



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider AT&T Mobility in Puerto Rico and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.0.1, Avaya Session Border Controller for Enterprise and various Avaya endpoints. The solution does not include the Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

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

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the AT&T Mobility in Puerto Rico SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server, Avaya Session Border Controller for Enterprise (Avaya SBCE) and various Avaya endpoints. The solution does not include the Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

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

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

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the AT&T Mobility SIP Trunk service by means of a broadband connection to the public Internet.

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

2.1. Interoperability Compliance Testing

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, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator soft phones using H.323 protocol, in both Road Warrior and Telecommuter modes.

- Various call types, including: local, long distance, international, outbound toll-free, emergency (911) and local directory assistance (411, 611).
- Codecs G729A and G.711MU and proper codec negotiation.
- DTMF tone transmissions passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Network Call Redirection, using the SIP REFER and the 302 Redirection methods for the transfer of inbound call back to PSTN.
- Inbound and outbound fax calls to the PSTN.

Items not supported or not tested included the following:

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

2.2. Test Results

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

- **T.38 Fax:** Even though incoming T.38 fax calls to the enterprise worked successfully, outbound T.38 fax calls to PSTN numbers other than subscribers of the AT&T Broadsoft switch failed to complete. Thus, T.38 Fax should not be used with this solution.
- **Network Call Redirection using REFER with redirected party Busy:** In the testing environment, when an inbound call was made to the enterprise, to a vector redirecting the call to another PSTN endpoint that was busy, the caller will hear a busy tone, but AT&T will not return a “486 Busy Here”, preventing any additional processing of the call by Communication Manager and the routing of the call to a secondary endpoint.
- **SIP User to User Information:** When a Communication Manager vector is programmed to send “User-to-User Information” (UUI) to a remote party, the information is generated and included in the REFER header sent to AT&T, but the UUI is not passed to the destination SIP endpoint.

2.3. Support

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

3. Reference Configuration

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

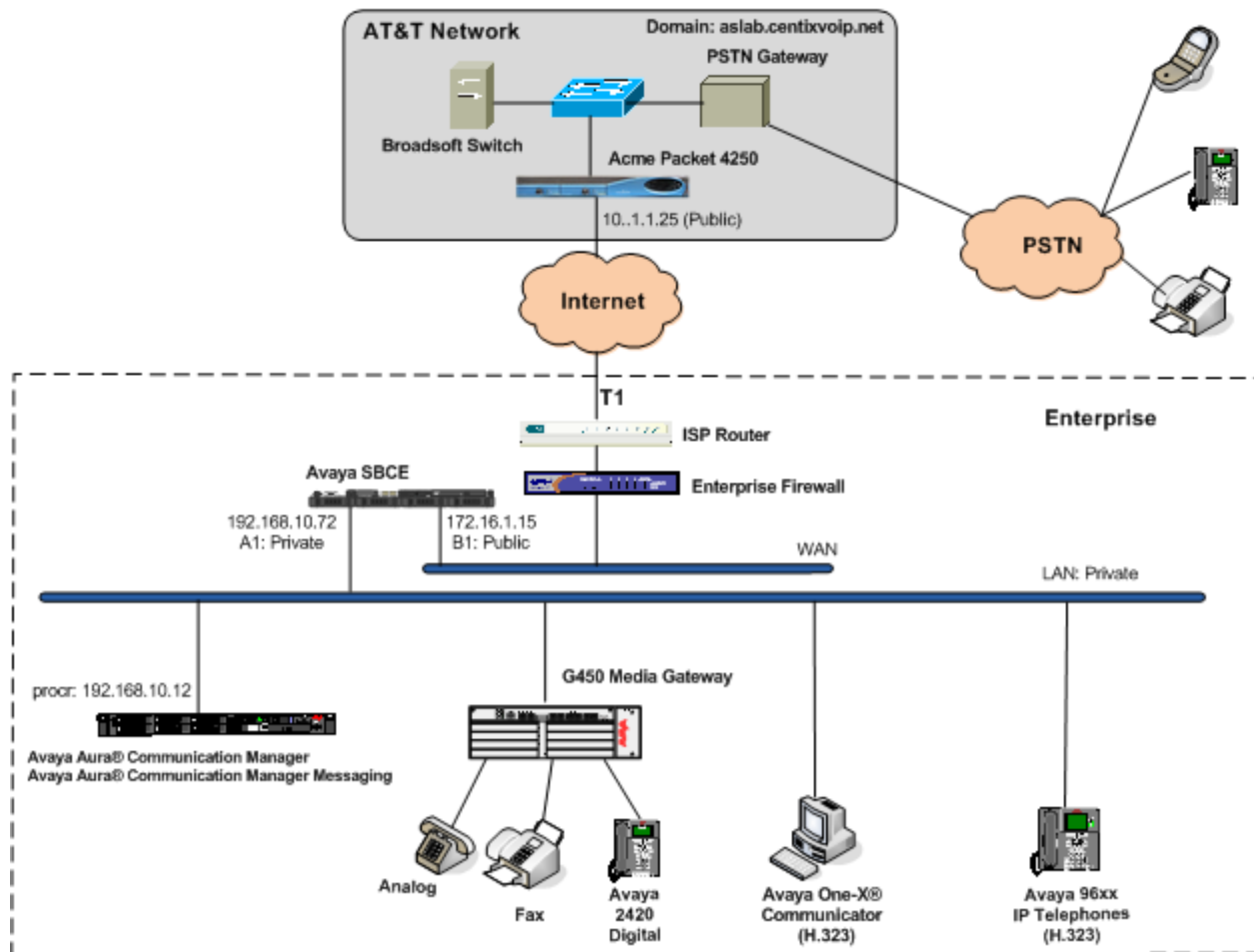


Figure 1: Avaya SIP Enterprise Solution connecting to AT&T Mobility SIP Trunk Service

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

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

- Avaya Aura® Communication Manager and Communication Manager Messaging, running on the Avaya Common Server HP Proliant DL360.
- Avaya Session Border Controller for Enterprise Server, on a Dell R210 V2 server.
- Avaya G450 Media Gateway
- Avaya 96x0 and 96x1 Series IP Telephones (H.323)
- Avaya one-X® Communicator soft phones (H.323)
- Avaya digital and analog telephones

The Avaya SBCE constitutes the single point of connection between the public network and the Local Area Network in the enterprise. In addition to providing comprehensive security to all SIP and RTP traffic entering the private network, the Avaya SBCE enables the interoperability with dissimilar SIP trunk service providers, by allowing the manipulation and adjustment of the elements in the packets flowing through its interfaces.

