Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3 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 6.3, and the Avaya Session Border Controller for Enterprise 6.3 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 6.3 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 6.3 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.

TABLE OF CONTENTS

1 Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.3 (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[1].

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 6.3 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya SBCE 6.3 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, (referred to in the remainder of this document as IPTF), is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT 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 s separate document.

2 General Test Approach and Test Results

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

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPTF and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, and the Avaya SBCE (see **Section 3.2** for call flow examples).

2.1 Interoperability Compliance Testing

Note – Documents used to provision the test environment are listed in **Section 10**. In the following sections, references to these documents are indicated by the notation **[x]**, where *x* is the document reference number.

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 IPTF network. Calls were made from the PSTN, across the IPTF network, to the CPE.

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

The following SIP trunking VoIP features were tested with the IPTF service:

- Inbound PSTN/IPTF calls to Communication Manager stations, Vector Directory Numbers (VDNs), Vectors, and Agents.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones/Agents via IPTF.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729A and G.711Mu codecs.
- T.38 fax calls via IPTF to Communication Manager G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833/4733 between Communication Manager and IPTF automated access systems.
- Inbound IPTF service calls to Communication Manager that are routed to Agent queues or directly to Agents.
- IPTF network features such as Legacy Transfer Connect and Alternate Destination Routing (ADR).
- Long duration calls.

2.2 Test Results

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

1. **IP Toll Free ADR Call Redirection feature in response to a ring-no-answer condition.** Depending on the configuration of Communication Manager, the IPTF ADR ring-no answer feature may, or may not work.
    a. If an inbound call is directed to a Communication Manager Agent VDN/Vector skill queue (see **Section 6.13**), Communication Manager will respond with a 180 (or 183 depending on provisioning). In this case, the IPTF ADR ring-no answer feature *will not trigger*.
    b. If an inbound call is sent directly to an Agent extension, Communication Manager returns a 180 in addition to a 181. In this case the IPTF ring-no answer feature *will trigger* and the alternate number is called.
        i. Whether 181 is sent or not is determined by the Direct Agent Calling setting in the Class of Restriction form on Communication Manager (see **Section 6.12**).

2. **G.726-32 codec support** – While Communication Manager supports G.726-32, the IPTF implementation of G.726-32 results in poor audio quality. Therefore, G.726-32 codec is not supported between Communication Manager and the IPTF service.

3. **G.711 and T.38 Fax support** - Communication Manager does not support the protocol negotiation required for G.711 fax to work with the IPTF service. T.38 fax is supported, however in the reference configuration (e.g., using a G430 Media Gateway), connections are limited to 9600. The sender and receiver of a T.38 fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3.

4. **The Avaya SBCE issues a Remote-Address header even though the option to do so is disabled** - During testing it was found that the Avaya SBCE was including a Remote-Address header to Invites, as well as 200OKs, even though the option to do so is disabled by default.
    a. No issues were caused by the inclusion of this header, however the Avaya SBCE was provisioned to remove this header (see **Section 7.3.3**, and **Item 5** below), to reduce overall packet size.

5. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block headers containing private addressing), the Avaya SBCE is provisioned to remove SIP headers not required by the IPTF service (see **Section 7.3.3**, and **item 4** above).

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 6.3 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 9611 Series IP Telephone (running H.323 firmware), a 9641 Series IP Telephone (running SIP firmware), a Avaya 6424 Digital Telephone, as well as Avaya one-X® Agent soft phone (H323).

- The Avaya SBCE 6.3 provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the CPE.
- The IPTF service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya SBCE. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya SBCE (e.g., UDP, TCP, or TLS) and Communication Manager (e.g., TCP or TLS). In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and Communication Manager.
- Inbound calls were placed from PSTN via the IPTF service, through the Avaya SBCE to the Session Manager, which routed the call to Communication Manager. Communication Manager terminated the calls to the appropriate Agent queue, Agent phone, or fax extension.

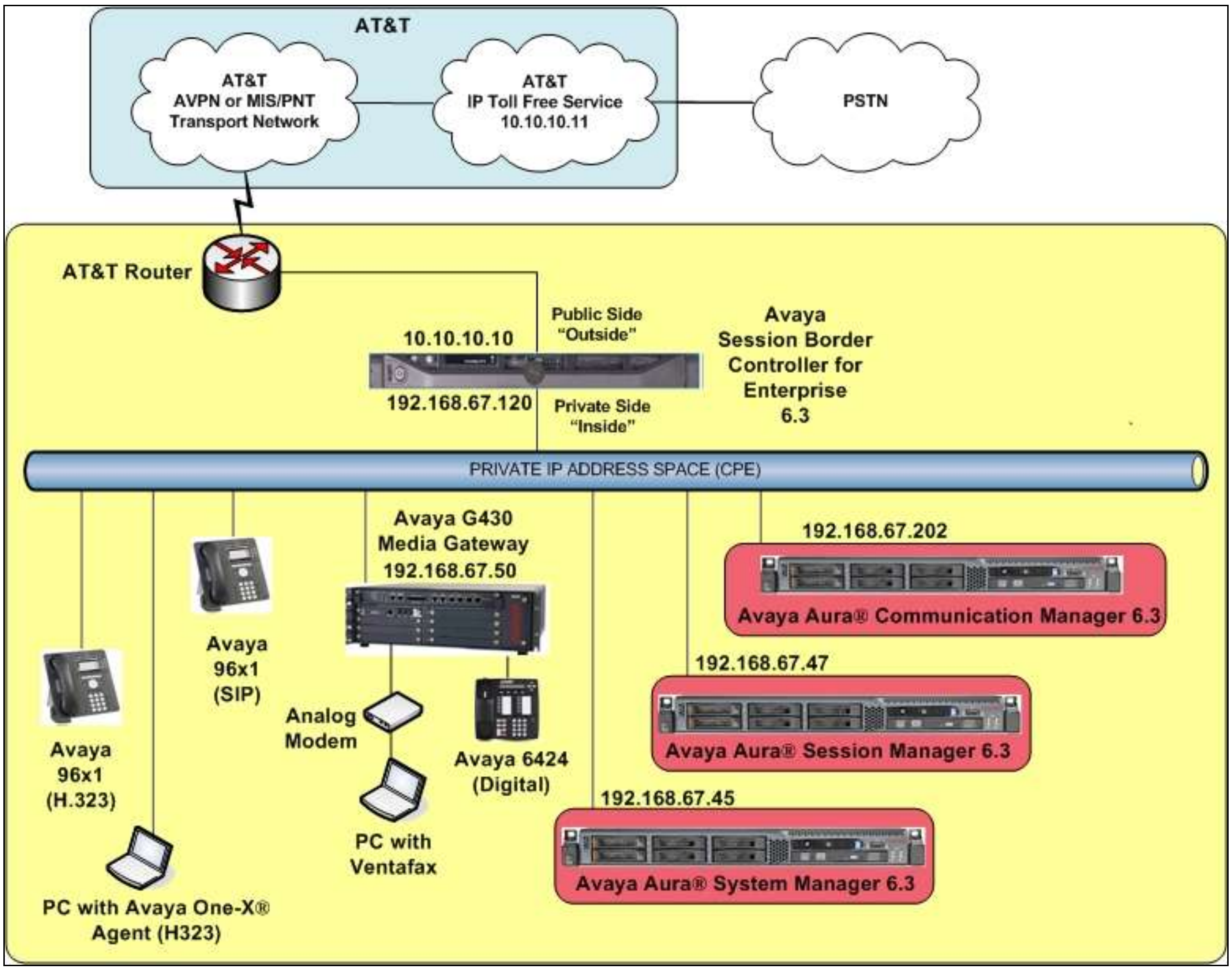


Figure 1: Reference configuration

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 = Agents and Agent skill queue VDNs
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Outside (Public) Interface (to AT&T IP Toll Free Service)	10.10.10.10
IP Address of Inside (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.120
AT&T IP Toll Free Border Element	
IP Address	10.10.10.11

Table 1: Illustrative Values Used in these Application Notes

Note – In the reference configuration, the IPTF service delivered 10 DNIS digits, with the format *00000xxxxx*. These DNIS digits are used in the provisioning defined in the following sections, not the dialed digits.

3.2 Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled by Session Manager and Communication Manager, a general call flow is described below. In **Figure 2** an inbound IPTF service call arrives at Session Manager and is subsequently routed to Communication Manager.

1. A PSTN telephone originates a call to an IPTF service number.
2. The PSTN routes the call to the IPTF service network.
3. The IPTF 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 an Agent queue or telephone.

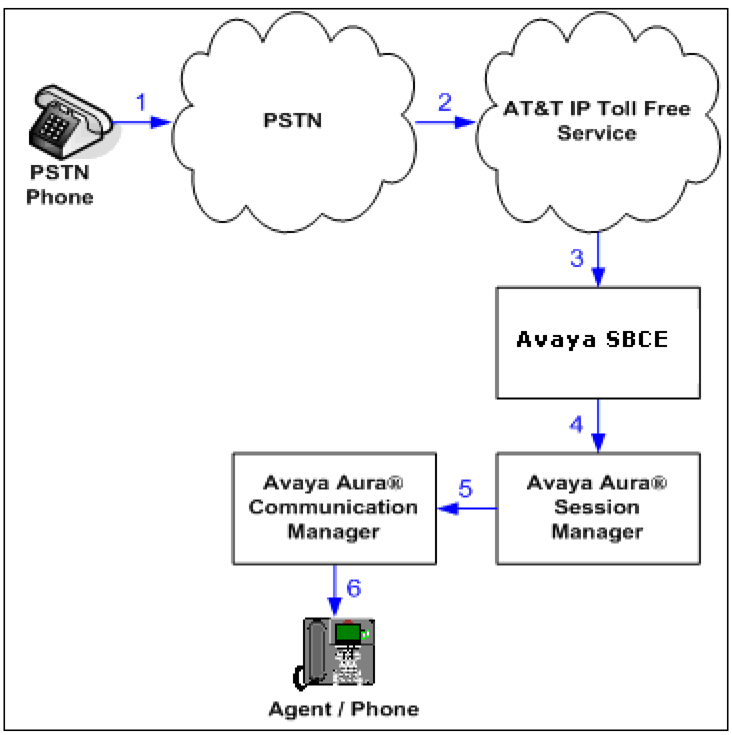


Figure 2: Inbound AT&T IP Toll Free Service Call to an Agent queue/telephone

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

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	 • 6.3.5.01003.0 • 6.3 SP 11 (6.3.11_r4802871)
Avaya 8800 server • Avaya Aura® Session Manager	 • 6.3 SP11 (6.3.11.0.631103)
Avaya 8800 server • System Platform • Avaya Aura® Communication Manager	 • 6.3.5.01003.0 • 6.3 SP8 (03.0.124.0-21588)
Avaya G430 Media Gateway	• g430_sw_36_9_0HW7 FW15
Dell R210 • Avaya Session Border Controller for Enterprise	 • 6.3.1-22-4653
Avaya 96x1 IP Telephones	• H.323 Version 6.4014 • SIP Version 6.4.125
Avaya one-X® Agent (H323)	• 2.5.50022.0
Ventafax Home Version (Windows based Fax device)	• 7.0.202.494

Table 2: Equipment and Software Versions

5 Configure Avaya Aura® Session Manager Release 6.3

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 Aura® Messaging are described.

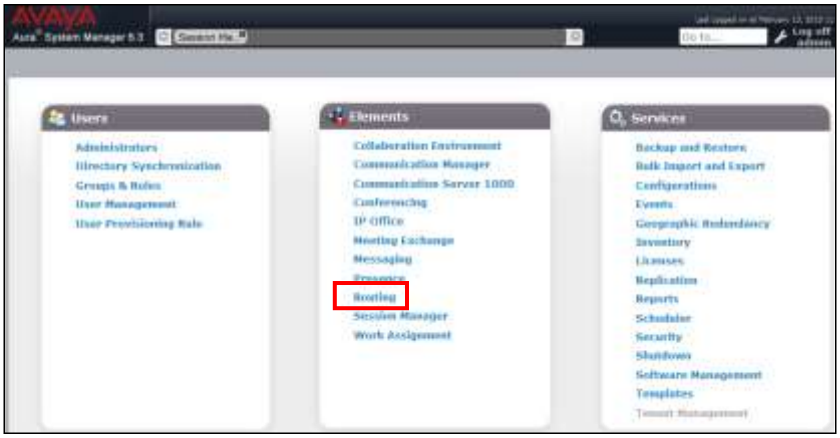
Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented as Entity Links.

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 a SIP Domain
- Define Locations.
- Configure the Adaptation Modules that will be associated with digit manipulations for calls between the SIP Entities for Communication Manager, and the Avaya SBCE.
- Define SIP Entities corresponding to Communication Manager, and the Avaya SBCE.
- Define Entity Links describing the SIP trunk between Communication Manager and Session Manager, and the SIP Trunk between Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, and the Avaya SBCE.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Session Manager 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, **Home** screen is displayed. From the **Home** screen, 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.

Step 3 - Click **Commit** to save (not shown).

5.2 Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, two Locations are specified:

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager, the G430 Media Gateway, and telephones.
- **Common** – This site contains the Avaya SBCE as well as the IPTF access router.

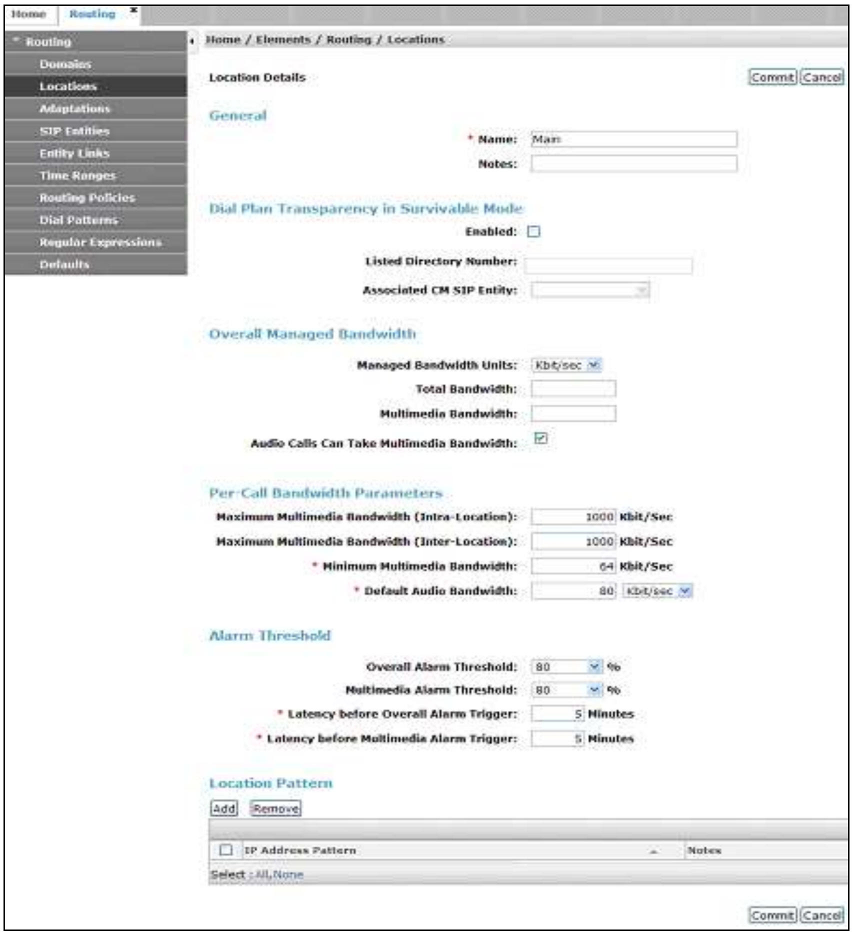
5.2.1 Main Location

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.

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

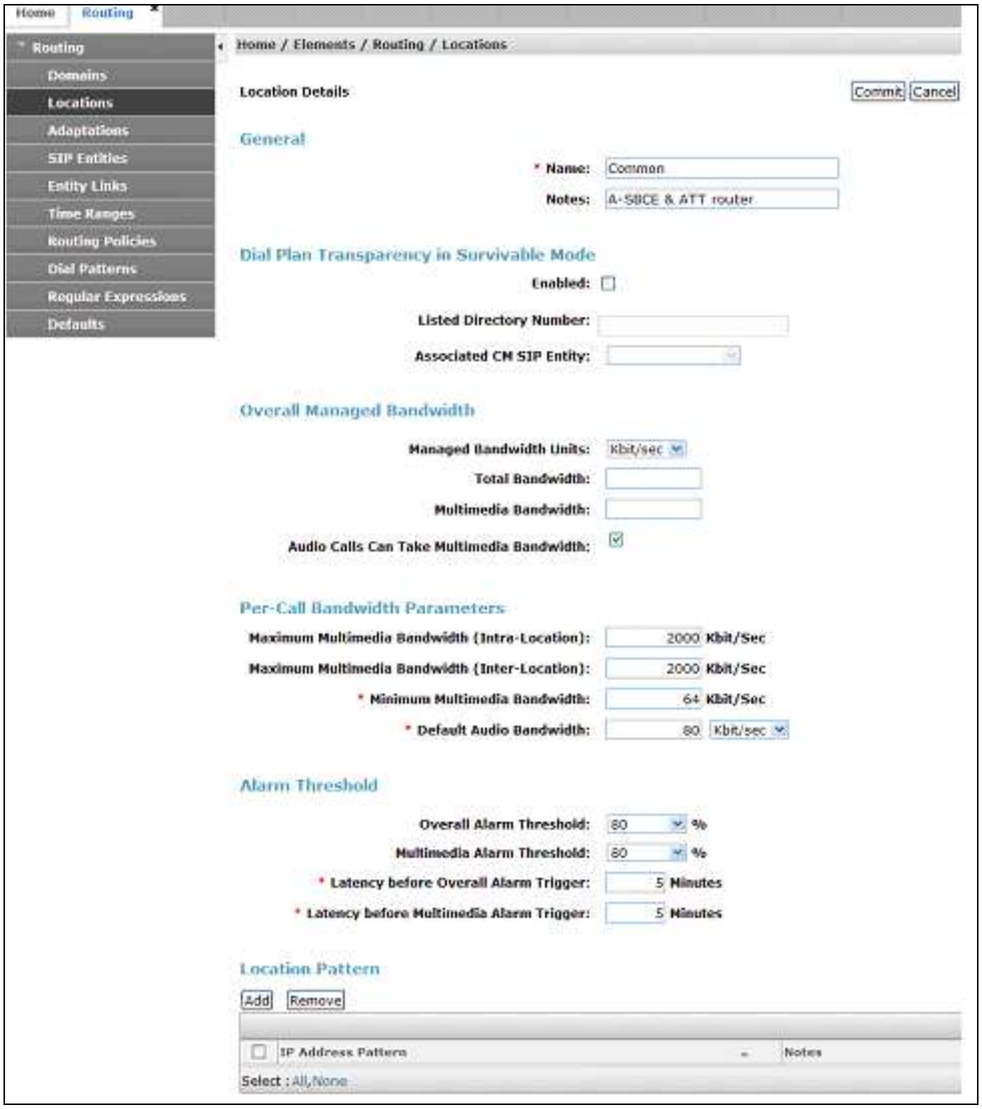
- **IP Address Pattern:** Leave blank.
- **Step 3** - Click **Commit** to save.

