AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 4.0.5 with AT&T IP Toll Free SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.2, and the Avaya Session Border Controller for Enterprise 4.0.5 with the AT&T IP Toll Free service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.2 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 4.0.5 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

JF; Reviewed:
SPOC 7/29/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
1 of 87
SM63CM62SBCETF

TABLE OF CONTENTS

JF; Reviewed:
SPOC 7/29/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
3 of 87
SM63CM62SBCETF

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.2, and the Avaya Session Border Controller for Enterprise 4.0.5 (referred to in the remainder of this document as *Avaya SBCE*) with the AT&T IP Toll Free service using AVPN or MIS/PNT transport connections.

Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.2 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Avaya SBCE is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT[1] transport.

> **Note** – These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. That solution is described in the document *Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 4.0.5 AT&T IP Transfer Connect Service – Issue 1.0.*

2. General Test Approach and Test Results

The test environment consisted of:
1. A simulated enterprise with System Manager, Session Manager, Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya SBCE, and Avaya Aura® Messaging.
2. A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise was connected via AVPN transport.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2** for examples) between Session Manager, Communication Manager, Session Border Controller, and the AT&T IP Toll Free service.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the AT&T network. Calls were made from the PSTN across the AT&T IP Toll Free service network. The following features were tested as part of this effort:

---

[1] MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does support cRTP..

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

5 of 87
SM63CM62SBCETF

- SIP trunking.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- PBX and AT&T IP Toll Free service features such as hold, resume, conference and transfer.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing were also tested.

2.2. Test Results

The main test objectives were to verify the following features and functionality:
- Inbound AT&T IP Toll Free service calls to Communication Manager telephones and VDNs/Vectors/Agents.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones/Agents via the AT&T Toll Free service.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- T.38 fax calls from the AT&T IP Toll Free service/PSTN to Communication Manager G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833/4733 between Communication Manager and the AT&T IP Toll Free service/PSTN automated access systems.
- Inbound AT&T IP Toll Free service calls to Communication Manager that is directly routed to stations, and if unanswered, can be covered to Avaya Messaging.
- Long duration calls.

The test objectives stated in **Section 2.1** with limitations as noted in **Section 2.2.1,** were verified.

2.2.1. Known Limitations

1. **G.711 Fax support** - G.711 faxing is not supported between Communication Manager and the AT&T IP Toll Free service. T.38 fax is supported, however fax speeds are limited to 9600 in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Communication Manager in the reference configuration.

2. **G.726 codec support** - G.726 codec is not supported between Communication Manager and the AT&T IP Toll Free service.

3. **Avaya SIP endpoints may generate SIP messages with Endpoint-View and AV-Correlation-ID headers.** The Endpoint-View and AV-Correlation-ID headers may be inserted in 18x responses (or in SIP requests), and contain private CPE information (local extensions, domains, etc). In addition, an "epv" parameter is inserted into the Contact header that also contains local network information. The Endpoint-View header has also been observed to cause issues with other AT&T services as well.

- The workaround is to have the Avaya SBCE remove the **Endpoint-View** and **AV-Correlation-ID** headers, as well as the "epv" parameter (see **Sections 8.3.9, 8.4.3.1** and **8.4.3.2**).

4. **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues.** Certain Avaya SIP endpoints (e.g., 9620, 9630, 9601, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 8.3.9**).
   a. Note - It was found that when all three Bandwidth headers are sent, the Avaya SBCE will only pass one of the headers to AT&T and block the other two.
      i. The Avaya SBCE support team has been notified and an MR submitted.

2.3. Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555. Avaya customers may obtain documentation and support for Avaya products by visiting: http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on http://support.avaya.com) to directly access specific support and consultation services based upon their Avaya support agreements.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Session Manager 6.3 provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya SIP endpoints register to Session Manager.
- System Manager 6.3 provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager 6.2 provides the voice communication services for a particular enterprise site. Avaya H.323 endpoints register to Communication Manager.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G430 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya desk telephones are represented with Avaya 1603(H.323), 960x Series IP Telephones (running H.323 firmware), and 96x1 Series IP Telephones (running H.323 or SIP firmware), Avaya 6424 Digital Telephones, as well as Avaya one-X® Agent soft phone (H323).

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

7 of 87
SM63CM62SBCETF

- The Avaya SBCE 4.0.5 provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network.
- The AT&T IP Toll Free service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya SBCE in this sample configuration. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya SBCE and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP and TLS to communicate with Communication Manager. UDP transport protocol is used between the Avaya SBCE and the AT&T IP Toll Free service.
- Avaya Messaging was used in the reference configuration to provide voice messaging capabilities. The provisioning of Avaya Messaging is beyond the scope of this document.
- Inbound calls were placed from PSTN via the AT&T IP Toll Free service, through the Avaya SBCE to Session Manager, which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate agent/phone or fax extension.

Note – Documents used to provision the reference configuration are listed in **Section 11**. Specific references to these documents are indicated in the following sections by the notation **[x]**, where x is the document reference number.
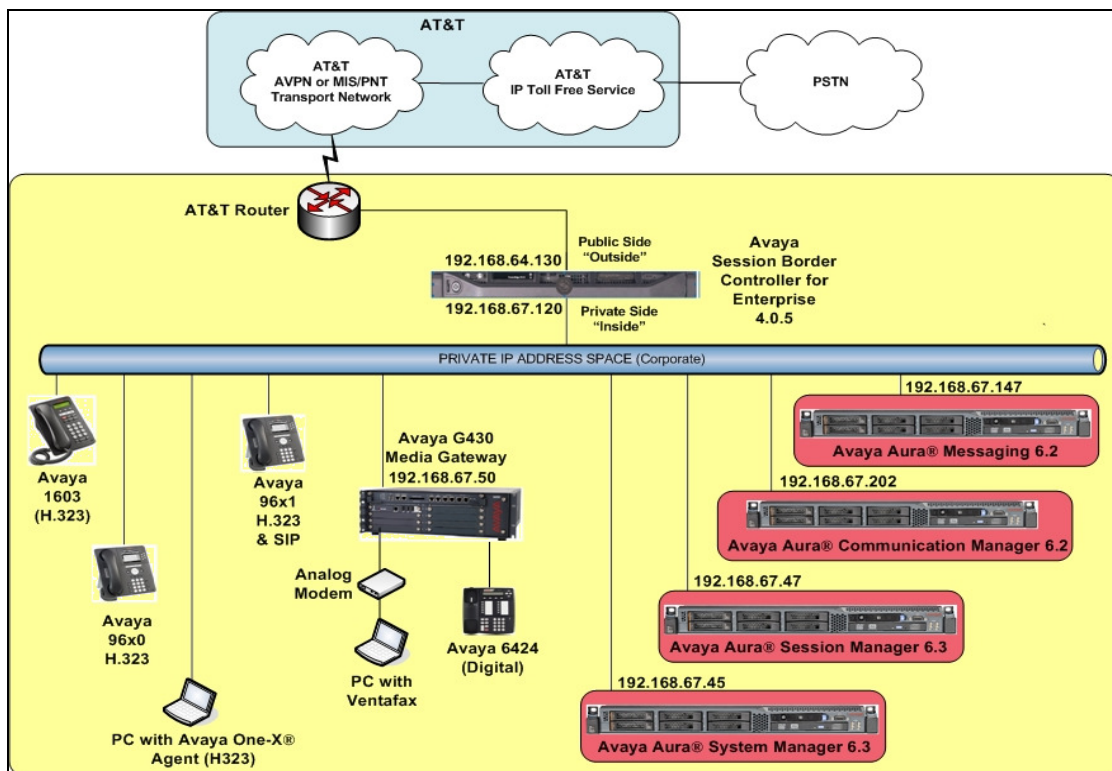
Figure 1: Reference configuration

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their own specific configurations.

Note - The AT&T IP Toll Free service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the AT&T Toll Free service) are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DNIS digits as part of the IP Toll Free provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura® System Manager	
IP Address	192.168.67.45
Avaya Aura® Session Manager	
Management IP Address	192.168.67.46
Network IP Address	192.168.67.47
Avaya Aura® Communication Manager	
IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	19xxx = Stations 4xxxx = VDNs
Voice Messaging Pilot Extension	36000
Avaya Session Border Controller for Enterprise (Avaya SBCE)	
IP Address of Outside (Public) Interface (to AT&T IP Toll Free Service)	192.168.64.130
IP Address of Inside (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.120
Avaya Aura® Messaging	
IP Address	192.168.67.147
Messaging Mailboxes	19xxx

Table 1: Illustrative Values Used in these Application Notes

3.2. Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled by Session Manager and Communication Manager, two general call flows are described in this section. The first call scenario illustrated in **Figure 2** is an inbound AT&T IP Toll Free service call that arrives on Session Manager and is subsequently routed to Communication Manager.

1. A PSTN telephone originates a call to an AT&T IP Toll Free service number.
2. The PSTN routes the call to the AT&T IP Toll Free service network.
3. The AT&T IP Toll Free service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a) a vector, which in turn, routes the call to an agent, or b) directly to an agent or telephone.
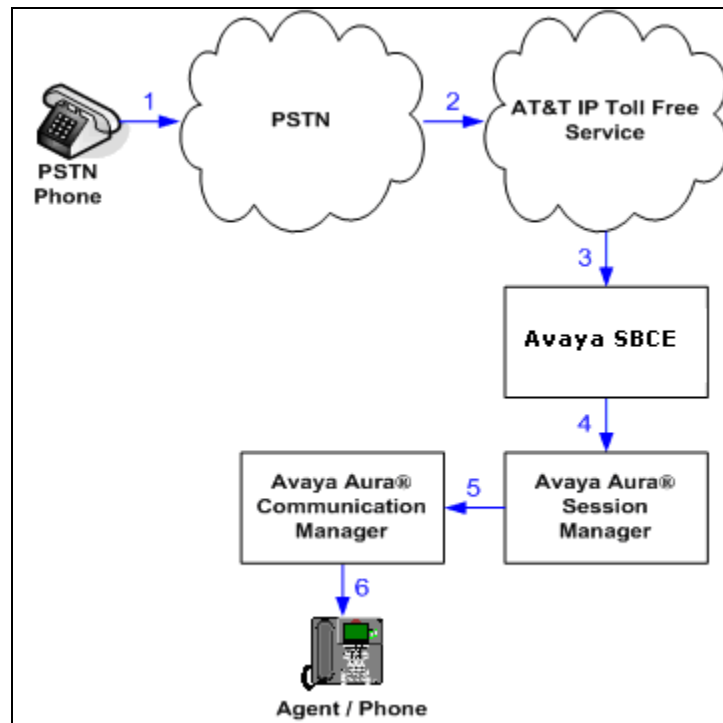
Figure 2: Inbound AT&T IP Toll Free Service Call to VDN/Agent/Telephone

Note that the IP Toll Free service features such as Legacy Transfer Connect and Alternate Destination Routing utilize this call flow as well.

The second call scenario illustrated in **Figure 3** is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Messaging system connected to Session Manager.

1. Same as the **Steps 1-5** and **Step 6b** from the first call scenario.
2. The called Communication Manager agent or telephone does not answer the call, and the call covers to the agent's or telephone's voicemail. Communication Manager forwards the call to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Avaya Messaging. Avaya Messaging answers the call and connects the caller to the called agent's or telephone's voice mailbox.
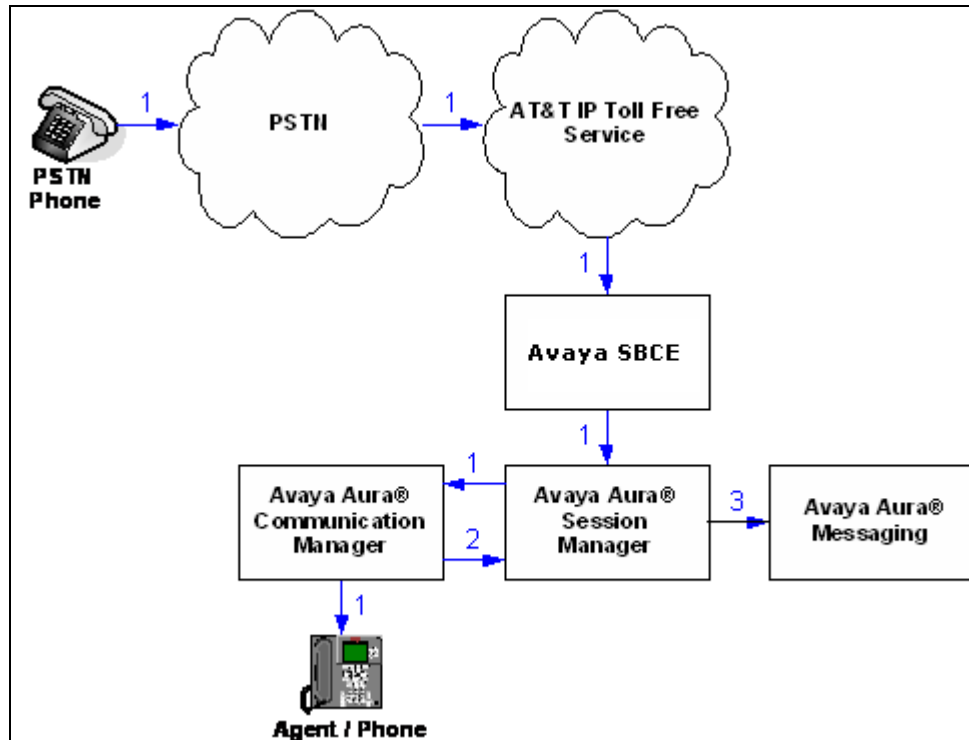
Figure 3: Inbound AT&T IP Toll Free Service Call to Agent / Telephone Covered to Avaya Aura® Messaging

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

11 of 87
SM63CM62SBCETF

4. Equipment and Software Validated

The following equipment and software was used for the reference configuration described in these Application Notes.

Equipment/Software	Release/Version
HP Proliant DL360 G7 server • System Platform • Avaya Aura® System Manager	• 6.2.1.0.9 with patch 6.2.2.08001 • 6.3 (6.3.1.9), with SP1 (r1212)
IBM 8800 server • Avaya Aura® Session Manager	• 6.3.0.0.630039 with SP1(6.3.1.0.631004)
IBM 8800 server • System Platform • Avaya Aura® Communication Manager	• 6.2.1.0.9 with patch 6.2.2.08001 • 6.2 SP6 (02.0.823.0-20558)
Dell R610 • System Platform • Avaya Aura® Messaging	• 6.2.1.0.9 • 6.2 SP2 (6.2.02.0.823.0-109_0202) with patch (m62109cd_pt+a.rpm)
Avaya G430 Media Gateway	32.26.0
MM711 Analog card	HW31 FW094
Dell R310 • Avaya Session Border Controller for Enterprise	• 4.0.5 Q19
Avaya 96x0 IP Telephone	H.323 Version S3.2
Avaya 96x1 IP Telephone	H.323 Version S6.2313 SIP Version 6.2.1.26
Avaya 9601 IP Telephone	SIP version 6.1.5.12
Avaya one-X® Agent	2.5.1072.11103
Avaya 1603 IP Telephone	H323 (ha1603ua1_3200.bin)
Avaya 6424 Digital telephone	-
Windows PC/ Ventafax Home Version (Fax device)	6.1.59.144

Table 2: Equipment and Software Versions

Note - Compliance testing of solutions that include the Avaya Session Border Controller for Enterprise (Avaya SBCE) version 4.0.5, also certify those solutions with the Avaya SBCE version 6.2 as well.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

12 of 87
SM63CM62SBCETF

5. Configure Avaya Aura® Session Manager Release 6.3

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

> **Note** – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult documents **[1]** through **[4]** for further details if necessary.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Avaya SBCE. In addition, provisioning for calls to Avaya Messaging are described also.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented as Entity Links. Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely System Manager.

When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as Adaptations, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of normalizing the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed Dial Patterns, and determines the destination SIP Entities based on Routing Policies specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

The following administration activities will be described:
* Define SIP Domain
* Define Locations for Communication Manager, Avaya SBCE, and Avaya Messaging.
* Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, Avaya SBCE, and Avaya Messaging.
* Define SIP Entities corresponding to Communication Manager, Avaya SBCE, and Avaya Messaging.
* Define Entity Links describing the SIP trunk between Communication Manager and Session Manager, the SIP Trunk between Session Manager and the Avaya SBCE, and the SIP trunk between Session manager and Avaya Messaging.

- Define Routing Policies associated with the Communication Manager, Avaya SBCE and Avaya Messaging.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager.