For inbound calls, the calls flow from the service provider to the external firewall, to the Avaya SBCE. After the Avaya SBCE performs the necessary security checks and interworking manipulation, the call is sent to Communication Manager, where incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN were processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to the Avaya SBCE for additional interworking treatment before egress to the AT&T network.

The transport protocol between the Avaya SBCE and AT&T Mobility across the public IP network is UDP. The transport protocol between the Avaya SBCE and the Avaya Aura® Communication Manager server across the enterprise IP network is TCP.

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

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on a HP® Proliant DL360 G7 Server.	6.0.1 SP7 (R016x.00.1.510.1)
Avaya Aura® Communication Manager Messaging	vcm-016-00.1.510.1 service pack 3
Avaya SBCE on a Dell R210 V2 server.	4.0.5.Q02
Avaya G450 Media Gateway	31.20.1
Avaya 96x0 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 3.1 SP4
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition 6.2
Avaya one-X Communicator (H.323)	6.1.2.06-SP2-33739
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
AT&T Puerto Rico SIP Trunking	
Acme-Packet Net-Net 4250 SBC	Firmware SC6.1.0 MR-9 GA (Build 938)
BroadWorks Soft Switch	R17
Nortel CS2K PSTN Gateway	CVM11

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the AT&T Mobility SIP Trunk Service. A SIP trunk is established between Communication Manager and the Avaya SBCE for use by signaling traffic to and from AT&T. It is assumed the general installation of Communication Manager, Messaging, Avaya G450 Media Gateway and endpoints has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **270** 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
```

OPTIONAL FEATURES	
IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks:	12000 10
Maximum Concurrently Registered IP Stations:	18000 2
Maximum Administered Remote Office Trunks:	12000 0
Maximum Concurrently Registered Remote Office Stations:	18000 0
Maximum Concurrently Registered IP eCons:	414 0
Max Concur Registered Unauthenticated H.323 Stations:	100 0
Maximum Video Capable Stations:	18000 0
Maximum Video Capable IP Softphones:	18000 2
Maximum Administered SIP Trunks:	24000 270
Maximum Administered Ad-hoc Video Conferencing Ports:	24000 0
Maximum Number of DS1 Boards with Echo Cancellation:	522 0
Maximum TN2501 VAL Boards:	128 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:	100 0

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

5.2. System Features

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

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

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

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

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

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

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

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

INTERNATIONAL CALL ROUTING PARAMETERS
  Local Country Code:
  International Access Code:
```


5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Communication Manager (**procr**) and the inside interface of the Avaya SBCE (**ASBCE_A1**). 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	
ASBCE_A1	192.168.10.72	
Acme_s0_p1	192.168.10.53	
asm	192.168.10.32	
default	0.0.0.0	
msgserver	192.168.10.12	
procr	192.168.10.12	
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 4 was used for this purpose. The AT&T SIP Trunk Service supports codecs G.729A and G.711MU, in this order of preference. Enter **G.729A** and **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 4		Page 1 of 2
IP Codec Set		
Codec Set: 4		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.729A	<u>n</u>	<u>2</u>
2: G.711MU	<u>n</u>	<u>2</u>
3: _____	<u>-</u>	<u>-</u>

Since T.38 fax testing was unsuccessful for outbound calls, it is recommended to disable T.38 Fax by setting the **Fax Mode** field to **off** on **Page 2**.

change ip-codec-set 4		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? <u>n</u>		
	Mode	Redundancy
FAX	<u>off</u>	<u>0</u>
Modem	<u>off</u>	<u>0</u>
TDD/TTY	<u>US</u>	<u>3</u>
Clear-channel	<u>n</u>	<u>0</u>

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 4 was chosen for the service provider trunk. Use the **change ip-network-region 4** command to configure region 4 with the following parameters:

- Leave the **Authoritative Domain** field blank. For the compliance test, IP addresses instead of domain names were used in the host portion of SIP URIs of packets flowing between Communication Manager and the Avaya SBCE. Since AT&T required the use of domain names in packets arriving to their network, the required header manipulation to comply with this requirement is performed by the Avaya SBCE, and it is shown in **Section 6.3.4** later in this document.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling could be further restricted at the trunk level on the Signaling Group form if necessary.
- 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 4		Page 1 of 20
IP NETWORK REGION		
Region: 4		
Location: 1	Authoritative Domain: _____	
Name: CM-Sipera		
MEDIA PARAMETERS		
Codec Set: 4	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 3329	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS	RSUP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

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

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Avaya SBCE for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise.

change signaling-group 4			Page	1 of	1
SIGNALING GROUP					
Group Number: 4		Group Type: sip			
IMS Enabled? n		Transport Method: tcp			
Q-SIP? n		SIP Enabled LSP? n			
IP Video? n		Enforce SIPS URI for SRTP? y			
Peer Detection Enabled? y		Peer Server: Others			
Near-end Node Name: procr		Far-end Node Name: ASBCE_A1			
Near-end Listen Port: 5060		Far-end Listen Port: 5060			
		Far-end Network Region: 4			
		Far-end Secondary Node Name:			
Far-end Domain:					
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? n			
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? n			
		Alternate Route Timer(sec): 6			

For the compliance test, signaling group 4 was used for this purpose and was configured using the following parameters:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- Set the **Transport Method** to *tcp*.
- Set the **Peer Detection Enabled** field to *y*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *ASBCE_A1*. This node name maps to the IP address of the inside interface of the Avaya SBCE, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** set to *5060*.

- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Leave the **Far-end Domain** field blank.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. Note that media shuffling can also be enabled or restricted on each IP network regions forms.
- Default values may be used for all other fields.

5.7. Trunk Group

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

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

change trunk-group 4		Page 1 of 21	
TRUNK GROUP			
Group Number: 4	Group Type: sip	CDR Reports: y	
Group Name: CM-Sipera	COR: 1	TN: 1	TAC: 604
Direction: two-way	Outgoing Display? n	Night Service: _____	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 4	
		Number of Members: 6	

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the default value of **600** seconds was used

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

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

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

Disconnect Supervision - In? y Out? y
```

On **Page 3**, set the **Numbering Format** field to **public**. 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.