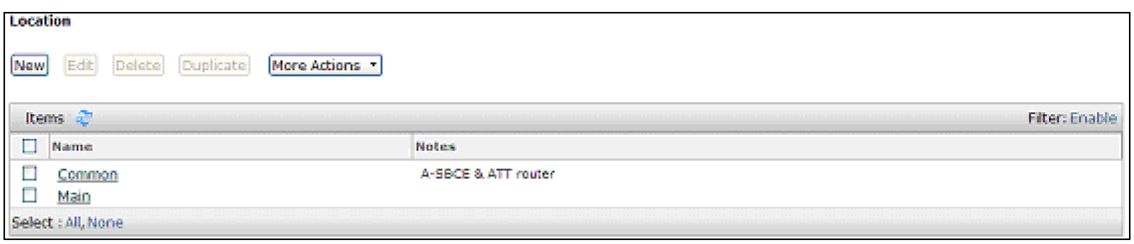


5.2.2 Common Location

Follow the steps from **Section 5.2.1** with the following changes:

- **Name:** Enter a descriptive name for the Location (e.g., **Common**).





5.3 Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent from AT&T to Communication Manager.

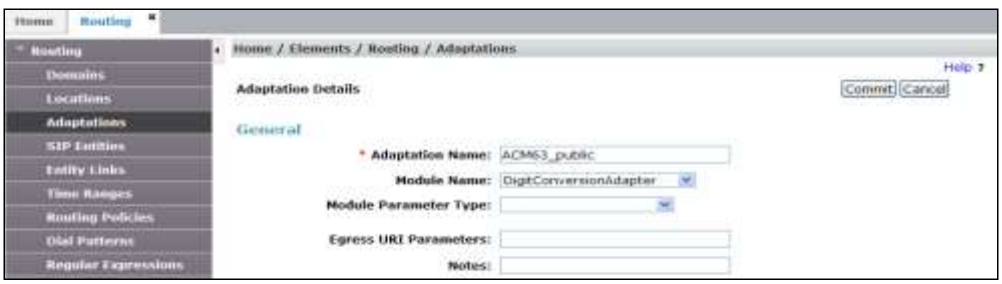
- Calls from AT&T - Modification of SIP messages sent to Communication Manager extensions.
    - The IP address of Session Manager (**192.168.67.47**) is replaced with the Avaya CPE SIP domain (**customera.com**) for destination domain.
    - The AT&T Border Element IP address (**10.10.10.11**) is replaced with **customera.com** for source domain.
    - The AT&T called number digit string in the Request URI is replaced with the associated Communication Manager extensions defined for Agent skill queue VDNs/telephones.

5.3.1 Adaptation for Avaya Aura® Communication Manager Extensions

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., **ACM63_public**).
- 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 their associated Communication Manager extensions before being sent to Communication Manager). 0000012345 is a DNIS string sent in the Request URI by the IPTF service that is associated with Communication Manager Agent/VDN skill queue 44002.

- Enter **0000012345** 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 IPTF DNIS numbers.

Step 5 - Click on **Commit** (not shown).

Digit Conversion for Outgoing Calls from SM

Add Remove

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
	* 0000012345	* 10	* 10		* 10	44002	destination	
	* 0000012346	* 10	* 10		* 10	44003	destination	
	* 0000012347	* 10	* 10		* 10	44004	destination	

Select : All, None

Note – No **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

5.4 SIP Entities

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

Note – The **Entity Links** section of these forms (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

In this section, SIP Entities are administered for the following SIP network elements:

- Session Manager (**Section 5.4.1**). Note that this Entity is normally created during Session Manager installation, but is shown here for completeness.
- 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 the IPTF service to Communication Manager via the Avaya SBCE.
- Communication Manager for local access (**Section 5.4.3**) – This entity, and its 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 IPTF service via the Avaya SBCE.

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).

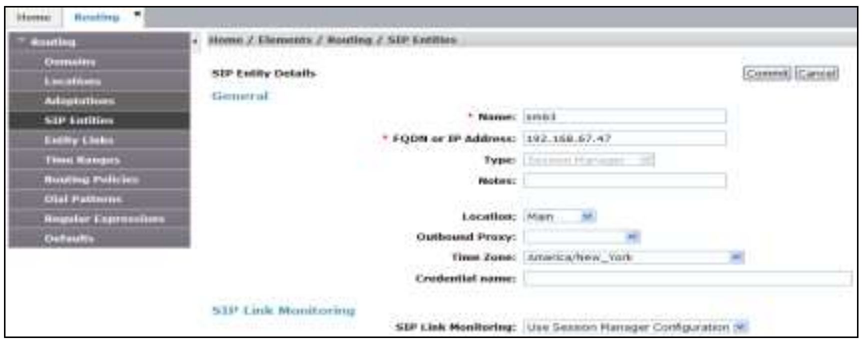
Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name (e.g., **sm63**).

- **FQDN or IP Address –** Enter the IP address of 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 Monitoring** section of the **SIP Entity Details** page configure as follows:

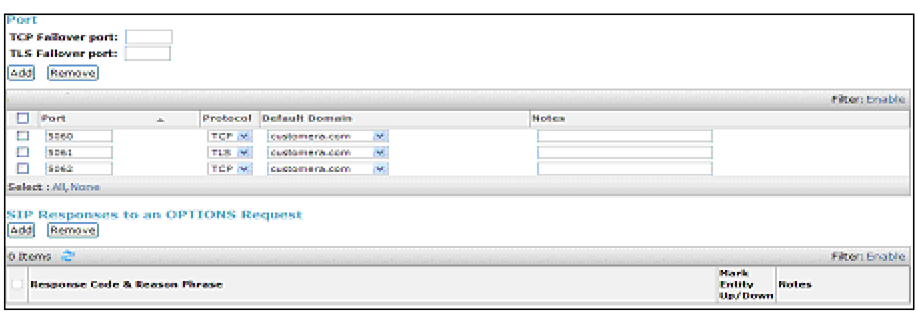
- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.



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

- **Port –** Enter **5060**.
- **Protocol –** Select **TCP**.
- **Default Domain –** Select a SIP domain administered in **Section 5.1** (e.g., **customera.com**).

Step 5 - Repeat **Step 4** to provision entries for **5062/TCP** and **5061/TLS**.
Step 6 – Enter any notes as desired and leave all other fields on the page blank/default.
Step 7 - Click on **Commit**.



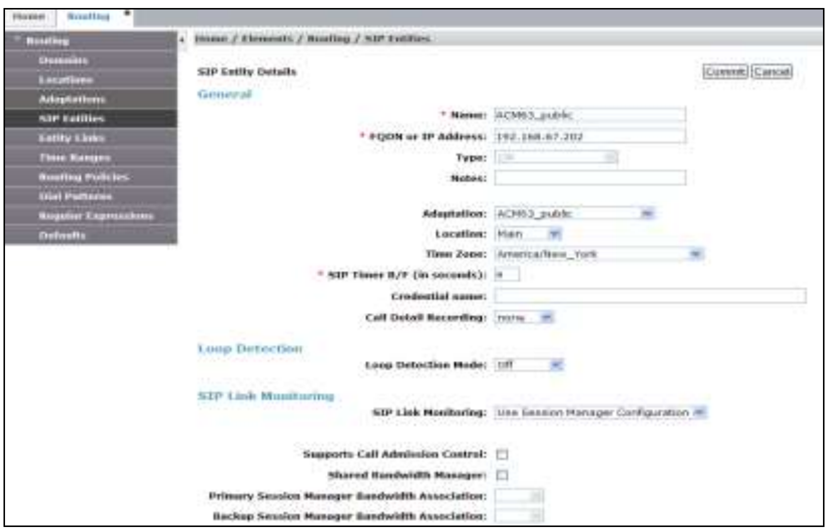
5.4.2 Avaya Aura® Communication Manager SIP Entity – Public Trunk

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 (e.g. **ACM63_public**).
- **FQDN or IP Address –** Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 6.5** (e.g. **192.168.67.202**).
- **Type –** Select **CM**.
- **Adaptation –** Select the Adaptation **ACM63_public** 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 Link Monitoring** section of the **SIP Entity Details** page select:
    - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.

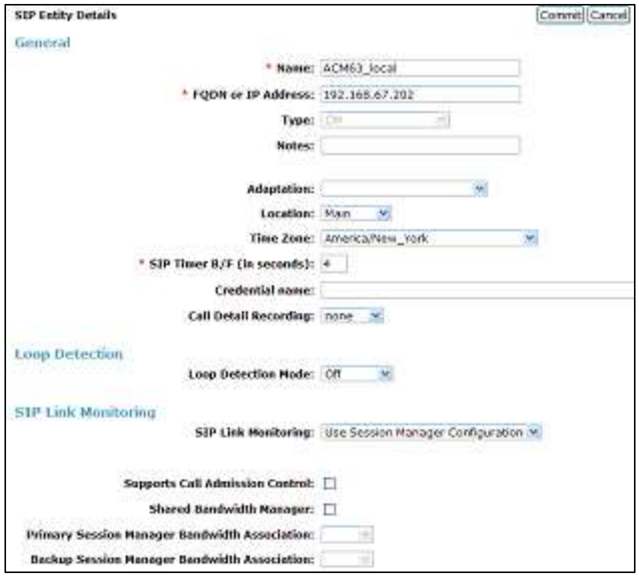
Step 3 - Click on **Commit**.



5.4.3 Avaya Aura® Communication Manager SIP Entity – Local Trunk

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 5.4.2** with the following changes:

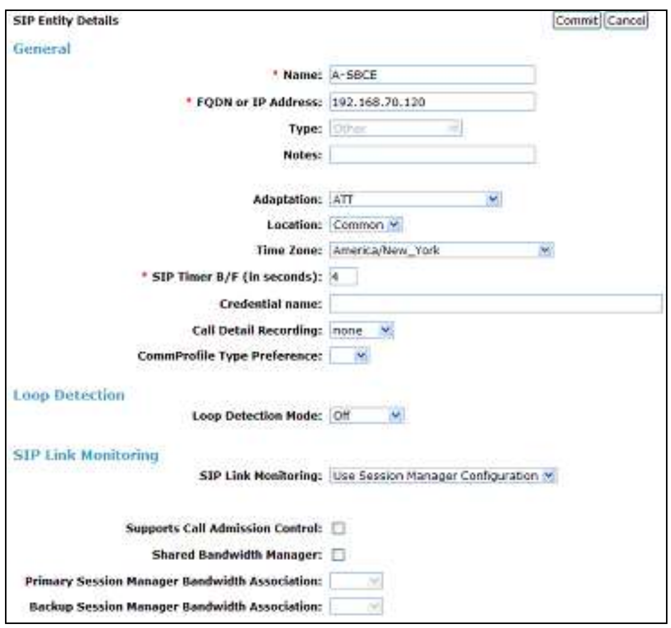
- **Name –** Enter a descriptive name (e.g. A**CM63_local**).
- Note that this Entity has no Adaptation defined.



5.4.4 Avaya Session Border Controller for Enterprise SIP Entity

Repeat the steps in **Section 5.4.1** with the following changes:

- **Name –** Enter a descriptive name (e.g., **A-SBCE**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **192.168.70.120**, see **Section 7.4.1**).
- **Type –** Verify **Other** is selected.
- **Adaptations –** Select Adaptation **ATT** (**Section 5.3.1**).
- **Location** – Select location **Common** (**Section 5.2.2**).



5.5 Entity Links

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

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

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 Trunk

Step 1 - In the left pane under **Routing**, click on **Entity Links**, then 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., **sm63_ACM63_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g., **sm63**).
- **SIP Entity 1 Port** – Enter **5062**.
- **Protocol –** Select **TCP** (see **Section 6.8.1**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **ACM63_public**).
- **SIP Entity 2 Port** - Enter **5062** (see **Section 6.8.1**).
- **Connection Policy –** Select **Trusted**.

Step 3 - Click on **Commit**.

5.5.2 Entity Link to Avaya Aura® Communication Manager – Local Trunk

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_local**).
- **SIP Entity 1 Port** – Enter **5060**.

- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local entity (e.g., **ACM63_local**).
- **SIP Entity 2 Port** - Enter **5060** (see **Section 6.8.2**).

5.5.3 Entity Link for the AT&T IP Toll Free Service via the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

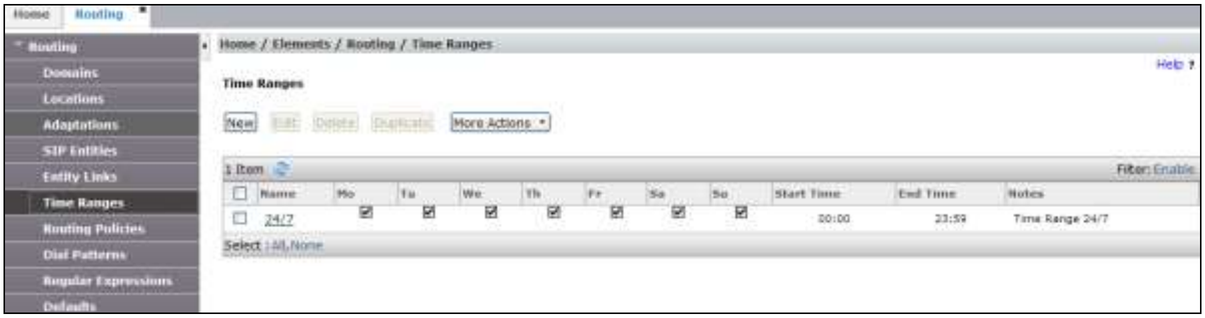
- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sm63_A-SBCE**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE entity (e.g., **A-SBCE**).

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 checkbox(s) for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on **Commit**. Repeat these steps to provision additional time ranges as required.



5.7 Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions.

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

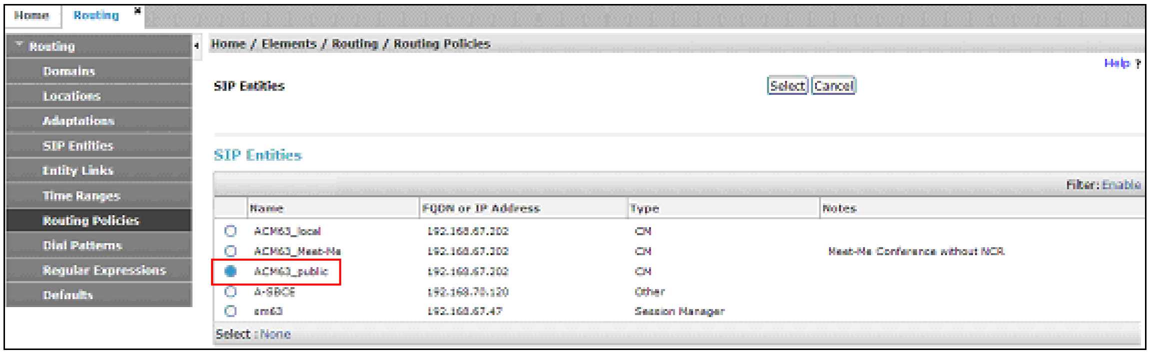
This Routing Policy is used for inbound calls from IPTF.

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., **ACM63_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 (**ACM63_Public**), and click on **Select**.



