. Below is 'SIP Service Provider Data' with fields for Service Provider (Generic), Port (5060), SIP Proxy IP Address1 (10.1.1.2), Signalling/Media Network1 (10.1.1.0), Signalling/Media Netmask1 (255.255.255.128), and optional fields for Address2, Network2, Netmask2, and a Hunting dropdown.
- SBC Network Data:** A table with columns Interface, IP Address, Net Mask, and Gateway. It lists Private (10.80.150.217, 255.255.255.0, 10.80.150.1) and Public (10.2.2.5, 255.255.255.128, 10.2.2.1) interfaces.
- Enterprise SIP Server:** Includes SIP Domain, IP Address1 (10.80.150.214), Transport1 (UDP), IP Address2 (Optional), Transport2 (Optional), and Hunting (Optional) dropdown.

At the bottom are 'Previous Step' and 'Next Step' navigation buttons.

## 7.2. Post Installation Configuration

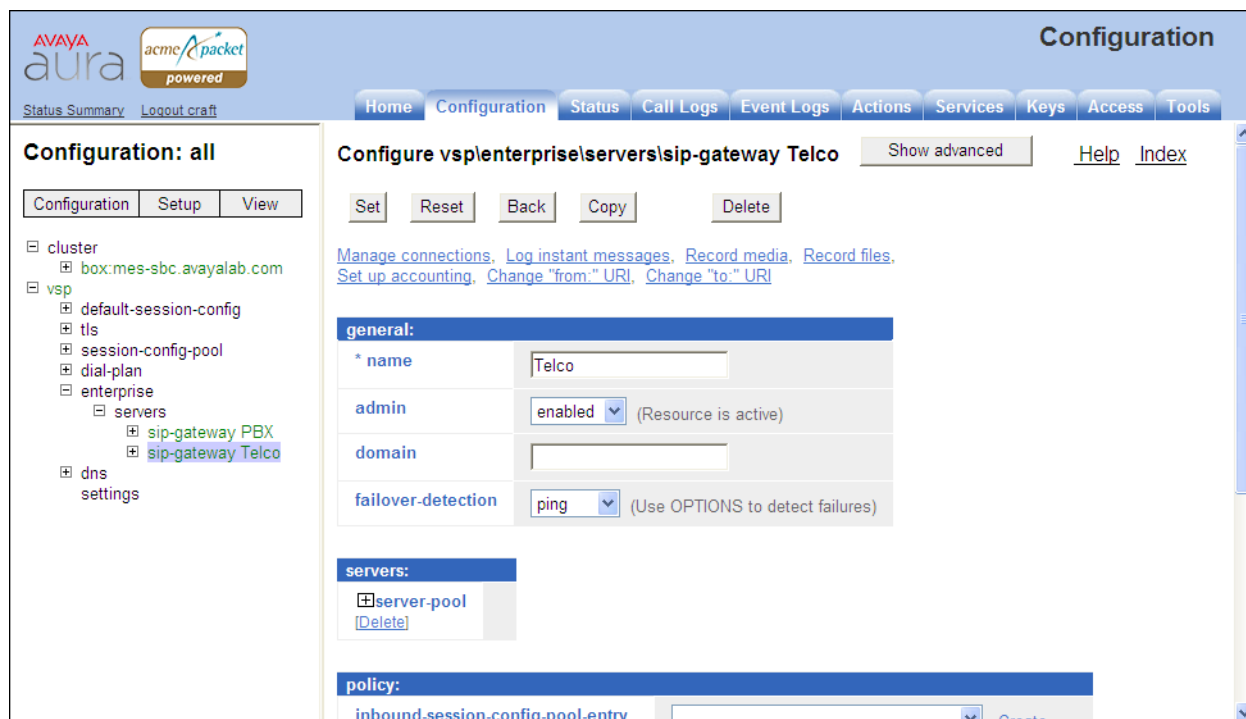
The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 7.1.3**. Since a different service provider other than PAETEC had to be selected in the installation wizard then additional manual changes must also be performed. These changes are performed 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 appropriate credentials set in **Section 7.1.2**.



The image shows the login interface for the Acme Packet Net-Net OS-E. It features a title bar with the text "Acme Packet Net-Net OS-E". Below the title bar, a message states: "To access the NNOS-E management interface, you must first log in. Please provide your user name and password." There are two input fields: "Username:" and "Password:". Below these fields is a "Login" button.