```
change trunk-group 4                                     Page 3 of 21
TRUNK FEATURES

  ACA Assignment? n                                     Measured: none
                                                         Maintenance Tests? y

                                     Numbering Format: public
                                                         UUI Treatment: service-provider

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

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

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

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

5.8. Calling Party Information

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

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2			4	Total Administered: 7 Maximum Entries: 9999
4	3			4	
4	3001	4	7871111234	10	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.
4	3002	4	7871111235	10	
4	3003	4	7871111236	10	
4	3004	4	7871111237	10	
4	3005	4	7871111238	10	

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

change public-unknown-numbering 1				
NUMBERING - PUBLIC/UNKNOWN FORMAT				
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len
4	3	4	787111	10

5.9. Inbound Routing

DID numbers received from AT&T can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 4					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	7871111234	10	3001	
public-ntwrk	10	7871111235	10	3002	
public-ntwrk	10	7871111236	10	3003	
public-ntwrk	10	7871111237	10	3004	
public-ntwrk	10	7871111238	10	3005	
public-ntwrk					

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

change inc-call-handling-trmt trunk-group 4					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	787111	6		
public-ntwrk					

5.10. Outbound Routing

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

change dialplan analysis			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	
1	4	ext							
2	4	ext							
3	4	ext							
4	4	ext							
5	5	ext							
6	3	dac							
7	5	ext							
8	1	fac							
9	1	fac							
*	3	dac							
#	2	dac							

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)		Page 1 of 11
Abbreviated Dialing List1 Access Code:			_____		
Abbreviated Dialing List2 Access Code:			_____		
Abbreviated Dialing List3 Access Code:			_____		
Abbreviated Dial - Prgm Group List Access Code:			_____		
Announcement Access Code:			#1		
Answer Back Access Code:			_____		
Attendant Access Code:			_____		
Auto Alternate Routing (AAR) Access Code:			8		
Auto Route Selection (ARS) – Access Code 1:			9	Access Code 2:	_____
Automatic Callback Activation:			_____	Deactivation:	_____
Call Forwarding Activation Busy/DA:			All: _____	Deactivation:	_____
Call Forwarding Enhanced Status:			Act: _____	Deactivation:	_____
Call Park Access Code:			_____		
Call Pickup Access Code:			_____		

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 1.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 4 which contains the SIP trunk group to the service provider.

change ars analysis 0							Page	2 of	2
ARS DIGIT ANALYSIS TABLE							Percent Full: 1		
Location: all									
Dialed String	Total	Min	Max	Route Pattern	Call Type	Node Num	ANI	Reqd	
011	10	10	18	4	intl		n		
787	10	10	10	4	hnpa		n		
1305	11	11	11	4	fnpa		n		
1786	11	11	11	4	fnpa		n		
1800	11	11	11	4	fnpa		n		
411	3	3	3	4	svcl		n		
611	3	3	3	4	svcl		n		
							n		

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

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 4 was used.
- **FRL:** Set the Facility Restriction Level (FRL) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 1** The prefix mark (Pfx Mrk) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for the long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- Default values were used for all other fields.

change route-pattern 4											Page	1 of	3
Pattern Number: 4					Pattern Name: CM-Sipera								
SCCAN? n					Secure SIP? n								
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts				DCS/ QSIG Intw	IXC	
1:	4	0	1								n	user	
2:											n	user	
3:											n	user	
4:											n	user	
5:											n	user	
6:											n	user	

6. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to the AT&T Mobility SIP Trunk service. This configuration is done in two stages. The first part or initial configuration is done via the Provisioning Script, which requires a serial connection between a terminal device and the Console port of the Avaya SBCE.

Once the Avaya SBCE is provisioned and ready to be used on the IP network, the remainder of the configuration is accomplished using the server's web interface.

It is assumed in these Application Notes that the Avaya SBCE is being provisioned for the first time, and it contains no previous configuration.

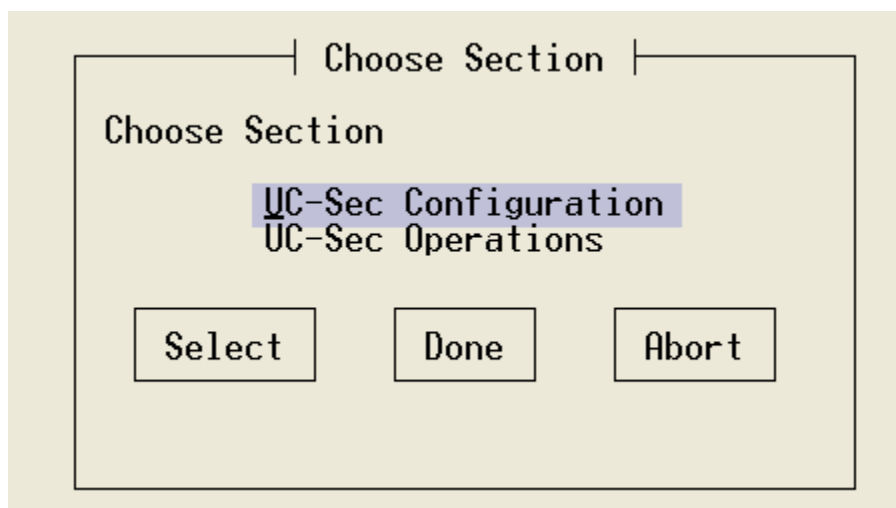
6.1. Provisioning Script

Use the following procedure to establish the initial serial connection to the Avaya SBCE:

- Connect a DB9 serial communications cable from a PC or terminal device to the Console port in the back of the server.
- Configure the communications parameters of the terminal program in the PC, like HyperTerminal or Putty, to the following settings: **Baud rate: 19200, Data Bits: 8, Stop Bits: 1, Parity: None**
- Apply power to the chassis.