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

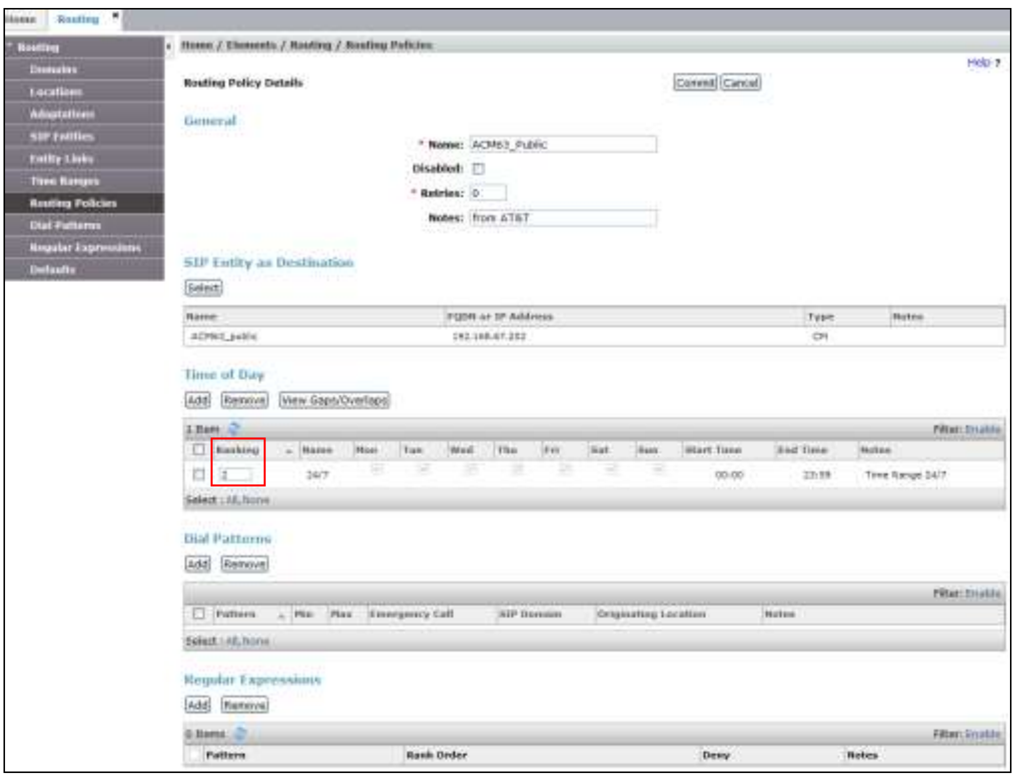
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, enter a **Ranking** of **2**, 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**.



5.8 Dial Patterns

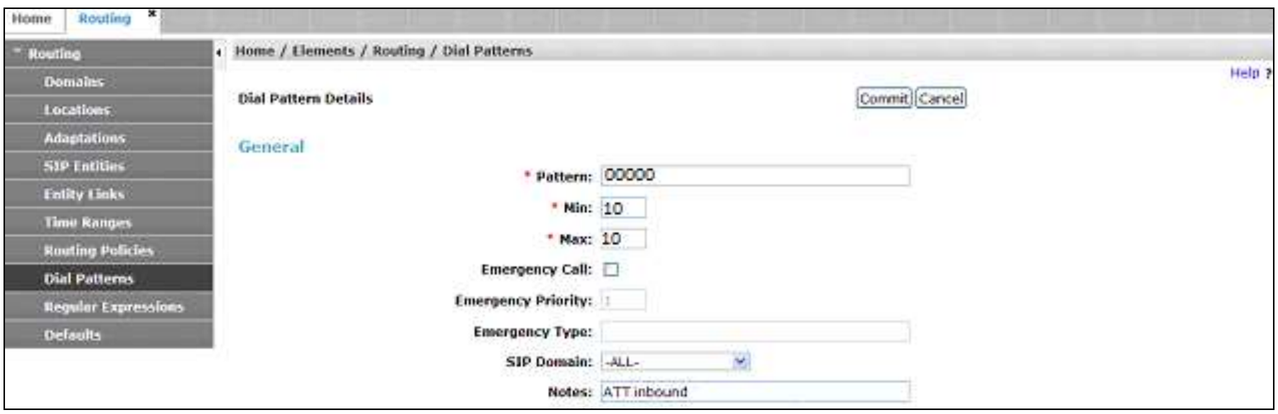
In this section, Dial Patterns are administered to match inbound PSTN calls via the IPTF service to Communication Manager. In the reference configuration inbound calls from the IPTF service sent 10 digits in the SIP Request URI. This pattern must be matched for further call processing.

Note – Be sure to match on the digit string specified in the AT&T Request URI, not the digit string that is 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 00000xxxx. Enter **00000**. Note - The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 00000xxxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max –** Enter **10**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.

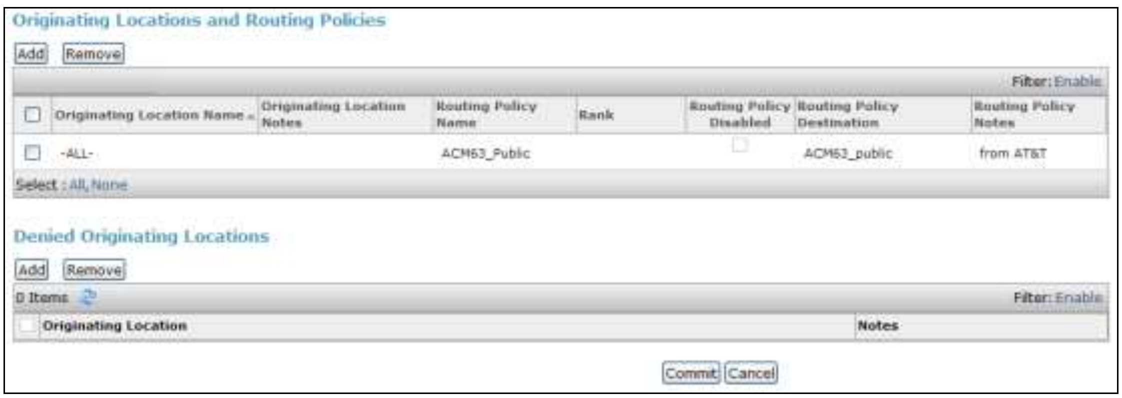


Step 3 – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.

Step 4 - In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to all Locations).

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** (e.g., **ACM63_Public**). Click on **Select**.

Step 6 - Returning to the Dial Pattern Details page click on **Commit**.



Step 7 - Repeat **Steps 1-7** for any additional inbound dial patterns from AT&T.

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 Customer-Options

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 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: 41000 0
                   Maximum Video Capable IP Softphones: 18000 5
                       Maximum Administered SIP Trunks: 24000 30
  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 2 - On **Page 5** of the 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? n      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
                                                                   Wireless? n
                         Remote Office? y
          Restrict Call Forward Off Net? y
                 Secondary Data Module? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

6.2 System-Parameters Features

Step 1 - Enter the **display system-parameters features** command. On **Page 1** of the form, verify that the **Trunk-to-Trunk Transfer** is set to **all**.

```
change system-parameters features                                Page   1 of  20
                              FEATURE-RELATED SYSTEM PARAMETERS
                                 Self Station Display Enabled? y
                                      Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                  AAR/ARS Dial Tone Required? y
              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

6.3 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 following dial plan.

- 5-digit extensions with a **Call Type** of **ext** beginning with:
    - The digits **1** and **4** for Communication Manager extensions.
- 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 6.8**.

```
change dialplan analysis        DIAL PLAN ANALYSIS TABLE        Page   1 of  12
Percent Full: 2                                              Location: all
    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   1           5   ext
   4           5   ext
   6           3   dac
```

6.4 IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used. Note that the Communication Manager procr name and IP address are entered during installation. 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:

- Avaya SBCE private network interface (e.g., **A-SBCE** and **192.168.70.120**).
- Session Manager SIP signaling interface (e.g., **SM63** and **192.168.67.47**).

```
change node-names ip              IP NODE NAMES                     Page   1 of 2
                                     Name                 IP Address
A-SBCE              192.168.70.120
SM63                192.168.67.47
default             0.0.0.0
procr               192.168.67.202
```

6.5 IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters defined during installation.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to **y**.
- In the reference configuration the procr is assigned to **Network Region: 1**.
- The default values are used for the remaining parameters.

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

6.6 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. Region 1 for the CPE access, and region 2 for SIP trunk access.

6.6.1 IP Network Region 1 – Local CPE Region

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., **Main**).
- Enter the enterprise domain (e.g., **customera.com**) in the **Authoritative Domain** field (see **Section 5.1**).
- 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 requirement**).
- **UDP Port Max**: – Set to **32767** (**AT&T requirement**).

Note – The port range for Region 1 does not have to be in the range required by AT&T. However the same range was used here in the reference configuration.

```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: customera.com
    Name: Main                  Stub Network Region: n
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 Enabled is set to **y**.

```
change ip-network-region 1          IP NETWORK REGION               Page   2 of  20

 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 **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **2** in the **dst rgn** column, enter **2** for the codec set (this means region 1 is permitted to talk to region 2 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
```

6.6.2 IP Network Region 2 – SIP Trunk Region

Repeat the steps in **Section 6.6.1** with the following changes:
Step 1 – On **Page 1** of the form (not shown)**:**

- Enter a descriptive name (e.g., **AT&T**).
- Enter **2** for the **Codec Set** parameter.

Step 2 – On **Page 4** of the form:

- Set codec set **2** for **dst rgn 1**.
- Note that **dst rgn 2** is pre-populated with codec set **2** (from page 1 provisioning).

```
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
```

6.7 IP Codec Parameters

Note – The IPTF service offers G.729A, G.726-32, and G.711MU codecs in their Invite SDP. G.726-32 codec is supported by Communication Manager, but testing found issues when G.726-32 codec is used (see **Section 2.2**, **item 2**). In addition, some calls could require support of G.729B (silence suppression). Therefore G.729B is also included in the codec lists.

6.7.1 Codecs for IP Network Region 1 (calls within the CPE)

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                IP Codec Set                Page   1 of   2
    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                IP Codec Set                Page   2 of   2
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
```

6.7.2 Codecs for IP Network Region 2 (calls from AT&T)

Step 1 – Repeat the steps in **Section 6.7.1** with the following changes.

- Provision the codecs in the order shown below. Note that the order of G.729A and G.729B codecs may be reversed as required.
- Set **Frames Per Pkt** to **3**. This will auto-populate **30** for the **Packet Size (ms)** field, and specify a PTIME value of 30 in the SDP (recommended by AT&T).

```
change ip-codec-set 2                IP Codec Set                Page   1 of   2
    Codec Set: 2
    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A           n          3        30
 2: G.729B           n          3        30
 3: G.711MU          n          3        30
```

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

6.8 SIP Trunks

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group. Three SIP trunks are defined on Communication Manager in the reference configuration:

- Inbound IPTF access – SIP Trunk 2
  - Note that this trunk will use TCP port 5062 as described in **Section 5.5.1**.
- Internal CPE access (e.g., Avaya SIP telephones, etc) – SIP Trunk 1
  - Note that this trunk will use TCP port 5060 as described in **Section 5.5.2**.

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

6.8.1 SIP Trunk for Inbound AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for inbound IPTF calls. This trunk corresponds to the **ACM63_Public** SIP 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 6.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.4** (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 set in **Section 6.6.2**.
- **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 directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **OPTIONAL**: If desired, set **Initial IP-IP Direct Media** is set to **Y**. Otherwise leave it disable (default).

Note - Enabling the **Initial IP-IP Direct Media** parameter allows Communication Manager to signal the IP address of Avaya SIP telephones during the initial setup of a call. This permits the Avaya SIP telephone and the AT&T caller to exchange Media directly, without allocating Communication Manager media resources. However, unless network routing permits direct IP access between the Avaya SIP telephone and the "inside" interface of the Avaya SBCE, a loss of audio can occur when this option is enabled. In addition, when this option is enabled, Communication Manager will not send SDP in 180 messages, and will not send 183 messages (if enabled).

- Use the default parameters on **page 2** of the form (not shown).

```
add signaling-group 2              SIGNALING GROUP                   Page   1 of   1
 Group Number: 1               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
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
   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 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 **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to 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                    TRUNK GROUP                       Page   1 of  21
Group Number: 2                        Group Type: sip            CDR Reports: y
  Group Name: ATT                          COR: 1        TN: 1         TAC: 602
   Direction: two-way         Outgoing Display? n
 Dial Access? n                                        Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 20
```

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

- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900**.

```
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 (see **Section 6.9**).

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

- 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, any History Info headers sent by Communication Manager 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              PROTOCOL VARIATIONS             Page   4 of  21
                                         Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected 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: From
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

6.8.2 Local SIP Trunk (Avaya SIP Telephone Access)

This trunk corresponds to the **ACM63_Local** SIP 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 6.8.1** with the following changes:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.6.1**.

```
add signaling-group 1           SIGNALING GROUP                Page   1 of   1
Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n
     IP Video? n         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: 5060                 Far-end Listen Port: 5060
                                         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? y
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 6.8.1** 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                TRUNK GROUP                     Page   1 of  21
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:

- Same as **Section 6.8.1**.

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

- Same as **Section 6.8.1**.

Step 5 - On **Page 4** of the **Trunk Group** form:

- Use default values for all settings.

Note – Enabling *Convert 180 to 183 for Early Media* will cause Communication Manager to issue 183 messages instead of 180 (see the note in **Section 6.8.1**).

```
add trunk-group 1             PROTOCOL VARIATIONS                Page   4 of  21
                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected 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
             Block Sending Calling Party Location in INVITE? n
                  Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

6.9 Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 6.8.1**), is used to convert Communication Manager local extensions to IPTF DNIS numbers, for inclusion in any SIP headers directed to the IPTF service via the public trunk.

Step 1 – 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 6.3** (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 2 – Add any Communication Manager station extensions and their 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., SIP phone **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., **0000012345**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 4 – Add any Communication Manager Agent skill VDN extensions and their 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 extension (e.g., Skill VDN **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., **0000012346**).
- **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: 4
 5  4                 1                               5         Maximum Entries: 540
 5  19005             2            0000012345         10
 5  44002             2            0000012346         10
```

6.10 Route Patterns for Local SIP Trunk

Route Patterns are use to direct calls to the Local SIP trunk for access to SIP phones or other destinations in the CPE. This form specifies the local SIP trunk (e.g., 1), based on the route-pattern selected by the AAR table in **Section 6.11** (e.g., calls SIP phone extensions).

Note – As IPTF is an inbound only service, no outbound route patterns are defined for the public SIP trunk.

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
     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
```

6.11 Automatic Alternate Routing (AAR) Dialing

AAR is used to direct calls to the local SIP trunk for Avaya SIP telephones, using the route pattern defined in **Section 6.10**.

Step 1 – Enter the following:

- **Dialed String -** In the reference configuration all SIP telephones used extensions in the range 1902x, therefore enter **1902**.
- **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
```

6.12 Class of Restriction (COR) for Agent Telephones

As described in **Section 2.2, Item 1**, an issue was found with the IP Toll Free ADR call redirection feature in response to a ring-no-answer condition. If the Communication Manager returns a 180 followed by 181, then the IP Toll Free ADR feature will trigger and the alternate number is called. However, if Communication Manager only sends 180, then ADR is not triggered. Setting the

Direct Agent Calling parameter in the **Class of Restriction** form, to **n**, will cause Communication Manager to send a 181 followed by a 180, thus triggering the ADR Ring-No-Answer feature. Note that the COR level is applied to the Agent form (see **Section 6.12**).

Step 1 – Using the **change cor x** command, where x is the COR used by the Agent phones (e.g., **2**), verify the **Direct Agent Calling** field is set to **n**.

```
change cor 2                     CLASS OF RESTRICTION                Page   1 of  23
               COR Number: 2
          COR Description: Agent
                      FRL: 0                                   APLT? y
  Can Be Service Observed? n           Calling Party Restriction: none
Can Be A Service Observer? n            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? n
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? n
                                    Can Use Directed Call Pickup? n
                                    Group Controlled Restriction: inactive
```

Step 2 – The Class of Restriction (COR) is applied to the Agent.

- 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:
- **COR** – Specify Class of Restriction **2**.

```
change agent-loginID 47002         AGENT LOGINID                Page   1 of   3
                Login ID: 47002                                      AAS? n
                    Name: Agent2                                   AUDIX? n
                      TN: 1                               LWC Reception: spe
                     COR: 2                       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
```

6.13 Provisioning for Simulated Call Center Functionality

In the reference configuration, a Call Center environment (skill queues and Agents) was simulated on Communication Manager. The administration of Communication Manager Call Center type elements – Agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult **[6** and **8]** for further details. The samples that follow are provided for reference purposes only.

- Agent form – **Page 1**

```
display agent-loginID 47002          AGENT LOGINID              Page   1 of   3
                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         AGENT LOGINID               Page   2 of   3
      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
```

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

```
display hunt-group 2                HUNT GROUP                Page   1 of   4
            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 Vector form – **Page 1**

```
display vector 2                CALL VECTOR                    Page   1 of   6
    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
```

- Skill 2 VDN form – **Page 1**

```
display vdn 44002              VECTOR DIRECTORY NUMBER           Page   1 of   3
                             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
```

6.14 Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateways is provisioned. The G430 is located in the Main site and is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. See **[7]** for additional information.

Step 1 – SSH to the G430 (not shown). Note that the Media Gateway prompt will contain *???* if the Media Gateway is not registered to Communication Manager (e.g., ***G430-???(super)#***).
Step 2 - Enter the **show system** command and note the G430 serial number (e.g., **10ISO123456**).
Step 3 – Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **192.168.67.202**, see **Section 6.4**).
Step 4 – Enter the **copy run copy start command** to save the G430 configuration.