### 7.2.1. Options Frequency

To set the frequency of the OPTIONS messages sent from the SBC to the service provider, first navigate to **vsp → enterprise → servers → sip-gateway Telco**. Click **Show Advanced**.



The image shows the Avaya Aura Configuration GUI. The top navigation bar includes "Home", "Configuration", "Status", "Call Logs", "Event Logs", "Actions", "Services", "Keys", "Access", and "Tools". The "Configuration" tab is selected. The left sidebar shows a tree view of the configuration hierarchy: "cluster" (containing "box:mes-sbc.avayalab.com"), "vsp" (containing "default-session-config", "tls", "session-config-pool", "dial-plan", "enterprise" (containing "servers" (containing "sip-gateway PBX" and "sip-gateway Telco"), and "dns settings"). The "sip-gateway Telco" configuration page is displayed. It has a "Configure vspenterprise\servers\sip-gateway Telco" title bar with "Show advanced" and "Help Index" links. Below the title bar are "Set", "Reset", "Back", "Copy", and "Delete" buttons. The main content area is divided into sections: "general:" (containing "name" (Telco), "admin" (enabled), "domain", and "failover-detection" (ping)), "servers:" (containing "server-pool" (Delete)), and "policy:" (containing "inbound-session-config-pool-entry" (Create)).

Scroll down to the **routing** section of the form. Enter the desired interval in the **ping-interval** field. For compliance testing **240** seconds was used. Click **Set** at the top of the form (shown in previous figure).

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy: Configuration: all, cluster, vsp, default-session-config, tls, session-config-pool, dial-plan, enterprise, servers, sip-gateway PBX, sip-gateway Telco, dns, and settings. The main content area is titled 'routing:' and contains several configuration fields. The 'routing-setting' field is a dropdown menu with options: normalization, auto-tag-match, auto-domain-match, and pstn-backup. Below it are 'Select All' and 'Unselect All' buttons. The 'domain-alias' field has a link 'Edit domain-alias'. The 'domain-subnet' field has a link 'Edit domain-subnet'. The 'loop-detection' field is a dropdown menu with the value 'tight' and a description '(Compare source and destination address/port/transport)'. The 'service-type' field is a dropdown menu with the value 'provider' and a description '(Provider peer)'. The 'ping-interval' field is a text input with the value '240' and a unit 'seconds'. Below the routing section is the 'registration:' section, which includes fields for 'peer-max-interval' (86400 seconds), 'peer-min-interval' (3600 seconds), and 'registration request timeout'.

Configuration: all

Configuration Setup View

cluster

box:mes-sbc.avayalab.com

vsp

default-session-config

tls

session-config-pool

dial-plan

enterprise

servers

sip-gateway PBX

sip-gateway Telco

dns

settings

routing:

routing-setting

normalization

auto-tag-match

auto-domain-match

pstn-backup

Select All Unselect All

domain-alias

Edit domain-alias

domain-subnet

Edit domain-subnet

loop-detection

tight (Compare source and destination address/port/transport)

service-type

provider (Provider peer)

ping-interval

240 seconds

registration:

peer-max-interval

86400 seconds

peer-min-interval

3600 seconds

registration request timeout

## 7.2.2. Blocked Headers

The P-Location and Alert-Info headers are sent in SIP messages from the Session Manager to the PAETEC network. These headers contain private IP addresses and SIP Domains from the enterprise. These should not be exposed external to the enterprise. 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**.

The screenshot displays the AVAYA aura Configuration interface. The top navigation bar includes tabs for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main content area is titled 'Configuration: all' and shows a tree view on the left with the following structure:

- cluster
  - box:mes-sbc.avayalab.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelco
      - to-uri-specification
      - from-uri-specification
      - request-uri-specification
      - p-asserted-identity-uri-specification
      - header-settings
    - entry ToPBX
    - entry Discard
  - dial-plan
  - enterprise
  - dns
  - settings

The right pane shows the configuration for 'Configure vsp\session-config-pool\entry ToTelco\header-settings'. It includes buttons for Set, Reset, Back, and Delete. The configuration table lists various settings with their corresponding actions:

Setting	Action
allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
reg-ex-header	<a href="#">Add reg-ex-header</a>
header-normalization	<a href="#">Add header-normalization</a>
altered-body	<a href="#">Add altered-body</a>
reg-ex-collector	<a href="#">Add reg-ex-collector</a>
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.)

