



## **Application Notes for Configuring PAETEC Dynamic IP SIP Trunk Service (BroadSoft Platform) with Avaya Aura® Communication Manager Evolution Server 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0 – 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® Session Border Controller, Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, 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.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing .....	4
2.2.	Test Results .....	5
2.3.	Support.....	5
3.	Reference Configuration.....	6
4.	Equipment and Software Validated .....	8
5.	Configure Avaya Aura® Communication Manager .....	9
5.1.	Licensing and Capacity.....	9
5.2.	System Features .....	10
5.3.	IP Node Names .....	11
5.4.	Codecs.....	11
5.5.	IP Network Region .....	12
5.6.	Signaling Group.....	13
5.7.	Trunk Group.....	15
5.8.	Inbound Routing .....	17
5.9.	Calling Party Information .....	18
5.10.	Outbound Routing.....	19
6.	Configure Avaya Aura® Session Manager .....	23
6.1.	Avaya Aura® System Manager Login and Navigation.....	24
6.2.	Specify SIP Domain.....	25
6.3.	Add Location .....	26
6.4.	Add SIP Entities.....	29
6.5.	Add Entity Links.....	33
6.6.	Add Routing Policies .....	35
6.7.	Add Dial Patterns.....	36
6.8.	Verify Avaya Aura® Session Manager Instance.....	40
7.	Configure Avaya Aura® Session Border Controller .....	42
7.1.	Installation Wizard.....	42
7.1.1.	Network Settings.....	43
7.1.2.	Logins .....	44
7.1.3.	VPN Access .....	45
7.1.4.	SBC .....	46
7.1.5.	Confirm Installation.....	48
7.2.	Post Installation Configuration .....	49
7.2.1.	Options Frequency .....	49
7.2.2.	Blocked Headers .....	51
7.2.3.	Diversion Header .....	53
7.2.4.	Third Party Call Control .....	57
7.2.5.	From URI .....	58
7.2.6.	REFER-To Header.....	60

7.2.7.	In/Out Hold Translation .....	65
7.2.8.	Save the Configuration .....	66
8.	Dynamic IP SIP Trunk Service Configuration .....	67
9.	Verification and Troubleshooting .....	67
9.1.	Verification .....	67
9.2.	Troubleshooting .....	68
10.	Conclusion .....	69
11.	References .....	69
12.	Appendix A: Avaya Aura® SBC Configuration File .....	71

# 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® Session Boarder 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 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.
- G.711 Faxing
- 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.
- **SendOnly SIP Parameter:** With the Network Call Redirection feature enabled, Communication Manager will use the SIP parameter *SendOnly* to signal any hold call conditions. The *SendOnly* SIP parameter is not supported by PAETEC Dynamic IP service. The SBC is used to replace the *SendOnly* parameter with the *SendRecv* parameter that the PAETEC Dynamic IP service does support. See **Section 7.2.7**.

## 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.

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

- Communication Manager
- Session Manager
- System Manager
- Session Boarder Controller
- Avaya G430 Media Gateway
- 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

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.



Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to 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® Communication Manger	R016x.00.1.510.1-19100 (SP 4)
Avaya Aura® Messaging	R016x.00.1.510.1-004_0302 (SP 3)
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.115
Avaya Aura® Session Manager	6.1.4.0.614005
Avaya Aura® Session Border Controller	E362M1P1
Avaya G430	31.18.1
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.102
Avaya 1608 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.3
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.1
Avaya 9621 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 6.0.1
Avaya 9611 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 6.0.1
Avaya 9608 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 6.0.1
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:** This solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.



## 5. Configure Avaya Aura® 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 G430 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:** 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 **257** 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	3
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	1
<b>Maximum Administered SIP Trunks:</b>	<b>12000</b>	<b>275</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 features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.

```
change system-parameters features                                     Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? 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 types of calls.

```
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 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>10.80.150.206</b>	
default	0.0.0.0	
<b>procr</b>	<b>10.80.150.225</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, G.711A and G.711MU. During compliance testing, each of the supported codecs were tested independently by changing the order of preference to list the codec being tested as the first choice. The true order of preference is defined by the end customer. In the example below, **G.729A** and **G.711MU** was entered in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 2		Page 1 of 2
		IP Codec Set
Codec Set: 2		
Audio Codec	Silence Suppression	Frames Per Pkt    Packet Size (ms)
1: <b>G.729A</b>	n	2            20
2: <b>G.711MU</b>	n	2            20
3:		

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

change ip-codec-set 2		Page 2 of 2
		IP Codec Set
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
<b>FAX</b>	<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 **Location** field to match the enterprise location for this SIP trunk.
- 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. To enable shuffling, set both **Intra-region** and **Inter-region IP-IP Direct Audio** fields 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
Codec Set: 2           Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 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
H.323 IP ENDPOINTS           AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y   RSVP Enabled? n
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 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 Communication Manager will serve as an Evolution Server for 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 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: 5070	
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. Set **Modify Tandem Calling Number** to **tandem-cpn-form**. 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
    Numbering Format: public
    UI Treatment: service-provider
    Replace Restricted Numbers? y
    Replace Unavailable Numbers? y
    Modify Tandem Calling Number: tandem-cpn-form
    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 **Reference [15]**. 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 necessary to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to **n**. Set the **Telephone Event Payload Type** to **101**, the value preferred by PAETEC.

**Note:** PAETEC's Enterprise Trunking Feature does not require the use of the Diversion header on re-directed calls. When using PAETEC's Enterprise Trunking Feature, set **the Send Diversion Header** field to **n**.

```

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
                                Network Call Redirection? y
                                Send Diversion Header? y
                                Support Request History? n
                                Telephone Event Payload Type: 101

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

```

## 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/      Number      Del Insert
                                Feature      Len      Digits
                                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	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
5	4			5	
5	5			5	
5	6			5	
5	7			5	
5	8			5	
5	12001	1	7135551234	10	
5	12002	1	7135551235	10	
5	12003	1	7135551236	10	
5	12004	1	7135551237	10	

Use the **change tandem-calling-party-num** command, to define the calling party number to send to the PSTN for tandem calls from SIP users.

In the example shown below, all calls originating from a 5-digit extension beginning with 13 and routed to trunk group 1 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case **pub-unk**.

change tandem-calling-party-num					Page 1 of 8
CALLING PARTY NUMBER CONVERSION FOR TANDEM CALLS					
CPN	Trk			Number	
Len Prefix	Grp(s)	Delete	Insert	Format	
5 13	1	5	7135551234	pub-unk	

## 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.

- **Dialed String:** enter the leading digits (e.g., **1303**) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., **11**) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., **11**) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., **1**) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type:** enter **fnpa**, the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter **hnpa**. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1. For more information and a complete list of Communication Manager call types, see **Reference [3]** and **[4]**.

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						Percent Full: 0	
Location: all							
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
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 **1** 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	

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DIDs to prevent these calls from going out the PSTN and using unnecessary SIP trunk resources. The example below shows the DID numbers assigned by PAETEC being converted to 5 digit extensions.

change ars digit-conversion 0					Page 1 of 2			
ARS DIGIT CONVERSION TABLE					Percent Full: 0			
Location: all								
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI	Req
7135551234	10	10	10	12001	ext	y		n
7135551235	10	10	10	12002	ext	y		n
7135551236	10	10	10	12003	ext	y		n
7135551237	10	10	10	12004	ext	y		n
								n
								n
								n
								n
								n
								n
								n
								n