Step 5 – On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown). Enter the following parameters:

- Set **Type** = **g430**
- Set **Name** = Enter a descriptive name (e.g., **G430**)
- Set **Serial Number** = Enter the serial number copied from **Step 2** (e.g., **10IS0123456**).
- Set the **Encrypt Link** parameter as desired (**n** was used in the reference configuration).
- Set **Network Region** = **1**

When the Media Gateway registers, the SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., ***G430-001(super)#***).
Step 6 – Enter the **display media-gateway 1** command, and verify that the G430 has registered.

```
display media-gateway 1            MEDIA GATEWAY 1                 Page   1 of   2
                    Type: g430
                    Name: g430
               Serial No: 10IS0123456
            Encrypt Link? n                   Enable CF? n
          Network Region: 1                    Location: 1
                                              Site Data:
           Recovery Rule: none
             Registered?  y
   FW Version/HW Vintage: 34 .5  .1  /1
       MGP IPV4 Address: 192.168.67.50
       MGP IPV6 Address:
   Controller IP Address: 192.168.67.202
```

6.15 Save Communication Manager Translations

After the Communication Manager provisioning is completed, enter the command **save translation**.

7 Configure Avaya Session Border Controller for Enterprise

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

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to **[9** and **10]** 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.

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (192.168.70.120), with access to the Main site. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 10.10.10.11).
The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

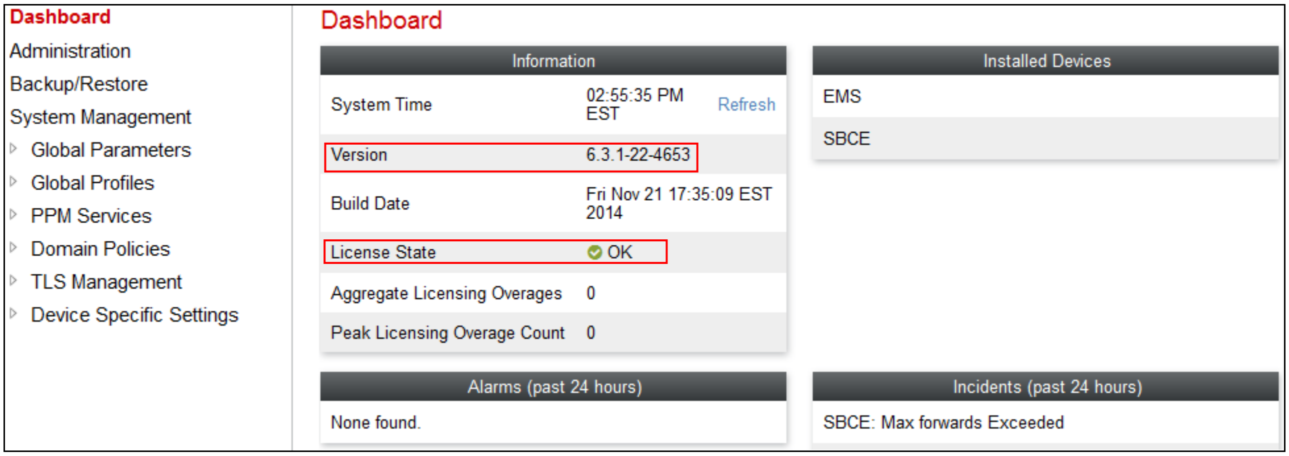
Step 1 - Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).

Step 2 - Enter the **Username** and click on **Continue**.

Step 3 - Enter the password and click on **Log In**.

Step 4 - The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

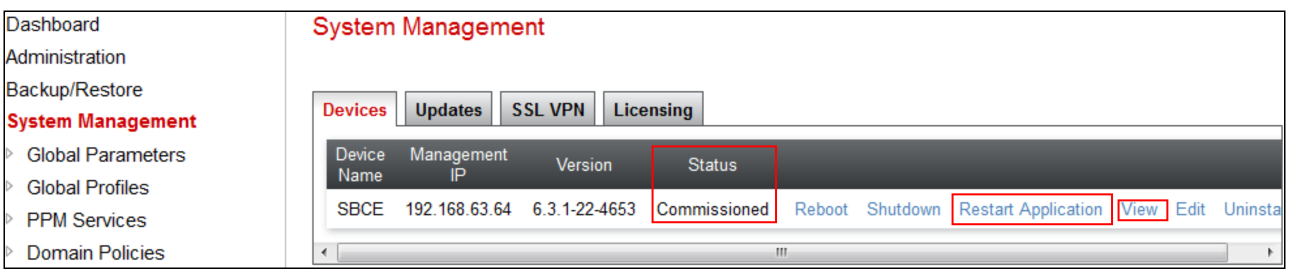
Note – The provisioning described in the following sections use the menu options listed in the left hand column shown below.



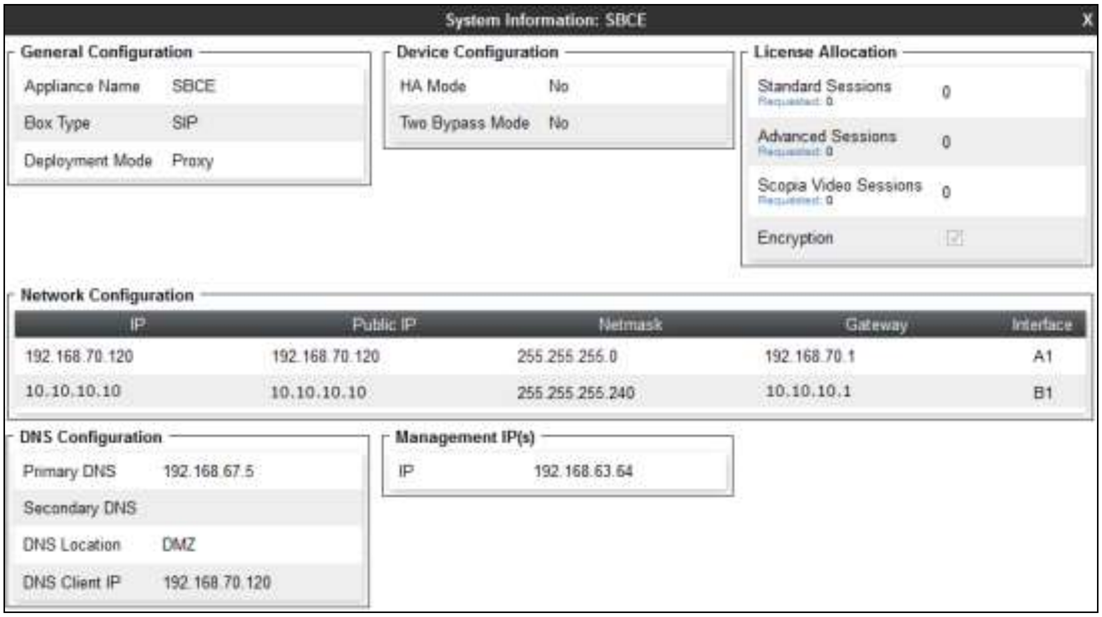
7.1 System Management – Status

Step 1 - Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.

Note – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.



Step 2 - Click on **View** (shown above) to display the **System Information** screen.



7.2 Global Profiles

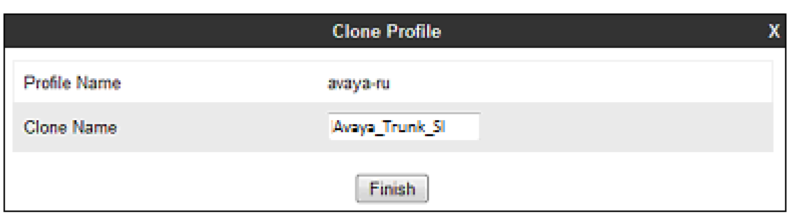
Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

7.2.1 Server Interworking – Avaya

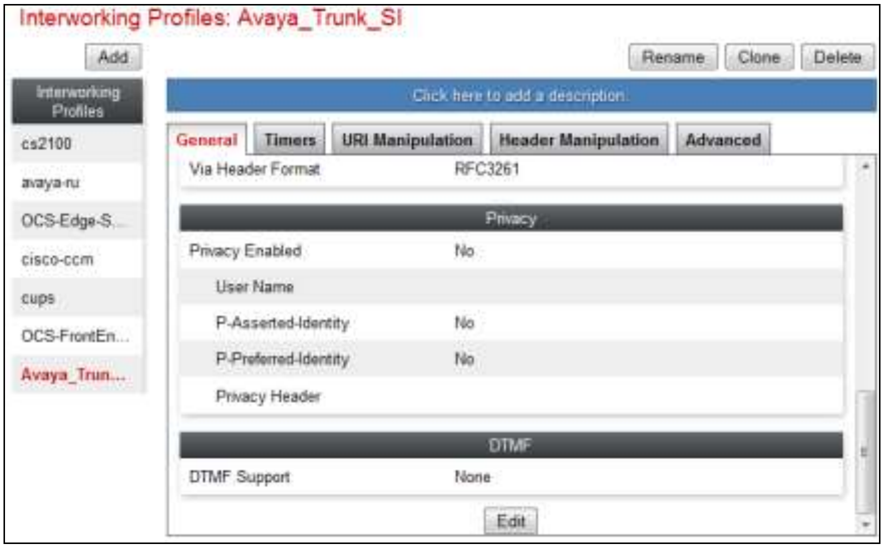
Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Session Manager.

Step 1 - Select **Global Profiles → Server Interworking** from the left-hand menu.
Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.

Step 3 - Enter profile name: (e.g., **Avaya_Trunk_SI**), and click **Finish**.



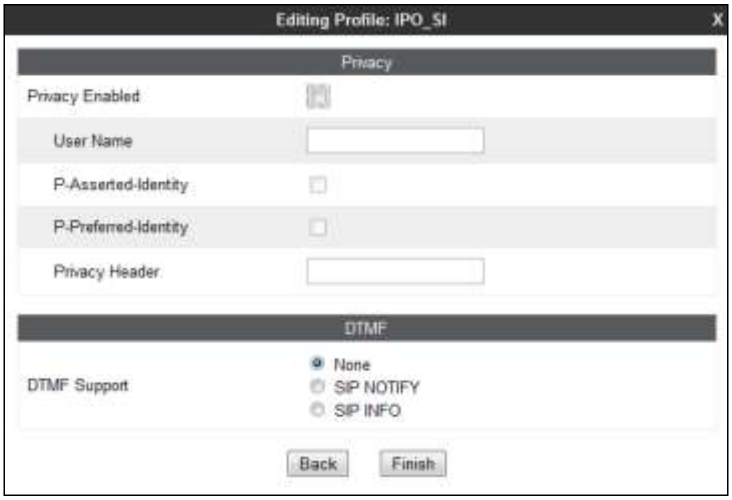
Step 4 - The new Avaya_Trunk_SI profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.



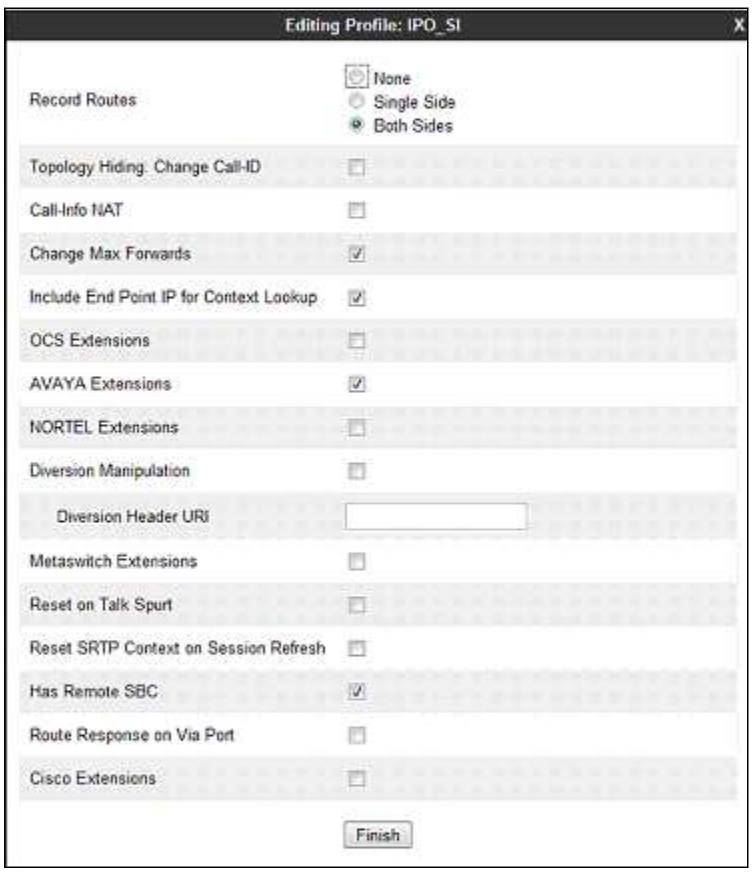
Step 5 - The **General** screen will open.

- Check **T38 Support**.
- All other options can be left with default values, and click **Next**.

Step 6 - On the **Privacy/DTMF** window, select **Finish** to accept default values.



Step 7 - Returning to the **General** screen, select the **Advanced** tab, accept the default values, and click **Finish**.



7.2.2 Server Interworking – AT&T

Repeat the steps shown in **Section 7.2.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

Step 1 - Select **Add Profile** (not shown) and enter a profile name**:** (e.g., **ATT_Trunk_SI**) and click **Next** (not shown).

Step 2 - The **General** screen will open (not shown):

- Check **T38 Support**.
- All other options can be left as default.
- Click **Next**.

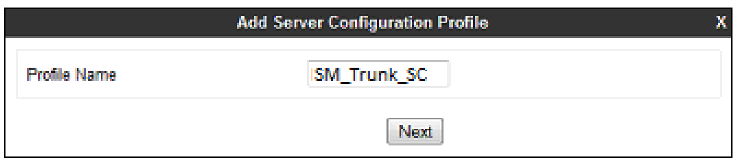
Step 3 - The **Privacy/DTMF**, **SIP Timers/Transport Timers**, and **Advanced** screens will open (not shown), accept default values for all the screens by clicking **Next**, then clicking on **Finish** when completed.

7.2.3 Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

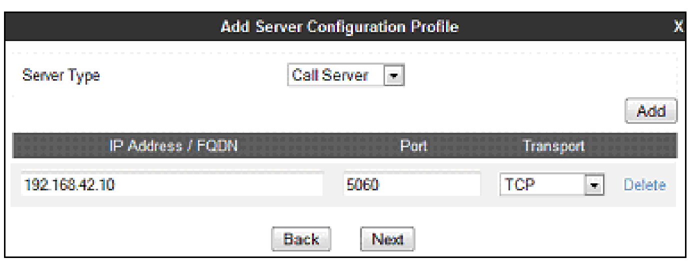
Step 1 - Select **Global Profiles → Server Configuration** from the left-hand menu.

Step 2 - Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM_Trunk_SC**) and click **Next**.



Step 3 - The **Add Server Configuration Profile** window will open.

- Select **Server Type**: **Call Server**.
- **IP Address**: **192.168.67.47** (Session Manager network IP Address)
- **Supported Transports**: Check **TCP**.
- **TCP Port**: **5060**.
- Select **Next**.



Step 4 - The **Authentication** and **Heartbeat** windows will open (not shown).

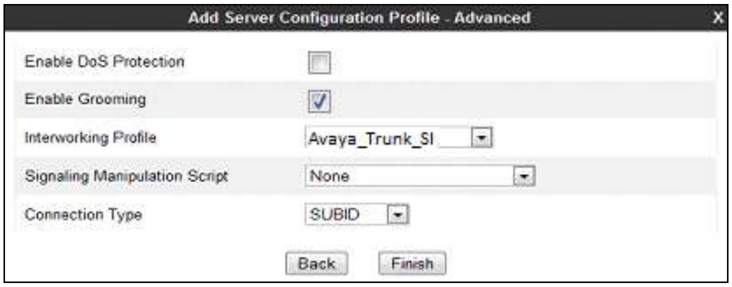
- Select **Next** to accept default values.

Step 5 - The **Advanced** window will open.

- Select **Avaya_Trunk_SI** (created in **Section 7.2.1**), for **Interworking Profile**.

- In the **Signaling Manipulation Script** field select **none.**
- Select **Finish**.

Note – Since TCP transport is specified in **Step 3**, then the **Enable Grooming** option should be enabled.



7.2.4 Server Configuration – AT&T

Note – The AT&T IPTF service may provide a Primary and Secondary Border Element. This section describes the connection to a single (Primary) Border Element. See **Addendum 1** for information on configuring two IPTF Border Elements (Primary & Secondary).

Repeat the steps in **Section 7.2.3**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

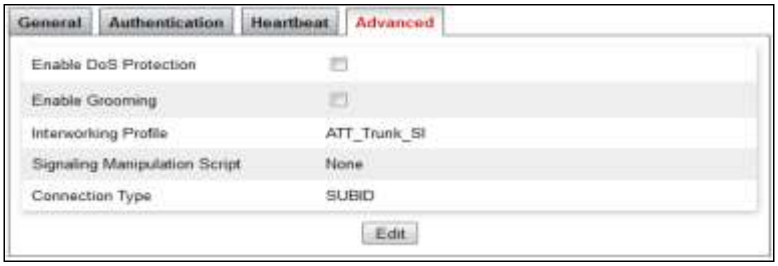
Step 1 - Select **Add Profile** and enter a Profile Name (e.g., **ATT_SC**) and select **Next**.

Step 2 - On the **General** window (not shown), enter the following.

- Select Server Type**: Trunk Server**.
- **IP Address: 10.10.10.11** (AT&T Border Element IP address)
- **Supported Transports**: Check **UDP**.
- **UDP Port: 5060**.
- Select **Next**.