At the bottom of the right pane are buttons for Set, Reset, and Back.

In the right pane that appears, click **Add**. In the blank field that appears, 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** header and the **Alert-Info** header were configured to be blocked for the compliance test.

**Configure vsp\session-config-pool\entry ToTelco\header-settings blocked-header**

Back

P-Location X

Alert-Info X

Add Remove All

OK

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

**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Status Summary Logout craft

**Configuration: all**

Configuration Setup View

- cluster
  - box:mes-sbc.avayalab.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelco
      - to-uri-specification
      - from-uri-specification
      - request-uri-specification
      - p-asserted-identity-uri-s
      - header-settings
    - entry ToPBX
    - entry Discard
  - dial-plan
  - enterprise
  - dns
    - settings

**Configure vsp\session-config-pool\entry ToTelco\header-settings** Show basic Help

Index

Set Reset Back Delete

pAssert-mode	disabled (Resource is inactive)
header-to-strip	<a href="#">Edit header-to-strip</a>
allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	P-Location Alert-Info <a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
reg-ex-header	<a href="#">Add reg-ex-header</a>
header-normalization	<a href="#">Add header-normalization</a>
altered-body	<a href="#">Add altered-body</a>

### 7.2.3. Diversion Header

A Diversion Header is applied to forwarded off-net calls when the SIP trunk group on the Communication Manager has Send Diversion Header set to yes (**Section 5.7**). The Diversion Header will contain the number associated with the Enterprise user, allowing PAETEC to admit the call, and the From Header will be populated with the true calling party identity, allowing the forwarded destination to see the true caller ID. For the host portion of the header, Communication Manager sends the information entered in the signaling group Far-end Domain field (**Section 5.6**). To prevent this information from being exposed external to the enterprise, the SBC can modify the header and replace the Domain name with the IP address of the PAETEC Dynamic IP SIP Trunk. To create a rule to modify the Diversion Header first navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Add altered-header**.

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 of configuration options, with 'session-config-pool' expanded to show 'entry ToTelco'. The main content area is titled 'Configure vspsession-config-poolentry ToTelcoheader-settings'. It features a table with various header settings and their corresponding actions. The 'Add altered-header' link is highlighted with an orange circle.

Header Type	Action
allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
reg-ex-header	<a href="#">Add reg-ex-header</a>
header-normalization	<a href="#">Add header-normalization</a>
altered-body	<a href="#">Add altered-body</a>
reg-ex-collector	<a href="#">Add reg-ex-collector</a>
apply-allow-block-to	<a href="#">requests-and-responses</a> (apply to requests and responses)
apply-to-allow-block-to-dialog	<a href="#">both</a> (Apply to both inbound and outbound dialogs.)

In the right pane that appears, enter any number in the **number** field and enter “**Diversion**” in the **source-header** field. In the **source-field** area, next to **type** choose “**selection**” from the drop-down list.

In the **value** field, enter a regular expression to match. In the sample configuration, “**^(.\*)@(.\*)\$**” was entered. In this expression, the first (.\*?) will match and store any user part of the Diversion header. The second instance of (.\*?) matches and stores any host part of the header.

In the **replacement** field, “**\1@10.1.1.2>**” was entered in the sample configuration. The variable “**\1**” is the stored user part from the original Diversion header containing the number associated with the DID. The IP Address 10.1.1.2 is the IP Address of the PAETEC Dynamic IP SIP Trunk.

In the **destination** field and enter “**Diversion**” in the **source-header** field. Select “**full**” for **type** field in **destination-field** section and click **Create**.

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 style="border: 1px solid #ccc;" type="button" value=" &lt;Not configured&gt; "/>	
* source-field	<div>* type <input style="border: 1px solid #ccc;" type="button" value=" selection "/></div> <div>* value <input type="text" value="^(.*)@(.*)\$"/> (regular expression)</div> <div>* replacement <input type="text" value="\1@10.1.1.2&gt;"/></div>	
* destination	enter <input type="text" value="Diversion"/> or select from <input style="border: 1px solid #ccc;" type="button" value=" &lt;Not configured&gt; "/>	
* destination-field	<div>* type <input style="border: 1px solid #ccc;" type="button" value=" full "/></div>	



The following screen is presented, select “**INVITE**” for **apply-to-methods** and “**both**” for **type** field in **apply-to-responses** section. Click **Set** to complete the configuration.