## 6. Configure Avaya Aura® Session Manager

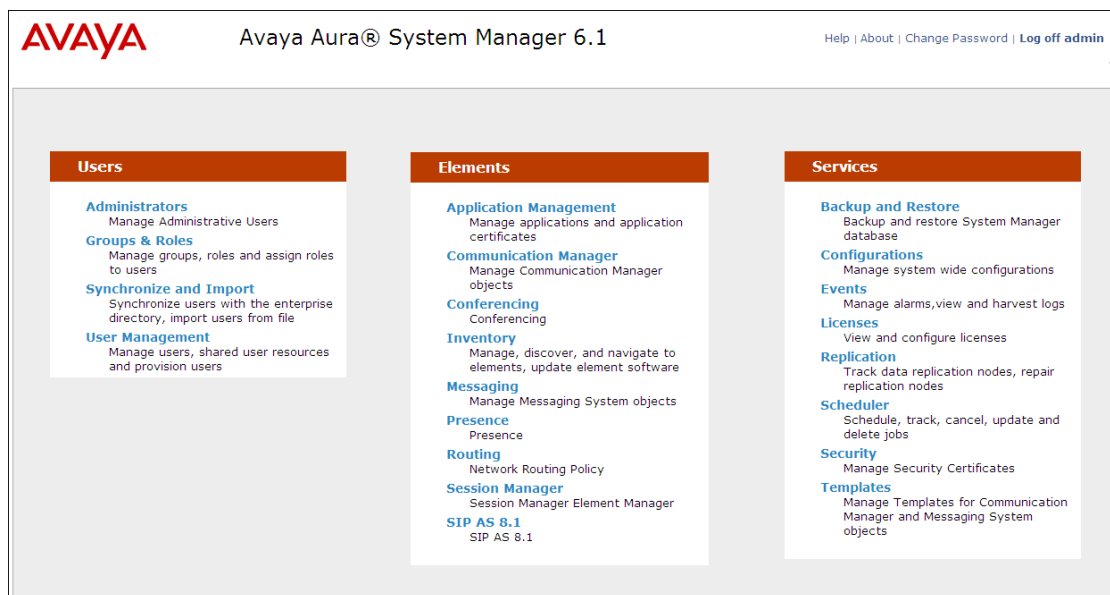
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- 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.

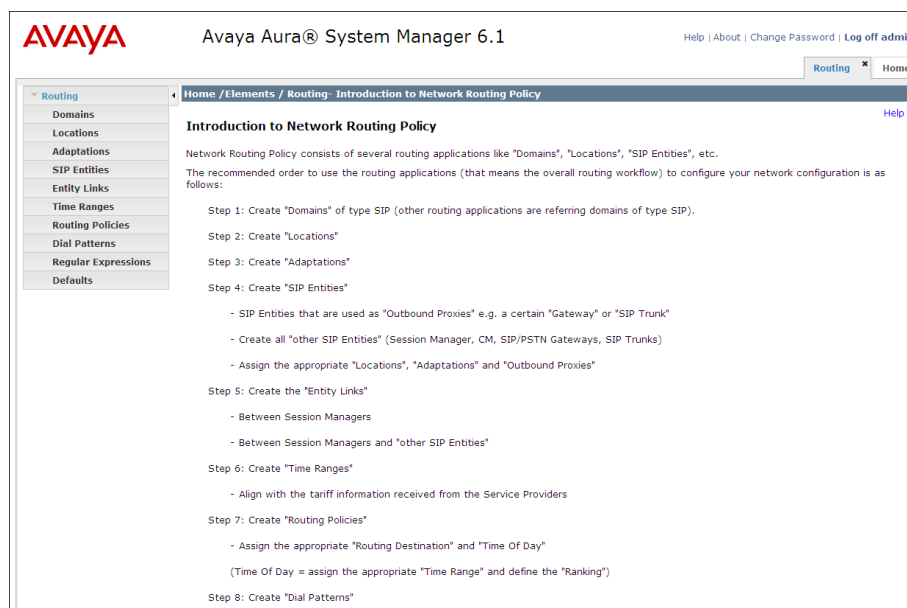
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

## 6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL <https://<ip-address>/SMGR>, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **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 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 indicating a new entry), 'Type' is 'sip' (selected from 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).

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.4**), so it was not necessary to add a pattern.

The screen below shows the addition of **Location\_150\_SM**, this location will be used for Session Manager. Click **Commit** to save.

Home / Elements / Routing / Locations - Location Details [Help ?](#)

**Location Details** [Commit](#) [Cancel](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.  
See Session Manager -> Session Manager Administration -> Global Setting

**General**

\* **Name:**

**Notes:**

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**

**Total Bandwidth:**

**Per-Call Bandwidth Parameters**

\* **Default Audio Bandwidth:**

**Location Pattern**

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
--------------------------	--------------------	-------

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

Repeat the preceding procedure to create a separate Location for Communication Manager and SBC. Displayed below is the screen for **Location\_150\_CM** used for Communication Manager.

[Home](#) / [Elements](#) / [Routing](#) / [Locations](#) - Location Details [Help ?](#)

**Location Details** [Commit](#) [Cancel](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.  
See [Session Manager -> Session Manager Administration -> Global Setting](#)

### General

\* **Name:**

**Notes:**

### Overall Managed Bandwidth

**Managed Bandwidth Units:**

**Total Bandwidth:**

### Per-Call Bandwidth Parameters

\* **Default Audio Bandwidth:**

### Location Pattern

[Add](#) [Remove](#)

0 Items | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
--------------------------	--------------------	-------

\* **Input Required** [Commit](#) [Cancel](#)

Below is the screen for AA-SBC\_150 used for the SBC.

Home / Elements / Routing / Locations - Location Details

Location Details

CommitCancelHelp ?

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.  
See [Session Manager -> Session Manager Administration -> Global Setting](#)

General

\* Name:

AA-SBC\_150

Notes:

Aura SBC for Loc 150

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

\* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

AddRemove

0 Items | RefreshFilter: Enable

	IP Address Pattern	Notes
--	--------------------	-------

\* Input Required

CommitCancel

## 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 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'. On the right, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The 'General' section is active, showing the following fields: 'Name' (required, value: ASM), 'FQDN or IP Address' (required, value: 10.80.150.206), 'Type' (dropdown menu, value: Session Manager), 'Notes' (text area, value: Session Manager), 'Location' (dropdown menu, value: Location\_150\_SM), 'Outbound Proxy' (dropdown menu, value: empty), 'Time Zone' (dropdown menu, value: America/Denver), and 'Credential name' (text area, value: empty). The 'SIP Link Monitoring' section is also visible, with a dropdown menu set to 'Use Session Manager Configuration'.

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

SIP Entity Details [Help ?](#)

**General**

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

**SIP Link Monitoring**

SIP Link Monitoring:

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 Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. 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 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 | [Refresh](#)
Filter: [Enable](#)

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

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 defined in **Section 5.3** of the procr interface on Communication Manager.

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

[Help ?](#)

SIP Entity Details

CommitCancel

General

\* Name:

CM601-TG1-Loc150

\* FQDN or IP Address:

10.80.150.225

Type:

CM

Notes:

CM Trunk Group 1 for SP Trunks

Adaptation:

Location:

Location\_150\_CM

Time Zone:

America/Denver

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.

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

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

**General**

\* Name: AA-SBC01

\* FQDN or IP Address: 10.80.150.253

Type: SIP Trunk

Notes: Avaya Aura SBC Loc 150

Adaptation:

Location: AA-SBC\_150

Time Zone: America/Denver

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 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 SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For 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 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:

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	Connection Policy	Notes
* ASM_CM601-TG1-Lo	* ASM	TCP	* 5070	* CM601-TG1-Loc150	* 5070	Trusted	

\* Input Required

Entity Link to the SBC:

[Home](#) / [Elements](#) / [Routing](#) / [Entity Links - Entity Links](#)

[Help ?](#)

**Entity Links**

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

1 Item | [Refresh](#)

Filter: [Enable](#)

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* <input type="text" value="ASM_AA-SBC01_506"/>	* <input type="text" value="ASM"/> ▼	<input type="text" value="TCP"/> ▼	* <input type="text" value="5060"/>	* <input type="text" value="AA-SBC01"/> ▼	* <input type="text" value="5060"/>	<input type="text" value="Trusted"/> ▼	<input type="text"/>

[<](#) [>](#)

\* Input Required

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

## 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).

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 SBC.

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

Routing Policy Details

Help ?

Commit Cancel

General

\* Name: To-CM601-TG1-LOC150

Disabled: ☐

Notes: Trunk Group 1 for SIP SP

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM601-TG1-Loc150	10.80.150.225	CM	CM Trunk Group 1 for SP Trunks

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

Routing Policy Details

Help ?

Commit Cancel

General

\* Name: To\_AA-SBC01

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AA-SBC01	10.80.150.253	SIP Trunk	Avaya Aura SBC Loc 150

## 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** originating from **Location\_150\_CM** uses route policy **To\_AA-SBC01**.

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

Dial Pattern Details

Commit Cancel

Help ?