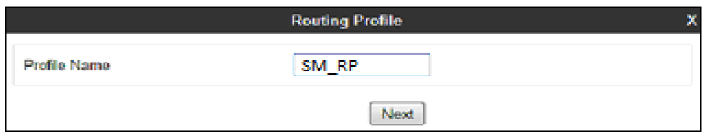
Step 3 - On the **Advanced** window, enter the following.

- Select **ATT_SI** (created in **Section 7.2.2**), for **Interworking Profile**.
- Select **Finish**.

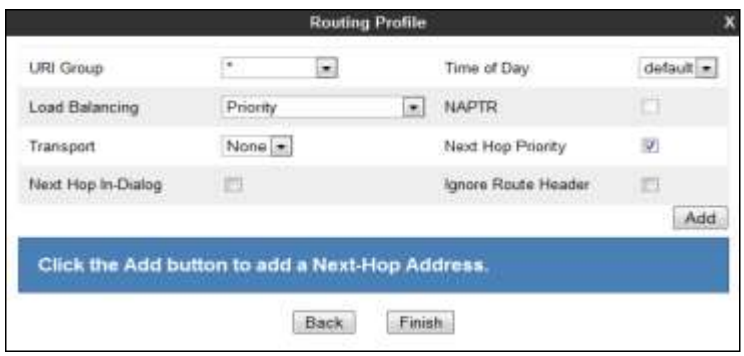


7.2.5 Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.
Step 1 - Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown)
Step 2 - Enter a **Profile Name**: (e.g., **SM_RP)** and click **Next**.

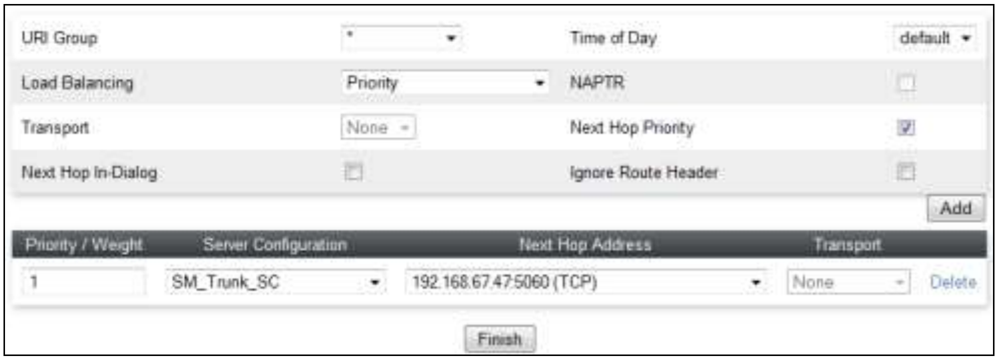


Step 3 - The Routing Profile window will open. Using the default values shown, click on **Add.**



Step 4 - The Next-Hop Address window will open. Populate the following fields:

- **Priority/Weight** = **1**
- **Server Configuration** = **SM_Trunk_SC** (from **Section 7.2.3**).
- **Next Hop Address** = Verify that the **192.168.67.47:5060 (TCP)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** fields are grayed out.
- Click on **Finish.**



7.2.6 Routing – To AT&T

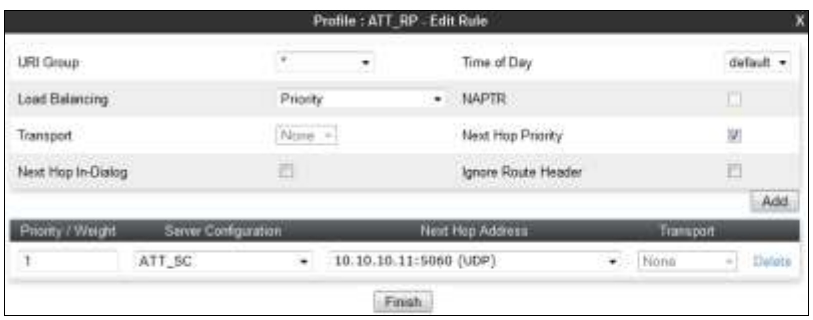
Repeat the steps in **Section 7.2.5**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

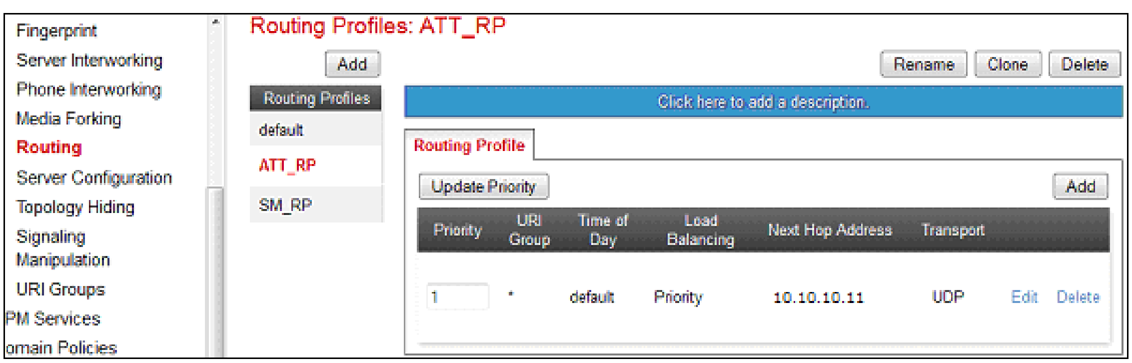
Step 1 - On the **Global Profiles → Routing window (not shown),** enter a Profile Name: (e.g., **ATT_RP)**.

Step 2 - On the Next-Hop Address window (not shown), populate the following fields:

- **Priority/Weight** = **1**
- **Server Configuration** = **ATT_SC** (**from Section 7.2.4**).
- **Next Hop Address:** Verify that the **10.10.10.11:5060** entry from the drop down menu is selected (AT&T Border Element IP address).
- Use default values for the rest of the parameters.

Step 4 - Click **Finish**.





7.2.7 Topology Hiding – Avaya Side

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

Step 1 - Select **Global Profiles → Topology Hiding** from the left-hand side menu.

Step 2 - Select the **Add** button, enter Profile Name: (e.g., **Avaya_TH**), and click **Next**.

Step 3 - The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until no new headers are added to the list, and the **Add Header** button is no longer displayed.

Step 4 - Populate the fields as shown below, and click **Finish**. Note that **customera.com** is the domain used by the CPE (see **Sections 5.1** and **6.6**).

7.2.8 Topology Hiding – AT&T Side

Repeat the steps in **Section 7.2.7,** with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

1. Enter a Profile Name: (e.g., **ATT_TH**).
2. Use the default values for all fields and click **Finish**.

The following screen shows the completed **Topology Hiding Profile** form.

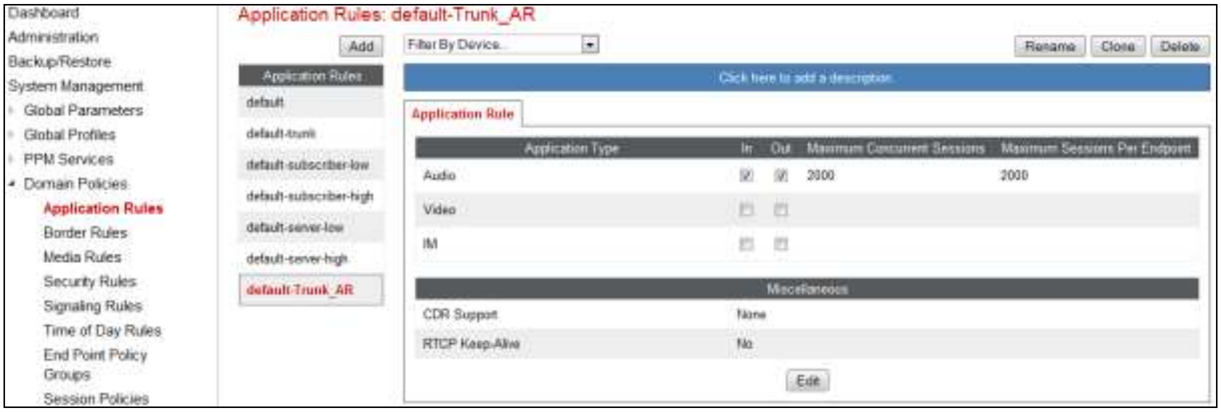
7.3 Domain Policies

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

7.3.1 Application Rules

Step 1 - Select **Domain Policies →Application Rules** from the left-hand side menu (not shown).
Step 2 - Select the **default-trunk** rule (not shown).
Step 3 - Select the **Clone** button (not shown), and the **Clone Rule** window will open (not shown).

- In the **Clone Name** field enter **default-Trunk_AR**
- Click **Finish** (not shown). The completed **Application Rule** is shown below.



7.3.2 Media Rules

Media Rules are used to define QOS parameters. The Media Rule described below will be applied to both directions, and therefore, only one rule is needed.

Step 1 - Select **Domain Policies → Media Rules** from the left-hand side menu (not shown).

Step 2 - From the Media Rules menu, select the **default-low-med** rule.

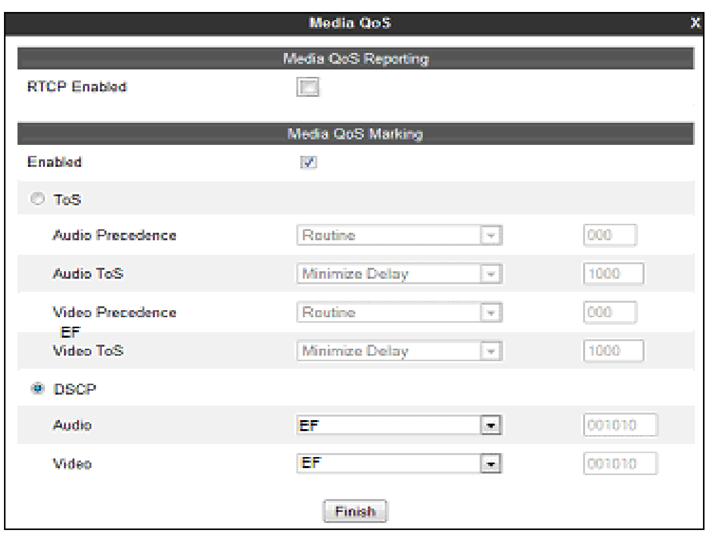
Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **Avaya-low-med_MR**
- Click **Finish.** The newly created rule will be displayed.

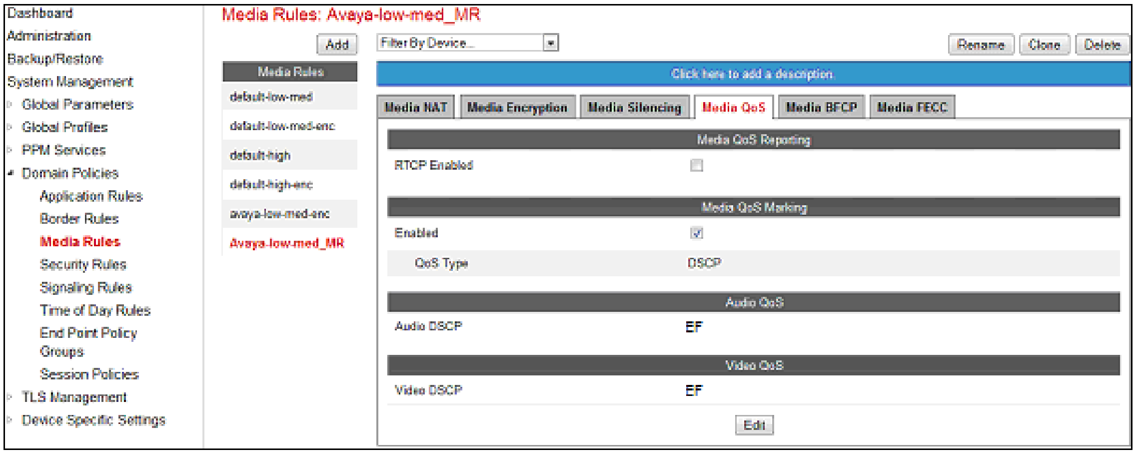
Step 4 - Highlight the **Avaya-low-med_MR** rule just created (not shown):

- Select the **Media QOS** tab (not shown).
- Click the **Edit** button and the **Media QOS** window will open.
- Check the **Media QOS Marking** field is **Enabled.**
- Select the **DSCP** box.
- **Audio**: Select **EF** from the drop-down.
- **Video**: Select **EF** from the drop-down.

Step 5 - Click **Finish.**



The completed **Media Rule** screen is shown below.



7.3.3 Signaling Rules

In the reference configuration, Signaling Rules are used to filter various SIP headers.

7.3.3.1 Avaya – Signaling Rules

Step 1 - Select **Domain Policies → Signaling Rules** from the left-hand side menu (not shown).
Step 2 - The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

- In the **Rule Name** field enter **Avaya_SR**
- Click **Finish.** The newly created rule will be displayed (not shown).

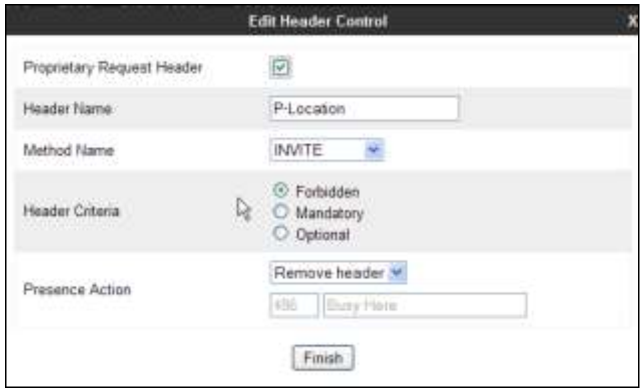
7.3.3.1.1 Avaya – Signaling Rule - Request Headers Tab

The following Signaling Rules remove SIP headers sent by Communication Manager SIP requests that are either not supported or required by AT&T.

Step 1 - Highlight and the **Avaya_SR** rule created in **Section 7.3.3.1**, select the **Request Headers** tab, 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.
- In the **Header Name** field, enter **P-Location**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

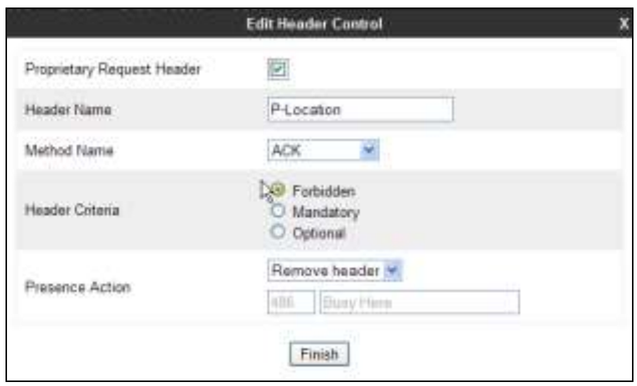
Step 2 - Click **Finish**



Step 3 - Repeat **Steps 1** & **2** with the following changes, to create a rule to remove the **P-Location** header from ACKs.

- From the **Method Name** menu select **ACK**.

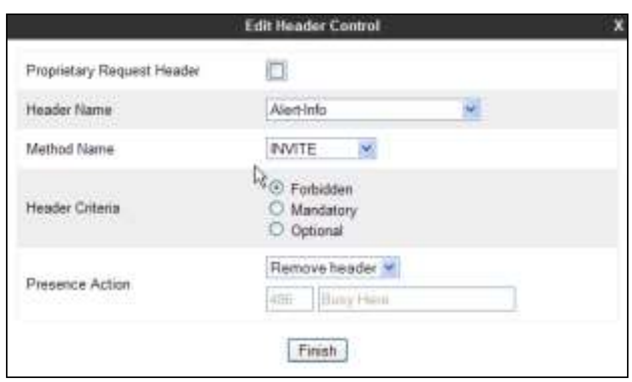
Step 4 - Click **Finish**.



Step 5 - Repeat **Steps Steps 1** & **2** to create a rule to remove the **Alert-Info** header.

- Verify the **Proprietary Request Header** box is *unchecked*.
- From the **Header Name** menu select **Alert-Info**.
- From the **Method Name** menu select **Invite**.

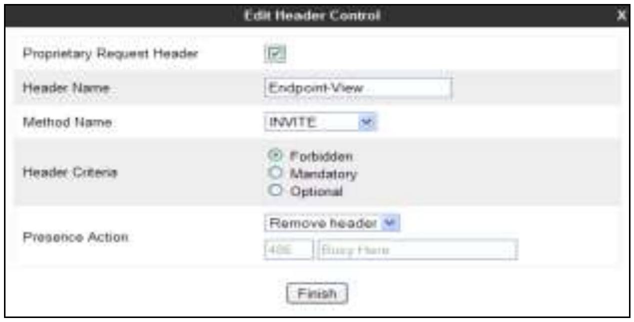
Step 6 - Click **Finish**.



Step 7 - Repeat **Steps Steps 1** & **2** to create a rule to remove the **Endpoint-View** header.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Method Name** menu select **Invite**.

Step 8 - Click **Finish**.



Step 9 - Repeat **Steps Steps 1** & **2** to create a rule to remove the **AV-Correlation-ID** header.

- In the **Header Name** field enter **AV-Correlation-ID**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.

Step 10 - Click **Finish**.

Step 11 - Repeat **Steps 1** & **2** to create a rule to remove the **AV-Global-Session-ID** header.