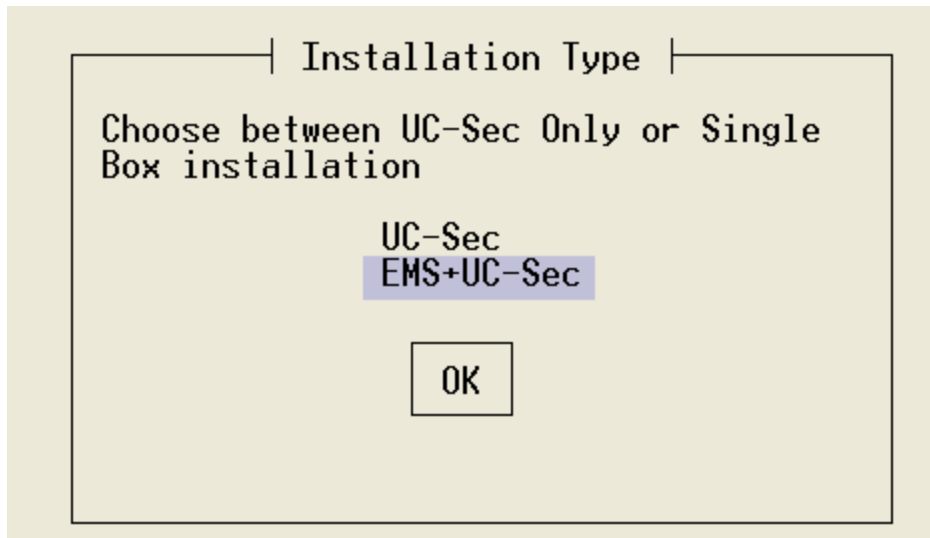
Once power has been applied to the Avaya SBCE, a series of scripts run automatically preparing the server to be configured. The provisioning process is ready to be completed when the prompt **Press ENTER to continue...** is displayed. Press the **ENTER** key.

The Top Level Provisioning Screen is displayed. Use the arrows to select **UC-Sec Configuration** and press **ENTER**.

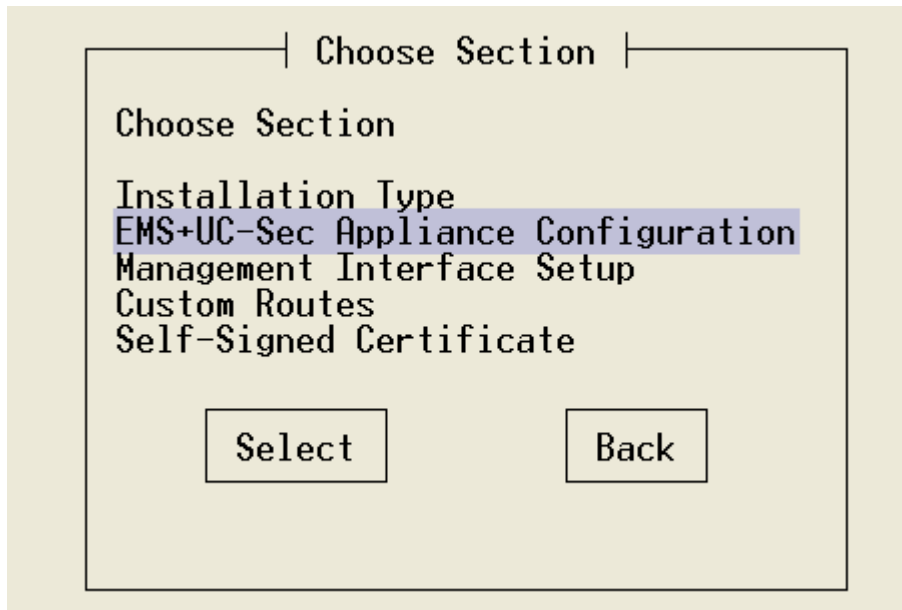


The Provisioning screen is displayed (not shown). Select **Installation Type**. Press **Select**.

In our test scenario, both the SBC (UC-Sec) and the Element Management System (EMS) reside in the same server. Select **EMS+UC-Sec** for a single box installation. Click **OK**.



On the next screen, the EMS+UC-Sec Provisioning screen, select **EMS+UC- SEC Appliance Configuration**. Press **Select**.



Enter the required information into the appropriate fields. Click **OK**.

UC-Sec+EMS Appliance Configuration

Configure Single Box Appliance

EMS Appliance Name

EMS

Domain Suffix (Optional)

List of DNS Servers

192.168.10.100

NTP Server IP Address (ipv4)

127.127.1.0

OK

Back at the EMS+UC-Sec Provisioning screen shown in the previous page, select **Management Interface Setup** and press **Select**. Select the **M1 Management Device**, and enter the IP address, Netmask and Gateway to be used to manage the SBC on the network. Click **OK**.

Management Interface Setup

Management Device

(*) M1

() M2

Management IP Address (ipv4)

192.168.10.70

Management Network Mask

255.255.255.0

Management Gateway IP Address (ipv4)

192.168.10.254

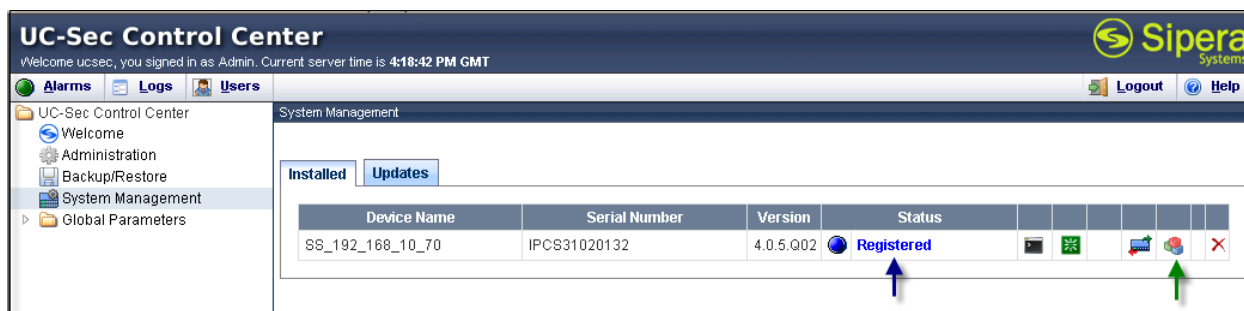
OK

Press **Back** at the EMS+UC-Sec Provisioning screen. This will bring up the Top Level Provisioning screen. Select **Done**.

At this point the initial configuration is complete and the Avaya SBCE is ready to be administered via the browser through the Management Interface.

6.2. Install Device

Logon to the SBC web interface pointing a browser to the previously configured management interface address. For the Compliance Test, this was **https://192.168.10.70**. Click the **UC-Sec Control Center** box. Login using the proper credentials. Once in the UC-Sec Control Center home page, on the left hand side navigation panel select **System Management**. Select the **Installed** tab.