**Configuration: all**

Configuration Setup View

cluster box:mes-sbc.avayalab.com

vsp

default-session-config

tls

session-config-pool

entry ToTelco

to-uri-specification

from-uri-specification

request-uri-specification

p-asserted-identity-uri

header-settings

entry ToPBX

entry Discard

dial-plan

enterprise

dns

settings

admin enabled (Resource is active)

\* number 1

\* source-header enter Diversion or select from Diversion

\* source-field

\* type selection (Regular expression based selection of portion of the URI.)

\* value ^(.\*)@(.\*)\$ (regular expression)

\* replacement \1@10.1.1.2>

\* destination enter Diversion or select from Diversion

\* destination-field

\* type full (Entire value of the URI.)

apply-to-methods

INVITE

REFER

MESSAGE

INFO

Select All Unselect All

apply-to-responses

\* type no (Do not apply to responses (requests only))

apply-to-dialog both (Apply to both inbound and outbound dialogs.)

session-persistent disabled (Resource is inactive)

## 7.2.4. Third Party Call Control

Disable third party call control. Navigate to **vsp** → **default-session-config** → **third-party-call-control**. Set the **admin** field to **disabled**.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy: cluster (box:mes-sbc.avayalab.com) > vsp > default-session-config > media > sip-directive > log-alert > **third-party-call-control**. The main content area is titled 'Configure vsp\default-session-config\third-party-call-control' and includes a 'Show advanced' button and a 'Help' link. Below the title are buttons for Set, Reset, Back, and Delete. The configuration table lists various settings:

Field	Value	Status
admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
refer-maintain-identity	false	
ringback-file		<a href="#">Browse System Files</a>
busy-file		<a href="#">Browse System Files</a>
pre-call-announcement		<a href="#">Browse System Files</a>
terminate-after-pre-call-announcement	disabled	(Resource is inactive)

### 7.2.5. From URI

When calls are presented to SIP clients registered to Session Manager the Caller ID and Call Log displays the entire URI in the format user@domain (e.g. 303-555-1234@10.1.1.2). When placing a call from the Call Log it is necessary for the domain to be one that is authorized on the Session Manager for the call to route properly. Therefore it is necessary to change the host portion of the From header to the enterprise domain.

In the left side menu, navigate to **vsp** → **session-config-pool** → **entry ToPBX**. Scroll down and click on **Configure** next to **from-uri-specification**.

The screenshot shows the Avaya Aura Configuration web 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 with 'cluster' expanded, containing 'box:mes-sbc.avayalab.com', 'vsp', 'default-session-config', 'tls', 'session-config-pool', 'entry ToTelco', and 'entry ToPBX'. The 'entry ToPBX' is selected, and the 'from-uri-specification' configuration page is displayed. The page has a table with the following rows:

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

In the new right pane that appears, choose **next-hop-domain** from the drop-down list in the **host** field and click **Set**. This will set the host portion of the From Header to the enterprise domain set in **Section 7.1.1**.