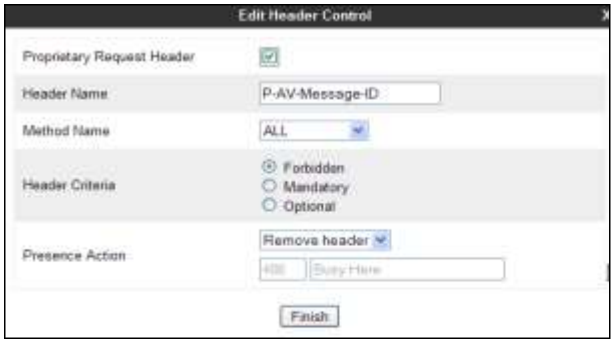
- In the **Header Name** field enter **AV-Global-Session-ID**.
- From the **Method Name** menu select **ALL**.

Step 12 - Click **Finish**.

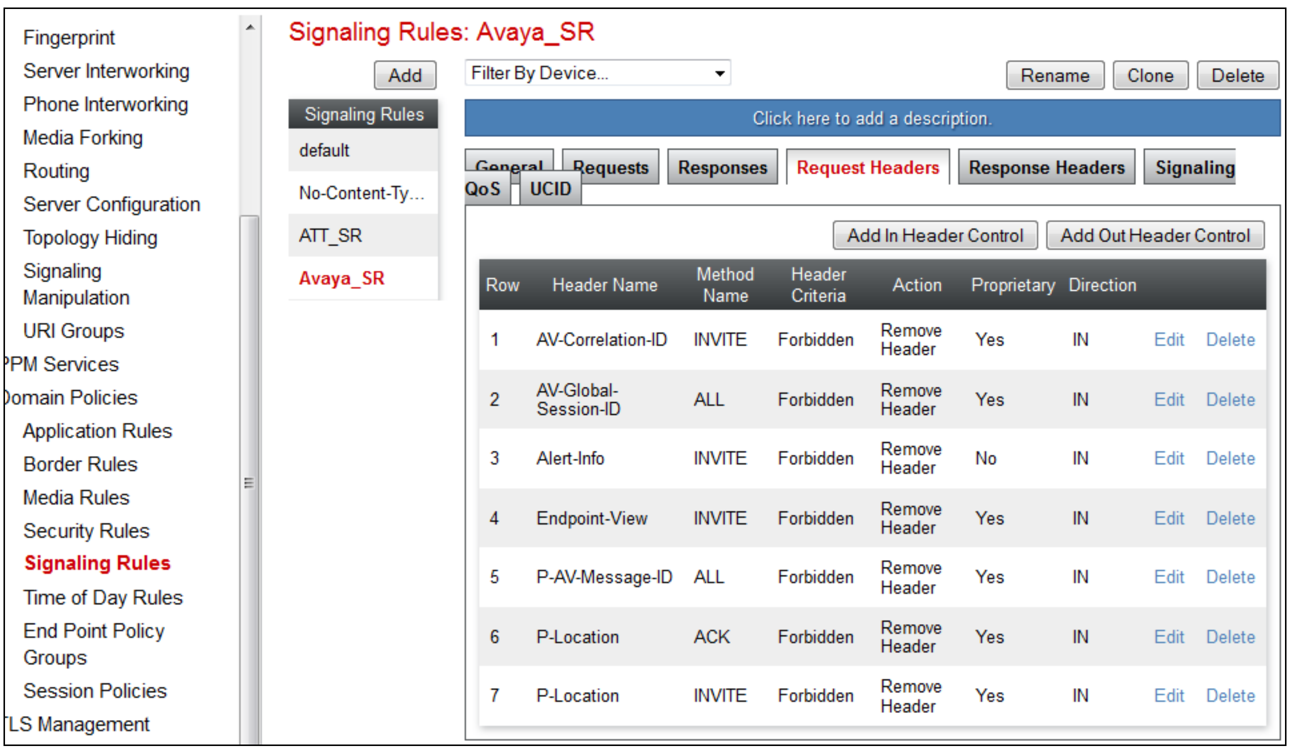
Step 13 - Repeat **Steps 1** & **2** to create a rule to remove the P-**AV-Message-ID** header.

- In the **Header Name** field enter P-**AV-Message-ID**.
- From the **Method Name** menu select **ALL**.

Step 14 - Click **Finish**.



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



7.3.3.1.2 Avaya – Signaling Rule Response Headers Tab

The following Signaling Rules remove headers sent by Communication Manager SIP responses (e.g., 1xx and/or 200OK) that are either not supported or required by AT&T.

Step 1 - Highlight the **Avaya_SR** rule created in **Section 7.3.3.1**, and using the same procedures shown in **Section 7.3.3.1.1**, remove the following headers:

- **P-Location header from 1xx responses:**
  - 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.
  - In the **Header Name** field, enter **P-Location**.
  - From the **Response Code** menu select **1xx**.
  - From the **Method Name** menu select **Invite**.
  - For **Header Criteria** select **Forbidden**.
  - From the **Presence Action** menu select **Remove Header**.
  - Click **Finish**.
- **P-Location header from 2xx responses.**
  - From the **Response Code** menu select **2xx**.
  - Click **Finish**.

- **Endpoint-View header from 1xx responses.**
  - In the **Header Name** field, enter **Endpoint-View**.
  - From the **Response Code** menu select **1xx**.
  - From the **Method Name** menu select **Invite**.
  - Click **Finish**.
- **Endpoint-View headers from 2xx responses.**
  - From the **Response Code** menu select **2xx**.
  - Click **Finish**.

- **P-AV-Message-ID header from 1xx responses.**
  - In the **Header Name** field, enter **Endpoint-View**.
  - From the **Response Code** menu select **1xx**.
  - From the **Method Name** menu select **ALL**.
  - Click **Finish**.
- **P-AV-Message-ID headers from 2xx responses.**
  - From the **Response Code** menu select **2xx**.
  - Click **Finish**.

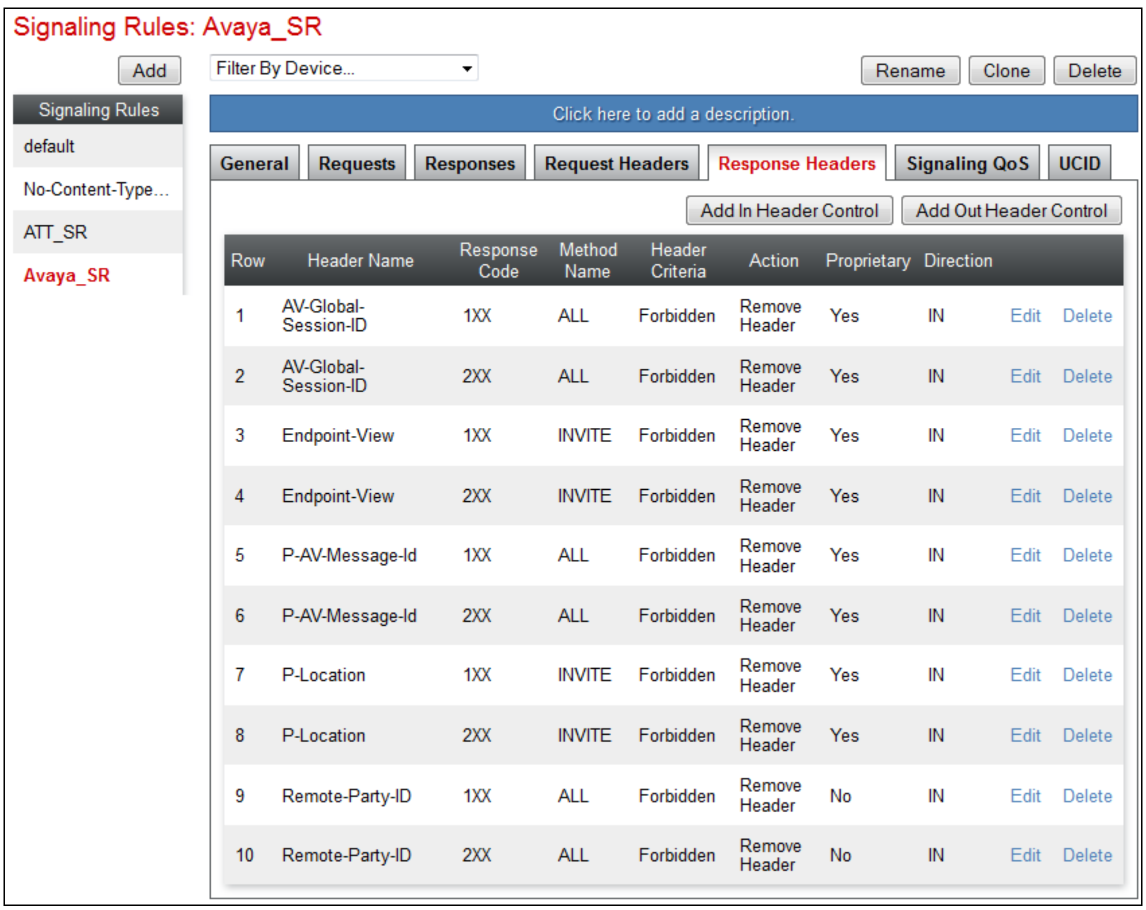
- **AV-Global-Session-ID header from 1xx responses**.
  - In the **Header Name** field, enter **Endpoint-View**.
  - From the **Response Code** menu select **1xx**.

- From the **Method Name** menu select **ALL**.
- Click **Finish**.

- **AV-Global-Session-ID** headers from **2xx** responses.
  - From the **Response Code** menu select **2xx**.
  - Click **Finish**.

- **Remote-Party-ID header from 1xx responses.**
  - In the **Header Name** field, enter **Remote-Party-ID**.
  - From the **Response Code** menu select **1xx**.
  - Verify the **Proprietary Request Header** box is *unchecked*.
  - From the **Method Name** menu select **ALL**.
  - Click **Finish**.
- **Remote-Party-ID headers from 2xx responses.**
  - From the **Response Code** menu select **2xx**.
  - Click **Finish**.

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



Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	Remote-Party-ID	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
10	Remote-Party-ID	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

Step 2 - Highlight the **Avaya_SR** rule, select the **Signaling QOS** tab and enter the following:

- Click the **Edit** button and the **Signaling QOS** window will open.
- Verify that **Signaling QOS** is selected.
- Select **DCSP**.
- Select **Value** = **EF**.

Step 3 - Click **Finish**.

7.3.3.2 AT&T – Signaling Rule Request Headers Tab

The Remote-Address header inserted by the Avaya SBCE is removed (see **Section 2.2, Item 3**).
Step 1 - Select **Domain Policies** from the menu on the left-hand side menu (not shown).
Step 2 - Select **Signaling Rules** (not shown).
Step 3 - From the Signaling Rules menu, select the **default** rule.
Step 4 - Select **Clone Rule** button

- Enter a name**: ATT_SR**

Step 5 - Click **Finish**
Step 6 - Highlight and edit the **ATT_SR** rule created in **Step 4**, enter the following:

- Select the **Add Out Header Control** button (not shown).
- 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 **Remote-Address**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

Step 7 - Click **Finish.** The completed Request Headers form is shown below.
Note that the Direction column says "OUT", and that no Response Header manipulation is required.

Step 8 - Highlight the **ATT_SR** rule, select the **Signaling QOS** tab and repeat **Steps 2** & **3** from **Section 7.3.3.1**.

7.3.4 Endpoint Policy Groups – Avaya Connection

Step 1 - Select **Domain Policies** from the menu on the left-hand side.
Step 2 - Select **End Point Policy Groups**.
Step 3 - Select **Add Group**.

- **Name**: **Avaya_default-low_PG**.
- **Application Rule**: **SIP_Trunk_AR** (created in **Section 7.3.1**).
- **Border Rule**: **default**.
- **Media Rule**: **Trunk_low_med_MR** (created in **Section 7.3.2**).
- **Security Rule**: **default-low.**
- **Signaling Rule**: **Avaya_SR** (created in **Section 7.3.3**).
- **Time of Day**: **default**.

Step 4 - Select **Finish** (not shown). The completed **Policy Groups** screen is shown below.

7.3.5 Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps **1** through **4** from **Section 7.3.4** with the following changes:

- **Group Name**: **ATT_default-low_PG**.
- **Signaling Rule**: **ATT_SR** (created in **Section 7.3.3**).

Step 2 - Select **Finish** (not shown).

7.4 Device Specific Settings

7.4.1 Network Management

Step 1 - Select **Device Specific Settings → Network Management** from the menu on the left-hand side.

Step 2 - The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.

Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

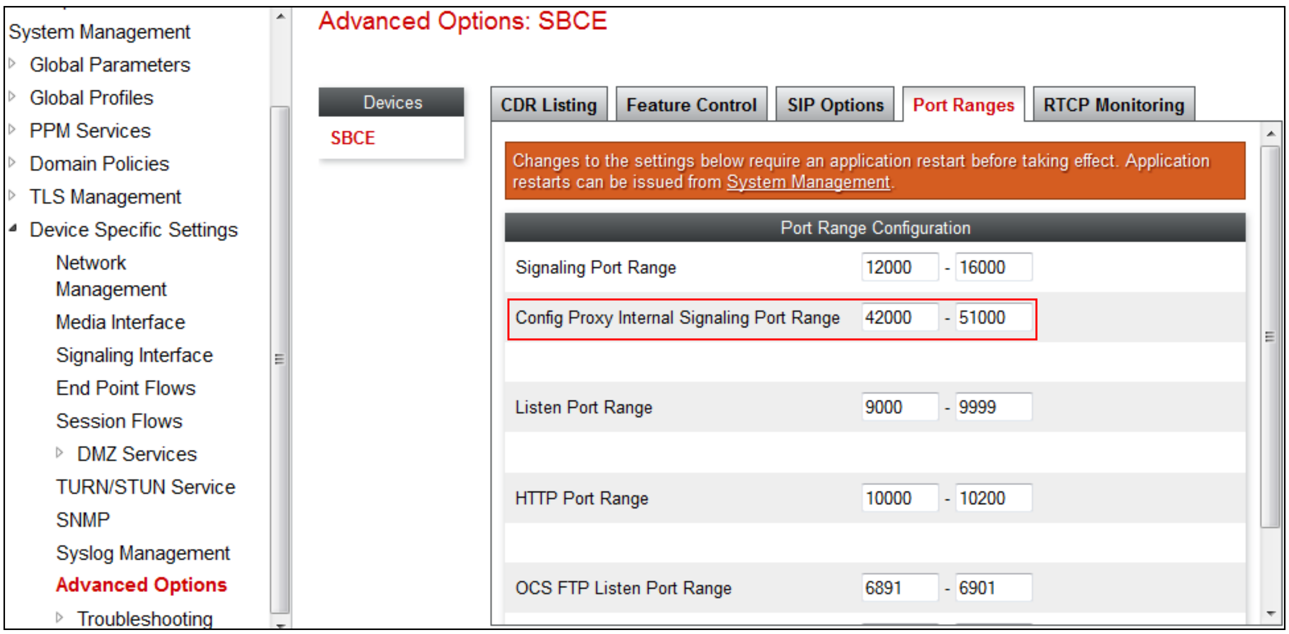
7.4.2 Advanced Options

In **Section 7.4.3**, the media UDP port ranges required by AT&T are configured (**16384 – 32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be defined in **Section 7.4.3**.

1. **Step 1** - Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side.
2. **Step 2** - Select the **Port Ranges** tab.

Step 3 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 4 - Scroll to the bottom of the window and select **Save** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).



7.4.3 Media Interfaces

As mentioned in **Section 7.4.2**, the IPTF service specifies that customers use RTP ports in the range of **16384** – **32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the IPTF service.

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).

Step 2 - Select **Media Interface.**

Step 3 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: **Inside_Trunk_MI**.
- **IP Address**: **192.168.70.120** (Avaya SBCE A1 address).
- **Port Range**: **16384** – **32767**.

Step 4 - Click **Finish** (not shown).

Step 5 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: **Outside_Trunk_MI**.
- **IP Address**: **10.10.10.10** (Avaya SBCE B1 address).
- **Port Range**: **16384 – 32767**.

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**). The completed **Media Interface** screen is shown below.

7.4.4 Signaling Interface

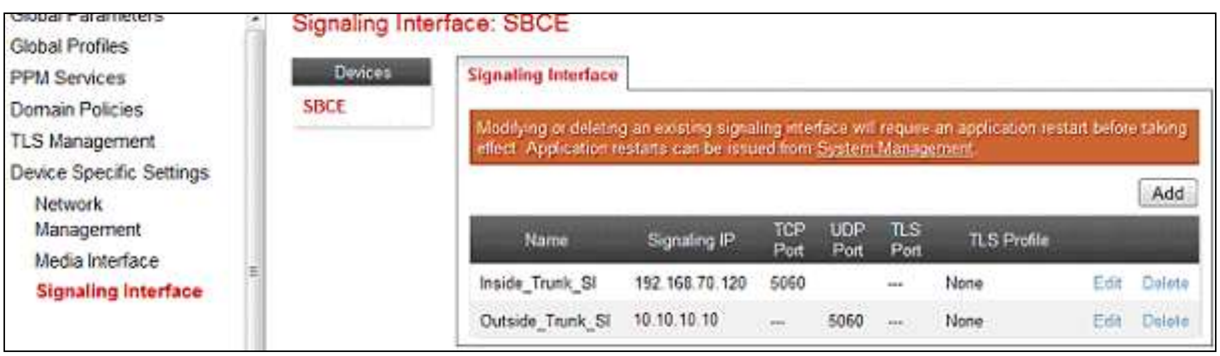
Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).
Step 2 - Select **Signaling Interface**.
Step 3 - Select **Add** (not shown) and enter the following:

- **Name**: **Inside_Trunk_SI**.
- **IP Address**: **192.168.70.120** (Avaya SBCE A1 address).
- **TCP Port**: **5060**.