General

\* Pattern: 1

\* Min: 11

\* Max: 11

Emergency Call:

SIP Domain: avayalab.com

Notes: 1+ OUTBOUND

Originating Locations and Routing Policies

Add Remove

2 Items | 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"/>	Location_140_CM	Subnet 140	To Sipera	0	<input type="checkbox"/>	Sipera	
<input type="checkbox"/>	Location_150_CM	Communication Manager	To_AA-SBC01	0	<input type="checkbox"/>	AA-SBC01	

Select : All, None

The second example shows that a 10 digit number **7135551234** to domain **avayalab.com** and originating from **AA-SBC\_150** uses route policy **To-CM601-TG1-LOC150**. This is a DID number assigned to the enterprise from PAETEC.

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

Dial Pattern Details
[Commit](#) [Cancel](#)

General

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item | Refresh
Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AA-SBC_150	Aura SBC for Loc 150	To-CM601-TG1-LOC150	0	<input type="checkbox"/>	CM601-TG1-Loc150	Trunk Group 1 for SIP SP

Select : All, None

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

Home / Elements / Routing / Dial Patterns- Dial Patterns

Dial Patterns

[Help ?](#)

Edit

New

Duplicate

Delete

More Actions ▾

8 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	0+ OUTBOUND
<input type="checkbox"/>	<u>1</u>	11	11	<input type="checkbox"/>	avayalab.com	1+ OUTBOUND
<input type="checkbox"/>	<u>303</u>	10	10	<input type="checkbox"/>	avayalab.com	
<input type="checkbox"/>	<u>411</u>	3	3	<input type="checkbox"/>	avayalab.com	OUTBOUND 411
<input type="checkbox"/>	<u>7133433761</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12001
<input type="checkbox"/>	<u>7133433762</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12002
<input type="checkbox"/>	<u>7133433763</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12003
<input type="checkbox"/>	<u>7133433764</u>	10	10	<input type="checkbox"/>	avayalab.com	DID to x12004

Select : All, None

## 6.8. Verify Avaya Aura® 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 instance 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.

Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration [Help ?](#)

### View Session Manager [Return](#)

[General](#) | [Security Module](#) | [NIC Bonding](#) | [Monitoring](#) | [CDR](#) | [Personal Profile Manager \(PPM\)](#) - [Connection Settings](#) | [Event Server](#) | [Expand All](#) | [Collapse All](#)

**General** ▼

**SIP Entity Name**

**Description**

**Management Access Point Host Name/IP**

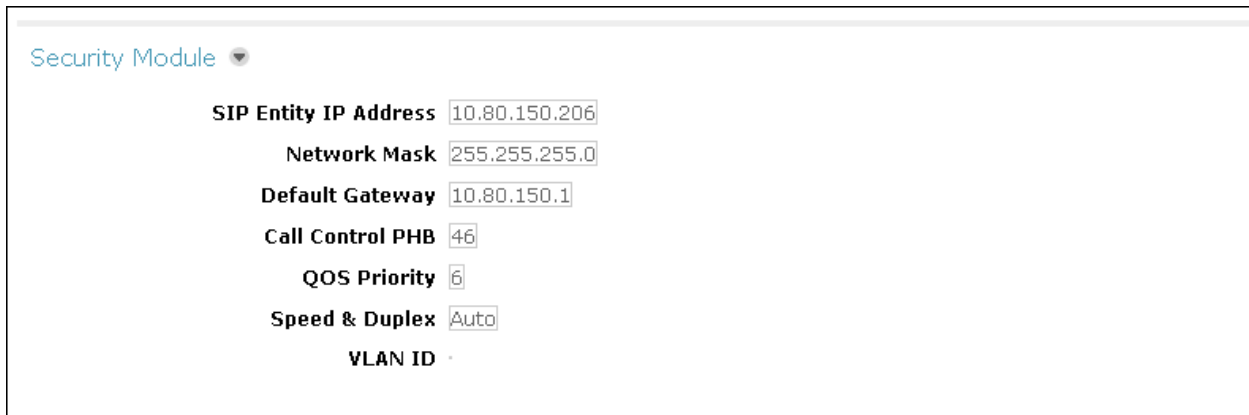
**Direct Routing to Endpoints**



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 page. It features a list of configuration fields with their respective values:

Field	Value
SIP Entity IP Address	10.80.150.206
Network Mask	255.255.255.0
Default Gateway	10.80.150.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

## 7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the SBC. This configuration is done in two parts. The first part is done during the SBC installation via the installation wizard. These Application Notes will not cover the SBC installation in its entirety but will include the use of the installation wizard. For information on installing the Avaya Aura® System Platform and the loading of the Avaya Aura® SBC template see **Reference [1]** and **[8]**.

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 Avaya Aura® SBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the SBC.

When it gets to “**Wait for User to Complete Data Entry**” (shown below), it will open another window for input. It may be necessary to enable pop-ups to view.

**Virtual Machine Management**  
[Template Installation](#)

**Template Installation In Progress**

Workflow Status						
Start Time	Task Description	State	% Complete	Estimate	Actual	
11:41:10	Download disk image for sbc	Complete	100		39s	✓
11:41:10	Download plugins for VMs	Complete	100		2s	✓
11:41:13	Check Template for Web Application	Complete	100		6s	✓
11:41:20	Download pre-install web application	Complete	100		0s	✓
11:41:20	Pre-Install Web Application Deployment	Complete	100		5s	✓
11:41:26	Wait For User To Complete Data Entry	In Progress	0			■■■■■
	Undeploy Web Application	Not Started	0			*
	Process EPW properties file if present	Not Started	0			*
	Configure Network	Not Started	0			*
	Install plugins	Not Started	0			*
	Install sbc	Not Started	0	22m 0s		*
	Restart network	Not Started	0			*
	Start all VMs	Not Started	0			*
	Wait until system and all VMs are stabilized	Not Started	0			*
	Run post-install plugin if present	Not Started	0			*
	Finalize Installation	Not Started	0			*

### 7.1.1. Network Settings

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

- **IP Address:** Enter the IP address of the private side of the SBC.
- **Hostname:** Enter a host name for the SBC.
- **Domain:** Enter the domain used for the enterprise. This should match the Domain set in Session Manager (**Section 6.2**) and the Communication Manager signaling group Far-end Domain (**Section 5.6**).

Click **Next Step** (not shown) to continue.

**AVAYA**

Home

Configuration

Installation

- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Finish

### Network Settings

Enter network settings

Domain-0 IP Address: 10.80.150.251

CDom IP Address: 10.80.150.252

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 (Optional):

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

Virtual Machine	IP Address	Hostname	Domain
SBC	10.80.150.253	aasbc	avayalab.com (Optional)

Default Domain: (Optional)

Apply to all VMs

Next Step

## 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.

The screenshot shows the Avaya web interface for configuring services logins. The left sidebar contains a navigation menu with 'Configuration' expanded and 'Installation' selected. Under 'Installation', the steps are: Network Settings, Logins (current), VPN Access, Session Border Controller, Summary, and Finish. The main content area is titled 'Logins' and 'Services logins for SBC (optional)'. It contains two tables for setting passwords.

Login name	Password	Re-type password
craft	<input type="password"/>	<input type="password"/>
init	<input type="password"/>	<input type="password"/>
dadmin	<input type="password"/>	<input type="password"/>

Login name	Password	Re-type password
root	<input type="password"/>	<input type="password"/>
sbadmin	<input type="password"/>	<input type="password"/>
sbccust	<input type="password"/>	<input type="password"/>

At the bottom of the main content area, there are two links: [Previous Step](#) and [Next Step](#).

### 7.1.3. VPN Access

VPN remote access to the SBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?**

Click **Next Step** to continue.

**AVAYA**

Home

Configuration

Installation

- Network Settings
- VPN Access
- SBC
- Summary
- Finish

## VPN Access

### Configure VPN Access

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

☐ Yes ☒ No

VPN Access Configuration

VPN Router IP Address

Remote Access Network

Remote Access Network Subnet Mask

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

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

If in doubt, please refer to the documentation.

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

#### 7.1.4. SBC

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

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

- **Service Provider:** From the pull-down menu, select the name of the service provider to which the SBC will connect. This will allow the wizard to 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:

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

In the **Enterprise SIP Server** section:

- **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.
- **SIP Domain** Enter the enterprise SIP domain.