After the Avaya SBCE has been initially installed and connected to the network, it will show the status of **Registered**. In addition, the **Install Device** icon, marked with a green arrow on the screen capture, is displayed only for the devices which have not yet been configured.

Click the **Install Device** icon. On the Installation Wizard that follows, fill the required information as shown in the screen below. Click **Finish** when done.

Installation Wizard

SIP Proxy

Device Settings

Appliance Name:

High Availability (HA): ☐

Secure Channel Type: ☒ None ☐ DMZ ☐ Core

DNS Configuration

Primary: Ex: 202.201.192.1

Secondary: Optional, Ex: 202.201.192.1

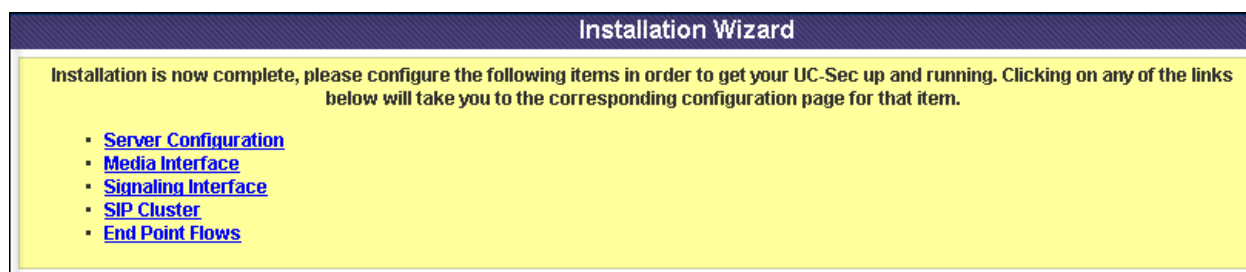
Network Settings

At least one address is required. Netmask and subnet must be common across the same interface.

	IP	Public IP	Netmask	Gateway	Interface	DNS Client
Address #1	<input type="text" value="192.168.10.72"/>	<input type="text" value="192.168.10.72"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.10.254"/>	<input type="text" value="A1"/>	<input checked="" type="radio"/>
Address #2	<input type="text" value="172.16.1.15"/>	<input type="text" value="172.16.1.15"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="172.16.1.254"/>	<input type="text" value="B1"/>	<input type="radio"/>
Address #3	<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text" value="A1"/>	<input type="radio"/>
Address #4	<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text" value="A1"/>	<input type="radio"/>
Address #5	<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text" value="A1"/>	<input type="radio"/>

Finish

The last screen in the Wizard is a basic reminder of topics that need to be visited in order to complete the configuration. Close this window.



6.3. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the EMS control.

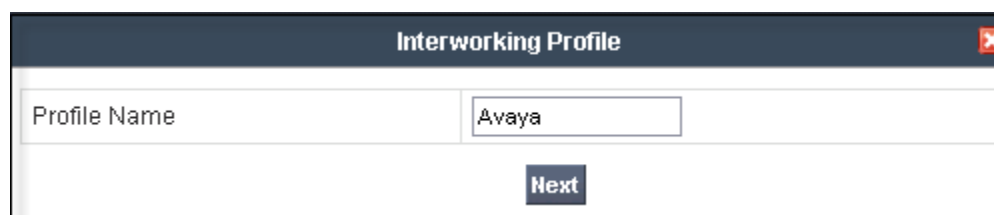
6.3.1. Server Interworking

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.


On the left navigation pane, select **Global Profiles → Server Interworking**. Several profiles have been already pre-defined and they populate the list under **Interworking Profiles**. If a different profile is needed, an existing default profile can be “cloned” and modified, or a new Interworking Profile can be created.



For the compliance test, a new profile was created. Click **Add Profile**. Add a profile name and click **Next**.



In the General screen, leave the T.38 Support box unchecked, since T.38 fax is not to be used in this configuration. Leave other settings with their default values. Click **Next** to continue.

Interworking Profile 	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<div> <div>Back</div> <div>Next</div> </div>	

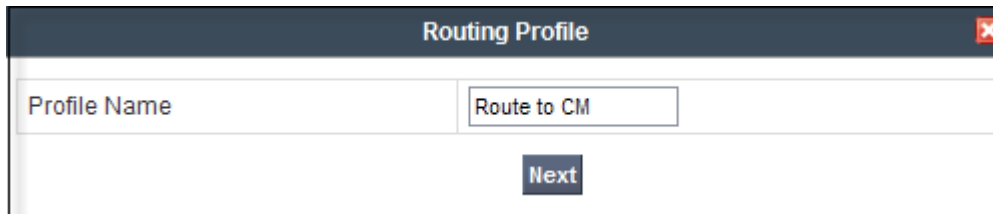
Click **Next** on the **Privacy** and **Timers** tabs and **Finish** on the **Advanced** tab (not shown) to save and exit

6.3.2. Routing Profiles

Routing profiles define a specific set of routing criteria to be used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination. Two Routing Profiles were created in the test configuration, one for inbound calls, with Communication Manager as the destination, and the second one for outbound calls, which are routed to the AT&T SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

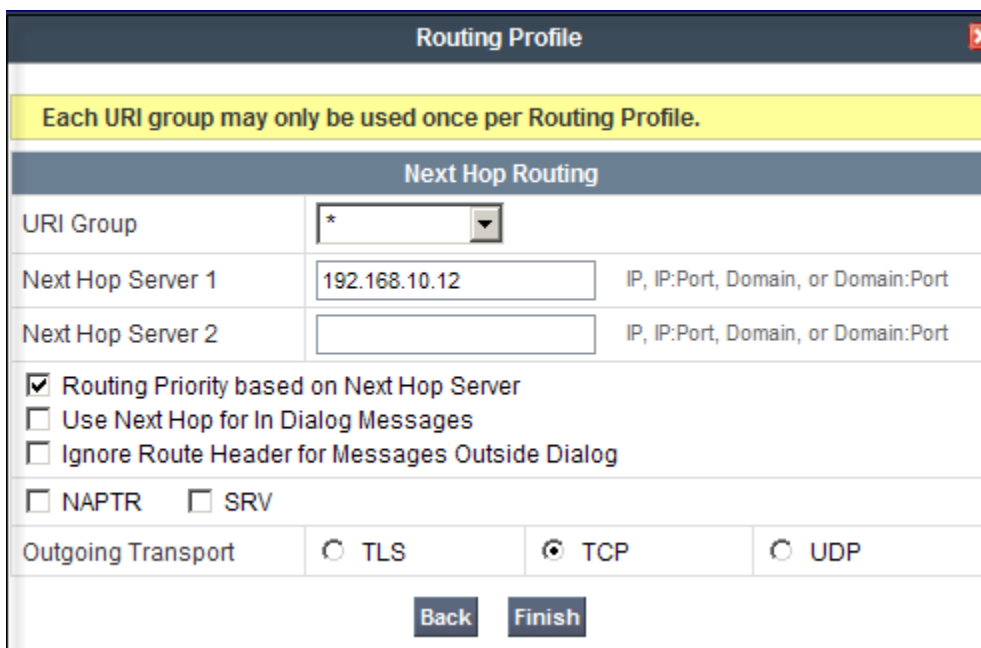
- Select the **Routing** tab.
- Select **Add Profile**.
- Enter Profile Name: **Route to CM**. Click **Next**.