Step 4 - Click **Finish** (not shown).
Step 5 - Select **Add** again, and enter the following:

- **Name**: **Outside_Trunk_SI**.
- **IP Address**: **10.10.10.10** (Avaya SBCE B1 address).
- **UDP Port**: **5060**.

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).



7.4.5 Endpoint Flows – For Session Manager

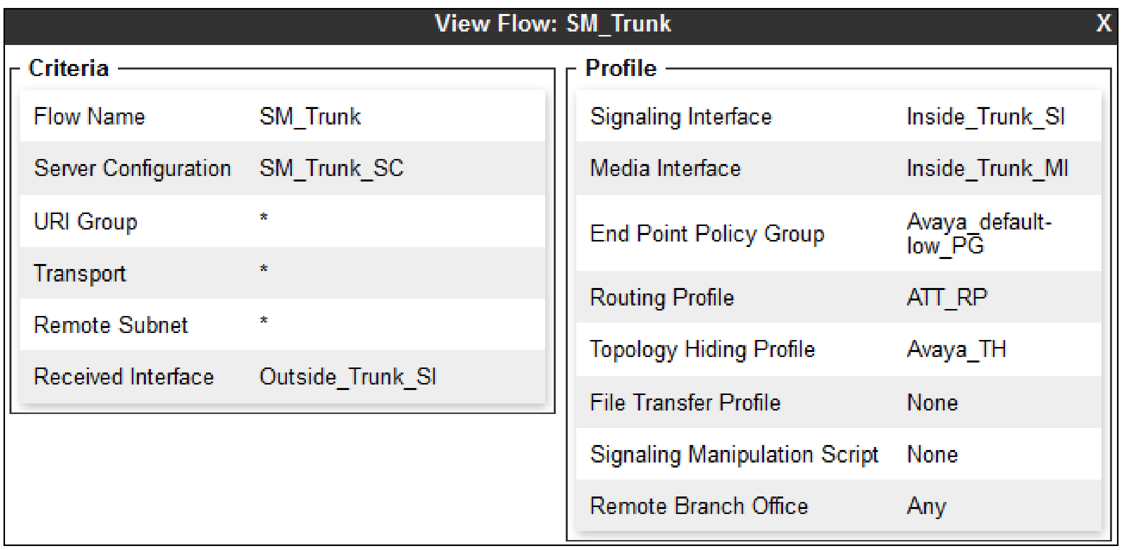
Step 1 - Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).

Step 2 - Select the **Server Flows** tab (not shown).

Step 3 - Select **Add**, (not shown) and enter the following:

- **Name**: **SM_Trunk**.
- **Server Configuration**: **SM_Trunk_SC** (**Section 7.2.3**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Outside_Trunk_SI** (**Section 7.4.4**).
- **Signaling Interface**: **Inside_Trunk_SI** (**Section 7.4.4**).
- **Media Interface**: **Inside_Trunk_MI** (**Section 7.4.3**).
- **End Point Policy Group**: **Avaya_default-low_PG** (**Section 7.3.4**).
- **Routing Profile**: **ATT_RP** (**Section 7.2.6**).
- **Topology Hiding Profile**: **Avaya_TH** (**Section 7.2.7**).
- Let other values default.

Step 4 - Click **Finish** (not shown).

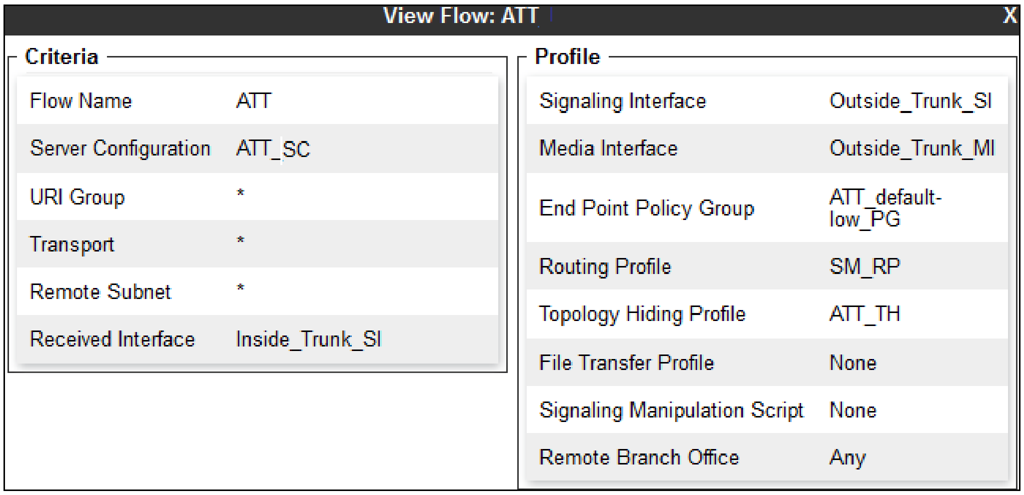


7.4.6 Endpoint Flows – For AT&T

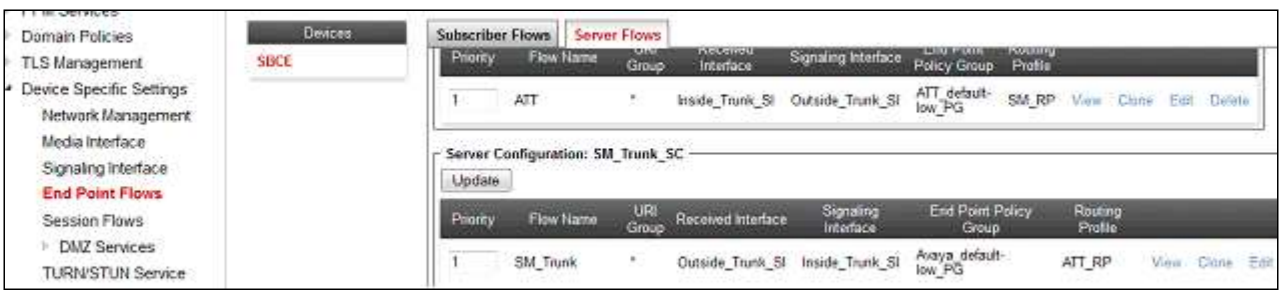
Step 1 - Repeat steps **1** through **4** from **Section 7.4.5**, with the following changes:

- **Name**: **ATT**.
- **Server Configuration**: **ATT_SC** (**Section 7.2.4**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****

- **Received Interface**: **Inside_Trunk_SI** (**Section 7.4.4**).
- **Signaling Interface**: **Outside_Trunk_SI (Section 7.4.4**).
- **Media Interface**: **Outside_Trunk_MI** (**Section 7.4.3**).
- **End Point Policy Group**: **ATT_default-low_PG** (**Section 7.3.5**).
- **Routing Profile**: **SM_RP (Section 7.2.5**).
- **Topology Hiding Profile**: **ATT_TH** (**Section 7.2.8**).



The completed **End Point Flows** screen is shown below.



8 Verification Steps

The following steps may be used to verify the configuration:

8.1 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. 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.

8.2 Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See **[6]** for more information.

- Tracing a SIP trunk.
    a. 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). Note that in the trace shown below, Session Manager has previously converted the IPTF DNIS number included in the Request URI, to the Communication Manager extension 19001, before sending the INVITE to Communication Manager.

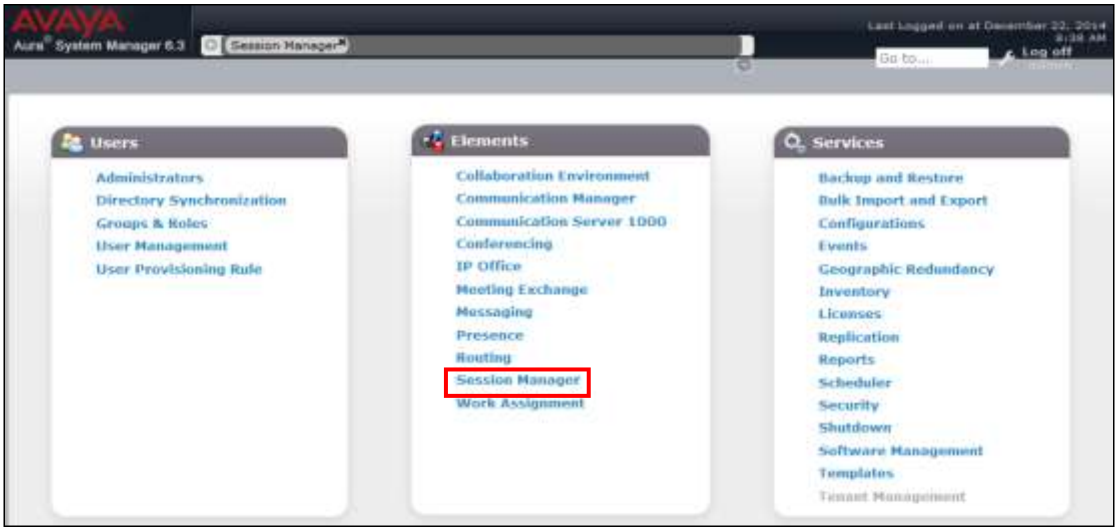
```
list trace tac 602                 LIST TRACE                     Page   1
time            data
15:55:06 TRACE STARTED 04/19/2013 CM Release String cold-02.0.823.0-20396
15:55:16 SIP<INVITE sip:19001@customera.com SIP/2.0
15:55:16     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16     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     G729B ss:off ps:30
             rgn:2 [192.168.70.120]: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     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:18     active station      19001 cid 0x2e9
```

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

8.3 Avaya Aura® Session Manager Status

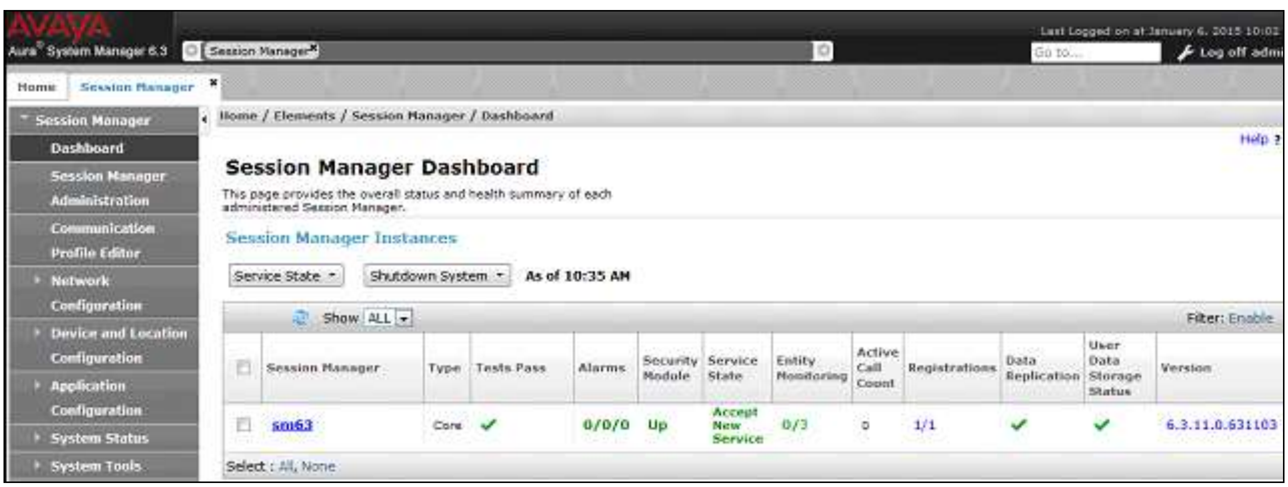
The Session Manager configuration may be verified via System Manager.

Step 1 – Using the procedures described in **Section 5**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.

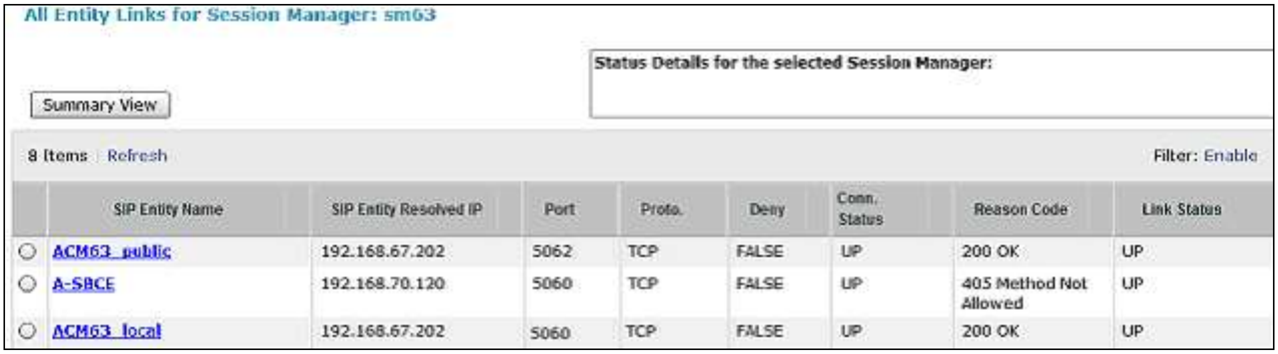


Step 2 – The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status.

In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **3** Entities defined.



Step 3 - Clicking on the **0/3** entry (shown above) in the **Entity Monitoring** column, results in the following display:



All Entity Links for Session Manager: sm63

Status Details for the selected Session Manager:

Summary View

8 Items | Refresh   Filter: Enable

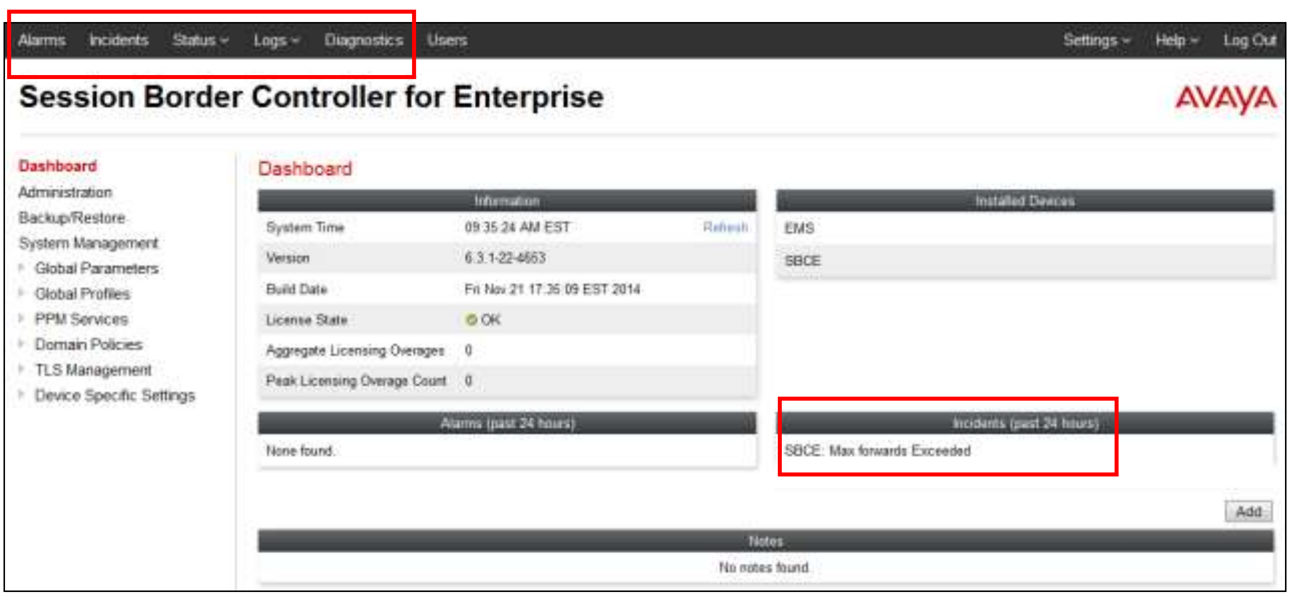
	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	ACM63_public	192.168.67.202	5062	TCP	FALSE	UP	200 OK	UP
○	A-SBCE	192.168.70.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP
○	ACM63_local	192.168.67.202	5060	TCP	FALSE	UP	200 OK	UP

Note the **A-SBCE** Entity from the list of monitored entities above. 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 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 IPTF Border Element, and it is the AT&T Border Element that is generating the 405 response, and the Avaya SBCE sends it back to Session Manager.

Another useful tool is to select **System Tools → Call Routing Test** (not shown) from the left hand menu. This tool allows specific call criteria to be entered, and the simulated routing of this call through Session Manager is then verified.

8.4 Avaya Session Border Controller for Enterprise Verification

Step 1 – Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.