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

Home

Configuration

Installation

Network Settings

Logins

VPN Access

SBC

Summary

Finish

SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider	Port		
Generic	5060		
IP Address1	Signalling/Media Network1	Signalling/Media Netmask1	
10.1.1.2	10.1.1.2	255.255.255.255	
IP Address2 (Optional)	Signalling/Media Network2 (Optional)	Signalling/Media Netmask2 (Optional)	Hunting (Optional)

SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	10.80.150.253	255.255.255.0	10.80.150.1
Public	10.2.2.5	255.255.255.128	10.2.2.1

Enterprise SIP Server

SIP Domain

avayalab.com

IP Address1

10.80.150.206

Transport1

TCP

IP Address2 (Optional)

Transport2 (Optional)

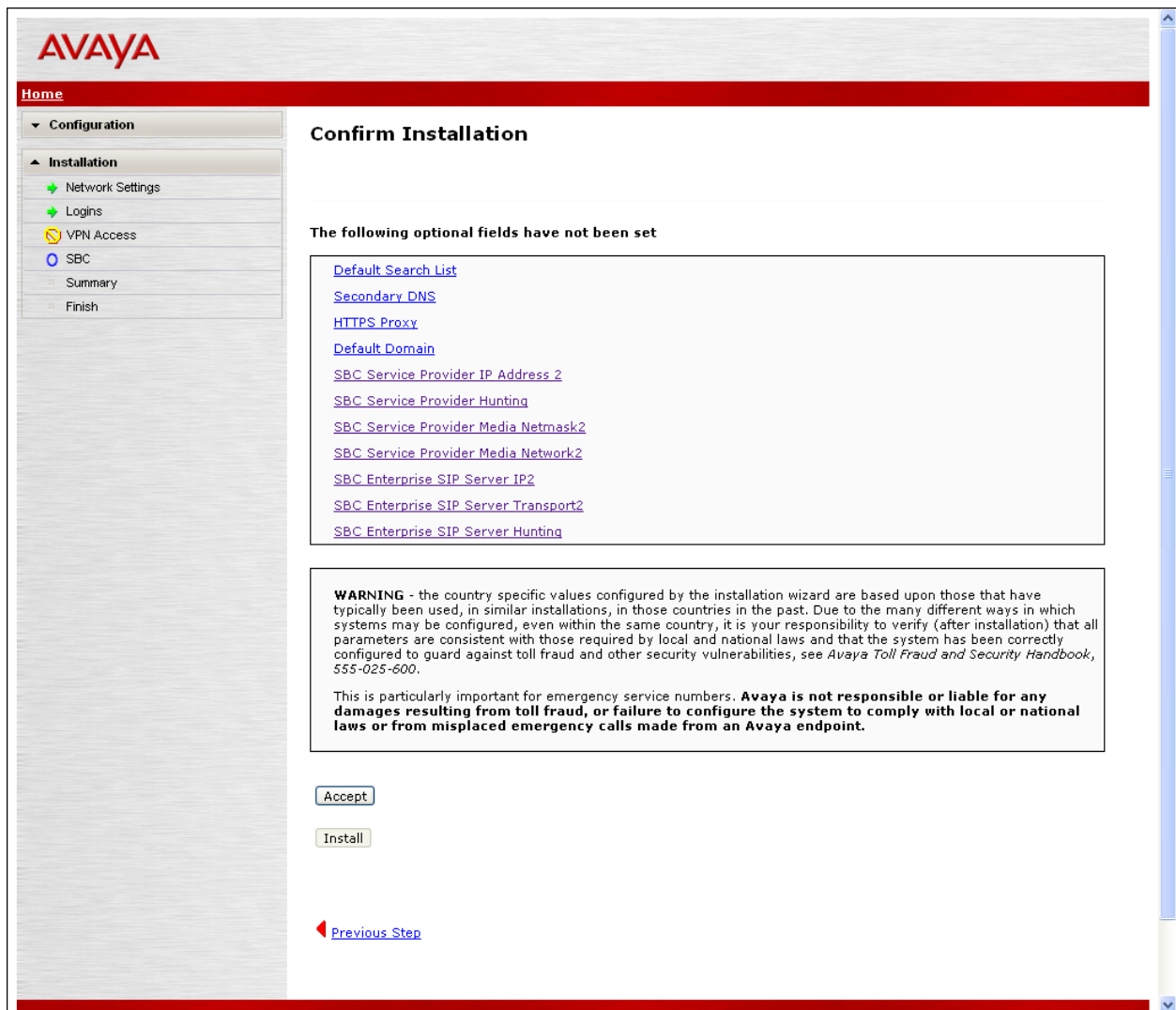
Hunting (Optional)

Previous Step

Next Step

### 7.1.5. Confirm Installation

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



The screenshot shows the Avaya web interface for the 'Confirm Installation' step. On the left is a navigation menu with 'Configuration' expanded and 'Installation' selected. Under 'Installation', the steps are: Network Settings, Logins, VPN Access, SBC (highlighted with a blue circle), Summary, and Finish. The main content area is titled 'Confirm Installation'. It contains a section 'The following optional fields have not been set' with a list of links: Default Search List, Secondary DNS, HTTPS Proxy, Default Domain, SBC Service Provider IP Address 2, SBC Service Provider Hunting, SBC Service Provider Media Netmask2, SBC Service Provider Media Network2, SBC Enterprise SIP Server IP2, SBC Enterprise SIP Server Transport2, and SBC Enterprise SIP Server Hunting. Below this is a 'WARNING' box with text about country-specific values and emergency service numbers. At the bottom are 'Accept' and 'Install' buttons, and a 'Previous Step' link with a left arrow.

**AVAYA**

Home

Configuration

Installation

- Network Settings
- Logins
- VPN Access
- SBC**
- Summary
- Finish

### Confirm Installation

The following optional fields have not been set

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

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

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

[Previous Step](#)



## 7.2. Post Installation Configuration

The installation wizard configures the Session Border Controller for use with the service provider chosen in **Section 7.1.3**. Since a 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 a login screen for 'Acme Packet Net-Net OS-E'. It has a title bar with the text 'Acme Packet Net-Net OS-E'. Below the title bar, it says '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, On the **Configuration** tab, navigate to **vsp → enterprise → servers → sip-gateway Telco**. Click **Show Advanced**.



The image shows the Session Border Controller Configuration GUI. The top navigation bar has tabs: Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, Tools. The 'Configuration' tab is selected. Below the navigation bar, the breadcrumb path is 'Configure vspenterprise\servers\sip-gateway Telco'. There is a 'Show advanced' button circled in orange. Below the breadcrumb path are buttons: Set, Reset, Back, Copy, Delete. There are links: Manage connections, Log instant messages, Record media, Record files, Set up accounting, Change from: URI, Change to: URI. Below these links is a table with the following rows:

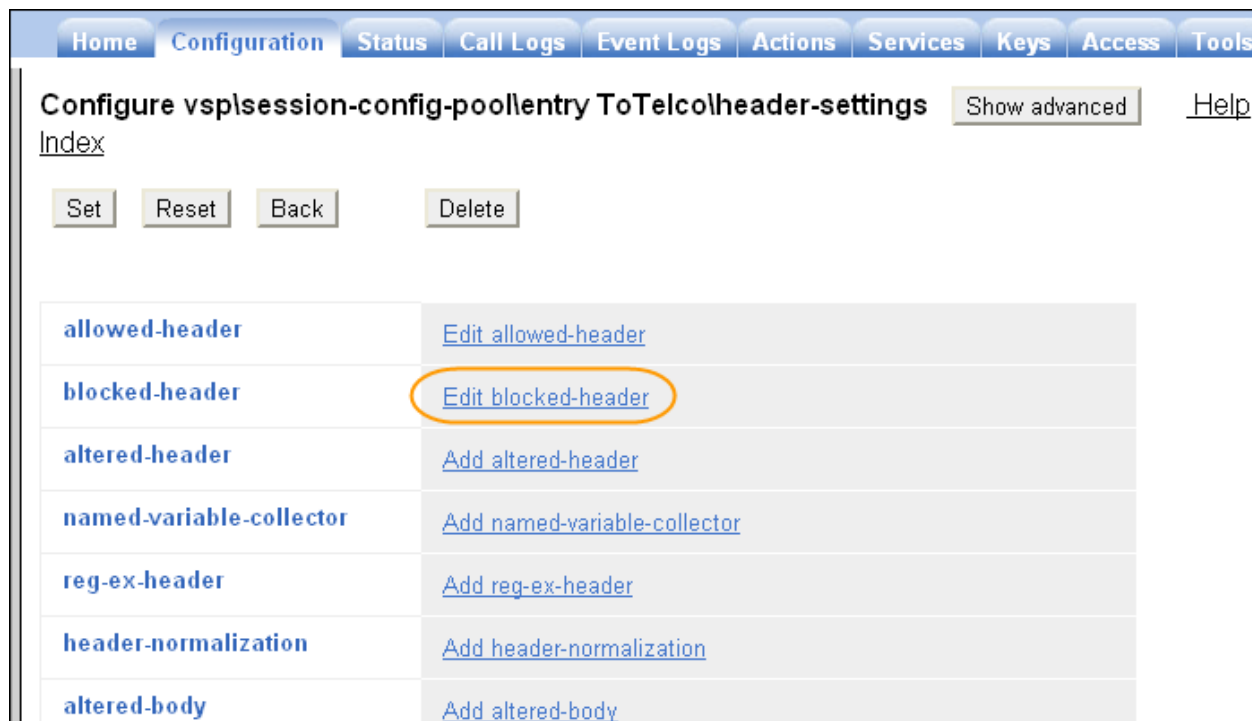
general:	
* name	Telco
admin	enabled (Resource is active)
domain	
failover-detection	ping (Use OPTIONS to detect failures)

