



## 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 6.2 with AT&T IP Toll Free SIP Trunk Service – Issue 1.1**

## **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 6.2 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 6.2 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.



6.4.	IP Interface for procr .....	40
6.5.	IP Network Regions .....	40
6.5.1.	IP Network Region 1 – Local Region .....	40
6.5.2.	IP Network Region 2 – AT&T Trunk Region .....	42
6.6.	IP Codec Parameters .....	43
6.6.1.	Codecs for IP Network Region 1 (local calls) .....	43
6.6.2.	Codecs for IP Network Region 2 .....	44
6.7.	SIP Trunks .....	44
6.7.1.	SIP Trunk for AT&T calls .....	45
6.7.2.	Local SIP Trunk (Avaya Aura® Messaging and Avaya SIP Telephones) .....	47
6.8.	Private Numbering .....	49
6.9.	Route Patterns for Local SIP Trunk .....	50
6.10.	Automatic Alternate Routing (AAR) Dialing .....	51
6.11.	Class of Restriction (COR) .....	51
6.12.	Provisioning for Coverage to Aura® Messaging .....	52
6.12.1.	Hunt Group for Station Coverage to Avaya Aura® Messaging .....	52
6.12.2.	Define Coverage Path for Station Coverage to Avaya Aura® Messaging .....	53
6.12.3.	Apply Station/Agent Coverage Path to Avaya Aura® Messaging and Agent Class of Restriction .....	53
6.13.	Call Center Provisioning .....	55
7.	Avaya Aura® Messaging .....	56
8.	Configure Avaya Session Border Controller for Enterprise .....	57
8.1.	Initial Installation/Provisioning .....	57
8.2.	Log into the Avaya SBCE .....	57
8.3.	Global Profiles .....	57
8.3.1.	Server Interworking – Avaya Side .....	57
8.3.2.	Server Interworking – AT&T Side .....	58
8.3.3.	Routing – Avaya Side .....	59
8.3.4.	Routing – AT&T Side .....	59
8.3.5.	Server Configuration – To Avaya Aura® Session Manager .....	60
8.3.6.	Server Configuration – To AT&T Border Element .....	61
8.3.7.	Topology Hiding – Avaya Side .....	62
8.3.8.	Topology Hiding – AT&T Side .....	63
8.3.9.	Signaling Manipulation .....	64
8.4.	Domain Policies .....	65
8.4.1.	Application Rules .....	65
8.4.2.	Media Rules .....	66
8.4.3.	Signaling Rules .....	67
8.4.4.	Endpoint Policy Groups – Avaya .....	72
8.4.5.	Endpoint Policy Groups – AT&T .....	73
8.5.	Device Specific Settings .....	73
8.5.1.	Network Management .....	73
8.5.2.	Media Interfaces .....	74
8.5.3.	Signaling Interface .....	75

8.5.4.	Endpoint Flows – To Avaya (Session Manager) .....	75
8.5.5.	Endpoint Flows – To AT&T .....	76
9.	Verification Steps.....	77
9.1.	AT&T IP Toll Free Service.....	77
9.2.	Avaya Aura® Session Manager .....	78
9.2.1.	Call Routing Test .....	80
9.3.	Avaya Aura® Communication Manager .....	81
9.4.	Protocol Traces.....	82
9.5.	Avaya Session Border Controller for Enterprise Verification .....	83
9.5.1.	Internal Tracing.....	83
10.	Conclusion .....	85
11.	References.....	86
12.	Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements.....	87
12.1.1.	Configure the Secondary Border Element Server Configuration.....	87
12.1.2.	Add Secondary Border Element IP Address to Routing .....	88
12.1.3.	Configure Secondary AT&T Border Element End Point Flow .....	89



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

## 2.2. Test Results

The main test objectives were to verify the following features and functionality:

- Inbound AT&T IP Toll Free service calls to Communication Manager telephones and VDNs/Vectors/Agents.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones/Agents via the AT&T Toll Free service.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- T.38 fax calls from the AT&T IP Toll Free service/PSTN to Communication Manager G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833/4733 between Communication Manager and the AT&T IP Toll Free service/PSTN automated access systems.
- Inbound AT&T IP Toll Free service calls to Communication Manager that is directly routed to stations, and if unanswered, can be covered to Avaya Aura® Messaging.
- Long duration calls.
- In addition, Avaya Remote Worker (SIP phone) configurations were tested.