8.4.1 Protocol Traces

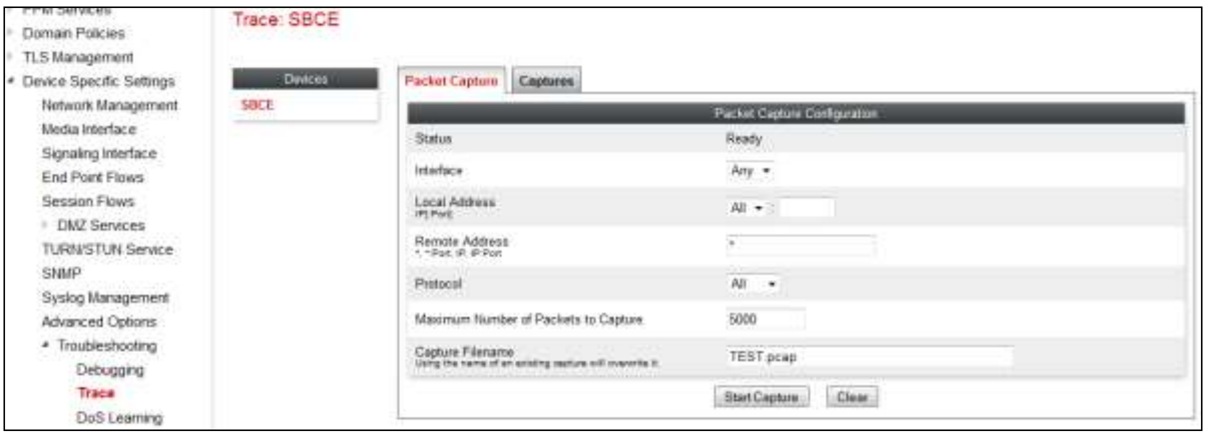
The Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to **Device Specific Settings → Troubleshooting → Trace**.

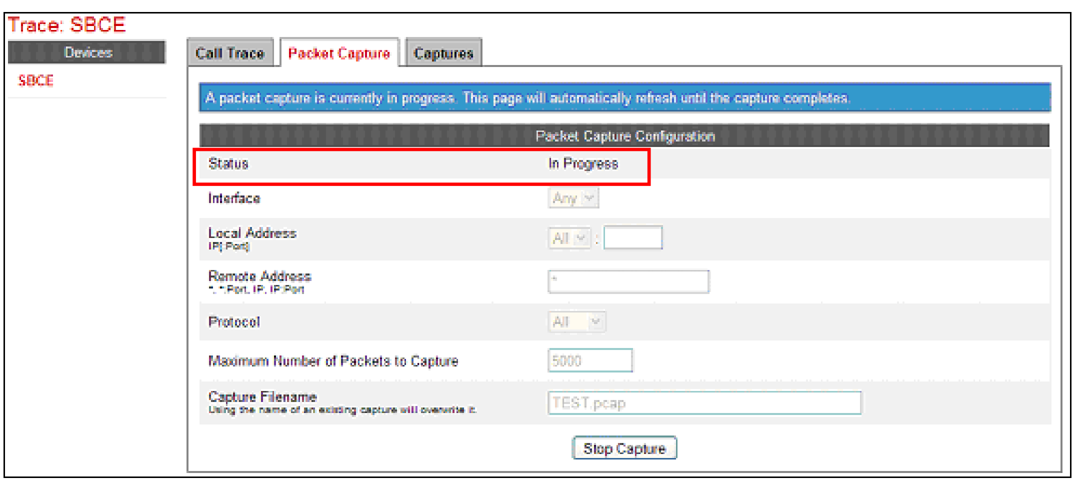
Step 2 - Select the **Packet Capture** tab and select the following:

- Select the desired **Interface** from the drop down menu (e.g., **All**).
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
- Click **Start Capture** to begin the trace.

Note – Specifying **All** in the **Interface** field will result in the Avaya SBCE capturing traffic from both the A1 and B1 interfaces defined in the reference configuration. Also, when specifying the **Maximum Number of Packets to Capture**, estimate a number large enough to include all packets for the duration of the test.



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

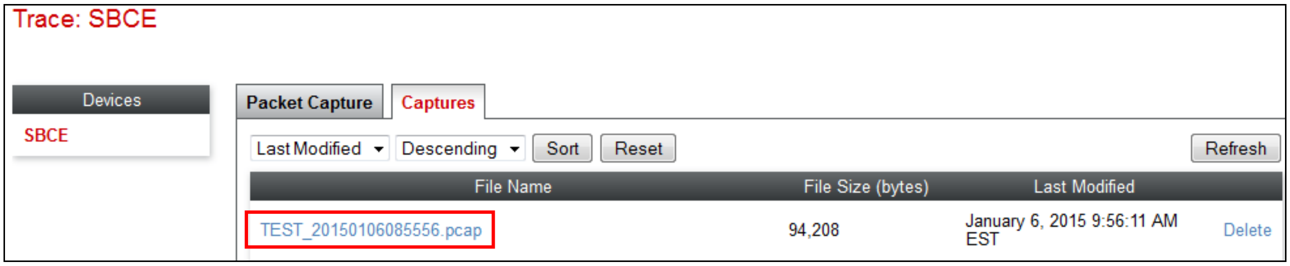


Step 3 – Run the test.

Step 4 – When the test is completed, 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.



9 Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.3, can be configured to interoperate successfully with the AT&T IP Toll Free service, within the constraints described in **Section 2.2.**

Testing was performed on a simulated AT&T IP Toll Free service circuit. The reference configuration shown in these Application Notes 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.

10 References

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

Avaya Aura® Session Manager/System Manager

1. Deploying Avaya Aura® Session Manager, Release 6.3, Issue 6, November 2014

2. Administering Avaya Aura® Session Manager, Release 6.3, Issue 7, September 2014

3. Deploying Avaya Aura® System Manager on System Platform, Release 6.3, Issue 4, June 2014

4. Administering Avaya Aura® System Manager for Release 6.3.10, Release 6.3, Issue 6, November 2014

Avaya Aura® Communication Manager

5. Deploying Avaya Aura® Communication Manager on System Platform, Release 6.3, 18-604394, Issue 6, June 2014

6. Administering Avaya Aura® Communication Manager, Release 6.3, 03-300509, Issue 10, June 2014

7. Administering Avaya G430 Branch Gateway, Release 6.3, 03-603228, Issue 5, October 2013

8. Programming Call Vectors in Avaya Aura® Call Center, 6.0, June 2010

Avaya Session Border Controller for Enterprise

9. Administering Avaya Session Border Controller for Enterprise, Release 6.3, Issue 4, October 2014

10. Deploying Avaya Session Border Controller for Enterprise, Release 6.3, Issue 4, October 2014

11. Application Notes, "*Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communications Manager Rel. 6.3 and Avaya Aura® Session Manager Rel. 6.3, Issue 1.0*" http://origin-support.avaya.com/css/P8/documents/100183254

AT&T IP Toll Free Service:

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

- AT&T IP Toll Free service support: (800) 325-5555.

11 Addendum 1 –Redundancy to Multiple AT&T Border Elements

The AT&T IPTF service 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 **10.10.10.11** and **10.10.10.12**, the Avaya SBCE is provisioned as follows to include the secondary trunk connection to 10.10.10.12 (the primary AT&T trunk connection to 10.10.10.11 is defined in **Section 7.2.4**).

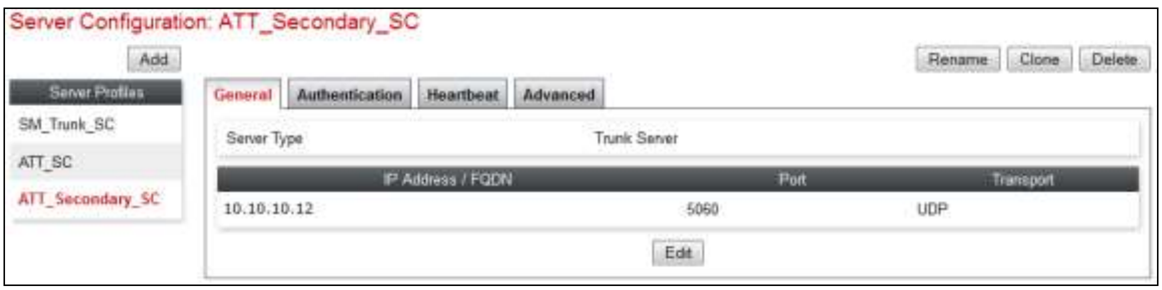
11.1 Secondary AT&T Border Element Server Configuration

Step 1 - Repeat the steps shown in **Section 7.2.4** with the following changes:

- Add a new **Server Configuration** (e.g., **ATT_Secondary_SC)**

Step 2 - On the **Add Server Configuration Profile – General** tab:

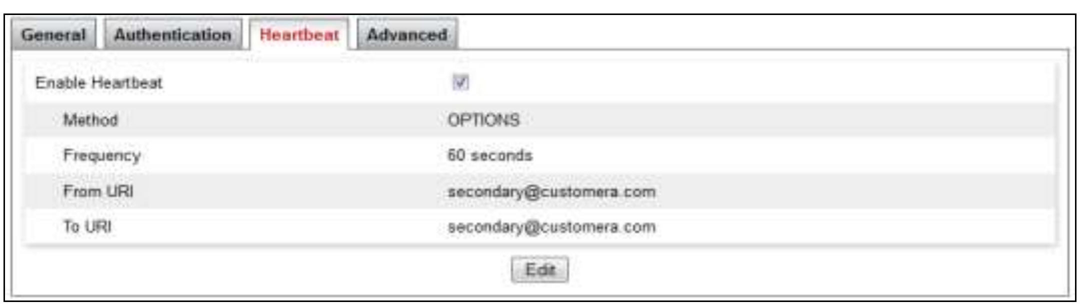
- Enter **the** IP address of the AT&T Secondary Border Element (e.g., **10.10.10.12**). The completed General tab is shown below.



Step 4 - On the **Heartbeat** tab:

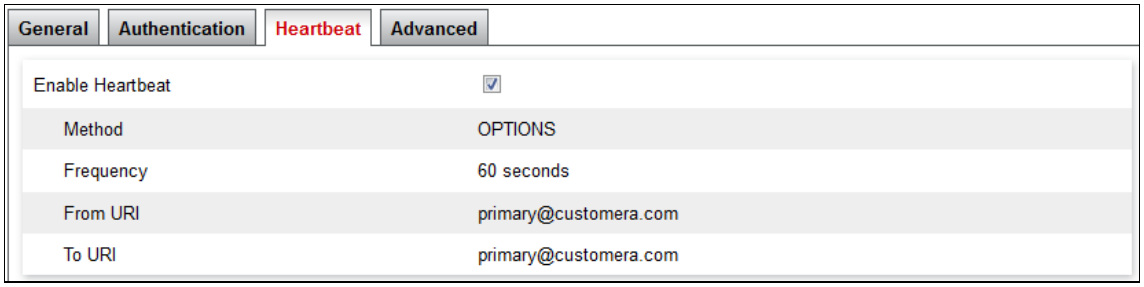
- Check **Enable Heartbeat**.
- **Method: OPTIONS**
- **Frequency:** As desired (e.g., **60** seconds).
- **From URI: secondary@customera.com**
- **To URI: secondary@customera.com**
- Select **Next** (not shown)

Step 5 - On the **Advanced** Tab, click **Finish** (not shown). The completed Heartbeat tab is shown below.



Step 6 - Select the AT&T **Server Configuration** created in **Section 7.2.4** (e.g., **ATT_SC), and** select the **Heartbeat Tab**

Step 7 - Select **Edit** (not shown) and repeat **Steps 4** & **5,** using the information shown below, and then click **Finish** (not shown).



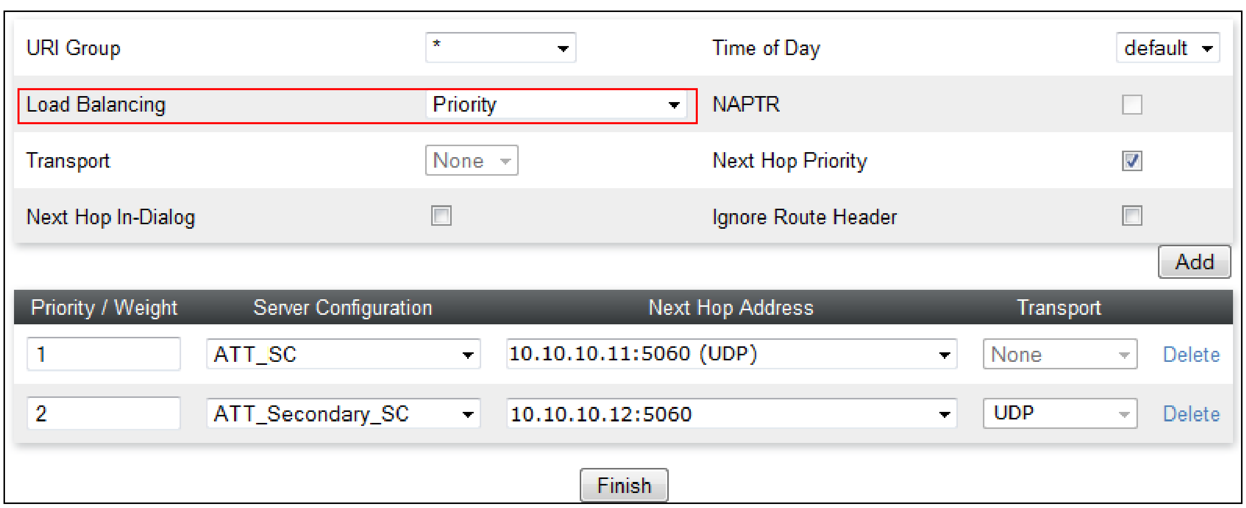
11.2 Add Secondary IP Address to Routing

Step 1 - Select **Global Profiles → Routing** from the left-hand menu.
Step 2 - Select the Routing profile created in **Section 7.2.6** (e.g., **ATT_RP**).
Step 3 - Click **Edit** (not shown), and enter the following:

- **Priority / Weight** : enter **2**.
- **Server Configuration:** Select **ATT_Secondary_SC** from the drop-down menu.
- **Next Hop Address:** enter **10.10.10.12:5060**.
- **Transport**: enter **UDP**.
- Use default values for the rest of the parameters.

Step 4 - Click **Finish**. Note that after selecting Finish, the Transport field will clear and (UDP) will appear in the Next Hop Address field (shown below in the **ATT_SC** Server Configuration entry).

Note – If desired, the **Load Balancing** parameter may be used to modify how the two defined AT&T Border Elements are accessed. **Priority** was used in the Reference Configuration.

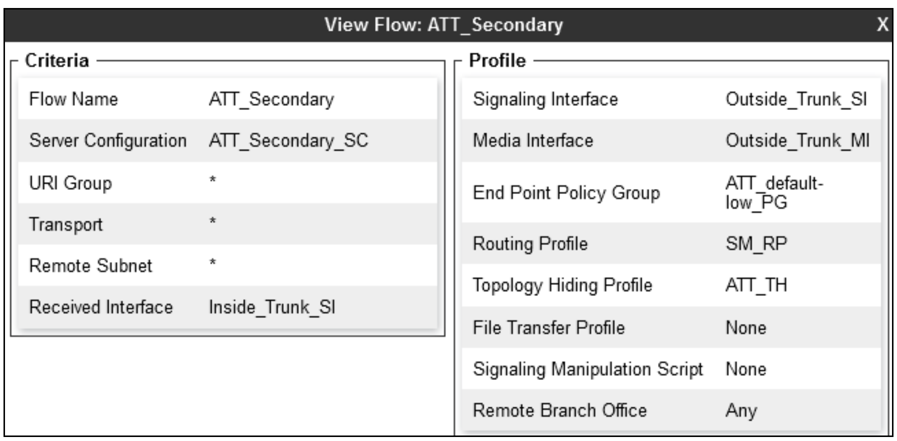


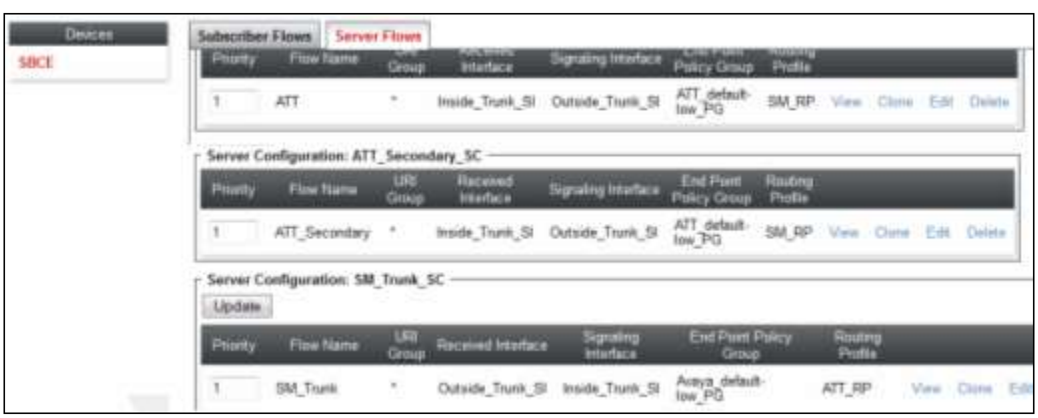
11.3 Configure End Point Flows – Server Flow - ATT_Secondary

Step 1 - Select **Device Specific Settings → Endpoint Flows** from the left-hand menu.
Step 2 - Select the **Server Flows** Tab, and select **Add Flow**. Repeating the steps in **Section 7.4.6**, enter the following:

- **Name: ATT_Secondary**
- **Server Configuration: ATT_Secondary_SC** (**Section 11.1**).
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Inside_Trunk_SI** (**Section 7.4.4**).
- **Signaling Interface: Outside_Trunk_ SI (Section 7.4.4**).
- **Media Interface: Outside_trunk_MI** (**Section 7.4.3**).
- **End Point Policy Group**: **ATT_default-low_PG** (**Section 7.3.5**).
- **Routing Profile: SM_RP** (**Section 7.2.5**).
- **Topology Hiding Profile: ATT_TH** (**Section 7.2.8**).
- Let other values default.

Step 3 - Click **Finish** (not shown). When completed, the Avaya SBCE will issue OPTIONS messages to the primary (10.10.10.11) and secondary (10.10.10.12) AT&T Border Elements.





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