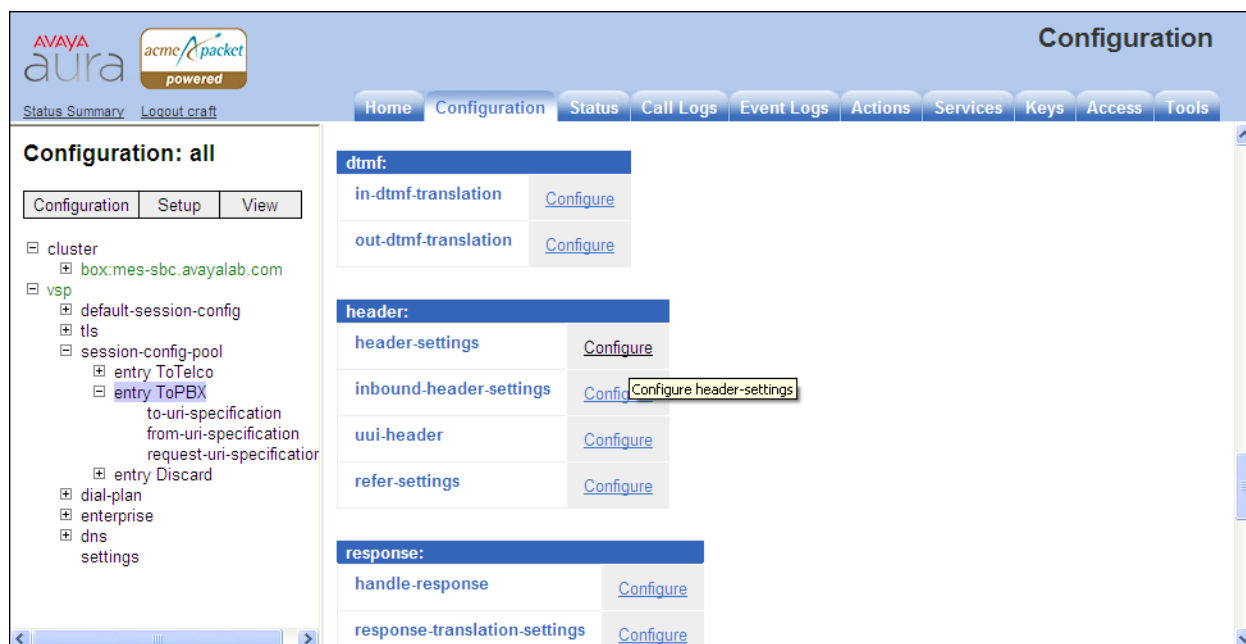
The screenshot shows the Avaya Aura Configuration interface. The left pane displays a tree view of the configuration hierarchy, with 'from-uri-specification' selected under 'session-config-pool'. The right pane shows the configuration for 'vsp|session-config-pool|entry ToPBX|from-uri-specification'. The 'host' field is highlighted with an orange circle, showing 'next-hop-domain' selected in the dropdown menu. Other fields include 'user' (from-uri), 'port' (from-uri), 'display' (from-uri), 'user-agent-aware-display-translation' (disabled), 'transport' (from-uri), 'user-param' (omit), 'user-truncate-non-digits' (disabled), and 'uri-parameter' (Add uri-parameter).

Field	Value	Description
user	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
host	next-hop-domain	(Net-Net OS-E uses the domain of the next-hop server.)
port	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
display	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
user-agent-aware-display-translation	disabled	(Resource is inactive)
transport	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
user-param	omit	
user-truncate-non-digits	disabled	(Resource is inactive)
uri-parameter	Add uri-parameter	

## 7.2.6. REFER-To Header

This section presents a sample configuration that will cause the SBC to modify the host portion of the Refer-To header in a REFER message, while preserving the user portion (containing the Refer-To destination telephone number) and any other information. In this example, the host portion was changed such that PAETEC would receive the PAETEC Dynamic SIP Trunk IP Address and port as the host portion.

In the left side menu, navigate to **vsp** → **session-config-pool** → **entry ToPBX**. Click on **Configure** next to **header-settings**.



On the right panel, select **Add reg-ex-header** as shown below.

The screenshot shows the AVAYA aura Configuration page. The left sidebar displays a tree view of the configuration hierarchy: cluster > vsp > session-config-pool > entry ToPBX > header-settings. The main content area is titled 'Configure vsp\session-config-pool\entry ToPBX\header-settings'. It features a table with the following rows:

Configuration	Setup	View
cluster		
box:mes-sbc.avayalab.com		
vsp		
default-session-config		
tls		
session-config-pool		
entry ToTelco		
entry ToPBX		
to-uri-specification		
from-uri-specification		
request-uri-specification		
header-settings		
entry Discard		
dial-plan		
enterprise		
dns		
settings		

The right panel shows the 'reg-ex-header' configuration table with the following rows:

Configuration	Setup	View
allowed-header		
blocked-header		
altered-header		
reg-ex-header		
header-normalization		
altered-body		
reg-ex-collector		
apply-allow-block-to		

The 'reg-ex-header' row is highlighted, and the 'Add reg-ex-header' link is visible. The 'apply-allow-block-to' row has a dropdown menu set to 'requests-and-responses' with the text '(apply to requests and responses)'.

In the new right pane that appears, enter any number in the **number** field and enter “**Refer-To**” in the **destination** field and click **Create**.

The screenshot shows the AVAYA aura Configuration page. The left sidebar displays a tree view of the configuration hierarchy: cluster > vsp > session-config-pool > entry ToPBX > header-settings. The main content area is titled 'Create vsp\session-config-pool\entry ToPBX\header-settings\reg-ex-header 0 - Step 1 of 1: Edit reg-ex-header 0'. It features a form with the following fields:

\* number: 1

\* destination: enter Refer-To or select from <Not configured>

Buttons: Create, Reset, Cancel

The following screen is presented, select **REFER** for **apply-to-methods** and **both** for **type** field in **apply-to-responses** section. Select the **Configure** link to the right of **create**.