In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, a Release 6.3 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.
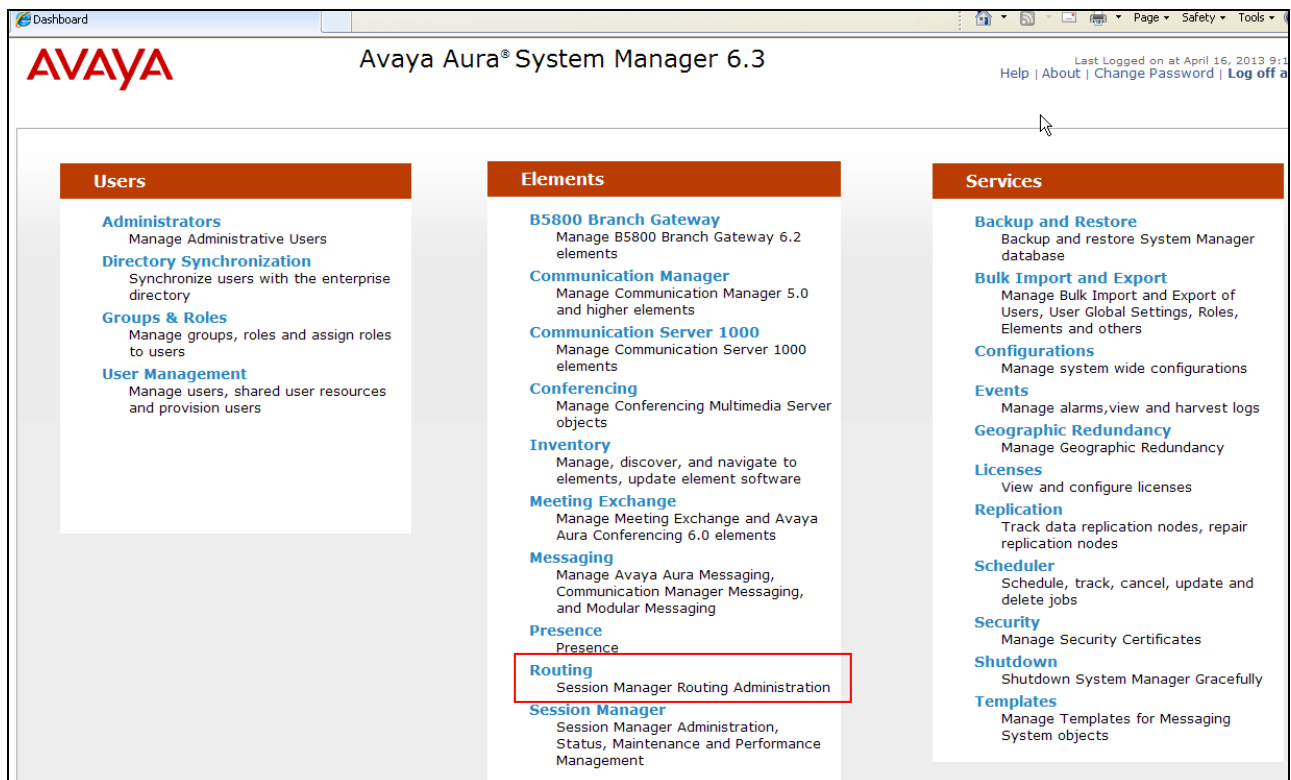
5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain **customera.com** was defined.

Step 2 - Click **New** (not shown)**.** Enter the following values and use default values for remaining fields**.**

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **customera.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description. [Optional]

Step 3 - Click **Commit** to save.

Avaya Aura® System Manager 6.3

Routing / Home

Home / Elements / Routing / Domains

Help ?

Domain Management   Commit Cancel

1 Item | Refresh   Filter: Enable

Name	Type	Notes
* customera.com	sip	

Commit Cancel

Note – Multiple SIP Domains may be defined if required.

5.2.   Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g., 192.168.67.x for all devices on a particular subnet), or individual devices (e.g., 192.168.67.46 for a device's specific IP address). In the reference configuration, the Location "**Main**" was defined for the entire Customer Premises Equipment (CPE) subnet **192.168.67.***.

5.2.1. Location for CPE Equipment

The location **Main** is used as a wild card for the CPE Avaya equipment (e.g., Communication Manager, Session Manager, Avaya SBCE, and Avaya Messaging).

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.
  • **Name:** Enter a descriptive name for the location (e.g., **Main**).
  • **Notes:** Add a brief description. [Optional]
Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.
  • **IP Address Pattern:** Enter the IP address of the CPE subnet (e.g., **192.168.67.***).
  • **Notes:** Add a brief description. [Optional]
Step 3 - Click **Commit** to save.

5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T, and for converting SIP headers sent between Communication Manager and Avaya Messaging. In the reference configuration the following adaptations were used.

- Calls from AT&T (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager.

- The IP address of Session Manager (**192.168.67.47**) is replaced with the Avaya CPE SIP domain (**customera.com**).
- The AT&T Border Element IP address (**135.25.29.74**) is replaced with **customera.com** for source domain.
- The AT&T called number digit strings in the Request URI is replaced with their associated Communication Manager extensions/VDNs.
- Calls to Avaya Messaging from AT&T/PSTN (**Section 5.3.2**).
  - The AT&T called number digit strings in the Request URI are replaced with the Avaya Messaging pilot number.

5.3.1. Adaptation for calls to Avaya Aura® Communication Manager

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager from AT&T, and to direct incoming calls to their associated Communication Manager extensions.

> **Note** – In the reference configuration, the AT&T E-IPFR service delivered 10 digit DNIS numbers. Also note that the following entries are based on the DNIS digits delivered in the AT&T Request URI. These digits may not be the same as the dialed digits.

Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

Step 2 - In the **Adaptation Details** page, enter:
- A descriptive **Name**, (e.g., **ACM62_public**).
- Select **DigitConversionAdapter** rom the **Module Name** drop down menu (if no module name is present, select <click to add module> and enter **DigitConversionAdapter**).
- In the **Module parameter** field enter **odstd=customera.com osrcd=customera.com.** The odstd parameter will replace the IP address of Session Manager (**192.168.67.47**) with **customera.com** in the *inbound* Request URI, and the osrcd parameter will replace the AT&T border element IP address (**135.25.29.74**) with **customera.com**, when Session Manager sends the Invite to Communication Manager.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

17 of 87
SM63CM62SBCETF

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager).

- Example: 7325553161 is a DNIS string sent in the Request URI by AT&T Toll Free service that is associated with Communication Manager Skill2 access VDN 44002.
  - Enter **0000001050** in the **Matching Pattern** column.
  - Enter **10** in the **Min/Max** columns.
  - Enter **10** in the **Delete Digits** column.
  - Enter **44002** in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

Step 4 – Repeat **Step 3** for all additional AT&T DNIS numbers.
Step 5 - Click on **Commit**.

Note – As shown in the screen below, no **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

Digit Conversion for Incoming Calls to SM

[Add] [Remove]
0 Items | Refresh   Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

[Add] [Remove]
14 Items | Refresh   Filter: Enable

	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
☐	* 0000001050	* 10	* 10		* 10	44002	destination ▼		IPTF
☐	* 0000011051	* 10	* 10		* 10	44003	destination ▼		IPTF
☐	* 0000021052	* 10	* 10		* 10	44002	destination ▼		IPTF
☐	* 0000031053	* 10	* 10		* 10	19003	destination ▼		IPTF

Select : All, None

[Commit] [Cancel]

5.3.2. Adaptation for calls to Avaya Aura® Messaging

The Adaptation administered in this section is used for modification of SIP messages from AT&T to Avaya Messaging.

Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

Step 2 - In the **Adaptation Details** page, enter:
- A descriptive **Name**, (e.g., **AAM_Digits**).

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

18 of 87
SM63CM62SBCETF

- Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select <click to add module> and enter **DigitConversionAdapter**).

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with the Avaya Messaging pilot number before being sent to Avaya Messaging.

  o Example: **0000041053** is a DNIS string sent in the Request URI by AT&T Toll Free service that is associated with Avaya Messaging pilot number 36000.

   - Enter **0000041053** in the **Matching Pattern** column.
   - Enter **10** in the **Min/Max** columns.
   - Enter **10** in the **Delete Digits** column.
   - Enter **36000** in the **Insert Digits** column.
   - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
   - Enter any desired notes.

Step 4 - Click on **Commit**.

Note – As shown in the screen below, no **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

19 of 87
SM63CM62SBCETF

5.4. SIP Entities

In this section, SIP Entities are administered for the following SIP network elements:
- Session Manager (**Section 5.4.1**).
- Communication Manager for AT&T access (**Section 5.4.2**) – This entity, and its associated Entity Link (using TCP with port 5062, is for calls from AT&T to Communication Manager via the Avaya SBCE.
- Communication Manager for local access (**Section 5.4.3**) – This entity, and it's associated Entity Link (using TLS with port 5061), is primarily used for traffic between Avaya SIP telephones and Communication Manager.
- Avaya SBCE (**Section 5.4.4**) - This entity, and its associated Entity Link (using TCP and port 5060), is for calls from the IP Toll Free service via the Avaya SBCE.
- Avaya Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using TCP and port 5060), is for traffic from Avaya Messaging to Communication Manager**.**

> **Note** – In the reference configuration, only the "Local" trunk defined between Session Manager and Communication Manager used TLS (port 5061). TCP is used as the transport protocol between Session Manager and the Communication Manager "Public" trunk (port 5062), the Avaya SBCE (port 5060), and Avaya Messaging (port 5060). The use of TCP transport was to facilitate protocol trace analysis. Avaya best practices call for TLS (port 5061) to be used as the transport protocol whenever possible.

5.4.1. Avaya Aura® Session Manager SIP Entity

Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:
- **Name –** Enter a descriptive name for Session Manager (e.g., **sm63**).
- **FQDN or IP Address –** Enter the IP address of the Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **192.168.67.47**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 5.2.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.

Step 3 - In the **SIP Link Monitoring** section of the **SIP Entity Details** page configure as follows:
- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.

Step 4 – Scrolling down to the **Port** section of the **SIP Entity Details** page, click on **Add** and provision an entry as follows:

- **Port** – Enter **5060** (see note above).
- **Protocol** – Select **TCP** (see note above).
- **Default Domain** – Select a SIP domain administered in **Section 5.1** for the selected **Default Domain** field (e.g., **customera.com**)

This is for connections to Avaya SBCE and Avaya Messaging.

Step 5 - Repeat **Step 4** to provision entries for:

- **5062** for **Port** and **TCP** for **Protocol**. This is for public traffic between the Communication Manager and the Avaya SBCE/AT&T.
- **5061** for **Port** and **TLS** for **Protocol**.

Step 6 – Enter any notes as desired and leave all other fields on the page blank/default.
Step 7 - Click on **Commit** (not shown).

Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

Note – The **SIP Responses to an OPTIONS Request** section of the form (not shown) is not used in the reference configuration.

5.4.2. Avaya Aura® Communication Manager SIP Entity - Public

Step 1 - In the **SIP Entities** page, click on **New** (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name for the Communication Manager public trunk (e.g. **ACM62_public**).
- **FQDN or IP Address –** Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g., **192.168.67.202**).
- **Type –** Select **CM**.
- **Adaptation –** Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location **Main** administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page select:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.

Step 3 - Click on **Commit** (not shown).

Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

Note – The **SIP Responses to an OPTIONS Request** section of the form (not shown) is not used in the reference configuration.

JF; Reviewed:
SPOC 7/29/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
22 of 87
SM63CM62SBCETF

5.4.3. Avaya Aura® Communication Manager SIP Entity – Local

To configure the Communication Manager Local trunk SIP entity, repeat the steps in **Section 5.4.2**. The F**QDN or IP Address** field is populated with the IP address of Communication Manager and the **Type** field is set to **CM**. See the figure below for the values used in the reference configuration.

5.4.4. Avaya Session Border Controller for Enterprise SIP Entity

To configure the Avaya SBCE SIP entity, repeat the steps in **Section 5.4.2**. The F**QDN or IP Address** field is populated with the IP address of the inside interface of the Avaya SBCE and the **Type** field is set to **SIP Trunk**. See the figure below for the values used in the reference configuration.

JF; Reviewed:
SPOC 7/29/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
24 of 87
SM63CM62SBCETF

5.4.5. Avaya Aura® Messaging SIP Entity

To configure the Avaya Messaging SIP entity, repeat the steps in **Section 5.4.2**. The F**QDN or IP Address** field is populated with the IP address of the Avaya Messaging Application and the **Type** field is set to **Modular Messaging** (note: use this type even with Avaya Messaging). See the figure below for the values used in the reference configuration.

5.5. Entity Links

In this section, Entity Links are administered between Session Manager and the following SIP Entities:

- Avaya Communication Manager – Public (**Section 5.5.1**).
- Avaya Communication Manager – Local (**Section 5.5.2**).
- Avaya SBCE (**Section 5.5.3**).
- Avaya Messaging (**Section 5.5.4**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 5.4**.

Note – See the information in **Section 5.4** regarding the transport protocols and ports used in the reference configuration.

5.5.1. Entity Link to Avaya Aura® Communication Manager - Public

Step 1 - In the left pane under **Routing**, click on **Entity Links**. In the **Entity Links** page, click on **New** (not shown).

Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **ACM62_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5062** (see **Section 5.4.1**).
- **Protocol –** Select **TCP**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **ACM62_public**).
- **SIP Entity 2 Port** - Enter **5062**.
- **Connection Policy –** Select **Trusted**.

Step 3 - Click on **Commit**.

5.5.2. Entity Link to Avaya Aura® Communication Manager Entity - Local

To configure this entity link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.3** for the Communication Manager local Entity (e.g., **ACM62_Local**). The **Protocol** is **TLS** and the **Port** is **5061**. See the figure below for the values used in the reference configuration.

5.5.3. Entity Link for the Avaya SBCE

To configure this entity link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.4** for the Avaya SBCE. The **Protocol** is **TCP** and the **Port** is **5060**. See the figure below for the values used in the reference configuration.

						Connection Policy	Deny New Service	Notes
Name	**SIP Entity 1**	**Protocol**	**Port**	**SIP Entity 2**	**Port**			
* A-SBCE	* sm63 ▾	TCP ▾	* 5060	* A-SBCE ▾	* 5060	Trusted ▾	☐	

Entity Links   Commit Cancel

1 Item | Refresh   Filter: Enable

5.5.4. Entity Link to Avaya Aura® Messaging

To configure this entity link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.5**. The **Protocol** is **TCP** and the **Port** is **5060**. See the figure below for the values used in the reference configuration.

Entity Links   Commit Cancel

1 Item | Refresh   Filter: Enable

						Connection Policy	Deny New Service	Notes
Name	**SIP Entity 1**	**Protocol**	**Port**	**SIP Entity 2**	**Port**			
* AA-M	* sm63 ▾	TCP ▾	* 5060	* AA-M ▾	* 5060	Trusted ▾	☐	

5.6. Time Ranges

Step 1 - In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New** (not shown).

Step 2 - Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkboxes for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on **Commit**.

Step 4 - Repeat **Steps 1 – 3** to provision additional time ranges.

AVAYA   Avaya Aura® System Manager 6.3   Last Logged on at April 16, 2013 9:15 AM
Help | About | Change Password | **Log off admin**

Routing ✕   Home

Home / Elements / Routing / Time Ranges

Routing	
Domains	**Time Ranges**
Locations	Help ?
Adaptations	New Edit Delete Duplicate More Actions ▾
SIP Entities	
Entity Links	1 Item	Refresh Filter: Enable
Time Ranges	
Routing Policies	
Dial Patterns	Select : All, None

	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Calls to Communication Manager from AT&T (**Section 5.7.1**).
- Avaya Messaging Message Wait Indicator (MWI) notification to Communication Manager, Avaya Messaging outbound dialing, and access to/from SIP phones (**Section 5.7.2**).
- Communication Manager call coverage to Avaya Messaging (**Section 5.7.3**)

5.7.1. Routing Policy for AT&T Routing to Avaya Aura® Communication Manager

This routing policy is used for inbound calls from AT&T.

Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **ACM62_Public**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.

Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**ACM62_Public**), and click on **Select** (not shown).

Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

28 of 87
SM63CM62SBCETF

Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, if multiple Time Ranges were selected, user may enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on **Commit**.

Step 8 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

Step 9 - No **Regular Expressions** were used in the reference configuration.

Step 10 - Click on **Commit**.