The screenshot shows a 'Routing Profile' dialog box. It has a title bar with a close button. Inside, there is a 'Profile Name' label and a text input field containing 'Route to CM'. Below the input field is a 'Next' button.

On the next screen, complete the following:

- **Next Hop Server 1: 192.168.10.12**. This is the IP address of the **procr** interface in Communication Manager.
- Check **Routing Priority Based on Next Hop Server**
- **Outgoing Transport: TCP**. This protocol must match the value used on the Communication Manager signaling group form in **Section 5.6**
- Click **Finish**



The screenshot shows the 'Routing Profile' dialog box with the 'Next Hop Routing' section expanded. A yellow warning banner at the top states: 'Each URI group may only be used once per Routing Profile.' The 'Next Hop Routing' section contains a table with the following fields:

Next Hop Routing	
URI Group	<input type="text" value="*"/>
Next Hop Server 1	<input type="text" value="192.168.10.12"/> IP, IP:Port, Domain, or Domain:Port
Next Hop Server 2	<input type="text"/> IP, IP:Port, Domain, or Domain:Port

Below the table, there are several checkboxes and radio buttons:

- ☒ Routing Priority based on Next Hop Server
- ☐ Use Next Hop for In Dialog Messages
- ☐ Ignore Route Header for Messages Outside Dialog
- ☐ NAPTR ☐ SRV
- Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

At the bottom, there are 'Back' and 'Finish' buttons.

Similarly, for the outbound route:

- Select **Add Profile**.
- Enter Profile Name: **Route to SP**
- Click **Next**.
- **Next Hop Server 1: 10.1.1.25** (service provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**
- **Outgoing Transport: UDP**

- Click **Finish**

6.3.3. Server Configuration

Server Profiles should be created for the Avaya SBCE two peers, Communication Manager (Call Server) and the SIP Proxy at the service provider's network (Trunk Server).

To add the profile for the Call Server, from the **Global Profiles** menu, select **Server Configuration**. Click **Add Profile** and enter the profile name: **Com. Manager**.

On the **Add Server Configuration Profile, General** Tab:

- Select **Server Type: Call Server**
- **IP Address: 192.168.10.12** (IP Address of the **procr** interface in Communication Manager)
- **Supported Transports:** Check TCP. The protocol and port defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**
- **TCP Port: 5060.**
- Click **Next**

Add Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma separated list	192.168.10.12
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
<div>Back Next</div>	

- Click **Next** on the **Authentication** tab
- Click **Next** on the **Heartbeat** tab
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu.
- Click **Finish**.

To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name. The name **Service Provider** was used.

On the **Add Server Configuration Profile, General Tab**:

- Select **Server Type: Trunk Server**
- **IP Address: 10.1.1.25** (service provider's SIP Proxy IP address)
- **Supported Transports: Check UDP.**
- **UDP Port:5060**
- Click **Next**

The screenshot shows a dialog box titled "Add Server Configuration Profile - General". It contains the following fields and options:

Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Comma separated list</small>	10.1.1.25
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	

At the bottom of the dialog are two buttons: "Back" and "Next".

- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave other fields with their default values.
- Click **Finish**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with the following items: Welcome, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration. The main area displays the "Global Profiles > Server Configuration: Service Provider" configuration page. It includes tabs for "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is active, showing the following configuration:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	10.1.1.25
Supported Transports	UDP
UDP Port	5060

At the bottom of the configuration table is an "Edit" button. Above the configuration table are buttons for "Add Profile", "Rename Profile", "Clone Profile", and "Delete Profile".

6.3.4. Topology Hiding

Topology Hiding is a security feature which allows the manipulation of several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Communication Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

For the test configuration, default values of the Topology Hiding Profile were used in the enterprise direction. Since modifying a default profile is generally not recommended, the default was duplicated, or “cloned”. That way if modifications are needed in the future, the default profile will not be affected by those changes.

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:



- Select **default** from the **Topology Hiding Profiles** list.
- Click **Clone Profile**.
- Enter the **Profile Name: Com. Manager**.
- Click **Finish**.

To add the Topology Hiding Profile in the SIP trunk direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select **default** from the **Topology Hiding Profiles** list.
- Click **Clone Profile**.
- Enter the **Profile Name: Service Provider**. Click **Finish**.
- Click **Edit** on the **Topology Hiding** tab.
- For the **To**, **From** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column.
- In the **Overwrite Value** column, enter **aslab.centixvoip.net**, the AT&T SIP domain used for the compliance test.

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	
To	IP/Domain	Overwrite	aslab.centixvoip.net
Via	IP/Domain	Auto	
Record-Route	IP/Domain	Auto	
From	IP/Domain	Overwrite	aslab.centixvoip.net
Request-Line	IP/Domain	Overwrite	aslab.centixvoip.net

Finish

- Click **Finish**

Global Profiles > Topology Hiding: Service Provider

Add Profile **Rename Profile** **Clone Profile** **Delete Profile**

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	aslab.centixvoip.net
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	aslab.centixvoip.net
Request-Line	IP/Domain	Overwrite	aslab.centixvoip.net

Edit

6.4. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

6.4.1. Network Management

The network information should have been previously completed in **Section 6.2**. To verify the network configuration, from the **Device Specific Menu** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various settings categories, with 'Device Specific Settings' expanded and 'Network Management' selected. The main panel is titled 'Device Specific Settings > Network Management: Avaya_SBCE'. It has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning banner states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.0), and 'B2 Netmask'. An 'Add IP' button is present. A yellow banner says: 'Changes will not take effect until the interface is updated.' Below this is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains two rows: one for IP 192.168.10.72 with gateway 192.168.10.254 and interface A1, and another for IP 172.16.1.15 with gateway 172.16.1.254 and interface B1. 'Save Changes' and 'Clear Changes' buttons are at the bottom right of the table.