Scroll down to the **routing** section of the form. Enter the desired interval in the **ping-interval** field. For compliance testing **60** seconds was used. Click **Set** at the top of the form (shown in previous figure).

routing:	
routing-setting	<div>normalization</div> <div>auto-tag-match</div> <div>auto-domain-match</div> <div>pstn-backup</div> <div>Select All</div> <div>Unselect All</div>
domain-alias	<a href="#">Edit domain-alias</a>
domain-subnet	<a href="#">Edit domain-subnet</a>
loop-detection	<div>tight</div> (Compare source and destination address/port/transport)
service-type	<div>provider</div> (Provider peer)
ping-interval	<div>60</div> seconds

## 7.2.2. Blocked Headers

The P-Location and Alert-Info headers are sent in SIP messages from 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 configuration page for the vsp session-config-pool entry ToTelco header-settings. The page includes a navigation bar with tabs: Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. Below the navigation bar, the page title is "Configure vsp\session-config-pool\entry ToTelco\header-settings", followed by a "Show advanced" button and a "Help" link. There are four buttons: Set, Reset, Back, and Delete. Below these buttons is a table with the following rows:

allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
named-variable-collector	<a href="#">Add named-variable-collector</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>

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.

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

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

Help Index

Set Reset Back Delete

allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<div>P-Location</div> <div>Alert-Info</div> <a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
named-variable-collector	<a href="#">Add named-variable-collector</a>
reg-ex-header	<a href="#">Add reg-ex-header</a>
header-normalization	<a href="#">Add header-normalization</a>

### 7.2.3. Diversion Header

A Diversion Header is applied to forwarded off-net calls when the SIP trunk group on Communication Manager has **Send Diversion Header** field 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 reg-ex-header**.

The screenshot shows a web interface for configuring header settings. At the top, there is a navigation bar with tabs: Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, and Access. Below the navigation bar, the page title is 'Configure vsp\session-config-pool\entry ToTelco\header-settings' with a 'Show advanced' button. There are links for 'Help' and 'Index'. Below these are buttons for 'Set', 'Reset', 'Back', and 'Delete'. The main content area is a table with two columns: a header name and an action link.

allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<div><div>P-Location</div><div>Alert-Info</div></div> <a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
named-variable-collector	<a href="#">Add named-variable-collector</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	<div>requests-and-responses <span>▼</span> (apply to requests and responses)</div>

In the new right pane that appears, enter **1** in the **number** field and enter **Diversion** in the **destination** field and click **Create**.

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

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

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

\* number

\* destination enter  or select from

Create Reset Cancel

The following screen is presented, select the **Configure** link to the right of **create**.

Set Reset Back Copy Delete

admin  (Resource is active)

\* number

\* destination enter  or select from

create [Configure](#)

append [Add append](#)

apply-to-methods

INVITE  
REFER  
MESSAGE  
INFO

Select All Unselect All

apply-to-responses

\* type  (Do not apply to responses (requests only))

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

session-persistent  (Resource is inactive)

The following screen is presented. In the **source** area, select **Diversion** from the drop-down list or type **Diversion** 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 UII if present. The domain **avayalab.com** is what the SBC would otherwise put in the Diversion 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 Diversion header containing the Called Party Number, corresponding to the first instance of `(.*)` from the **expression**. The variable `\2` is anything from the original Diversion 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. For more information about the use of regular expressions, see **Reference [9]**.

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

The following screen shows the completed rule. Select **INVITE** for **apply-to-methods** and **both** for **type** field in **apply-to-responses** section. Click **Set** to complete the configuration.

<b>admin</b>	enabled <input type="button" value="v"/> (Resource is active)
<b>* number</b>	1
<b>* destination</b>	enter <input type="text" value="Diversion"/> or select from <input type="text" value="Diversion"/> <input type="button" value="v"/>
<b>+ create</b>	<div> <div> <b>* source</b> </div> <div> enter <input type="text" value="Diversion"/> or select from <input type="text" value="Diversion"/> <input type="button" value="v"/> </div> </div> <div> <b>* expression</b> </div> <div> <input type="text" value="&lt;sip:(.*)@avayalab\.com( regular expression)"/> </div> <div> <b>* replacement</b> </div> <div> <input type="text" value="&lt;sip:\1@r:\R\2&gt;"/> </div>
<b>append</b>	<a href="#">Add append</a>
<b>apply-to-methods</b>	<div> <div> <div>INVITE</div> <div>REFER</div> <div>MESSAGE</div> <div>INFO</div> </div> <div> <input type="button" value="v"/> </div> </div> <div> <input type="button" value="Select All"/> <input type="button" value="Unselect All"/> </div>
<b>apply-to-responses</b>	<b>* type</b> <input type="button" value="no"/> <input type="button" value="v"/> (Do not apply to responses (requests only))
<b>apply-to-dialog</b>	<input type="button" value="both"/> <input type="button" value="v"/> (Apply to both inbound and outbound dialogs.)
<b>session-persistent</b>	disabled <input type="button" value="v"/> (Resource is inactive)
<input type="button" value="Set"/> <input type="button" value="Reset"/> <input type="button" value="Back"/> <input type="button" value="Copy"/>	



### 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**. Click **Set** to complete the configuration.

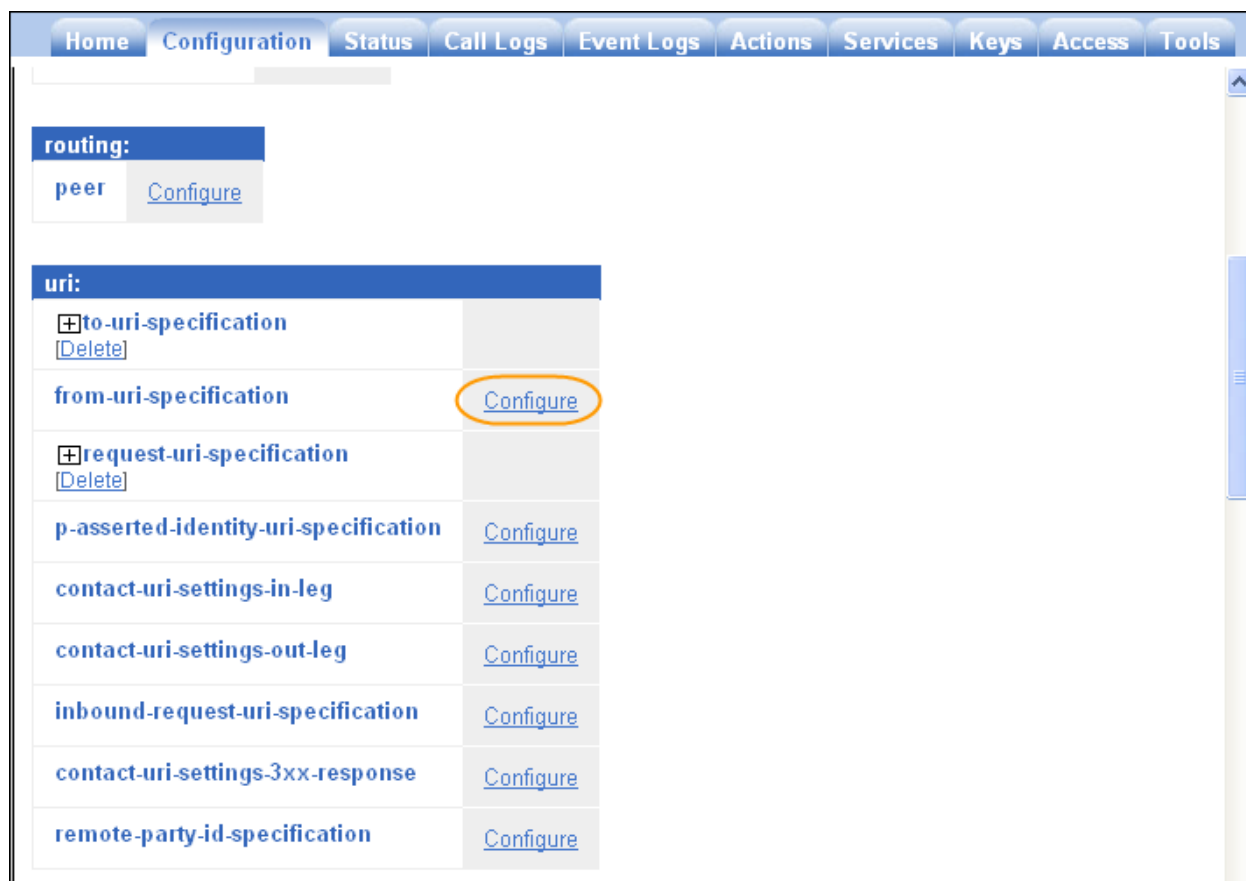
The screenshot shows a web interface for configuring third-party call control. At the top, there is a navigation bar with tabs: Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. Below the navigation bar, the page title is "Configure vsp\default-session-config\third-party-call-control". To the right of the title are buttons for "Show advanced" and "Help". Below the title is an "Index" link. Below the "Index" link are four buttons: "Set", "Reset", "Back", and "Delete". The main configuration area is a table with the following rows:

admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)
refer-maintain-identity	false	
ringback-file	<input type="text"/>	<a href="#">Browse System Files</a>
busy-file	<input type="text"/>	<a href="#">Browse System Files</a>
pre-call-announcement	<input type="text"/>	<a href="#">Browse System Files</a>
terminate-after-pre-call-announcement	disabled	(Resource is inactive)
handle-replaces-locally	disabled	(Resource is inactive)
delayed-ack	disabled	(Resource is inactive)

## 7.2.5. From URI

The Caller ID and Call Log of SIP clients registered to Session Manager 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 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** (not shown). Scroll down and click on **Configure** next to **from-uri-specification**.



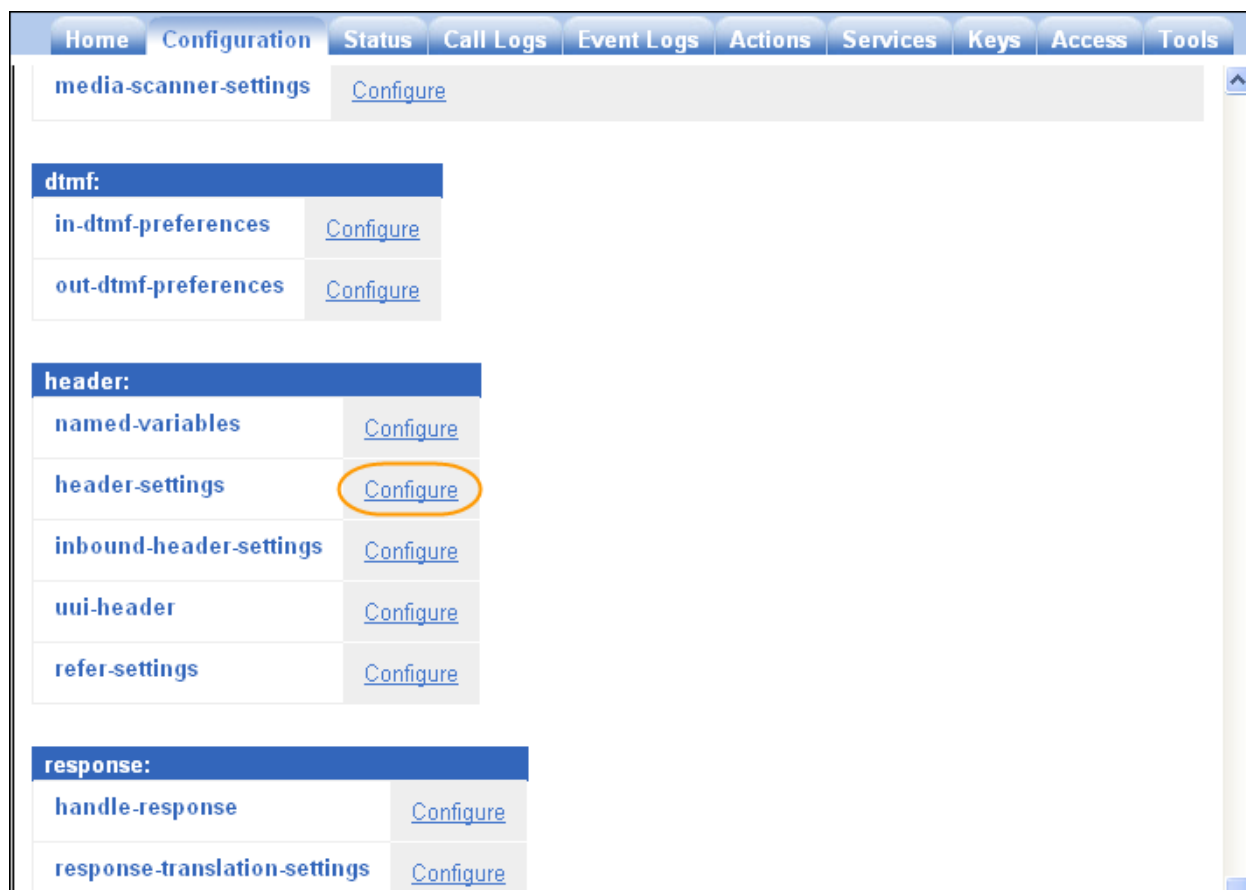
In the new right pane that appears, choose **next-hop-domain** from the drop-down list in the **host** field and click **Set**. This will set the host portion of the From Header to the enterprise domain set in **Section 7.1.1**.

Home	Configuration	Status	Call Logs	Event Logs	Actions	Services	Keys	Access	Tools
<b>Configure vsp session-config-pool entry ToPBX from-uri-specification</b> <a href="#">Help</a> <a href="#">Index</a>									
<input type="button" value="Set"/> <input type="button" value="Reset"/> <input type="button" value="Back"/> <input type="button" value="Delete"/>									
<b>user</b>	enter <input type="text" value="from-uri"/> or select from <input type="text" value="from-uri"/> (Net-Net OS-E uses the value from the incoming FROM URI.)								
<b>host</b>	enter <input type="text" value="next-hop-domain"/> or select from <input type="text" value="next-hop-domain"/> (Net-Net OS-E uses the domain of the next-hop server.)								
<b>port</b>	enter <input type="text" value="from-uri"/> or select from <input type="text" value="from-uri"/> (Net-Net OS-E uses the value from the incoming FROM URI.)								
<b>display</b>	enter <input type="text" value="from-uri"/> or select from <input type="text" value="from-uri"/> (Net-Net OS-E uses the value from the incoming FROM URI.)								
<b>user-agent-aware-display-translation</b>	<input type="text" value="disabled"/> (Resource is inactive)								

## 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** (not shown). Click on **Configure** next to **header-settings**.



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

The screenshot shows a web interface with a navigation bar at the top containing links: Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. Below the navigation bar is the title 'Configure vspsession-config-poolentry ToPBX\header-settings' followed by a 'Show advanced' button and a 'Help' link. Under the title are four buttons: Set, Reset, Back, and Delete. The main content area is a table with two columns. The first column lists various settings, and the second column contains links to configure them. The 'reg-ex-header' row is highlighted, and its link 'Add reg-ex-header' is circled in orange. Other rows include 'allowed-header', 'blocked-header', 'altered-header', 'named-variable-collector', 'header-normalization', 'altered-body', 'reg-ex-collector', 'apply-allow-block-to' (with a dropdown set to 'requests-and-responses'), 'apply-to-allow-block-to-dialog' (with a dropdown set to 'both'), and 'sip-manipulation' (with a dropdown and a 'Create' link).


allowed-header	<a href="#">Edit allowed-header</a>
blocked-header	<a href="#">Edit blocked-header</a>
altered-header	<a href="#">Add altered-header</a>
named-variable-collector	<a href="#">Add named-variable-collector</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	<input type="button" value="requests-and-responses"/> (apply to requests and responses)
apply-to-allow-block-to-dialog	<input type="button" value="both"/> (Apply to both inbound and outbound dialogs.)
sip-manipulation	<input type="button" value="Create"/>

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 a web interface for creating a new reg-ex-header. The navigation bar is the same as in the previous screenshot. The title is 'Create vspsession-config-poolentry ToPBX\header-settings\reg-ex-header 0 - Step 1 of 1: Edit reg-ex-header 0' followed by 'Help' and 'Index' links. Below the title is a message: 'Please provide some basic information for reg-ex-header 0. Then press "Create".' The main content area is a form with two fields: '\* number' with a text input containing '2', and '\* destination' with a text input containing 'Refer-To' and a dropdown menu set to '<Not configured>'. At the bottom of the form are three buttons: Create, Reset, and Cancel.