**AVAYA aura** acme packet powered

Status Summary Logout craft

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

**Configuration: all**

Configuration Setup View

- cluster
  - box:mes-sbc.avayalab.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelco
    - entry ToPBX
      - to-uri-specification
      - from-uri-specification
      - request-uri-specification
      - header-settings
        - entry Discard
  - dial-plan
  - enterprise
  - dns
  - settings

**Configure vsplsession-config-poolentry ToPBX\header-settings\reg-ex-header 1**

Show advanced Help Index

Set Reset Back Copy Delete

**admin** enabled (Resource is active)

**\* number** 1

**\* destination** enter Refer-To or select from Refer-To

**create** [Configure](#)

**append** [Add append](#)

**apply-to-methods**

- INVITE
- REFER
- MESSAGE
- INFO

Select All Unselect All

**apply-to-responses**

\* type no (Do not apply to responses (requests only))

**apply-to-dialog** both (Apply to both inbound and outbound dialogs.)

**session-persistent** disabled (Resource is inactive)

Set Reset Back Copy

The following screen is presented. In the **source** area, select **Refer-To** from the drop-down list or type **Refer-To** in the **enter** field.

In the **expression** field, enter a regular expression to match. In the sample configuration, `<sip:(.*)@avayalab.com(.*)>` was entered. In this expression, the first `(.*)` will match and store any user part of the Refer-To header. The second instance of `(.*)` matches and stores any UUI if present. The domain **avayalab.com** is what the SBC would otherwise put in the Refer-To header host part.

In the **replacement** field, `<sip:\1@\r:\R\2>` was entered in the sample configuration. The variable `"\1"` is the stored user part from the original Refer-To header containing the Refer-To number, corresponding to the first instance of `(.*)` from the **expression**. The variable `\2` is any stored UUI from the original Refer-To header, corresponding to the second instance of `(.*)` from the **expression**. The `\r` inserts the remote IP Address corresponding to the PAETEC Dynamic IP SIP Trunk IP Address. This is followed by a colon and `\R` corresponding to the PAETEC Dynamic IP SIP Trunk signaling port, which is 5060 in this case.

After completing the **source**, **expression** and **replacement** fields as appropriate, click **Create**.

Create vsplsession-config-poolentry ToPBX\header-settings\reg-ex-header 1\create - Step 1 of 1: Edit create [Help](#) [Index](#)

Please provide some basic information for create. Then press "Create".

* source	enter <input type="text" value="Refer-To"/> or select from <input type="button" value="&lt;Not configured&gt;"/>
* expression	<input type="text" value="p:(.*)@avayalab.com(.*)&gt;"/> (regular expression)
* replacement	<input type="text" value="&lt;sip:\1@\r:\R\2&gt;"/>



The following screen shows the completed rule. Click **Set** to complete the configuration.

The screenshot shows the Avaya Aura Configuration interface. The left pane displays a tree view of the configuration hierarchy, with 'reg-ex-header 1' selected under 'header-settings'. The main pane shows the configuration for 'Configure vsp|session-config-pool|entry ToPBX|header-settings|reg-ex-header 1'. The configuration includes fields for 'admin' (enabled), 'number' (1), 'destination' (Refer-To), 'source' (Refer-To), 'expression' (< sip:(.\*)@avayalab\.com(.\*) (regular expression)), 'replacement' (< sip:1@r:\R2>), 'apply-to-methods' (INVITE, REFER, MESSAGE, INFO), 'apply-to-responses' (no), 'apply-to-dialog' (both), and 'session-persistent' (disabled). Buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete' are visible at the top and bottom of the configuration pane.

### 7.2.7. 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**.

The screenshot shows the 'Configuration: all' menu. The 'Configuration' tab is selected, and the 'Update and save configuration' option is highlighted. A tooltip for 'Update and save configuration' is displayed, stating 'Update and save the current configuration.' The menu also includes options for 'Reload configuration', 'Validate configuration', 'Analyze configuration', 'Search configuration', 'Save as XML', and 'Load from XML'. The left pane shows the configuration hierarchy with 'sip-gateway PBX' and 'sip-gateway Telco' selected under 'servers'.