IP Address	Public IP	Gateway	Interface
192.168.10.72		192.168.10.254	A1
172.16.1.15		172.16.1.254	B1

In the event that changes need to be made to the network configuration information, they could be entered here.

On the Interface Configuration tab, click the **Toggle State** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **Disabled**, so it is very important to perform this step, or the SBC will not be able to communicate on any of its interfaces.

The screenshot shows the UC-Sec Control Center interface, specifically the 'Interface Configuration' tab for device 'Avaya_SBCE'. The left sidebar is the same as the previous screenshot. The main panel is titled 'Device Specific Settings > Network Management: Avaya_SBCE'. It has two tabs: 'Network Configuration' and 'Interface Configuration' (active). The interface configuration is shown in a table with columns: Name, Administrative Status, and Toggle State. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Disabled). Each interface has a 'Toggle State' button next to it.

Name	Administrative Status	Toggle State
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

6.4.2. Signaling Interface

Signaling Interfaces need to be created for both the private and public Avaya SBCE network interfaces.

To create the Signaling Interface toward Communication Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**, then **Add Signaling Interface**:

- **Name:** Private_sig
- **IP Address:** 192.168.10.72 (inside IP address of the Avaya SBCE)
- **TCP Port:** 5060. The Avaya SBCE will listen for SIP requests on the port specified here. The protocol and port defined in this screen must match the values used on the Communication Manager signaling group form in **Section 5.6**
- Click **Finish**

Add Signaling Interface

Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

Name	Private_sig
IP Address	192.168.10.72
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	
Cluster TLS Only for use with Cisco SIP Clusters	<input type="checkbox"/>
Enable Stun Requires a UDP Port	<input type="checkbox"/>

Finish

Similarly, to add the Signaling Interface toward the AT&T SIP Trunk:

- Click **Add Signaling Interface**:
- **Name:** Public_sig
- **IP Address:** 172.16.1.15 (Outside IP Address of the Avaya SBCE)
- **UDP Port:** 5060
- Click **Finish**

UC-Sec Control Center

Device Specific Settings > Signaling Interface: Avaya_SBCE

Signaling Interface

Add Signaling Interface

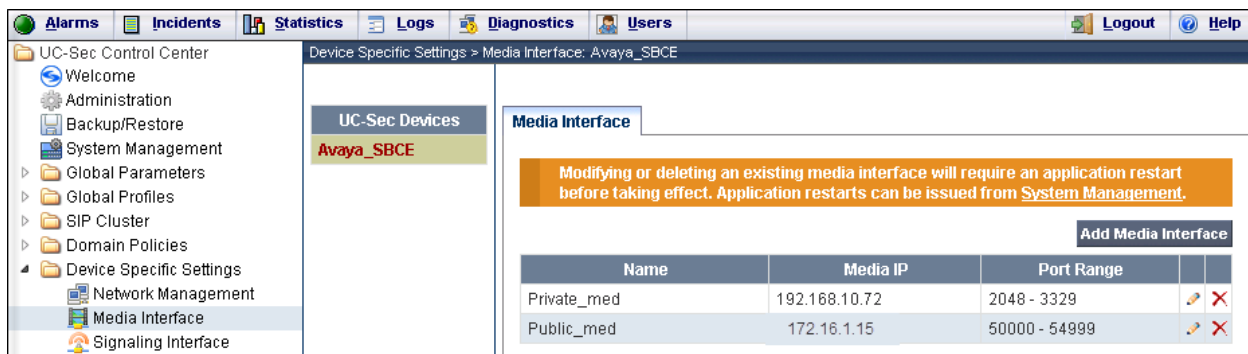
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Private_sig	192.168.10.72	5060	---	---	None		
Public_sig	172.16.1.15	---	5060	---	None		

6.4.3. Media Interface

Media Interfaces were created to specify the port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise one of the ports in this range as the listening port in which it will accept media from the Call or Trunk Server. The Private interface was made to match the range specified in the IP-Network-Region in Communication Manager of 2048 to 3349, and the Public interface to match the range specified by AT&T for the compliance test of 50000 to 54999.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**

- Select **Add Media Interface**
- **Name: Private_med**
- **IP Address: 192.168.10.72** (Inside IP Address of the Avaya SBCE)
- **Port Range: 2048-3329**
- Click **Finish**
- Select **Add Media Interface**
- **Name: Public_med**
- **IP Address: 172.16.1.15** (Outside IP Address of the SBC, toward AT&T)
- **Port Range: 50000-54999**
- Click **Finish**.




6.4.4. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules, profiles, etc. previously configured, to be applied to the packets traveling in each direction.

To create the call flow toward the AT&T SIP trunk, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add Flow**.