* number	<input type="text" value="2"/>
* destination	enter <input type="text" value="Refer-To"/> or select from <input type="button" value="Not configured"/>

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

<a href="#">Home</a> <a href="#">Configuration</a> <a href="#">Status</a> <a href="#">Call Logs</a> <a href="#">Event Logs</a> <a href="#">Actions</a> <a href="#">Services</a> <a href="#">Keys</a> <a href="#">Access</a> <a href="#">Tools</a>	
<b>admin</b>	enabled <input type="button" value="v"/> (Resource is active)
<b>* number</b>	<input type="text" value="2"/>
<b>* destination</b>	enter <input type="text" value="Refer-To"/> or select from <input type="text" value="Refer-To"/> <input type="button" value="v"/>
<b>create</b>	<a href="#">Configure</a> 
<b>append</b>	<a href="#">Add append</a>
<b>apply-to-methods</b>	<div><div>INVITE</div><div>REFER</div><div>MESSAGE</div><div>INFO</div></div> <div><input type="button" value="Select All"/> <input type="button" value="Unselect All"/></div>
<b>apply-to-responses</b>	<b>* type</b> <input type="button" value="no"/> <input type="button" value="v"/> (Do not apply to responses (requests only))
<b>apply-to-dialog</b>	<input type="button" value="both"/> <input type="button" value="v"/> (Apply to both inbound and outbound dialogs.)
<b>session-persistent</b>	disabled <input type="button" value="v"/> (Resource is inactive)
<input type="button" value="Set"/> <input type="button" value="Reset"/> <input type="button" value="Back"/> <input type="button" value="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 UII 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 UII 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**.

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

Create vsp\session-config-poolentry ToPBX\header-settings\reg-ex-header 2\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="text" value="&lt;Not configured&gt;"/>
* expression	<input type="text" value="&lt;sip:(.*)@avayalab\.com(.*)&gt;"/> (regular expression)
* replacement	<input type="text" value="&lt;sip:\1@\r:\R\2&gt;"/>

Create Reset Cancel

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

Home	Configuration	Status	Call Logs	Event Logs	Actions	Services	Keys	Access	Tools
<b>Configure vsp\session-config-pool\entry ToPBX\header-settings\reg-ex-header 2</b> <a href="#">Show advanced</a>									
<a href="#">Help</a> <a href="#">Index</a>									
<div> <div>Set</div> <div>Reset</div> <div>Back</div> <div>Copy</div> <div>Delete</div> </div>									
<b>admin</b>		<div>enabled <input type="button" value="v"/></div> <div>(Resource is active)</div>							
<b>* number</b>		<div>2</div>							
<b>* destination</b>		<div>enter <div>Refer-To</div> or select from <div>Refer-To <input type="button" value="v"/></div></div>							
<b>+ create</b>		<div> <div> <div>* source</div> <div>enter <div>Refer-To</div> or select from <div>Refer-To <input type="button" value="v"/></div></div> <div> <div>* expression</div> <div>&lt;sip:(.*)@avayalab\.com(. (regular expression)</div> </div> <div> <div>* replacement</div> <div>&lt;sip:\1@r:\R\2&gt;</div> </div> </div> </div>							
<b>append</b>		<div><a href="#">Add append</a></div>							
<b>apply-to-methods</b>		<div> <div> <div>INVITE</div> <div>REFER</div> <div>MESSAGE</div> <div>INFO</div> </div> <div> <div>Select All</div> <div>Unselect All</div> </div> </div>							
<b>apply-to-responses</b>		<div> <div>* type</div> <div>no <input type="button" value="v"/></div> <div>(Do not apply to responses (requests only))</div> </div>							
<b>apply-to-dialog</b>		<div> <div>both <input type="button" value="v"/></div> <div>(Apply to both inbound and outbound dialogs.)</div> </div>							
<b>session-persistent</b>		<div> <div>disabled <input type="button" value="v"/></div> <div>(Resource is inactive)</div> </div>							



### 7.2.7. In/Out Hold Translation

With Communication Manager's Network Call Redirection feature enabled, Communication Manager will use the SIP parameter *SendOnly* to signal any hold call conditions. The *SendOnly* SIP parameter is not supported by PAETEC Dynamic IP service. In this sample configuration the SBC replaces the *SendOnly* parameter with the *SendRecv* parameter that PAETEC Dynamic IP service does support. To modify the SIP parameter of an inbound call, navigate to **vsp → session-config-pool → entry ToPBX → in-hold-translation**.

Select **sendrecv** for the **offer-attribute** field and click **Set** to complete the configuration.

The screenshot shows a web-based configuration interface for a SIP service. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main title is "Configure vsp\session-config-pool\entry ToPBX\in-hold-translation". Below the title are buttons for Set, Reset, Back, and Delete. The configuration table has five rows: admin (enabled), offer-address (pass), offer-attribute (sendrecv), answer-address (pass), and answer-attribute (pass). The 'offer-attribute' row is highlighted with an orange circle. At the bottom are buttons for Set, Reset, and Back.

Field	Value	Description
admin	enabled	(Resource is active)
offer-address	pass	(Do not change the SDP connection address(es))
offer-attribute	sendrecv	(Set offered SDP hold attributes to 'a=sendrecv')
answer-address	pass	(Do not change the SDP connection address(es))
answer-attribute	pass	(Do not change the answered SDP hold attributes)

To modify the SIP parameter of an outbound call, navigate to **vsp → session-config-pool → entry ToTelco → out-hold-translation**.

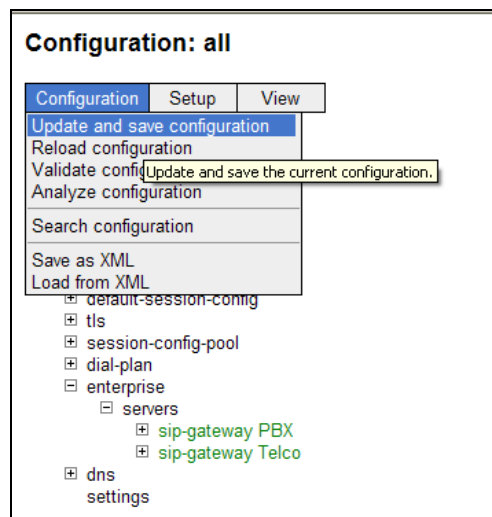
Select **sendrecv** for the **offer-attribute** field and click **Set** to complete the configuration.

The screenshot shows a web interface for configuring a session-config-pool entry. The breadcrumb path is **vsp | session-config-pool | entry ToTelco | out-hold-translation**. The page has tabs for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. Below the tabs are buttons for Set, Reset, Back, and Delete. The configuration table has the following fields:

admin	enabled	(Resource is active)
offer-address	pass	(Do not change the SDP connection address(es))
offer-attribute	sendrecv	(Set offered SDP hold attributes to 'a=sendrecv')
answer-address	pass	(Do not change the SDP connection address(es))
answer-attribute	pass	(Do not change the answered SDP hold attributes)

## 7.2.8. Save the Configuration

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



## 8. 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 Session Manager by logging in to System Manager and executing 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 route via the SBC to PAETEC. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

[Home](#) / [Elements](#) / [Session Manager](#) / [System Tools](#) / [Call Routing Test - Call Routing Test](#)[Help ?](#)

### Call Routing Test

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 based on current administration.