Routing Policy Details   Commit Cancel

General

* Name:	ACM62_Public
Disabled:	☐
* Retries:	0
Notes:	from AT&T

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM62_public	192.168.67.202	CM	

Time of Day

Add   Remove   View Gaps/Overlaps

1 Item | Refresh   Filter: Enable

☐	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	1	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add   Remove

Filter: Enable

☐	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Select : All, None

Regular Expressions

Add   Remove

0 Items | Refresh   Filter: Enable

☐	Pattern	Rank Order	Deny	Notes

Commit Cancel

5.7.2. Routing Policy for Local Routing to/from Avaya Aura® Communication Manager

This routing policy is used for Avaya Messaging Message Wait Indicator (MWI) notification to Communication Manager, Avaya Messaging outbound dialing, and access to/from SIP phones. Repeat the steps in **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing local calls to Communication Manager (e.g. **ACM62_Local**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local SIP Entity (e.g. **ACM62_Local**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details   Commit Cancel

General

* **Name:** ACM62_Local

Disabled: ☐

* **Retries:** 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM62_local	192.168.67.202	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh   Filter: Enable

	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0		24/7		✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

2 Items | Refresh   Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Select : All, None

Regular Expressions

Add Remove

0 Items | Refresh   Filter: Enable

	Pattern	Rank Order	Deny	Notes

5.7.3. Routing Policy for Inbound Routing to Avaya Aura® Messaging

This routing policy is used for Call Coverage from Communication Manager to Avaya Messaging, as well as inbound calls to Avaya Messaging, for message retrieval. Repeat **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Avaya Messaging (e.g. **To_AAM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.5** for Avaya Messaging (e.g. **AA-M**), and click on **Select**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details   [Commit] [Cancel]

General

* Name:	To_AAM
Disabled:	☐
* Retries:	0
Notes:	

SIP Entity as Destination

[Select]

Name	FQDN or IP Address	Type	Notes
AA-M	192.168.67.147	Modular Messaging	

Time of Day

[Add] [Remove] [View Gaps/Overlaps]

1 Item | Refresh   Filter: Enable

	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

[Add] [Remove]

Filter: Enable

	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Select : All, None

Regular Expressions

[Add] [Remove]

0 Items | Refresh   Filter: Enable

	Pattern	Rank Order	Deny	Notes

5.8. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:
- Inbound PSTN calls via the AT&T IP Toll Free service to Communication Manager stations/agents.
- Inbound PSTN calls for message retrieval, via Avaya Messaging pilot extension defined on Communication Manager.
- Message Wait Indicator (MWI) from Avaya Messaging to Communication Manager.

5.8.1. Matching Inbound PSTN Calls to Avaya Aura® Communication Manager

In the reference configuration inbound calls from the AT&T IP Toll Free service used the 10 digit pattern 00000xxxxx in the SIP Request URI. This pattern is matched for further call processing.

> **Note** – Be sure to match on the digit string specified in the Request URI of the inbound Invite, not the digit string that was dialed. They may be different.

Step 1 - In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** (not shown).

Step 2 - In the **General** section of the **Dial Pattern Details** page, provision the following:
- **Pattern** – In the reference configuration, AT&T sends a 10 digit number in the Request URI with the format 00000xxxxx. Enter **00000**. Note - The adaptation defined for Communication Manager in **Section 5.3.1** will convert the various DNIS numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the SIP Domain defined in **Section 5.1** or **-ALL-**, to select all of the administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if **-ALL-** is selected) can match this Dial Pattern.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

32 of 87
SM63CM62SBCETF

Step 3 – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Main** see **Section 5.2.1**). Note that only those calls that originate from the selected Location(s), or all administered Locations if **-ALL-** is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7.1** (e.g., **ACM62_Public**).

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

Filter: Enable

☐	Name	Notes
■	Main	

Select : All, None

Routing Policies

Filter: Enable

☐	Name	Disabled	Destination	Notes
☐	ACM62_Local	☐	ACM62_local	
■	ACM62_Public	☐	ACM62_public	from AT&T
☐	A-SBCE_to_ATT	☐	A-SBCE	
☐	To_AAM	☐	AA-M	

Select : All, None

[Select] [Cancel]

Step 6 - In the Originating Location and Routing Policy List page, click on **Select**.

Step 7 - Returning to the Dial Pattern Details page click on **Commit**.

Notes: ATT Production inbound 7 digits

Originating Locations and Routing Policies

[Add] [Remove]

1 Item | Refresh

Filter: Enable

☐	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Main		ACM62_Public	1	☐	ACM62_public	from AT&T

Select : All, None

Denied Originating Locations

[Add] [Remove]

0 Items | Refresh

Filter: Enable

☐	Originating Location		Notes

[Commit] [Cancel]

Step 8 - Repeat **Steps 1-7** for any additional inbound dial patterns.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

33 of 87
SM63CM62SBCETF

5.8.2. Matching Inbound Calls to Avaya Aura® Messaging Pilot Extension via Avaya Aura® Communication Manager

Communication Manager stations cover to the Avaya Messaging pilot extension (**36000** in the reference configuration). Additionally stations may dial this pilot extension to retrieve messages or modify mailbox settings. Repeat **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to Avaya Messaging (e.g. **36000**).
- Enter a **Min** and **Max** pattern of **5**.
- In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to "**Apply The Selected Routing Policies to All Originating Locations**" (not shown).
- In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox (not shown) corresponding to the Routing Policy administered for routing calls to Avaya Messaging in **Section 5.7.3** (e.g., **To_AA-M**).

Dial Pattern Details
General

* Pattern:	36000
* Min:	5
* Max:	5
Emergency Call:	☐
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	AA-M Pilot Number

Originating Locations and Routing Policies

[Add] [Remove]
1 Item | Refresh   Filter: Enable

	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	To_AA-M	0	☐	AA-M	

Select : All, None

Denied Originating Locations

[Add] [Remove]
0 Items | Refresh   Filter: Enable

	Originating Location	Notes
☐		

* **Input Required**   [Commit] [Cancel]

5.8.3. Message Wait Indicator (MWI) Notification from Avaya Aura® Messaging to Avaya Aura® Communication Manager

Avaya Messaging signals MWI by sending a SIP Notify message to the associated Communication Manager extension. In addition, this entry covers routing of calls to Avaya SIP endpoints. Repeat **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter the Communication Manager extension pattern based on the 5 digit dial plan defined in **Section 6.2**. In the reference configuration, station extensions used the pattern **19xxx**.
- Enter a **Min** and **Max** pattern of **5**.
- In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox (not shown) corresponding to the Location defined in **Section 5.2.1** (e.g., **Main**).
- In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox (not shown) corresponding to the Routing Policy administered for routing calls to Communication Manager local trunk in **Section 5.7.2** (e.g., **ACM62_Local**).

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

35 of 87
SM63CM62SBCETF

6. Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult **[5]** and **[6]** for further details if necessary.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these application notes. Other parameter values may or may not match based on local configurations.

6.1. System Parameters

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

NOTE - **For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.**

Step 1 - Enter the **display system-parameters customer-options** command. On **Page 2** of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

```
display system-parameters customer-options                    Page   2 of  11
                              OPTIONAL FEATURES
IP PORT CAPACITIES                                                 USED
                      Maximum Administered H.323 Trunks: 12000 0
            Maximum Concurrently Registered IP Stations: 18000 4
              Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
                Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                         Maximum Video Capable Stations: 18000 1
                   Maximum Video Capable IP Softphones: 18000 2
                        Maximum Administered SIP Trunks: 24000 24
  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: 300   0
        (NOTE: You must logoff & login to effect the permission changes.)
```

Step 3 - On **Page 4** of the system-parameters customer-options form:
Verify that the **Enhanced EC500?** , **IP Stations?**, **ISDN-PRI?**, **IP Trunks?**, and **ISDN/SIP** fields are set to **y**.

```
display system-parameters customer-options                    Page   4 of  11

                             OPTIONAL FEATURES

    Emergency Access to Attendant? y                          IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                    ISDN Feature Plus? n
                 Enhanced EC500? y      ISDN/SIP Network Call Redirection? y
     Enterprise Survivable Server? n                       ISDN-BRI Trunks? y
        Enterprise Wide Licensing? n                            ISDN-PRI? y
               ESS Administration? y             Local Survivable Processor? n
            Extended Cvg/Fwd Admin? y                  Malicious Call Trace? y
        External Device Alarm Admin? y             Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                 Flexible Billing? n
     Forced Entry of Account Codes? y                 Multifrequency Signaling? y
        Global Call Classification? y         Multimedia Call Handling (Basic)? y
              Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
  Hospitality (G3V3 Enhancements)? y            Multimedia IP SIP Trunking? y
                       IP Trunks? y
             IP Attendant Consoles? y
             (NOTE: You must logoff & login to effect the permission changes.)
```

Step 5 - On **Page 5** of the **System-Parameters Customer-options** form, verify that the **Private Networking** and **Processor Ethernet** fields are set to **y**.

```
display system-parameters customer-options                    Page   5 of  11

                             OPTIONAL FEATURES

                Multinational Locations? n           Station and Trunk MSP? y
  Multiple Level Precedence & Preemption? y      Station as Virtual Extension? y
                     Multiple Locations? n
                                               System Management Data Transfer? n
         Personal Station Access (PSA)? y                Tenant Partitioning? y
                     PNC Duplication? n         Terminal Trans. Init. (TTI)? y
                 Port Network Support? y                Time of Day Routing? y
                     Posted Messages? y         TN2501 VAL Maximum Capacity? y
                                                         Uniform Dialing Plan? y
                 Private Networking? y        Usage Allocation Enhancements? y
        Processor and System MSP? y
                 Processor Ethernet? y                    Wideband Switching? y
                       Remote Office? y                            Wireless? n
        Restrict Call Forward Off Net? y
             Secondary Data Module? y
```

6.2. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

Step 1 - Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings used in the reference configuration:

- 3-digit dial access codes (indicated with a **Call Type** of **dac**) beginning with ***** and **#** for Feature Access Code (FAC) access.
- 5-digit extensions with a **Call Type** of **ext** beginning with:
    1. The digit **1** for Communication Manager stations (the pattern 19xxx was used for stations, with the pattern 1902x reserved for SIP stations).
    2. The digit **3** for Avaya Messaging pilot number (36000).
    3. The digit **4** for Communication Manager VDNs and announcements (4xxxx).
- 3-digit dial access code (indicated with a **Call Type** of **dac**) (e.g., access code **6xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 6.7**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g., access code **8** for Automatic Alternate Routing dialing, see **Section 6.10**).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g., access code **9** for outbound Automatic Route Selection dialing, see **Section 6.10**).

```
change dialplan analysis                                         Page    1 of   12

                            DIAL PLAN ANALYSIS TABLE

                                    Location: all           Percent Full: 2
   Dialed    Total   Call     Dialed   Total  Call     Dialed    Total   Call
   String   Length  Type      String   Length Type     String   Length  Type
   1           5     ext
   3           5     ext
   4           5     ext
   6           3     dac
   8           1     fac
   9           1     fac
   *           3     fac
   #           3     fac
```

6.3. IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. Note that a Processor Ethernet (procr) based Communication Manager platform is used in the reference configuration. The Processor Ethernet node name and IP Address (**procr** & **192.168.67.202**) appear automatically based on the address defined during installation (as does the **default** and **procr6** entries). The procr IP address was used to define the Communication Manager SIP Entities in **Section 5.4**.

Step 1 - Enter the **change node-names ip** command, and add a node name and IP address for the
following:
- Session Manager signaling interface (e.g., **SM** and **192.168.67.47**).
- Avaya Messaging (**AAM** and **192.168.67.147**).
- Avaya SBCE private network interface (**A-SBCE** and **192.168.67.120**).

```
change node-names ip                                            Page   1 of 2
IP NODE NAMES
    Name              IP Address
A-SBCE              192.168.67.120
AAM                 192.168.67.147
SM63                192.168.67.47
default             0.0.0.0
procr               192.168.67.202
procr6              ::
```

6.4. IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr)
parameters. The following screen shows the parameters used in the reference configuration.
- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?**
  fields are set to **y**.
- Assign a **Network Region** (e.g., **1**).
- Use default values for the remaining parameters.

```
display ip-interface procr                                      Page   1 of   2
                              IP INTERFACES

                 Type: PROCR
                                                   Target socket load: 1700
       Enable Interface? y                       Allow H.323 Endpoints? y
                                                  Allow H.248 Gateways? y
        Network Region: 1                         Gatekeeper Priority: 5
                              IPV4 PARAMETERS
            Node Name: procr                      IP Address: 192.168.67.202
          Subnet Mask: /24
```

6.5. IP Network Regions

Network Regions are used to group various Communication Manager resources such as codecs,
UDP port ranges, and inter-region communication. In the reference configuration, two network
regions are used, one for local calls and one for AT&T calls.

6.5.1. IP Network Region 1 – Local Region

In the reference configuration, local Communication Manager elements (e.g., procr) as well as
other local Avaya devices (e.g., SIP and IP telephones, Avaya Messaging) are assigned to **ip-network-region 1**.

Step 1 – Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region **1**). This IP network region will be used to represent the local CPE. Populate the form with the following values:
- Enter a descriptive name (e.g., **Local**).
- Enter **customera.com** in the **Authoritative Domain** field.
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min**: – Set to **16384** (**AT&T recommendation**).
- **UDP Port Max**: – Set to **32767** (**AT&T recommendation**).

```
change ip-network-region 1                                      Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location: 1         Authoritative Domain: customera.com
    Name: Local
MEDIA PARAMETERS                      Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                    Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                           IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                    RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

Step 2 - On **page 2** of the form:
- Verify that RTCP reporting and monitoring are set to **y**.

```
change ip-network-region 1                                      Page   2 of  20
                            IP NETWORK REGION
 RTCP Reporting Enabled? y
 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? y
```

Step 3 - On **page 4** of the form:
- Verify that next to region **3** in the **dst rgn** column, the codec set is **1**.
- Next to region **4** in the **dst rgn** column, enter **2** for the codec set (this means region 3 is permitted to talk to region 4 and it will use codec set 2 to do so). The **direct WAN** and **Units** columns will self populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

```
change ip-network-region 1                                       Page   4 of  20

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

6.5.2. IP Network Region 2 – AT&T Trunk Region

In the reference configuration, AT&T SIP trunk calls are assigned to **ip-network-region 2**. Repeat the steps in **Section 6.5.1** with the following changes:

Step 1 – On **Page 1** of the form**:**
- Enter a descriptive name (e.g., **AT&T**).
- Enter **2** for the **Codec Set** parameter.

```
change ip-network-region 2                                       Page   1 of  20
                              IP NETWORK REGION
  Region: 2
Location: 1        Authoritative Domain: customera.com
    Name: ATT
MEDIA PARAMETERS                    Intra-region IP-IP Direct Audio: yes
      Codec Set: 2                  Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                        IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

Step 2 – On **Page 4** of the form:
- Verify that codec set **2** is listed for **dst rgn 3** and **4**.

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

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

6.6. IP Codec Parameters
6.6.1. Codecs for IP Network Region 1 (local calls)

In the reference configuration, IP Network Region 1 uses codec set 1.

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., **1**). On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, **G.729A**, and **G.729B** are included in the codec list. Note that the packet interval size will default to 20ms.

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

Step 2 - On **Page 2** of the ip-codec-set form, set **FAX Mode** to **t.38-standard**.

```
change ip-codec-set 1                                          Page   2 of   2
                        IP Codec Set
                        Allow Direct-IP Multimedia? y
           Maximum Call Rate for Direct-IP Multimedia:  2048:Kbits
    Maximum Call Rate for Priority Direct-IP Multimedia:  2048:Kbits
                   Mode            Redundancy
         FAX       t.38-standard        0
         Modem     off                  0
         TDD/TTY   off                  0
         Clear-channel  n               0
```

6.6.2. Codecs for IP Network Region 2

In the reference configuration IP Network Region **2** uses codec set **2** for calls from AT&T.

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g., **2**). This IP codec set will be used for IPTF calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown, however the order of G.729B and G.729A may be reversed if desired. For G729B and G729A set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms). Let G711MU default to **20**.

```
change ip-codec-set 2                                          Page   1 of   2
                           IP Codec Set

    Codec Set: 2
    Audio         Silence       Frames    Packet
    Codec         Suppression   Per Pkt   Size(ms)
 1: G.729B            n            3         30
 2: G.729A            n            3         30
 3: G.711MU           n            2         20
```

Step 2 - On **Page 2** of the ip-codec-set form, set **FAX Mode** to **t.38-standard**.

```
change ip-codec-set 2                                          Page   2 of   2
                           IP Codec Set
                            Allow Direct-IP Multimedia? y
             Maximum Call Rate for Direct-IP Multimedia:   2048:Kbits
       Maximum Call Rate for Priority Direct-IP Multimedia:  2048:Kbits
                      Mode             Redundancy
       FAX            t.38-standard        0
       Modem          off                  0
       TDD/TTY        off                  0
       Clear-channel  n                    0
```

6.7. SIP Trunks

Two SIP trunks are defined on Communication Manager in the reference configuration:
- AT&T access trunk – SIP Trunk 2
  - o Note that this trunk will use TCP port 5062 as described in **Section 5.5.1**.
- Local trunk for Avaya Messaging and Avaya SIP telephone access – SIP Trunk 1
  - o Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group.

Note – Although TCP and TLS are used as the transport protocols between the Avaya CPE components, the transport protocol used between the Avaya SBCE and the IPTF service is UDP. See the Note in **Section 5.4** regarding the use of TCP and TLS transport protocols in the CPE.

6.7.1. SIP Trunk for AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for IPTF calls. This trunk corresponds to the **ACM62_Public** Entity defined in **Section 5.4.2**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **2**), and provision the following:
- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp** (see the note at the beginning of this section).
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.3**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g., **SM63**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5062**.
- **Far-end Network Region** – Set the IP network region to **2**, as defined in **Section 6.5.2**.
- **Far-end Domain** – Enter **customera.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This initiates Communication Manager to send SIP OPTIONS messages to Session Manager to provide link status.