## 8. Dynamic IP SIP Trunk Service Configuration

To use the Dynamic IP SIP Trunk Service, a customer must request the service from PAETEC using their sales processes. This process can be initiated by contacting PAETEC via the corporate web site at [www.paetec.com](http://www.paetec.com) and requesting information via the online sales links or telephone numbers.

## 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.

### 9.1. Verification

The following steps may be used to verify the configuration:

1. Verify the call routing administration on the Session Manager by logging in to System Manager and execute the Call Routing Test. Expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to PSTN via PAETEC. Under **Routing Decisions**, observe the call will rout via the SBC to PAETEC. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

The screenshot shows the 'Call Routing Test' page in the System Manager. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager, Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, System Tools, Maintenance Tests, SIP Tracer, Configuration, SIP Trace Viewer, and Call Routing Test. The main content area has a breadcrumb trail: Home / Elements / Session Manager / System Tools / Call Routing Test. The title is 'Call Routing Test'. Below the title is a description: 'This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed administration.' The form is divided into two main sections: 'SIP INVITE Parameters' and 'Routing Decisions'. The 'SIP INVITE Parameters' section includes fields for 'Called Party URI' (sip:13035551997@avayalab.com), 'Calling Party URI' (sip:7135551234@avayalab.com), 'Day Of Week' (Tuesday), 'Time (UTC)' (15:31), 'Called Session Manager Instance' (SessionManager1), 'Calling Party Address' (10.80.150.210), 'Session Manager Listen Port' (5070), and 'Transport Protocol' (TCP). There is an 'Execute Test' button. The 'Routing Decisions' section shows the result: 'Route < sip:13035551997@avayalab.com > to SIP Entity SBC1 (10.80.150.212). Terminating Location is SP-SIP-Trunk-SBC.'

2. 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.
3. 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.
4. Verify that the user on the PSTN can end an active call by hanging up.

5. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Use **status trunk n** to verify the active call has ended. Where **n** is the trunk group number used for PAETEC Dynamic IP SIP Trunk Service.

Below is an example of an active call.

```
status trunk 1
```

TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	<b>in-service/active</b>	<b>no</b>	<b>S00000</b>
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

Verify the port returns to **in-service/idle** after the call has ended.

```
status trunk 1
```

TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	<b>in-service/idle</b>	<b>no</b>	
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

## 9.2. Troubleshooting

1. Session Border Controller:
  - **Call Logs** - On the web user interface of the SBC, 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 station** <extension number> - Displays signaling and media information for an active call on a specific station.
  - **status trunk** <trunk access code number> - Displays trunk group information.
3. Session Manager:
  - **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Solution for Midsize Enterprise to the PAETEC Dynamic IP SIP Trunk Service. The PAETEC Dynamic IP SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The PAETEC Dynamic IP SIP Trunk Service provides businesses 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] *Installing and Configuring Avaya Aura® Solution for Midsize Enterprise, Release 2.1, Issue 3 July 2011.*
- [4] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.1 Intelligent Workbook. July 2011.*
- [5] *Administering Avaya Aura™ Communication Manager, June 2010, Document Number 03-300509.*
- [6] *Avaya Aura™ Communication Manager Feature Description and Implementation, June 2010, Document Number 555-245-205.*
- [7] *Installing and Upgrading Avaya Aura™ System Manager 6.1 GA Version, November 2010.*
- [8] *Installing and Configuring Avaya Aura® Session Manager, April 2011, Document Number 03-603473*
- [9] *Administering Avaya Aura® Session Manager, November 2010, Document Number 03-603324.*
- [10] *Installing and Configuring Avaya Aura® Session Border Controller, November 2010.*
- [11] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x, April 2010, Document Number 16-601443.*
- [12] *4600 Series IP Telephone LAN Administrator Guide, July 2008, Document Number 555-233-507.*
- [13] *Avaya one-X Deskphone H.323 Administrator Guide, May 2011, Document Number 16-300698.*
- [14] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1, December 2010, Document Number 16-603838*
- [15] *Administering Avaya one-X Communicator, July 2011*
- [16] *RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>*
- [17] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method, <http://www.ietf.org/>*
- [18] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>*
- [19] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, <http://www.ietf.org/>*