#### SIP INVITE Parameters

<b>Called Party URI</b> <input type="text" value="sip:13035551997@avayalab.com"/>	<b>Calling Party Address</b> <input type="text" value="10.80.150.225"/>
<b>Calling Party URI</b> <input type="text" value="sip:7135551234@avayalab.com"/>	<b>Session Manager Listen Port</b> <input type="text" value="5070"/>
<b>Day Of Week</b> <input type="text" value="Friday"/>	<b>Time (UTC)</b> <input type="text" value="22:02"/>
<b>Called Session Manager Instance</b> <input type="text" value="ASM"/>	<b>Transport Protocol</b> <input type="text" value="TCP"/>

---

#### Routing Decisions

Route < sip:13035551997@avayalab.com > to SIP Entity AA-SBC01 (10.80.150.253). Terminating Location is AA-SBC\_150.

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 the SAT interface on Communication Manager to verify status of SIP trunks. Specifically use the **status trunk n** command to verify the active call has ended. Where **n** is the trunk group number used for PAETEC Dynamic IP SIP Trunk Service defined in **Section 5.7**.

Below is an example of an active call.

```
status trunk 1
```

TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
<b>0001/001</b>	<b>T00001</b>	<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	
<b>0001/001</b>	<b>T00001</b>	<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® Session Border Controller, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager Evolution Server 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] *Administering Avaya Aura™ Communication Manager, June 2010, Document Number 03-300509.*
- [4] *Avaya Aura™ Communication Manager Feature Description and Implementation, June 2010, Document Number 555-245-205.*
- [5] *Installing and Upgrading Avaya Aura™ System Manager 6.1 GA Version, November 2010.*
- [6] *Installing and Configuring Avaya Aura® Session Manager, April 2011, Document Number 03-603473*
- [7] *Administering Avaya Aura® Session Manager, November 2010, Document Number 03-603324.*
- [8] *Installing and Configuring Avaya Aura® Session Border Controller, November 2010.*
- [9] *Avaya Aura® Session Border Controller Session Services Guide, September 2010*
- [10] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x, April 2010, Document Number 16-601443.*
- [11] *4600 Series IP Telephone LAN Administrator Guide, July 2008, Document Number 555-233-507.*
- [12] *Avaya one-X Deskphone H.323 Administrator Guide, May 2011, Document Number 16-300698.*
- [13] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1, December 2010, Document Number 16-603838*
- [14] *Administering Avaya one-X Communicator, July 2011*

- [15] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>
- [16] RFC 3515, The Session Initiation Protocol (SIP) Refer Method, <http://www.ietf.org/>
- [17] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>
- [18] 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: 15:29:48 Thu 2011-10-13
#
config cluster
config box 1
    set hostname aasbc.avayalab.com
    set timezone America/Denver
    set name aasbc.avayalab.com
    set identifier 00:ca:fe:99:89:31
config interface eth0
    config ip inside
        set ip-address static 10.80.150.253/24
        config ssh
        return
    config snmp
        set trap-target 10.80.150.252 162
        set trap-filter generic
        set trap-filter dos
        set trap-filter sip
        set trap-filter system
        set trap-filter tls
        set trap-filter-dos sip-policy
        set trap-filter-dos transport-policy
        set trap-filter-dos url-policy
        set trap-filter-sip media-session-dropped-packets
        set trap-filter-sip media-verification-fail
        set trap-filter-sip server-state-change
        set trap-filter-system EventLogTrap
        set trap-filter-system license-expiring
        set trap-filter-system master-service-change
        set trap-filter-system master-service-host-change
        set trap-filter-system monitor-alert
        set trap-filter-system process-core-dump
        set trap-filter-system process-dead
        set trap-filter-system process-down
        set trap-filter-system process-fault
        set trap-filter-system SIP-parse-errors-trap
        set trap-filter-system skb-usage
        set trap-filter-system storage-device-full
        set trap-filter-system syn-cookies
        set trap-filter-system system-halt
        set trap-filter-system tcp-skb-congestion-dropped-pkts
        set trap-filter-system vx-bind
        set trap-filter-system vx-unbind
        set trap-filter-system web-service-availability-change
        set trap-filter-tls cert-expired
        set trap-filter-tls cert-expiring
        set trap-filter-tls cert-missing
    return
```

```

config web
return
config web-service
  set protocol https 8443
  set authentication certificate "vsp\tls\certificate ws-cert"
return
config sip
  set udp-port 5060 "" "" any 0
  set tcp-port 5060 "" "" any 0
  set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
return
config icmp
return
config media-ports
return
config routing
  config route Default
    set gateway 10.80.150.1
  return
  config route Static0
    set destination network 192.11.13.4/30
    set gateway 10.80.150.251
  return
  config route Static1
    set admin disabled
  return
  config route Static2
    set admin disabled
  return
  config route Static3
    set admin disabled
  return
  config route Static4
    set admin disabled
  return
  config route Static5
    set admin disabled
  return
  config route Static6
    set admin disabled
  return
  config route Static7
    set admin disabled
  return
return
return
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 aasbc.avayalab.com
return
return
return

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

```

```

    set filter dosTransport alert
    set filter dosUrl alert
    set count 3
    return
    config file krnlsys
    set filter krnlsys debug
    set count 3
    return
    return
    config tasks
    config config-update-task Avaya
    set action run
    set arguments "/usr/sbin/nnose_avaya_update.py -e /cxc_common/avaya/ovf-
env.txt -l /cxc_common/avaya/config-change-log.txt -a %f"
    return
    return
    config monitors
    config monitor Default
    set parameter storage-devices all 90
    return
    return
    config collect
    config default-collect-settings
    set directory /cxc_common/avaya
    return
    return
    return
    return

config master-services
    config database
    set media enabled
    return
    return

config vsp
    set admin enabled
    config default-session-config
    config media
    set anchor enabled
    set rtp-stats enabled
    return
    config sip-directive
    set directive allow
    return
    config log-alert
    set apply-to-methods-for-filtered-logs
    return
    config header-settings
    return
    config third-party-call-control
    set admin disable
    set handle-refer-locally disabled
    set always-apply-req-uri-spec disabled
    return
    return
    config tls

```

```

config default-ca
    set ca-file /cxc/certs/sipca.pem
return
config certificate ws-cert
    set certificate-file /cxc/certs/ws.cert
return
config certificate aasbc.p12
    set certificate-file /cxc/certs/aasbc.p12
    set passphrase-tag aasbc-cert-tag
return
return
config session-config-pool
config entry ToTelco
    config to-uri-specification
        set host next-hop
    return
    config from-uri-specification
        set host local-ip
    return
    config request-uri-specification
        set host next-hop
    return
    config p-asserted-identity-uri-specification
        set host local-ip
    return
    config out-hold-translation
        set admin enabled
        set offer-attribute sendrecv
    return
    config header-settings
        set blocked-header P-Location
        set blocked-header Alert-Info
        config reg-ex-header 1
            set destination Diversion
            set create Diversion "<sip:(.*)@avayalab\.com(.*)>" "<sip:\1@\r:\R\2>"
        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 in-hold-translation
        set admin enabled
        set offer-attribute sendrecv
    return
    config header-settings
        config reg-ex-header 2
            set destination Refer-To
            set create Refer-To "<sip:(.*)@avayalab\.com(.*)>" "<sip:\1@\r:\R\2>"

```

```

        set apply-to-methods REFER
    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 10.80.150.206
            return
        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
config dns
    config resolver
        config server 10.80.150.201
            set preference 101
        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
    set login-attempts 3
return
config permissions read-only
    set config view
    set actions disabled
    set debug disabled
    set login-attempts 3
return
config users
config password-policy
    set minimum-length 8
    set allow-sequences false
    set recycle-check 1
return
config user sbcadmin
    set password 0x0081b51fad0e2f355219eaed741523332f4d783be2641d8702c37c65e1
    set permissions access\permissions superuser
return
config user sbccust
    set password 0x0080153df8eadabda496d514fae74d47fed0559f56a23dec069c6f0199
    set permissions access\permissions read-only
return
config user init
    set password 0x00cd857f18bb0d41f7361db9c00b5ed10738f75b18138b02d3120de1e6
    set permissions access\permissions superuser
return
config user craft
    set password 0x008e3e5d4e9d9103d6e8317e4a602d2d1bc7375c8720aea3409800c297
    set permissions access\permissions superuser
return
config user dadmin
    set password 0x00a844cec40e77364dbe4427e25a8061acf36e7bf2af95c521abf8edd1
    set permissions access\permissions read-only
return
return

```

```
return
```

```
config features  
return
```

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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