```
add signaling-group 2                                         Page   1 of   1
                              SIGNALING GROUP

 Group Number: 2                    Group Type: sip
  IMS Enabled? n          Transport Method: tcp
        Q-SIP? n
    IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Near-end Node Name: procr                    Far-end Node Name: SM63
 Near-end Listen Port: 5062                    Far-end Listen Port: 5062
                                             Far-end Network Region: 2
                                      Far-end Secondary Node Name:
Far-end Domain: customera.com
                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload        Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3              IP Audio Hairpinning? n
        Enable Layer 3 Test? y              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **2**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **ATT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **602**).
- **Direction** – Set to **incoming**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **2**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **20**).

```
add trunk-group 2                                            Page   1 of  21
                               TRUNK GROUP

Group Number: 2                      Group Type: sip         CDR Reports: y
  Group Name: ATT                         COR: 1      TN: 1      TAC: 602
   Direction: incoming        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 2
                                                     Number of Members: 20
```

Step 3 - On **Page 2** of the **Trunk Group** form:

- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900**. This entry will actually cause a value of 1800 to be generated in the SIP Session-Expires header.

```
add trunk-group 2                                            Page   2 of  21

Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                          Redirect On OPTIM Failure: 6000
           SCCAN? n                                  Digital Loss Group: 18
               Preferred Minimum Session Refresh Interval(sec): 900
 Disconnect Supervision - In? y  Out? y
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Step 4 - On **Page 3** of the **Trunk Group** form:

- Set N**umbering Format:** to **private**.

Note – Typically a trunk defined as public-ntwrk (see **Step 2** above), will use a public numbering format. However, when a public numbering format is selected, Communication Manager will insert a plus sign prefix. When a private numbering format is specified, Communication Manager does not insert the plus prefix. The IPTF service does not require number formats with plus, so private numbering was used for the public trunk.

```
add trunk-group 2                                             Page   3 of  21
                              TRUNK FEATURES


        ACA Assignment? n            Measured: none    Maintenance Tests? y
        Numbering Format: private

                                          UUI Treatment: service-provider
                                           Replace Restricted Numbers? y
                                          Replace Unavailable Numbers? y
                                  Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
```

Step 5 - On **Page 4** of the **Trunk Group** form:
  - Verify **Network Call Redirection** and **Send Diversion Header** are set to **n** (default).
  - Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPTF service (e.g., **100**).

> **Note** – The IPTF service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, the History Info header is automatically removed from SIP signaling by Session Manager, as part of the AttAdapter (see **Section 5.3.1**). Alternatively, History Info may be disabled here.

```
add trunk-group 2                                             Page   4 of  21
                           PROTOCOL VARIATIONS


                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
       Send Transferring Party Information? n
                     Network Call Redirection? n
                       Send Diversion Header? n
                       Support Request History? y
                  Telephone Event Payload Type: 100
        Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
        Identity for Calling Party Display: P-Asserted-Identity
                              Enable Q-SIP? n
```

6.7.2. Local SIP Trunk (Avaya Aura® Messaging and Avaya SIP Telephones)

This section describes the steps for administering the local SIP trunk to Session Manager. This trunk is used for Avaya Messaging and Avaya SIP station calls. This trunk corresponds to the **ACM62_Local** Entity defined in **Section 5.4.3**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **1**), and repeat the steps in **Section 6.7.1** with the following changes:
  - **Transport Method** – Set to **tls** (see the note at the beginning of this section).
  - **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061** (see the note at the beginning of this section).
  - **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.5.1**.

```
add signaling-group 1                                             Page   1 of   1
                              SIGNALING GROUP


 Group Number: 1                    Group Type: sip
  IMS Enabled? n          Transport Method: tls
        Q-SIP? n
    IP Video? y            Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
    Near-end Node Name: procr                    Far-end Node Name: SM63
 Near-end Listen Port: 5061                   Far-end Listen Port: 5061
                                            Far-end Network Region: 1
Far-end Domain: customera.com      Far-end Secondary Node Name:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3             IP Audio Hairpinning? n
         Enable Layer 3 Test? y              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n       Alternate Route Timer(sec): 6
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **1**). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.7.1** with the following changes:
  - **Group Name** – Enter a descriptive name (e.g., **Local**).
  - **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **601**).
  - **Service Type** – Set to **tie**.
  - **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **1**).

```
add trunk-group 1                                                Page   1 of  21
                              TRUNK GROUP

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: Local                        COR: 1      TN: 1        TAC: 601
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                      Auth Code? n
                                          Member Assignment Method: auto
                                                 Signaling Group: 1
                                                 Number of Members: 20
```

Step 3 - On **Page 2** of the **Trunk Group** form:
  - Configure the same as **Section 6.7.1**.

Step 4 - On **Page 3** of the **Trunk Group** form:
- Configure the same as **Section 6.7.1**.

Step 5 - On **Page 4** of the **Trunk Group** form:
- Set **Telephone Event Payload Type** to the RTP payload type required by the IPTF service (e.g., **100**).
- Use default for all other values.

```
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? n
                    Send Diversion Header? n
                   Support Request History? y
           Telephone Event Payload Type: 100
        Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
        Identity for Calling Party Display: P-Asserted-Identity
                            Enable Q-SIP? n
```

6.8. Private Numbering

In the reference configuration, the private-numbering form is used to:
- a) Convert Communication Manager local extensions to IPTF DNIS numbers, (previously identified by AT&T), for inclusion in any SIP headers directed to the IPTF service via the public trunk (e.g., 2) defined in **Section 6.7.1**.
- b) Define local extension ranges to facilitate call coverage to Avaya Messaging via the local trunk (e.g., 1) defined in **Section 6.7.2**.

Step 1 - Using the **change private-numbering 0** command, enter the following for the messaging pilot number (for the local trunk):
- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension assigned to the Avaya Messaging coverage hunt group defined in **Section 6.11.1** (e.g., **36000**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 2 – Add all Communication Manager local extension patterns (for the local trunk).
- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 6.2** (e.g., **1** and **4**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 3 – Add a Communication Manager station extension and its corresponding IPTF DNIS number (for the public trunk):
- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).

- **Ext Code** – Enter the Communication Manager station extension (e.g., **19005**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **0000001050**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 4 – Add a Communication Manager Skill VDN extension and its corresponding IPTF DNIS number (for the public trunk):
- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager station extension (e.g., **44002**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **0000041050**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 5 – Repeat **Steps 3** and **4** for all IPTF DNIS numbers and their corresponding Communication Manager station, Skill, or Agent extensions.

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


Ext Ext           Trk        Private        Total
Len Code          Grp(s)     Prefix         Len
 5  1             1                         5      Total Administered: 10
 5  36000         1                         5         Maximum Entries: 540
 5  4             1                         5
 5  19005         2          0000001050     10
 5  19020         2          0000001051     10
 5  19021         2          0000001052     10
 5  19022         2          0000031053     10
 5  44002         2          0000041050     10
 5  44003         2          0000021050     10
 5  44004         2          0000011050     10
```

6.9. Route Patterns for Local SIP Trunk

Route Patterns are use to direct calls to the Local SIP trunk for access to SIP phones and Avaya Messaging.

This form specifies the local SIP trunk (e.g., 1), based on the route-pattern selected by the AAR table in **Section 6.10** (e.g., calls to the Avaya Messaging pilot number 36000, or SIP phone extensions 1902x).

Step 1 – Enter the **change route-pattern 1** command and enter the following:
- In the **Grp No** column enter 1 for SIP trunk 1 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the Numbering Format column, across from line **1:** enter **unk-unk**.

```
change route-pattern 1                                              Page   1 of   3
                  Pattern Number: 1   Pattern Name: Local Trunk
                            SCCAN? n      Secure SIP? n
   Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
   No          Mrk Lmt List Del  Digits                              QSIG
                            Dgts                                      Intw
1: 1    0                                                             n   user
2:                                                                    n   user
3:                                                                    n   user
4:                                                                    n   user
5:                                                                    n   user
6:                                                                    n   user
    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                     Subaddress
 1: y y y y y n  n           rest                                unk-unk  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
```

6.10. Automatic Alternate Routing (AAR) Dialing

AAR is used to direct coverage calls for Avaya Messaging (36000) to the route pattern defined in
Section 6.9.1.

Step 1 – Enter the following:

- **Dialed String**
  - o Avaya Messaging Pilot Number, enter **36000**.
  - o SIP telephone extension range (see **Section 6.2**), enter **1902** (to match 1902x).
- **Min** & **Max** – Enter **5**.
- **Route Pattern** – Enter **1**.
- **Call Type** – Enter **aar**.

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

         Dialed          Total     Route     Call   Node  ANI
         String          Min  Max  Pattern   Type   Num   Reqd
    1902                 5    5     1         aar          n
    36000                5    5     1         aar          n
```

6.11. Provisioning for Coverage to Aura® Messaging

To provide coverage to Avaya Messaging for Communication Manager extensions, a hunt group is defined using the Avaya Messaging pilot number (e.g., **36000**), as well as a coverage path that is defined to the various stations.

6.11.1. Hunt Group for Station Coverage to Avaya Aura® Messaging

Step 1 – Enter the command **add hunt-group x**, where **x** is an available hunt group (e.g., **1**), and on **Page 1** of the form enter the following:
- **Group Name** – Enter a descriptive name (e.g., **AAM**).
- **Group Extension** – Enter an available extension (e.g., **36000**). Note that the hunt group extension need *not* be the same as the Avaya Messaging pilot number.
- **ISDN/SIP Caller Display** – Enter **mbr-name**.
- Let all other fields default.

```
add hunt-group 1                                          Page   1 of  60
                            HUNT GROUP
              Group Number: 1                          ACD? n
                Group Name: AAM                       Queue? n
           Group Extension: 36000                    Vector? n
                Group Type: ucd-mia         Coverage Path:
                        TN: 1        Night Service Destination:
                       COR: 1                 MM Early Answer? n
             Security Code:             Local Agent Preference? n
    ISDN/SIP Caller Display: mbr-name
```

Step 2 – On **Page 2** of the form enter the following:
- **Message Center** – Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Avaya Messaging pilot number (e.g., **36000**).
- **Voice Mail Handle** – Enter the Avaya Messaging pilot number (e.g., **36000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 6.2** (e.g., **8**).

```
change hunt-group 1                                       Page   2 of  60
                            HUNT GROUP

                    Message Center: sip-adjunct      Routing Digits
       Voice Mail Number       Voice Mail Handle     (e.g., AAR/ARS Access Code)
           36000                   36000                     8
```

6.11.2. Coverage Path for Station Coverage to Avaya Aura® Messaging

After the coverage hunt group is provisioned, it is associated with a coverage path.

Step 1 – Enter the command **add coverage path x**, where **x** is an available coverage path (e.g., **1**), and on **Page 1** of the form enter the following:
- **Point1** – Specify the hunt group defined in the previous section (e.g., **h1**).
- **Rng** – Enter the number of rings before the stations go to coverage (e.g., **4**).
- Let all other fields default.

```
add coverage path 1                                               Page    1 of   1
                               COVERAGE PATH
                   Coverage Path Number: 1
    Cvg Enabled for VDN Route-To Party? n       Hunt after Coverage? n
                      Next Path Number:      Linkage
COVERAGE CRITERIA
    Station/Group Status     Inside Call     Outside Call
             Active?              n               n
              Busy?              y               y
        Don't Answer?           y               y        Number of Rings: 4
             All?               n               n
 DND/SAC/Goto Cover?           y               y
   Holiday Coverage?           n               n
COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1              Rng: 4  Point2:
 Point3:                         Point4:
```

6.11.3. Station/Agent Coverage Path to Avaya Aura® Messaging

The coverage path configured in the previous section is then defined on the station/agent form.

Step 1 – Enter the command **change station xxxxx**, where **xxxxx** is a previously defined station
   (e.g., **19001**), and on **Page 1** of the form enter the following:
   • **Coverage path** – Specify the coverage path defined in **Section 6.11.2**. Note that the
     coverage path field will appear at different positions on the form depending on whether
     agent or station extensions are being provisioned.
Step 2 – Enter the command **change agent xxxxx**, where **xxxxx** is a previously defined agent (e.g.,
   47002), and on **Page 1** of the form enter the following:
   • **Coverage path** – Specify the coverage path defined in **Section 6.11.2**.

```
change station 19001                                             Page    1 of   5
                               STATION
Extension: 19001                    Lock Messages? n              BCC: 0
    Type: 9630                      Security Code:                 TN: 1
    Port: S00000                    Coverage Path 1: 1            COR: 1
    Name: 9630 H323                 Coverage Path 2:              COS: 1
                                    Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
            Loss Group: 19        Personalized Ringing Pattern: 1
                                           Message Lamp Ext: 19001
        Speakerphone: 2-way           Mute Button Enabled? y
    Display Language: english           Button Modules: 0
 Survivable GK Node Name:
         Survivable COR: internal        Media Complex Ext:
  Survivable Trunk Dest? y               IP SoftPhone? n
                                             IP Video? n
                         Short/Prefixed Registration Allowed: default
                                        Customizable Labels? y
change agent-loginID 47002                                       Page    1 of   3
```

```
                         AGENT LOGINID

         Login ID: 47002                                AAS? n
             Name: Agent2                              AUDIX? n
               TN: 1                           LWC Reception: spe
              COR: 1                   LWC Log External Calls? n
    Coverage Path: 1              AUDIX Name for Messaging:
    Security Code:
                                      LoginID for ISDN/SIP Display? y
                                                      Password: 2580
                                      Password (enter again): 2580
                                                   Auto Answer: all
                                             MIA Across Skills: system
                                      ACW Agent Considered Idle: system
                                      Aux Work Reason Code Type: system
                                        Logout Reason Code Type: system
                    Maximum time agent in ACW before logout (sec): system
                                        Forced Agent Logout Time:    :


    WARNING:  Agent must log in again before changes take effect
```

6.12. Call Center Provisioning

The administration of Communication Manager Call Center elements – agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult **[6]** for further details, if necessary. The samples that follow are provided for reference purposes only.

- Agent form – **Page 1**

```
display agent-loginID 47002                              Page   1 of   3
                         AGENT LOGINID
         Login ID: 47002                                AAS? n
             Name: Agent2                              AUDIX? n
               TN: 1                           LWC Reception: spe
              COR: 1                   LWC Log External Calls? n
    Coverage Path: 1              AUDIX Name for Messaging:
    Security Code:                LoginID for ISDN/SIP Display? n
                                                      Password: 2580
                                      Password (enter again): 2580
                                                   Auto Answer: station
                                             MIA Across Skills: system
                                      ACW Agent Considered Idle: system
                                      Aux Work Reason Code Type: system
                                        Logout Reason Code Type: system
                    Maximum time agent in ACW before logout (sec): system
                                        Forced Agent Logout Time:    :
```

- Agent form – **Page 2**

```
display agent-loginID 47002                                    Page    2 of   3
                              AGENT LOGINID
     Direct Agent Skill:                              Service Objective? n
Call Handling Preference: skill-level           Local Call Preference? n
   SN   RL SL          SN   RL SL          SN   RL SL          SN   RL SL
 1: 2        1
 2:
```

- Skill 2 Hunt Group form – **Page 1**

```
display hunt-group 2                                           Page    1 of   4
                              HUNT GROUP
            Group Number: 2                              ACD? y
              Group Name: Skill2                       Queue? y
         Group Extension: 43002                       Vector? y
              Group Type: ead-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:              Local Agent Preference? n
 ISDN/SIP Caller Display:
             Queue Limit: unlimited
 Calls Warning Threshold:       Port:
  Time Warning Threshold:       Port :
```

- Skill 2 VDN form – **Page 1**

```
display vdn 44002                                              Page    1 of   3

                        VECTOR DIRECTORY NUMBER

                     Extension: 44002
                         Name*: Skill2
                   Destination: Vector Number       2
            Attendant Vectoring? n
           Meet-me Conferencing? n
            Allow VDN Override? n
                           COR: 1
                           TN*: 1
                      Measured: none
     VDN of Origin Annc. Extension*:
                     1st Skill*:
                     2nd Skill*:
                     3rd Skill*:
* Follows VDN Override Rules
```

- Skill 2 Vector form – **Page 1**

```
display vector 2                                               Page   1 of   6

                               CALL VECTOR

    Number: 2                  Name: Skill2
Multimedia? n     Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y   G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 announcement 42002
03 queue-to     skill 2    pri m
04 wait-time    10  secs hearing music
05 announcement 42005
06 goto step    3              if unconditionally
07 stop
08
```

7. Avaya Aura® Messaging

In this reference configuration, Avaya Messaging is used to verify DTMF, Message Waiting Indicator (MWI), as well as basic call coverage functionality. The administration for Avaya Messaging is beyond the scope of these Application Notes. Consult **[7]** for further details.

8. Configure Avaya Session Border Controller for Enterprise

Note: Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes.

8.1. Initial Installation/Provisioning

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to **[8]** and **[9]** for additional information.
IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE <u>must</u> be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

In the reference configuration, the Avaya SBCE interface B1 (192.168.64.130) was used for the public interface (toward AT&T), and interface A1 (192.168.67.120) was the private interface.
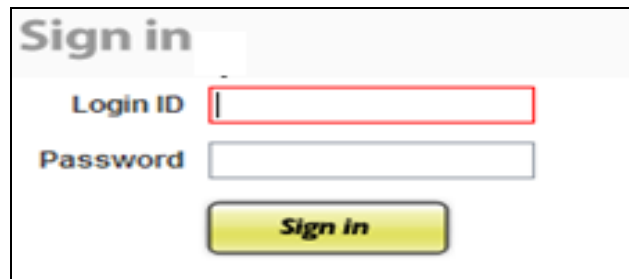
8.2. Log into the Avaya SBCE

The follow provisioning is performed via the Avaya SBCE GUI interface.

1. Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Select **UC-SEC Control Center**.
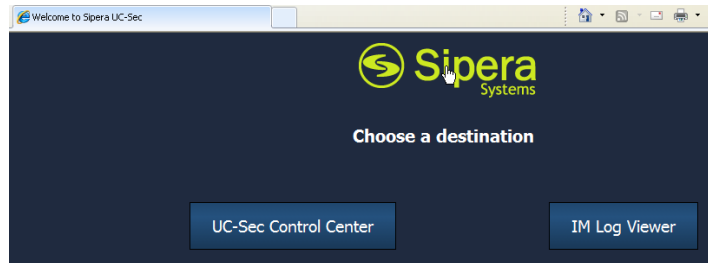
3. Enter the login ID and password.

8.3. Global Profiles

Global Profiles allow for configuration of parameters across all UC-Sec appliances.

8.3.1. Server Interworking – Avaya Side

Server Interworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking**.
3. Select the default profile **avaya-ru** and select the **Clone Profile** button. The **Clone Profile** name window will open (not shown). Enter a profile name (e.g., **Avaya**).
4. Select the **General** Tab, and click on **Edit** (not shown):
    a. Enter profile name**: Avaya_SI**
    b. Check **T38 Support →Yes**
    c. All other options on the General Tab can be left at default
    d. Select **Next**

5. On the **Privacy** window (not shown), select **Next** to accept default values.
6. On the **SIP Timers** window (not shown), select **Next** to accept default values.
7. On the **Advanced Settings** window (not shown), select **Next** to accept default values.
8. Click **Finish** (not shown).

8.3.2. Server Interworking – AT&T Side

Repeat the steps shown in **Section 8.3.1** to add an Interworking Profile for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking**.
3. Select **Add Profile**.
4. On the **General** Tab:
   a. Enter a profile name**:** (e.g., **ATT_SI**)
   b. Check **T38 Support**
   c. All other options on the General Tab can be left at default
   d. Select **Next**
5. At the **Privacy** tab (not shown), select **Next** to accept default values.
6. At the **Interworking Profile** tab (not shown), select **Next** to accept default values.
7. On the **Advanced** Tab (not shown), select **Next** to accept default values.
8. Click **Finish**. The completed form is shown below.
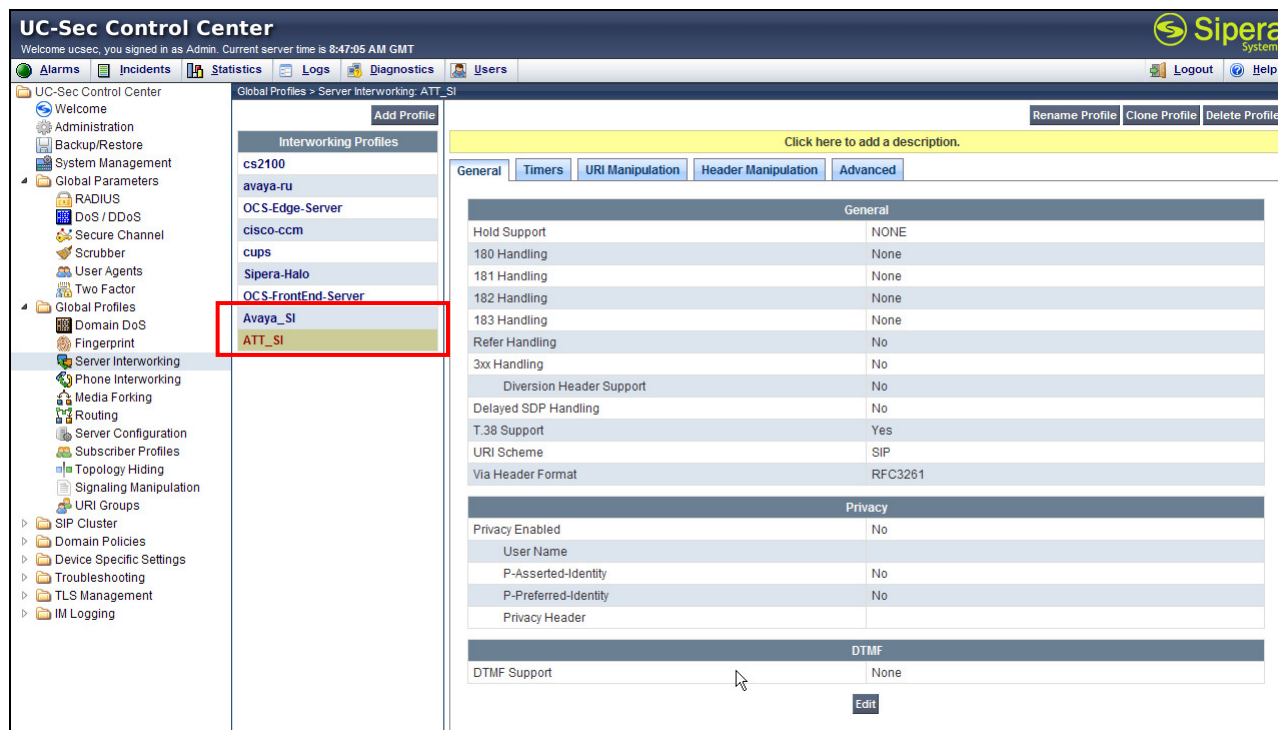
8.3.3. Routing – Avaya Side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select the **Routing** tab (not shown).
3. Select **Add Profile** (not shown).
4. Enter Profile Name: (e.g., **To_Avaya**).
5. Click **Next** and enter:
    a. **Next Hop Server 1: 192.168.67.47** (Session Manager IP address)
    b. Select **Routing Priority Based on Next Hop Server**
    c. **Outgoing Transport**: TCP
6. Click **Finish**.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

58 of 87
SM63CM62SBCETF

8.3.4. Routing – AT&T Side

Repeat the steps in **Section 8.3.3** to add a Routing Profile for the AT&T connection. Note that the AT&T IPTF service provides a Primary and Secondary Border Element.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select the **Routing** tab.
3. Select **Add Profile**.
4. Enter Profile Name: (e.g., **ATT_Production**).
5. Click **Next**, then enter the following:
   a. **Next Hop Server 1: 135.25.29.74** (AT&T Border Element IP address)
   b. Select **Routing Priority Based on Next Hop Server**
   c. **Outgoing Transport**: **UDP**
6. Click **Finish**.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

59 of 87
SM63CM62SBCETF

8.3.5. Server Configuration – To Avaya Aura® Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**, and select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **Avaya_SC**) and select **Next**.
3. The **Add Server Configuration Profile - General** window will Open (not shown).
   a. Select Server Type**: Call Server**
   b. **IP Address: 192.168.67.47** (Session Manager IP Address)
   c. **Supported Transports**: Check **UDP** and **TCP**
   d. **TCP Port: 5060**
   e. **UDP Port: 5060**
   f. Select **Next**
4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
   a. Select **Next** to accept default values.
5. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
   a. Select **Next** to accept remaining default values.
6. The **Add Server Configuration Profile - Advanced** window will open.
   a. For **Interworking Profile** select **Avaya_SI** created in **Section 8.3.1**.
   b. For the **Signaling Manipulation Script** select the **epv_parameter_in_Contact** script defined in **Section 8.3.9**.
   c. Select **Finish**, accepting remaining default values.

The following screen shots show the completed **General** and **Advanced** tabs.
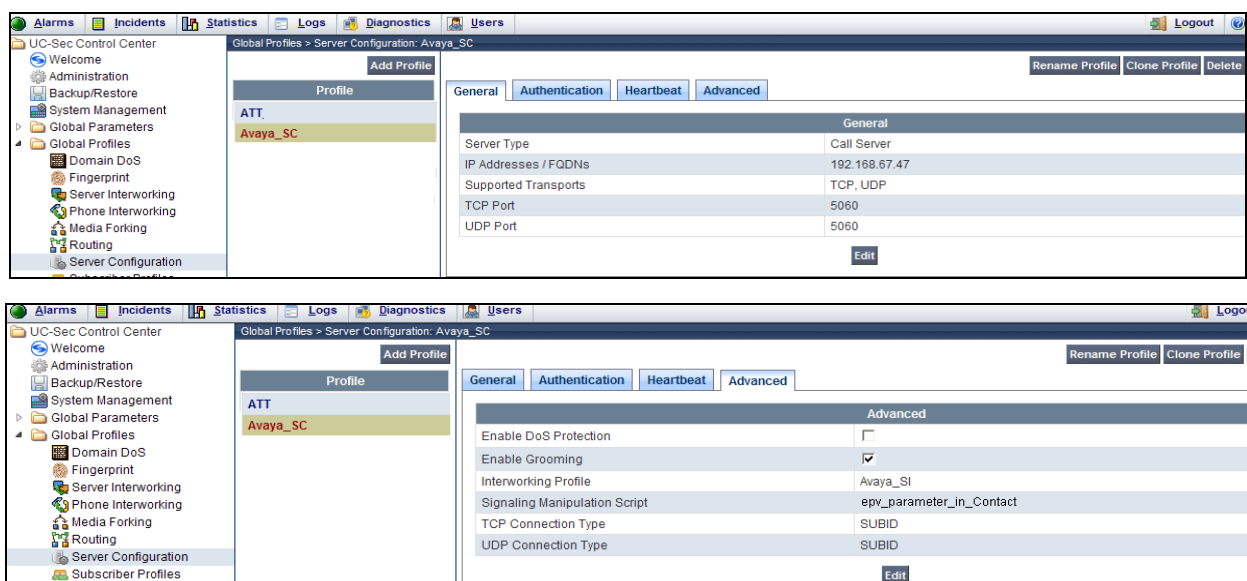
8.3.6. Server Configuration – To AT&T Border Element

Repeat the steps in **Section 8.3.5** to create a Server Configuration for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**.
3. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **ATT**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will Open (not shown).
   a. Select Server Type**: Trunk Server**
   b. **IP Address: 135.25.29.74** (IPTF Border Element IP Address).
   c. **Supported Transports**: Check **UDP**
   d. **UDP Port: 5060**
   e. Select **Next**.
5. The **Add Server Configuration Profile - Authentication** window will open (not shown).
   a. Select **Next** to accept default values.
6. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
   a. Select **Next** to accept default values.
7. The **Add Server Configuration Profile - Advanced** window will open.
   a. Select **ATT_SI** for **Interworking Profile** (created in **Section 8.3.2**).
   b. Select the **Remove_Bandwidth** Signaling Manipulation created in **Section 8.3.9**, **Step 2**.
   c. Select **Finish**.

The following screen shots show the completed **General** and **Advanced** tabs.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

61 of 87
SM63CM62SBCETF
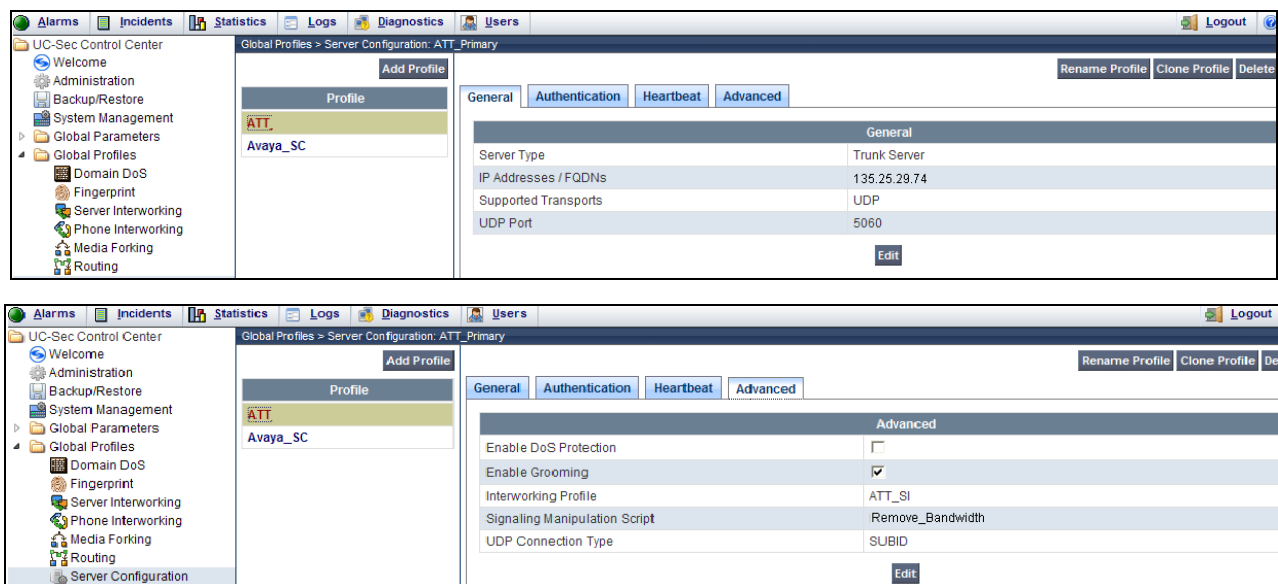
8.3.7. Topology Hiding – Avaya Side

The **Topology Hiding** screen allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.
3. Click **default** profile and select **Clone Profile**.
4. Enter Profile Name: (e.g., **Avaya_TH**).
5. For the Header **To**,
   a. In the **Criteria** column select **IP/Domain**
   b. In the **Replace Action** column select**: Overwrite**
   c. In the **Overwrite Value** column**: customera.com**
6. For the Header **From**,
   a. In the **Criteria** column select **IP/Domain**
   b. In the **Replace Action** column select**: Overwrite**
   c. In the **Overwrite Value** column**: customera.com**
7. For the Header **Request Line**,
   a. In the **Criteria** column select **IP/Domain**
   b. In the **Replace Action** column select**: Overwrite**
   c. In the **Overwrite Value** column**: customera.com**
8. Click **Finish** (not shown).

8.3.8. Topology Hiding – AT&T Side

Repeat the steps in **Section 8.3.7** to create a Topology Hiding Profile for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.
3. Click **default** profile and select **Clone Profile**.
4. Enter Profile Name: (e.g., **ATT_TH**).
5. Set all **Replace Action** to **Auto**.
6. Click **Finish**.

JF; Reviewed:
SPOC 7/29/2013
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.
62 of 87
SM63CM62SBCETF
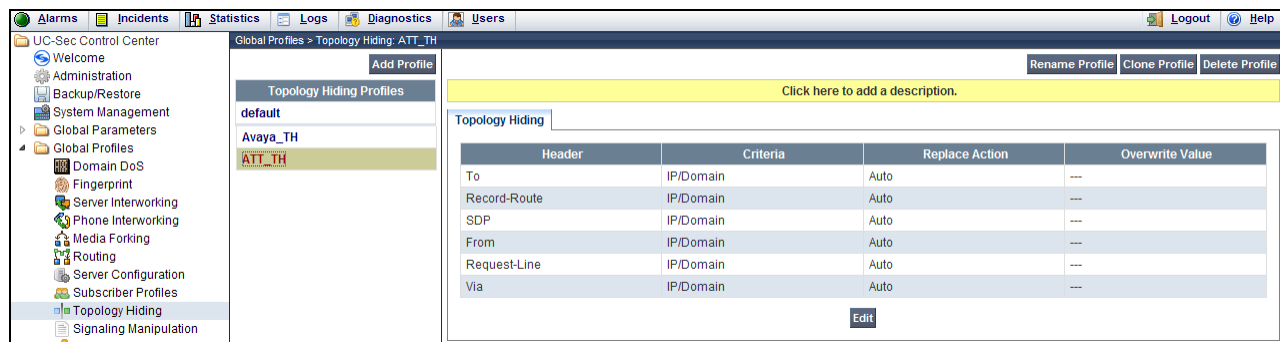
8.3.9. Signaling Manipulation

The Avaya SBCE can manipulate inbound and outbound SIP headers. In the reference configuration, one signaling manipulation scripts is used to remove a header parameter.

> **Note** – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 8.4.3**) does not meet the desired result. Refer to **[9]** for information on the Avaya SBCE scripting language.