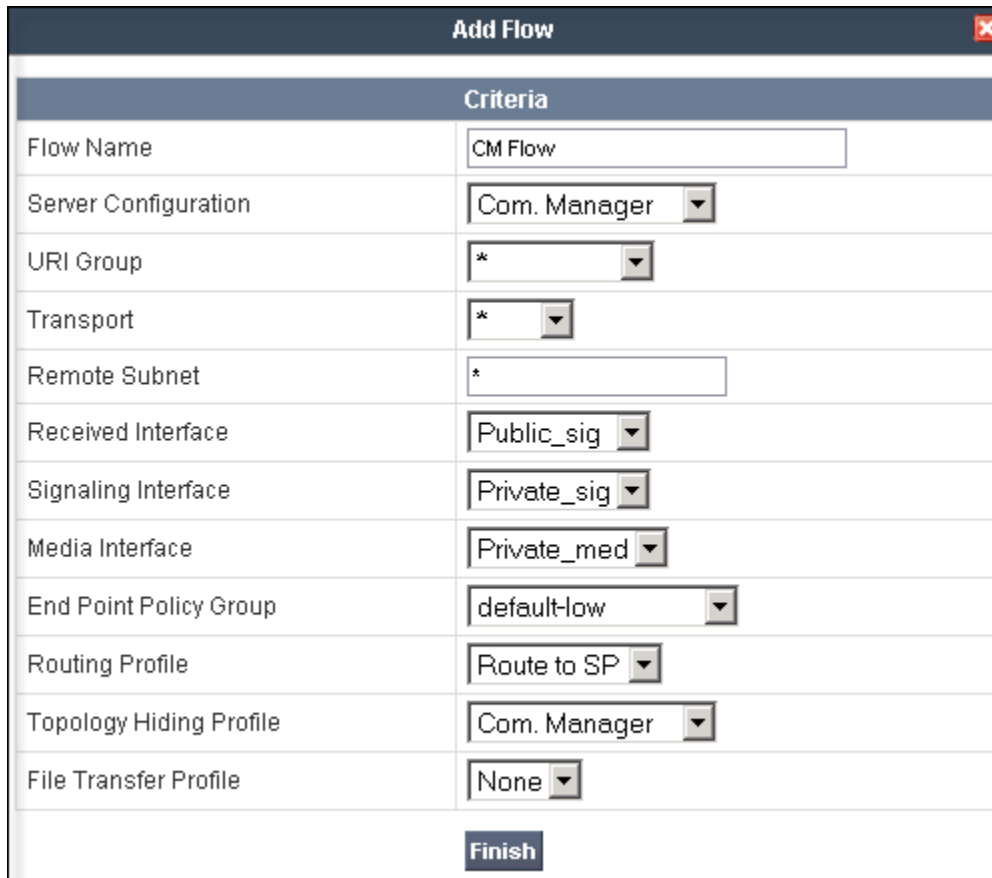
- **Name: SIP Trunk Flow**
- **Server Configuration: Service Provider.**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Private_sig**

- **Signaling Interface: Public_sig**
- **Media Interface: Public_med**
- **End Point Policy: default-low**
- **Routing Profile: Route to CM** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service Provider**
- **File Transfer Profile: None**
- **Click Finish.**

Add Flow 	
Criteria	
Flow Name	<input type="text" value="SIP Trunk Flow"/>
Server Configuration	<input type="text" value="Service Provider"/>
URI Group	<input type="text" value="*"/>
Transport	<input type="text" value="*"/>
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="Private_sig"/>
Signaling Interface	<input type="text" value="Public_sig"/>
Media Interface	<input type="text" value="Public_med"/>
End Point Policy Group	<input type="text" value="default-low"/>
Routing Profile	<input type="text" value="Route to CM"/>
Topology Hiding Profile	<input type="text" value="Service Provider"/>
File Transfer Profile	<input type="text" value="None"/>
<input type="button" value="Finish"/>	

To create the call flow toward Communication Manager, click **Add Flow**.

- **Name: CM Flow**
- **Server Configuration: Com. Manager**
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Public_sig**
- **Signaling Interface: Private_sig**
- **Media Interface: Private_med**
- **End Point Policy Group: default-low**
- **Routing Profile: Route to SP** (Note that this is the reverse route of the flow)
- **Topology Hiding Profile: Com. Manager**
- **File Transfer Profile: None**
- Click **Finish**



The screenshot shows a window titled "Add Flow" with a close button in the top right corner. Below the title bar is a table with the following structure:

Criteria	
Flow Name	CM Flow
Server Configuration	Com. Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	default-low
Routing Profile	Route to SP
Topology Hiding Profile	Com. Manager
File Transfer Profile	None

At the bottom of the table is a "Finish" button.

The two Server Flows created in the sample configuration are summarized on the screen below:

Device Specific Settings > End Point Flows: Avaya_SBCE													
<div>UC-Sec Devices</div> <div>Avaya_SBCE</div>													
<div>Subscriber Flows</div> <div>Server Flows</div>													
Click here to add a row description.													
Server Configuration: Com. Manager													
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
1	CM Flow	*	*	*	Public_sig	Private_sig	Private_med	default-low	Route to SP	Com. Manager	None		
Server Configuration: Service Provider													
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
1	SIP Trunk Flow	*	*	*	Private_sig	Public_sig	Public_med	default-low	Route to CM	Service Provider	None		

7. AT&T Mobility SIP Trunk Service Configuration

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

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

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

This information is used to complete the configuration of Communication Manager and the Avaya SBCE discussed in the previous sections.

8. Verification and Troubleshooting

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

Verification Steps:

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

Troubleshooting:

1. Communication Manager:
 - **list trace station** <extension number>
Traces calls to and from a specific station.
 - **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
 - **status signaling-group** <signaling group number>
Displays signaling group service state.
 - **status trunk** <trunk group number>
Displays trunk group service state.
 - **status station** <extension number>
Displays signaling and media information for an active call on a specific station.
2. Avaya SBCE:

There are several links and menus located on the taskbar in the UC-Sec Control Center that can provide useful diagnostic or troubleshooting information:

 - **Alarms.** Provides information about the health of the SBC.
 - **Incidents.** Provides detailed reports of anomalies, errors, policies violations, etc.
 - **Diagnostics.** This screen provides a variety of tools to aid in troubleshooting the SBC network connectivity and its operation.

Other useful tools can also be found on the **Troubleshooting Menu**, on the left hand side of the UC-Sec Control Center page.

- **Packet Capture.** Allows to capture the packets in any of the SBC interfaces, and save them as *pcap* files. From the menu on the left hand side, click **Troubleshooting → Trace Settings → Packet Capture** tab.

9. Conclusion

AT&T Mobility in Puerto Rico SIP Trunk Service passed compliance testing. Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2**.

These Application Notes describe the configuration necessary to connect the above service to an Avaya SIP telephony solution consisting of Avaya Aura® Communication Manager 6.0.1 and Avaya Session Border Controller for Enterprise.

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

10. 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] *Sipera Systems E-SBC 1U Installation Guide. Release 4.0.5*. November 2011.
- [6] *Sipera Systems E-SBC Administration Guide. Release 4.0.5*. November 2011.
- [7] *Sipera Systems E-SBC Release Notes. Release 4.0.5.Q02*. November 2011.
- [8] *Avaya one-X® Deskphone H.323 Administrator Guide Release 6.1*, May 2011, Document Number 16-300698.
- [9] *Administering Avaya one-X® Communicator*, October 2011.
- [10] *Using Avaya one-X® Communicator, Release 6.1*, October 2011.
- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [13] *Recommendation ITU-T T-38. Procedures for real-time Group 3 facsimile communication over IP networks*. September 2010.

©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.