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

### 2.2.1. Known Limitations

1. **IP Toll Free ADR call redirection feature in response to a ring-no-answer condition.** If the called Agent returns a 180 followed by 181, then the IP Toll Free ADR feature will trigger and the alternate number is called. However, if the Agent only sends 180, then ADR is not triggered. 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 6.11**).
2. **G.711 Fax support** - G.711 faxing is not supported between Avaya Aura® Communication Manager and the AT&T IP Toll Free service. T.38 fax is supported. The sender and receiver of a 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. Fax speeds are limited to 9600 in the configuration tested.
3. **G.726 codec support** - G.726 codec is not supported between Communication Manager and the AT&T IP Toll Free service.

4. **Avaya SIP endpoints may generate SIP messages with Endpoint-View and AV-Correlation-ID headers.** The Endpoint-View and AV-Correlation-ID headers may be inserted in 18x responses (or in SIP requests), and contain private CPE information (local extensions, domains, etc). In addition, an “epv” parameter is inserted into the Contact header that also contains local network information. The Endpoint-View header has also been observed to cause issues with other AT&T services as well.
  - The workaround is to have the Avaya SBCE remove the **Endpoint-View** and **AV-Correlation-ID** headers, as well as the “epv” parameter (see **Sections 8.3.9, 8.4.3.1 and 8.4.3.2**).
5. **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues.** Certain Avaya SIP endpoints (e.g., 9620, 9630, 9601, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 8.3.9**).
  - **Note** - It was found that when all three Bandwidth headers are sent, the Avaya SBCE will only pass one of the headers to AT&T and block the other two.
    - The Avaya SBCE support team has been notified and an MR was submitted.

## 2.3. Support

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

## 3. Reference Configuration

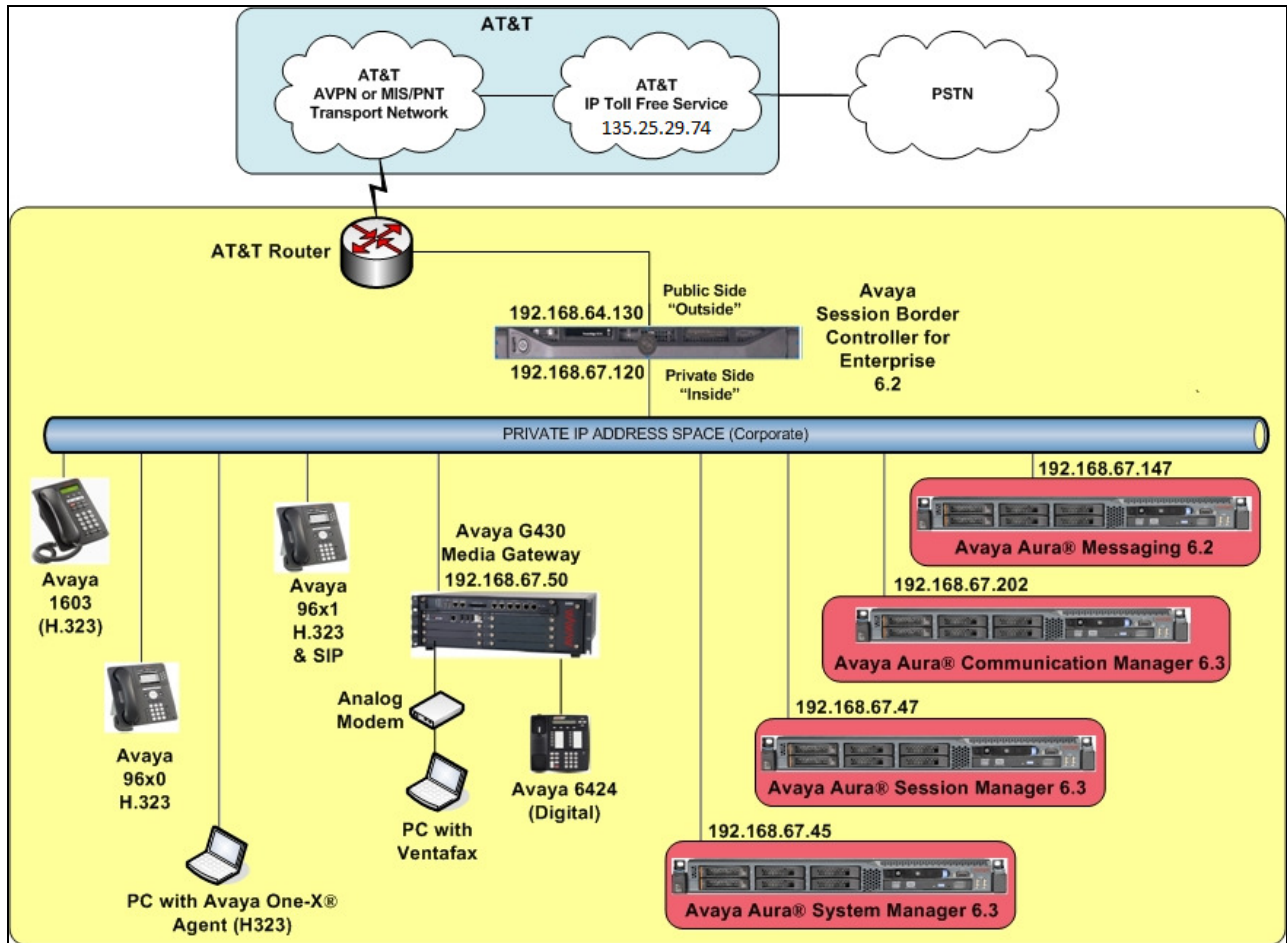
The reference configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Session Manager 6.3 provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya SIP endpoints register to Session Manager.
- System Manager 6.3 provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager 6.3 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 1603(H.323), 960x Series IP Telephones (running H.323 firmware), and 96x1 Series IP Telephones (running H.323 or SIP firmware), Avaya 6424 Digital Telephones, as well as Avaya one-X® Agent soft phone (H.323).
- The Avaya SBCE 6.2 provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network.
- The AT&T IP Toll Free service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya SBCE in this sample configuration. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya SBCE and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP and TLS to communicate with Communication Manager. UDP transport protocol is used between the Avaya SBCE and the AT&T IP Toll Free service.
- Avaya Aura® Messaging was used in the reference configuration to provide voice messaging capabilities. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Inbound calls were placed from PSTN via the AT&T IP Toll Free service, through the Avaya SBCE to the Session Manager, which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate agent/phone or fax extension.