Step 1 - As described in **Section 2.2.1**, **Item 3**, Avaya SIP endpoints may send requests with Endpoint-View headers containing private network information. These are removed in **Section 8.4.3**. However an "epv" parameter is also inserted into the Contact header of these requests. This parameter also contains private network information. The following signaling manipulation is used to remove this "epv" parameter from the Contact header.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **epv_parameter_in_Contact**). This script is applied to the Avaya Server Configuration in **Section 8.3.5**, **Step 6**.
5. The following script is defined:

```
Title  epv_parameter_in_Contact

1  // Remove epv paramater from Contact in SIP endpoint Invite
2
3  within session "INVITE"
4  {
5    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6    {
7    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
8    }
9  }
```

6. Click on **Save**. The script editor will test for any errors, and the window will close.

Step 2 - As described in **Section 2.2.1**, **Item 4**, some Avaya SIP endpoints may send Bandwidth headers that may cause issues with the AT&T network. The following signaling manipulation is used to remove these Bandwidth headers.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **Remove_Bandwidth**). This script is applied to the AT&T Server Configuration in **Section 8.3.6**, **Step 2**.
5. The following script is defined:

```
Title  Remove_Bandwidth

 1  // Remove Bandwidth Headers to AT&T (IPXC)
 2
 3  within session "INVITE"
 4  {
 5     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
 6     {
 7     %BODY[1].regex_replace("b=AS:64\r\n","");
 8     %BODY[1].regex_replace("b=CT:64\r\n","");
 9     %BODY[1].regex_replace("b=TIAS:64000\r\n","");
10     }
11  }
```

6. Click on **Save**. The script editor will test for any errors, and the window will close.

8.4. Domain Policies

The Domain Policies feature allows you to configure, apply, and manage various rule sets (policies) to control communications based upon various criteria of sessions, originating from or terminating in the enterprise.

8.4.1. Application Rules

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Application Rules**
3. Select the **default** Rule
4. Select **Clone Rule** button
   a. Name**: new-default**
   b. Click **Finish**
5. Highlight the rule just created: **new-default**
   a. Click the **Edit** button
   b. In the **Voice** row:
      i. Change the **Maximum Concurrent Sessions** to an appropriate amount (e.g., **1000)**
      ii. Change the **Maximum Sessions per Endpoint** to an appropriate amount (e.g.,**1000)**
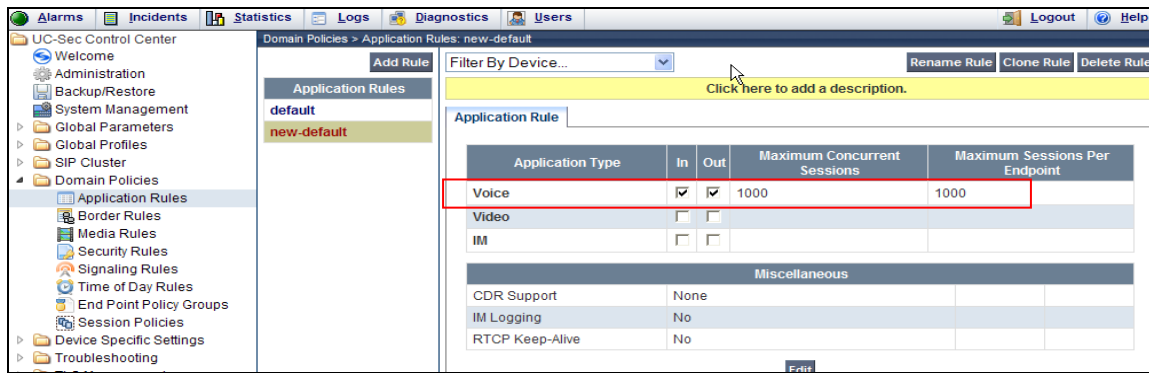
8.4.2. Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed.

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Media Rules** (not shown).
3. The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule
4. Select **Clone Rule** button
   a. Name**: default-low-med-QOS**
   b. Click **Finish**
5. Highlight the rule just created from the Media Rules menu: **default-low-med-QOS**
   a. Select the **Media QOS** tab (not shown).
   b. Click the **Edit** button and the **Media QOS** window will open.
   c. Check the **Media QOS Marking - Enabled**
   d. Select the **DSCP** box
   e. **Audio:** Select **AF11** from the drop-down
   f. **Video**: Select **AF11** from the drop-down
6. Click **Finish**

The screen shot below shows the completed **Media Rules** window.
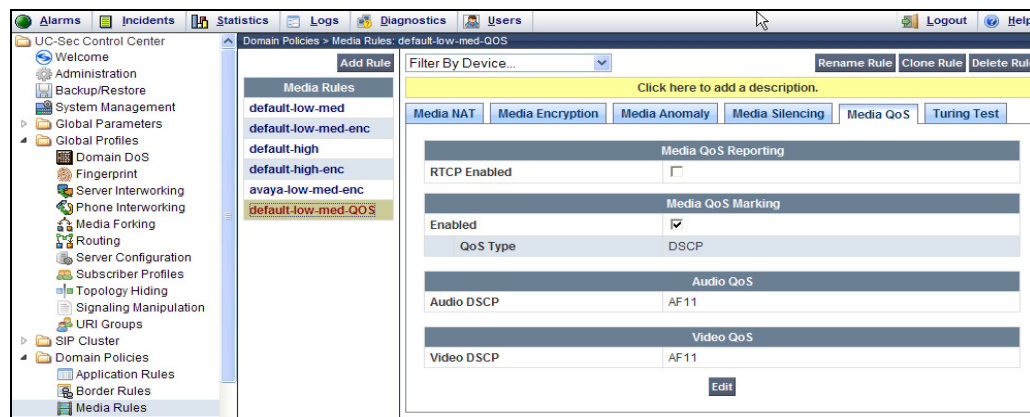
8.4.3. Signaling Rules

Signaling Rules may be used to remove various SIP headers.
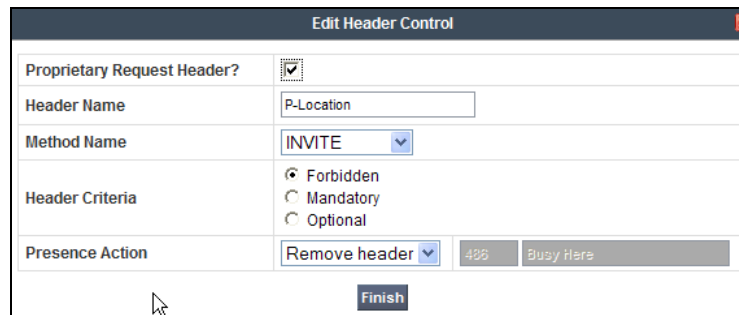
8.4.3.1 Avaya - Requests

The following Signaling Rules remove SIP headers sent by Communication Manager SIP requests that are either not supported by AT&T, (History-Info), or headers that may contain internal CPE information such as IP addresses, domains, extensions, etc (Alert-Info, Endpoint View, AV-Correlation-ID, and P-Location).

> **Note** – In configurations that include Avaya Aura® Session Manager, the History-Info header is removed by Session Manager (see **Section 5.3.1**). Alternatively it may be removed by Communication Manager (see **Section 6.7.1**).

Use the following steps to remove the **P-Location** header:
1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button
   - Enter a name**: Avaya_with_SM**
   - Click **Finish**
5. Highlight the **Avaya_with_SM** rule created in **Step 4** and enter the Following:
   - Select the **Add In Header Control** button (not shown). The Add Header Control window will open.
   - Select the **Request Headers** tab (not shown).
   - Click the **Edit** button and the **Edit Header Control** window will open.
   - Check the **Proprietary Request Header** box.
   - From the **Header Name** menu select **P-Location**.
   - From the **Method Name** menu select **Invite**.
   - For **Header Criteria** select **Forbidden**.
   - From the **Presence Action** menu select **Remove Header**.
6. Click **Finish**

7. Repeat **Steps 5** and **6** to create a rule to remove the **Alert-Info** header.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

66 of 87
SM63CM62SBCETF

- o Click the **Edit** button and the **Edit Header Control** window will open.
- o Verify the **Proprietary Request Header** box is unchecked.
- o From the **Header Name** menu select **Alert-Info**
- o From the **Method Name** menu select **Invite**.
- o For **Header Criteria** select **Forbidden**
- o From the **Presence Action** menu select **Remove Header**.
8. Click **Finish**

9. Repeat **Steps 5** and **6** to create a rule to remove the **Endpoint-View** header
   - o Click the **Edit** button and the **Edit Header Control** window will open.
   - o Check the **Proprietary Request Header** box.
   - o In the **Header Name** field enter **Alert-Info**
   - o From the **Method Name** menu select **Invite**.
   - o For **Header Criteria** select **Forbidden**
   - o From the **Presence Action** menu select **Remove Header**.
10. Click **Finish**

11. Repeat **Steps 5** through **6** to create a rule to remove the **AV-Correlation-ID** header.
    - o Click the **Edit** button and the **Edit Header Control** window will open.
    - o Check the **Proprietary Request Header** box.
    - o In the **Header Name** field enter **AV-Correlation-ID**
    - o From the **Method Name** menu select **Invite**.
    - o For **Header Criteria** select **Forbidden**
    - o From the **Presence Action** menu select **Remove Header**.
12. Click **Finish**

The completed Request Headers form is shown below. Note that the Direction column says "IN".

8.4.3.2 Avaya - Responses

The following Signaling Rules remove **P-Location** and **Endpoint-View** headers sent by Communication Manager SIP responses (e.g., 1xx and/or 200OK).

1. Using the same procedures shown in **Section 8.4.3.1**, the following steps remove the **P-Location** header from **1xx** responses. Highlight the **Avaya_with_SM** rule created in **Section 8.4.3.1** and enter the following:
   - o Select the **Response Headers** tab (not shown).
   - o Click the **Edit** button and the **Edit Header Control** window will open.
   - o Check the **Proprietary Request Header** box.
   - o From the **Header Name** menu enter **P-Location**.
   - o From the **Response Code** menu select **1xx**.
   - o From the **Method Name** menu select **Invite**.
   - o For **Header Criteria** select **Forbidden**.
   - o From the **Presence Action** menu select **Remove Header**.
   - o Click **Finish**
2. Repeat **Step 1** to create a rule to remove the **P-Location** header from **200** responses.
   - o From the **Response Code** menu select **200**.
   - o Click **Finish**.
3. Repeat **Step 1** to create a rule to remove the **Endpoint-View** header from **200** responses.
   - o Select the **Response Headers** tab (not shown).

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

68 of 87
SM63CM62SBCETF

- Select the **Response Headers** tab (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- From the **Header Name** menu enter **Endpoint-View**.
- From the **Response Code** menu select **200**.
- From the **Method Name** menu select **All**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

4. Repeat **Step 3** to remove **Endpoint-View** headers from **1xx** responses.
- From the **Response Code** menu select **1xx**.
- Click **Finish**

The completed Response Headers form is shown below. Note that the Direction column says "IN".

8.4.3.3 Avaya – Signaling QOS

1. Highlight the **Avaya_with_SM** rule created in **Section 8.4.3.1** and enter the following:
- Select the **Signaling QOS** tab (not shown).
- Click the **Edit** button and the **Signaling QOS** window will open.
- Enter a name (e.g., **ATT**, not shown).
- Select **DCSP**.
- Select **Value = AF11**.
2. Click **Finish**

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

69 of 87
SM63CM62SBCETF
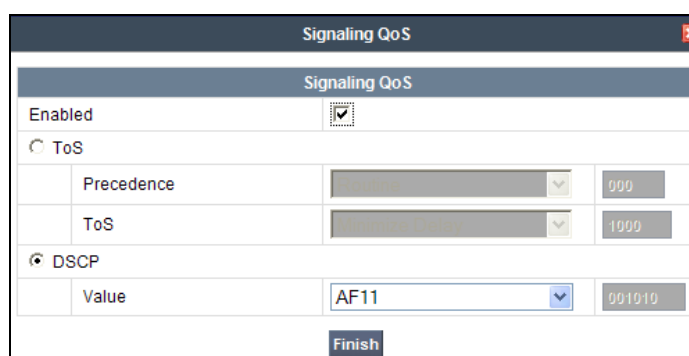
8.4.3.4 AT&T – Signaling QOS
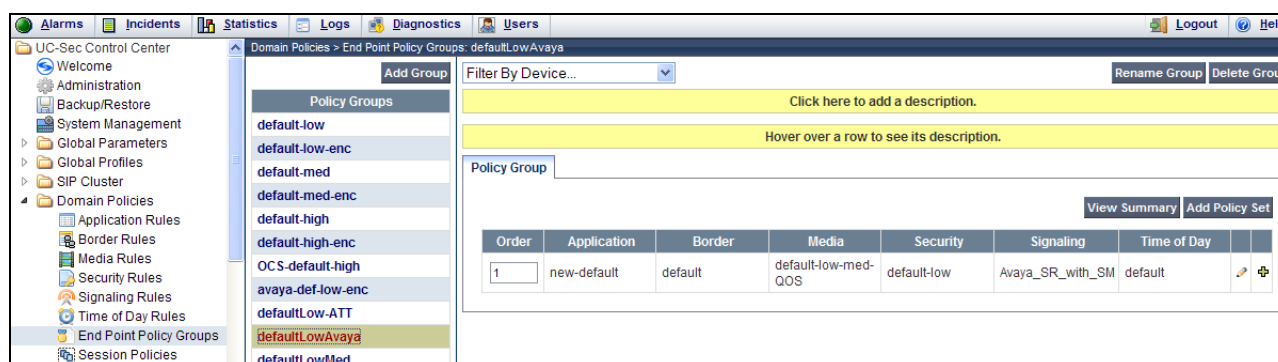
1. Highlight the **ATT** rule created in **Section 8.4.3.3** and enter the following:
   o Select the **Signaling QOS** tab (not shown).
   o Click the **Edit** button and the **Signaling QOS** window will open.
   o Select **DCSP**.
   o Select **Value = AF11**.
2. Click **Finish**

8.4.4. Endpoint Policy Groups – Avaya

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
   a) **Name: defaultLowAvaya**
   b) **Application Rule: new-default**
   c) **Border Rule: default**
   d) **Media Rule: default-low-med-QOS**
   e) **Security Rule: default-low**
   f) **Signaling Rule: Avaya_SR_with_SM**
   g) **Time of Day: default**
4. Select **Finish** (not shown)

8.4.5. Endpoint Policy Groups – AT&T

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
   a. **Name: defaultLow-ATT**
   b. **Application Rule: new-default**
   c. **Border Rule: default**
   d. **Media Rule: default-low-med-QOS**
   e. **Security Rule: default-low**
   f. **Signaling Rule: ATT_SR**
   g. **Time of Day: default**
4. Select Finish (not shown)
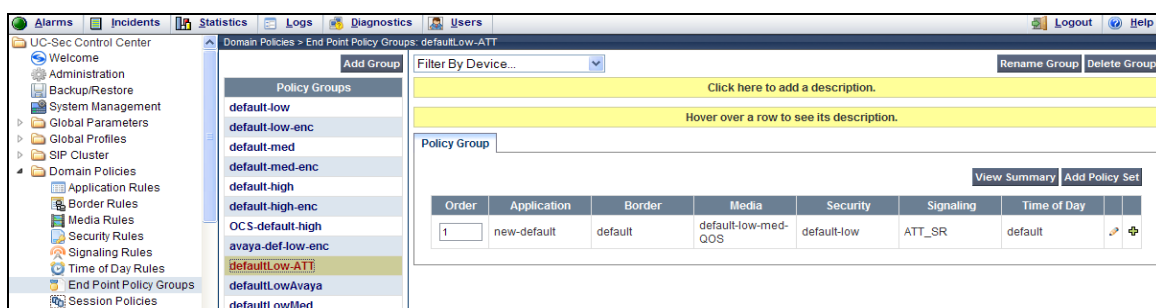
8.5. Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view system information, and manage various device-specific network parameters. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows, and Network Management.

8.5.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
   a) The network interfaces were provisioned during installation. However if these values need to be modified, do so via this tab.
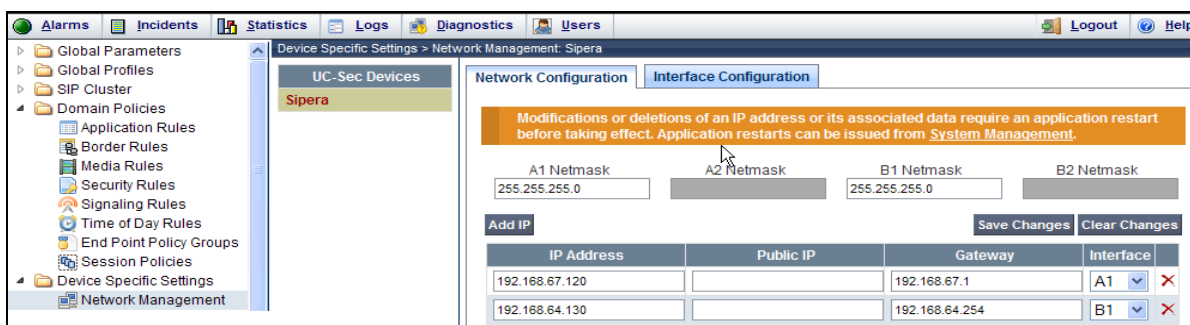
3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab.
    a) Toggle the State of the physical interfaces being used.
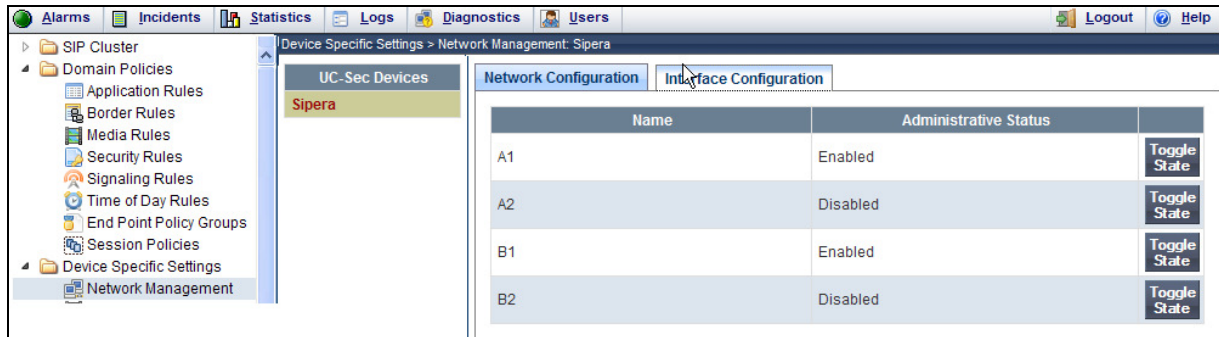
8.5.2. Media Interfaces

AT&T requires customers to use RTP ports in the range of 16384 – 32767. Both inside and outside ports have been changed but only the outside is recommended by AT&T.