## 12. Appendix A: Avaya Aura® SBC Configuration File

```
#
# Copyright (c) 2004-2011 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 16:15:02 Thu 2011-08-04
#
config cluster
config box 1
    set hostname mes-sbc.avayalab.com
    set timezone America/Denver
    set name mes-sbc.avayalab.com
    set identifier 00:ca:fe:11:57:10
config interface eth0
    config ip mgmt
        set ip-address static 10.80.150.212/24
    config ssh
        set mode ssh-2
    return
    config snmp
        set trap-target 10.80.150.208 162
        set trap-filter generic
        set trap-filter dos
        set trap-filter sip
        set trap-filter system
    return
    config web
        set ciphers
        TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA
    return
    config web-service
        set protocol https 8443
        set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config icmp
    return
    config routing
        config route Default
            set gateway 10.80.150.1
        return
        config route Static0
            set destination network 192.11.13.4/30
            set gateway 10.80.150.207
        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
config route MgmtDefault
    set gateway 10.80.150.1
return
return
return
return
config interface eth1
    config ip inside
        set ip-address static 10.80.150.217/24
    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 media-ports
    return
    config routing
        config route Default
            set admin disabled
        return
    return
return
return
config interface eth2
    config ip outside
        set ip-address static 10.2.2.5/25
    config sip
        set udp-port 5060 "" "" any 0
    return
    config media-ports
    return
    config routing
        config route Default
            set admin disabled
        return
        config route external-sip-media-1
            set destination host 10.1.1.2
            set gateway 10.2.2.1
        return
    return
    config kernel-filter
        config allow-rule allow-sip-udp-from-peer-1

```

```

        set destination-port 5060
        set source-address/mask 10.1.1.2/32
        set protocol udp
    return
    config deny-rule deny-all-sip
        set destination-port 5060
    return
return
return
return
config cli
    set prompt mes-sbc.avayalab.com
return
return
return

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

```

```

    set count 3
    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 tracing enabled
        set apply-to-methods-for-filtered-logs INVITE+REFER
    return
    config third-party-call-control
    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
        set host local-ip
    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 ^(.*)@(.*)$ "\1@10.1.1.2>"
        set destination Diversion
        set destination-field full
    return
return
return
config entry ToPBX
    config to-uri-specification
        set host next-hop-domain
    return
    config from-uri-specification
        set host next-hop-domain
    return
    config request-uri-specification
        set host next-hop-domain
    return
    config header-settings
        config reg-ex-header 1
            set destination Refer-To
            set create Refer-To "<sip:(.*)@avayalab\.com(.*)>" "<sip:\1@\r:\R\2>"
            set apply-to-methods REFER
        return
    return
return
config entry Discard
    config sip-directive
    return
return
return
config dial-plan
    config route Default
        set priority 500
        set location-match-preferred exclusive
        set session-config vsp\session-config-pool\entry Discard
    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 avayalab.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 10.80.150.214
    return
return
config sip-gateway Telco
    set failover-detection ping
    set ping-interval 240
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
        config server Telco1
            set host 10.1.1.2
        return
    return
return
return
return
config dns
    config resolver
        config server 10.80.150.201
    return
return
return
config settings
    set read-header-max 8191
return
return

config external-services
return

config preferences
    config gui-preferences
        set enum-strings SIPSourceHeader Diversion
        set enum-strings SIPSourceHeader Refer-To
        set enum-strings SIPSourceHeader 1
        set show-unlicensed-features false
    return
return

config access
    config permissions superuser
        set cli advanced
    return
    config permissions read-only
        set config view
        set actions disabled
        set debug disabled
    return
    config users
        config user admin
            set password 0x00ef423a29a2107ee58ec0550339f5a61b5dba23c695975082403e542b
            set permissions access\permissions superuser
        return
        config user cust
            set password 0x00061a2062a4b3d3bc15918b0cebbe9bb5050eb8a42c63fb28a6ebd5ac

```

```
    set permissions access\permissions read-only
return
config user init
    set password 0x00755c995b232018224ae8f5484dce1ec3cb4dc2cb763694294c1a084d
    set permissions access\permissions superuser
return
config user craft
    set password 0x00c6cb901342e52636a403606bc1f3c1930bcbdbe54fbc3a99fa171f
    set permissions access\permissions superuser
return
config user dadmin
    set password 0x007058db732aabf006eb0db4778db99706cb63e6e54631f7719165b568
    set permissions access\permissions read-only
return
return
return

config features
return
```

---

**©2010 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](mailto:devconnect@avaya.com).