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





**Figure 1: Reference configuration**

### 3.1. Illustrative Configuration Information

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

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

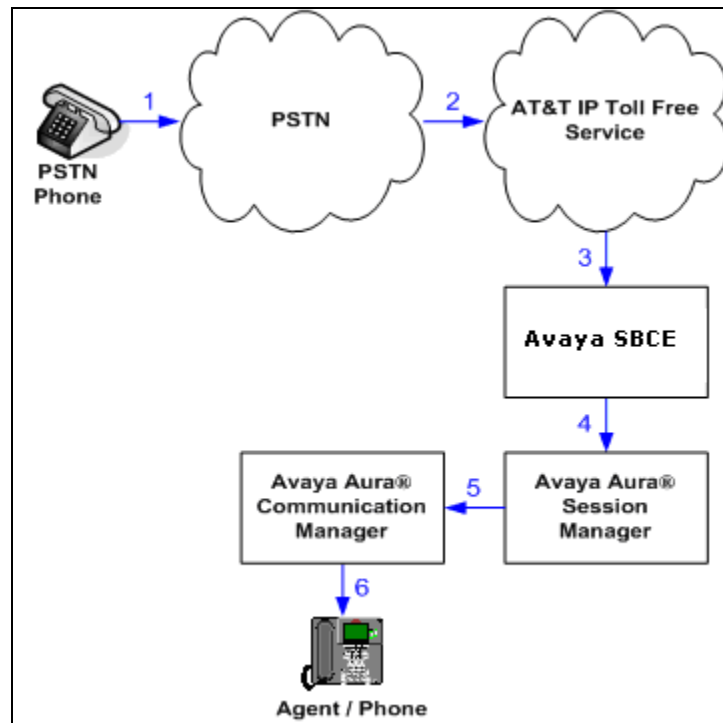
Component	Illustrative Value in these Application Notes
<b>Avaya Aura® System Manager</b>	
IP Address	192.168.67.45
<b>Avaya Aura® Session Manager</b>	
Management IP Address	192.168.67.46
Network IP Address	192.168.67.47
<b>Avaya Aura® Communication Manager</b>	
IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	19xxx = Stations 4xxxx = VDNs
Voice Messaging Pilot Extension	36000
<b>Avaya Session Border Controller for Enterprise (SBCE)</b>	
IP Address of Outside (Public) Interface (to AT&T IP Toll Free Service)	192.168.64.130
IP Address of Inside (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.120
<b>Avaya Aura Messaging</b>	
IP Address	192.168.67.147
Messaging Mailboxes	19xxx
<b>AT&amp;T IP Toll Free Border Element</b>	
IP Address	135.25.29.74