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Media Interface**
3. Select **Add Media Interface**
    a) **Name: Media-Inside**
    b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
    c) **Port Range: 16384 - 32767**
4. Click **Finish** (not shown)
5. Select **Add Media Interface**
    a) **Name: Media-Outside**
    b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
    c) **Port Range: 16384 - 32767**
6. Click **Finish** (not shown)
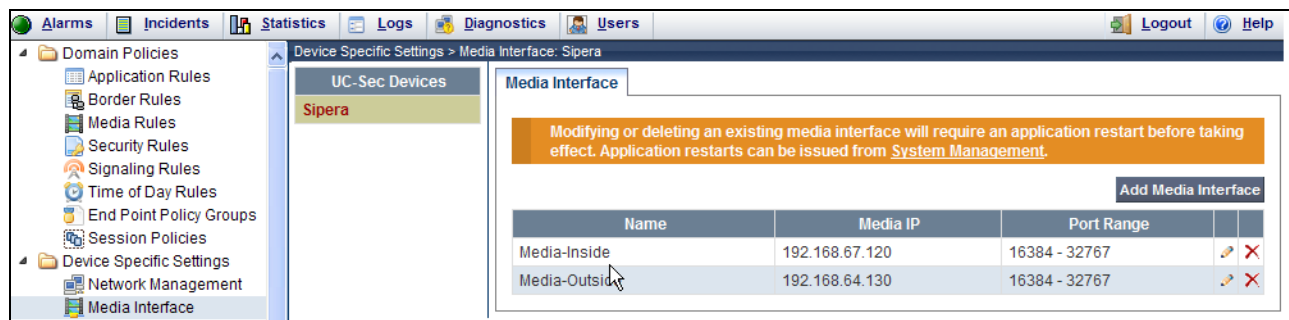
8.5.3. Signaling Interface

Both TCP and UDP transport protocols (ports 5060) are allowed on the CPE network connections (inside), however only UDP transport (port 5060) is supported by AT&T (outside).

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Signaling Interface**
3. Select **Add Signaling Interface**
   a) **Name: Sig-Inside**
   b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
   c) **TCP Port: 5060**
   d) **UDP Port: 5060**
4. Click **Finish**
5. Select **Add Media Interface**
   a) **Name: Sig-Outside**
   b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
   c) **UDP Port: 5060**
6. Click **Finish**
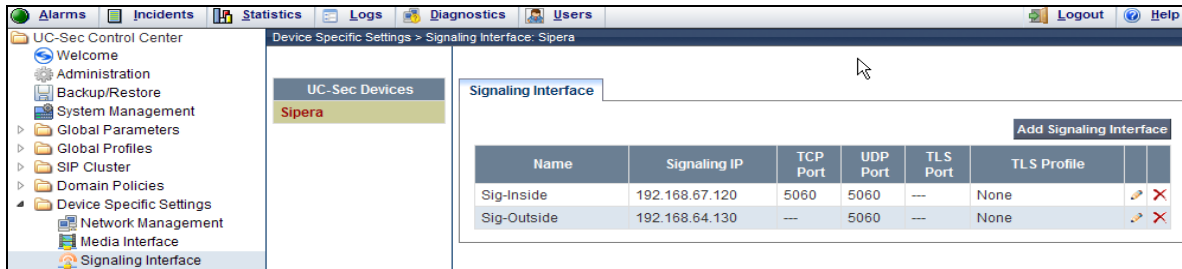
8.5.4. Endpoint Flows – To Avaya (Session Manager)

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add Flow**, and enter the following:
   a) **Name: Avaya**
   b) **Server Configuration**: **Avaya_SC** (**Section 8.3.5**)
   c) **URI Group: ***
   d) **Transport: ***
   e) **Remote Subnet: ***
   f) **Received Interface**: **Sig-Outside**
   g) **Signaling Interface: Sig-Inside**
   h) **Media Interface**: **Media-Inside**
   i) **End Point Policy Group: defaultLowAvaya** (**Section 8.4.4**)
   j) **Routing Profile: ATT_Production** (**Section 8.3.4**)
   k) **Topology Hiding Profile: Avaya _TH** (**Section 8.3.7**)
   l) **File Transfer Profile: None**
5. Click **Finish** (not shown)

8.5.5. Endpoint Flows – To AT&T

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add Flow**, and enter the following:
   a) **Name: ATT**
   b) **Server Configuration: ATT** (**Section 8.3.6**)
   c) **URI Group: ***
   d) **Transport: ***
   e) **Remote Subnet: ***
   f) **Received Interface: Sig-Inside**
   g) **Signaling Interface: Sig-Outside**
   h) **Media Interface: Media-Outside**
   i) **End Point Policy Group**: **defaultLow-att** (**Section 8.4.5**)
   j) **Routing Profile: To_Avaya** (**Section 8.3.3**)
   k) **Topology Hiding Profile: ATT_TH** (**Section 8.3.8**)
   l) **File Transfer Profile: None**
5. Click **Finish** (not shown)
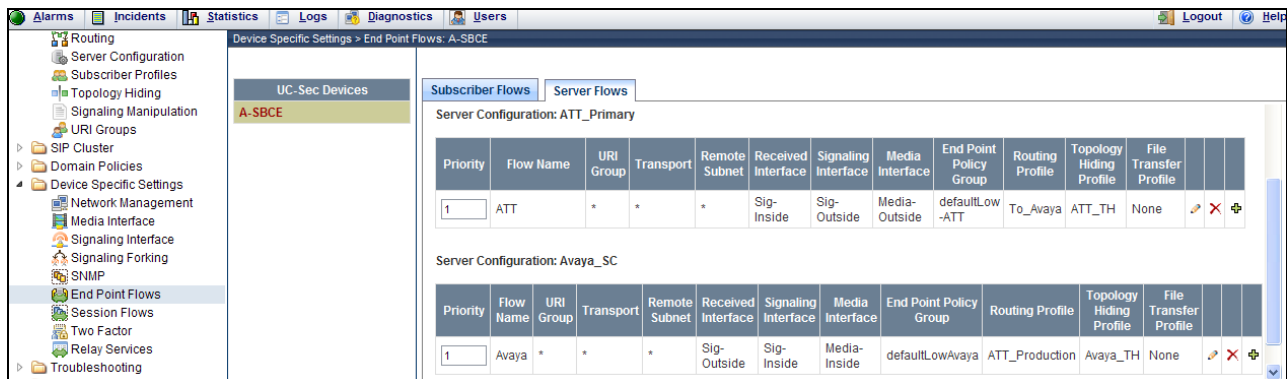
8.6. Troubleshooting Port Ranges

The default port range in this section needs to be changed to exclude the AT&T RTP port range of 16384 – 32767 (**Section 8.5.2**).

1. Select **Troubleshooting** from the menu on the left-hand side
2. Select **Advanced Options**
3. Select **Sipera** in the list of UC-Sec devices
4. Select **the Port Ranges** Tab
   a) **Signaling Port Range: 12000 – 16000**
   b) **Config Proxy Internal Signaling Port Range: 42000 – 51000** (or a range not being used)
5. Click **Save**
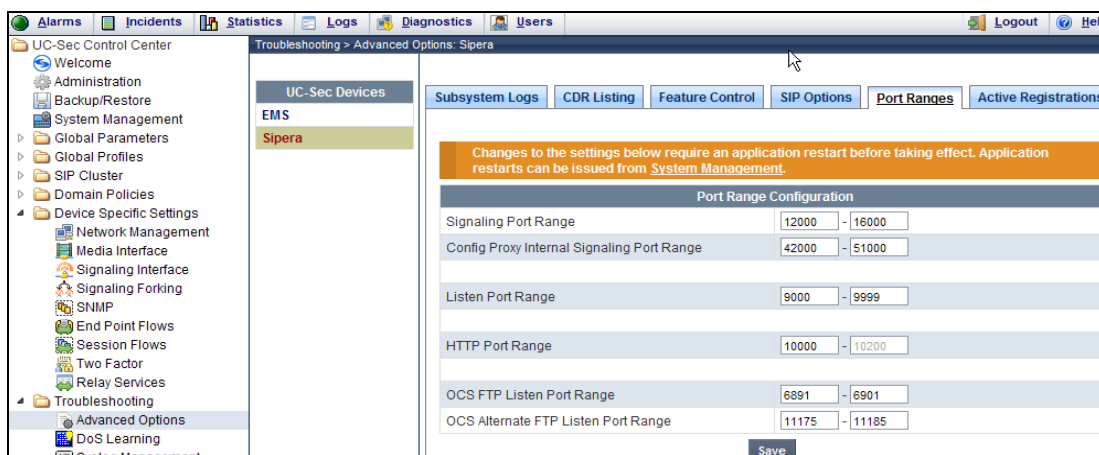
9. Verification Steps

The following steps may be used to verify the configuration:

9.1. AT&T IP Toll Free Service

1. Place an inbound call, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.
4. Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to Avaya Messaging voicemail. Retrieve the message from Avaya Messaging either locally or from PSTN.
5. Using the appropriate IPTF access numbers and DTMF codes, verify that the following IPTF features are successful:
   a. Legacy Transfer Connect DTMF triggered Agent Hold, Conference and Transfer capabilities.
   b. Alternate Destination Routing call redirection capabilities based on Busy, Ring-No-Answer, and other SIP error codes.

9.2. Avaya Aura® Session Manager

Session Manager configurations may be verified via System Manager.

Step 1 - Access the System Manager GUI, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. Once logged in, a Release 6.3 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Session Manager**.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

75 of 87
SM63CM62SBCETF

Step 2 – The Session Manager Dashboard is displayed. In the example below, there are no alarms and all SIP Entities are active (0/4). You may click on any of these columns for further information.

For example, clicking on the **Entity Monitoring** column results in the following display:

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

76 of 87
SM63CM62SBCETF

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: sm63

[Summary View]

Status Details for the selected Session Manager:

Refresh   Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ACM62_local	192.168.67.202	5061	TLS	FALSE	UP	200 OK	UP
○	ACM62_public	192.168.67.202	5062	TCP	FALSE	UP	200 OK	UP
○	AA-M	192.168.67.147	5060	TCP	FALSE	UP	200 OK	UP
○	A-SBCE	192.168.67.120	5060	TCP	FALSE	UP	405 Method Not	UP

Note the **A-SBCE** Entity, from the list of monitored entities. Under normal operating conditions, the **Link Status** should be **Up** as shown by the other displayed entities. The **Reason Code** column indicates that Session Manager has received a SIP **405 Method Not Allowed** response to the SIP OPTIONS it generated. This response normal and is sufficient for SIP Link Monitoring to consider the link up. Also note that the Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T Border Element, and it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends it back to Session Manager.

9.2.1. Call Routing Test

The Call Routing Test verifies the routing for a particular source /destination. To run the routing test, expand **Elements → Session Manager → System Tools → Call Routing Test**. The following example shows an inbound call to Communication Manager from the IPTF service. Note that the Request URI called number was **0000001050** and Session Manager converts this to Communication Manager Skill 2 VDN extension **440002** before routing the call.

Step 1 – **Called Party URI** field = the information passed in the Request URI sent by the Avaya SBCE (e.g., **0000001050@ customera.com**).
Step 2 – **Calling Party Address** field = the IP address of the inside interface of the Avaya SBCE (e.g., **192.168.67.120**).
Step 3 – **Calling Party URI** field = The contents of the From header (e.g., **7325551000@192.168.67.120**).
Step 4 – **Session Manager Listening Port** = **5060** and **Transport protocol** = **TCP** (see the note in **Section 5.4** regarding the use of TCP).
Step 5 – Populate the **Day of Week** and **Time (UTC)** fields, or let them default to current.
Step 6 – Verify that the **Called Session Manager** instance is correct (e.g., sm63).
Step 7 - Click on **Execute Test**.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

77 of 87
SM63CM62SBCETF

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

Called Party URI
0000001050@customera.com

Calling Party URI
7325551000

Day Of Week   Time (UTC)
Monday   19:52

Called Session Manager Instance
sm63

Calling Party Address
192.168.67.120

Session Manager Listen Port
5060

Transport Protocol
TCP

[Execute Test]

The results of the test are shown below. The ultimate routing decision is displayed under the heading **Routing Decisions.** The example shows that a PSTN call to IPFR-EF service, delivering **0000001050** in the Request URI, is sent to Communication Manager VDN extension **44002**. Further down, the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated).Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 5.8**.

Routing Decisions

Route < sip:44002@customera.com > to SIP Entity ACM62_public (192.168.67.202). Terminating Location is Main.

Routing Decision Process

NRP Adaptations: ATT_Production_via_SBCE applied.

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Conference Factory Well-Known URIs: No matches for uri < 0000001050@customera.com >.

Originating Location is Main. Using digits < 0000001050 > and host < customera.com > for routing.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 00000 > Min/Max length 9/10 and domain < customera.com >.

NRP Routing Policies: Ranked destination NRP SIP Entities: ACM521_public, ACM62_public.

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP SIP Entities: ACM62_public.

NRP Dial Patterns: Checking NRP Dial Patterns that specify -ALL- NRP Locations.

NRP Dial Patterns: No matches for digits < 0000001050 > and domain < customera.com >.

NRP Dial Patterns: No matches for digits < 0000001050 > and domain < null >.

NRP Dial Patterns: Chose route matching pattern 00000

END EMERGENCY CALL CHECK: This is not an emergency call.

Adapting and proxying for SIP Entity ACM62_public.

NRP Entity Links: Found direct link to destination. Link uses TCP to port 5062.

NRP Adaptations: ACM62_public applied.

NRP Adaptations: P-Asserted-Identity set to <sip:customera.com>

NRP Adaptations: Request-URI set to sip:44002@customera.com

NRP Adaptations: Request URI set to sip:44002@customera.com

Route < sip:44002@customera.com > to SIP Entity ACM62_public (192.168.67.202). Terminating Location is Main.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

78 of 87
SM63CM62SBCETF

9.3. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See **[5]** for more information.

SIP trunk activity may be monitored by selecting a Trunk Access Code (TAC) associated with a particular SIP trunk. In the reference configuration the SIP trunk used for AT&T access is trunk 2 (see **Section 6.7.1**). This trunk was assigned TAC code 602.

- From the Communication Manager console connection enter the command *list trace tac xxx*, where *xxx* is a trunk access code defined for the SIP trunk to AT&T (e.g., 602). Then place the inbound call. The sample output is shown below.

  Note that Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 19001, before sending the INVITE to Communication Manager.
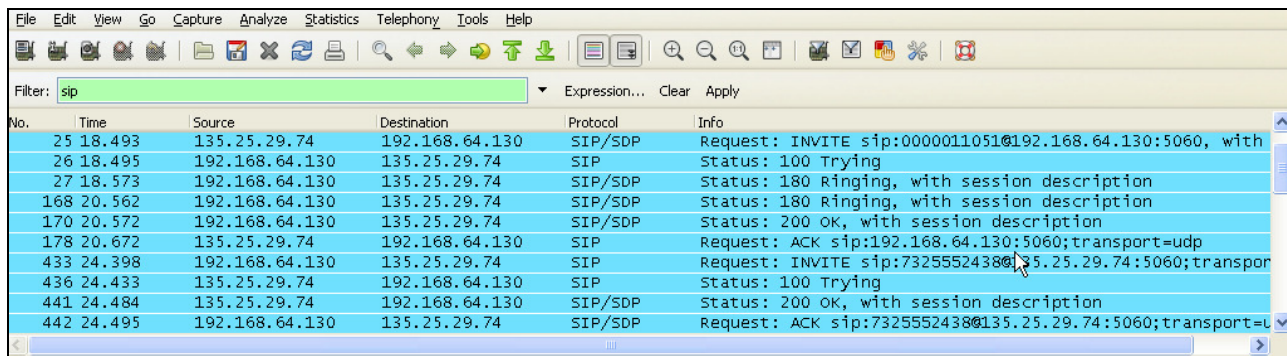
```
list trace tac 602                                                    Page   1
                              LIST TRACE
time            data

15:55:06 TRACE STARTED 04/19/2013 CM Release String cold-02.0.823.0-20396
15:55:16 SIP<INVITE sip:19001@customera.com SIP/2.0
15:55:16     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16     7ok0
15:55:16     active trunk-group 2 member 1    cid 0x2e9
15:55:16 SIP>SIP/2.0 180 Ringing
15:55:16     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16     7ok0
15:55:16     dial 19001
15:55:16     ring station       19001 cid 0x2e9
15:55:16     G711MU ss:off ps:20
             rgn:1 [192.168.67.75]:18828
             rgn:1 [192.168.67.50]:16388
15:55:16     G729B ss:off ps:30
             rgn:2 [192.168.67.120]:16388
             rgn:1 [192.168.67.50]:16392
15:55:16     xoip options: fax:T38 modem:off tty:US  uid:0x5000b
             xoip ip: [192.168.67.50]:16392
15:55:18 SIP>SIP/2.0 200 OK
15:55:18     active station       19001 cid 0x2e9
15:55:18 SIP<ACK sip:7327373940@192.168.67.202:5062;transport=tcp SI
15:55:18 SIP>INVITE sip:192.168.67.120:5060;transport=tcp;gsid=14e31
15:55:18 SIP<SIP/2.0 100 Trying
15:55:18 SIP<SIP/2.0 200 OK
15:55:18 SIP>ACK sip:192.168.67.120:5060;transport=tcp;gsid=14e31350
```

- Similar Communication Manager commands are, *list trace station*, *list trace vdn*, and *list trace vector*. Other useful commands are *status trunk* and *status station*.

9.4. Protocol Traces

Using a SIP protocol analyzer (e.g., Wireshark), monitor the SIP traffic at the Avaya SBCE public outside interface connection to the AT&T IP Toll Free service.
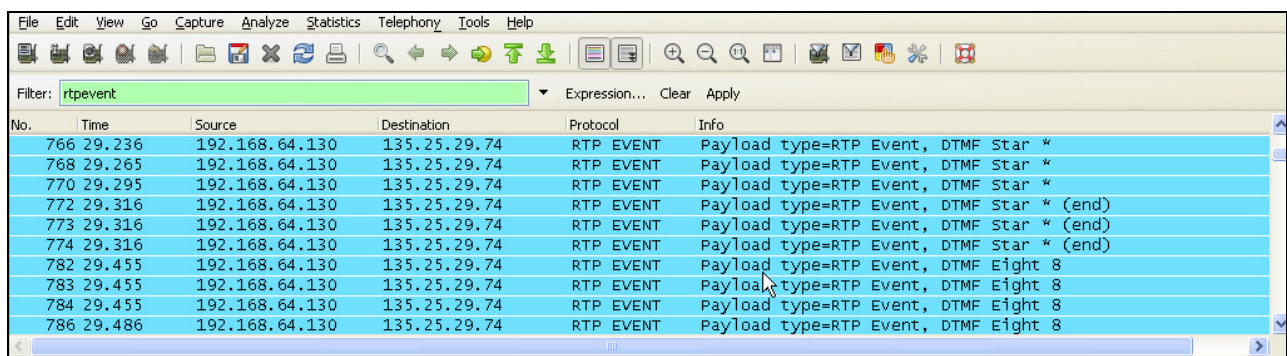
The following is an example of an inbound call filtering on the SIP protocol.

The following is an example of a call filtering on DTMF.

The following is an example of a call filtering on RTP.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

80 of 87
SM63CM62SBCETF

9.5. Avaya Session Border Controller for Enterprise Verification

The Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

Step 2 - Select the **Packet Capture** tab and select the following:

- Select the desired Interface from the drop down menu (e.g., **B1**, the interface to AT&T)
- Specify the Maximum Number of Packets to Capture (e.g., **1000**)
- Specify a Capture Filename.
- Click **Start Capture** to begin the trace.

The capture process will initialize and then display the following status window:

Step 3 – Run the test.

Step 4 - Select **Stop Capture** button shown above.

Step 5 - Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.

Step 6 - Click on the **File Name** link to download the file and use Wireshark to open the trace.
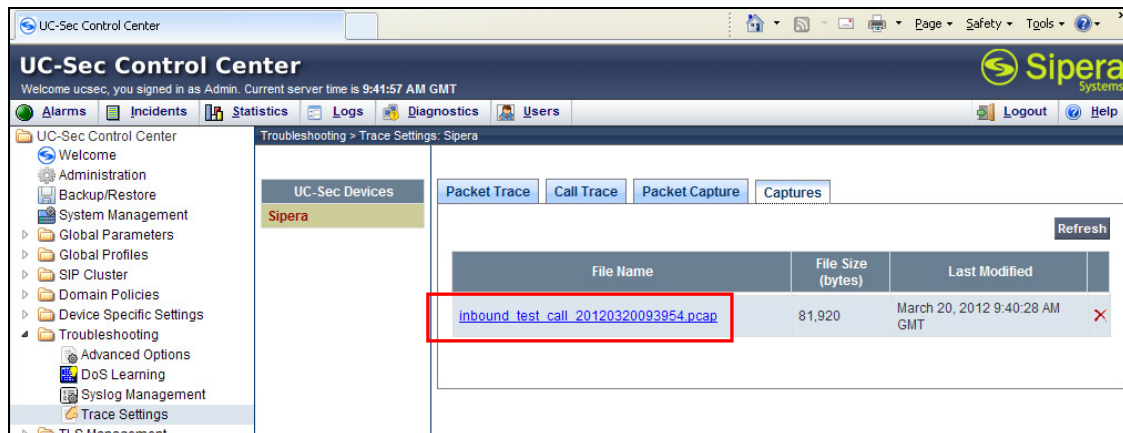
10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.2, and the Avaya Session Border Controller for Enterprise 4.0.5 can be configured to interoperate successfully with the AT&T IP Toll Free service, within the limitations described in **Section 2.2.1**. This solution provides users of Avaya Aura® Communication Manager the ability to support inbound toll free calls over an AT&T IP Toll Free SIP trunk service connection.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

JF; Reviewed:
SPOC 7/29/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

82 of 87
SM63CM62SBCETF

11.   References

The Avaya product documentation is available at http://support.avaya.com unless otherwise noted.

Avaya Aura® Session Manager/System Manager

1. *Administering Avaya Aura® Session Manager,* Release 6.3, December, 2012
2. *Implementing Avaya Aura® Session Manager,* Release 6.3, March, 2013
3. *Implementing Avaya Aura® System Manager,* Release 6.3, Issue 1, December, 2012
4. *Administering Avaya Aura® System Manager,* Release 6.3, Issue 1.0, December, 2012

Avaya Aura® Communication Manager

5. *Administering Avaya Aura® Communication Manager,* Release 6.2 03-300509, Issue 7, December, 2012
6. *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya Aura® Messaging

7. *Administering Avaya Aura® Messaging,* Release 6.2, Issue 2.1, February, 2013

Avaya Session Border Controller for Enterprise
Product documentation for UC-Sec version 4.0.5, can be obtained from Sipera using the link at http://www.sipera.com

8. *E-SBC 1U Installation Guide, Release 4.0.5,* Part Number: 101-5225-405v1.00, Release Date: November 2011
9. *E-SBC Administration Guide, Release 4.0.5,* Part Number: 010-5424-405v1.00, Release Date: November 2011

AT&T IP Toll Free Service Descriptions:

AT&T IP Toll Free Service description - http://www.business.att.com/enterprise/Service/voice-services/contact-center-solutions/ip-toll-free/#

12. Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements

AT&T may provide multiple network border elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to 135.25.29.75 (the primary AT&T trunk connection to 135.25.29.74 is defined in **Section 8.3.6**).

12.1. Step 1: Configure the Secondary Location in Server Configuration

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
   a) **Name: ATT_Secondary**
4. On the **Add Server Configuration Profile – General** tab:
   a) Select **Server Type: Trunk Server**
   b) **IP Address: 135.25.29.75** (Sample address for a secondary location)
   c) **Supported Transports**: Check **UDP**
   d) **UDP Port: 5060**
   e) Select **Finish** (not shown). The completed General tab is shown below.
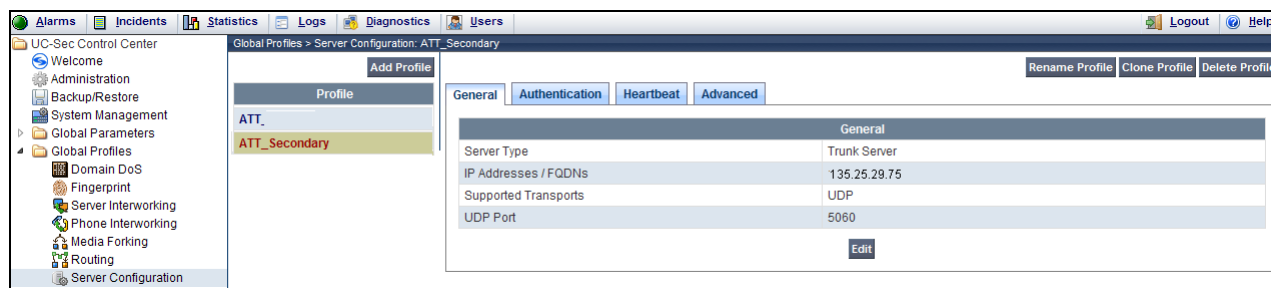
5. On the **Authentication** tab:
   a) Select **Next** (not shown)
6. On the **Heartbeat** tab:
   a) Check **Enable Heartbeat**
   b) **Method: OPTIONS**
   c) **Frequency:** As desired (e.g., 60 seconds).
   d) **From URI: secondary@customera.com**
   e) **To URI: secondary@customera.com**
   f) Select **Next** (not shown)
7. On the **Advanced** Tab
   a) Click **Finish** (not shown). The completed Heartbeat tab is shown below.
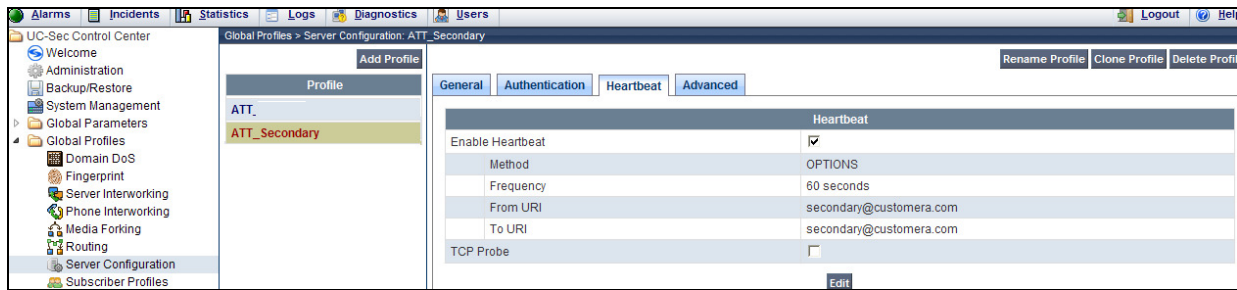
8. Select the Server Configuration created in **Section 8.3.6** (e.g., **ATT**)
9. Select the **Heartbeat Tab**
10. Select **Edit**
11. Repeat **Steps 6 – 7**, but with information for the Primary Trunk as shown below.
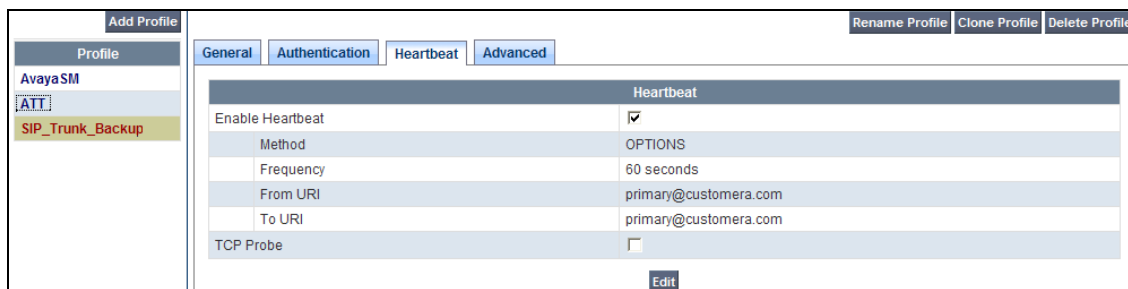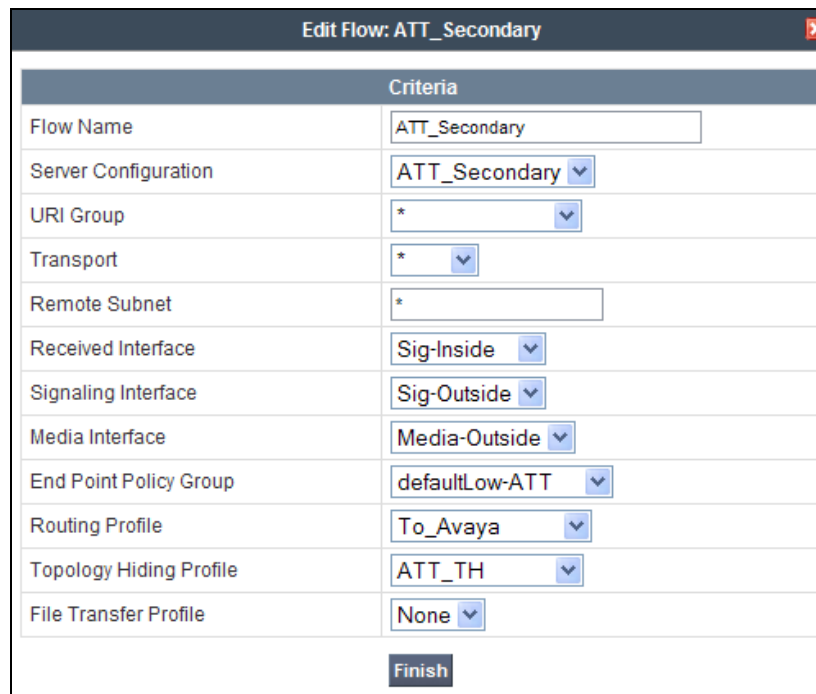

12.2. Step 2: Add Secondary IP Address to Routing

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Routing**
3. Select the routing profile created in **Section 8.3.4** (e.g., **ATT_Production**)
4. Click the pencil icon at the end of the line to edit (not shown)
   a) Enter the IP Address of the secondary location in the **Next Hop Server 2** (e.g., **135.25.29.75**)
5. Click **Finish**
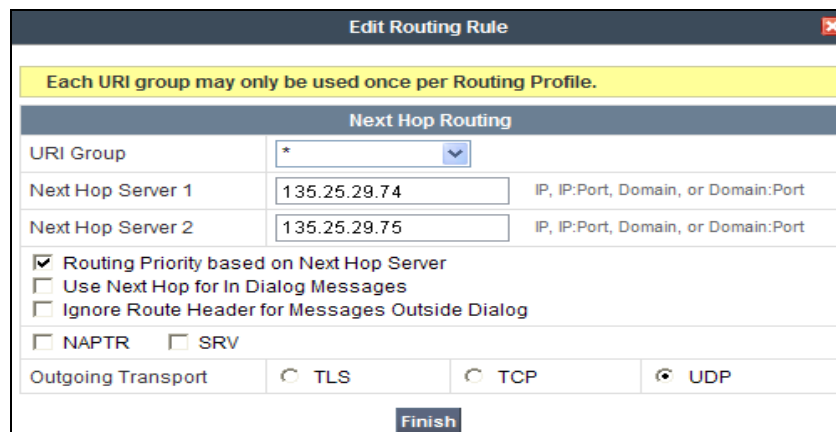
12.3. Step 3: Configure End Point Flows – ATT_Secondary

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** Tab
4. Select **Add Flow**
   a) **Name: Backup**
   b) **Server Configuration: ATT_Secondary**
   c) **URI Group: ***
   d) **Transport: ***
   e) **Remote Subnet: ***
   f) **Received Interface: Sig-Inside**
   g) **Signaling Interface: Sig-Outside**
   h) **Media Interface: Media-Outside**
   i) **End Point Policy Group**: **defaultLow-ATT** (**Section 8.4.5**)
   j) **Routing Profile: To_Avaya** (**Section 8.3.3**)
   k) **Topology Hiding Profile: ATT_TH** (**Section 8.3.8**)
   l) **File Transfer Profile: None**
5. Click **Finish**

Edit Flow: ATT_Secondary	
Criteria	
Flow Name	ATT_Secondary
Server Configuration	ATT_Secondary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-Inside
Signaling Interface	Sig-Outside
Media Interface	Media-Outside
End Point Policy Group	defaultLow-ATT
Routing Profile	To_Avaya
Topology Hiding Profile	ATT_TH
File Transfer Profile	None
	Finish

When completed the Avaya SBCE will issue OPTIONS messages to the primary (135.25.29.74) and secondary (135.25.29.75) border elements.