**Table 1: Illustrative Values Used in these Application Notes**

### 3.2. Call Flows

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

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

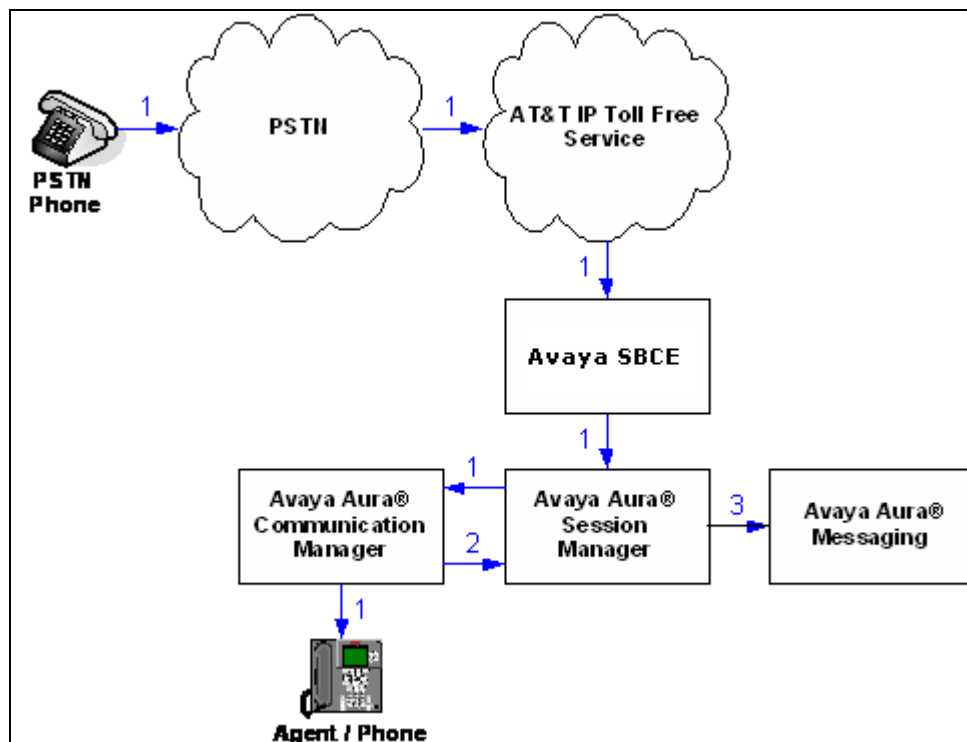


**Figure 2: Inbound AT&T IP Toll Free Service Call to VDN/Agent/Telephone**

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

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

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



**Figure 3: Inbound AT&T IP Toll Free Service Call to Agent / Telephone Covered to Avaya Aura® Messaging**

## 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 <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura® System Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3.0.0.18002</li> <li>6.3.2.4 with SP1 (r1212) and patch 2 (r1451)</li> </ul>
IBM 8800 server <ul style="list-style-type: none"> <li>Avaya Aura® Session Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3 SP2 (6.3.2.632023)</li> </ul>
IBM 8800 server <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura® Communication Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3.0.0.18002</li> <li>6.3 SP0 (06.3-03.0.124.0-20553)</li> </ul>
Dell R610 <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura® Messaging</li> </ul>	<ul style="list-style-type: none"> <li>6.2.1.0.9</li> <li>6.2 SP3 (MSG-02.0.823.0-109_0304)</li> </ul>
Avaya G430 Media Gateway <ul style="list-style-type: none"> <li>MM712 Digital card</li> </ul>	33.13.0 <ul style="list-style-type: none"> <li>HW7 FW11</li> </ul>
Dell R310 <ul style="list-style-type: none"> <li>Avaya Session Border Controller for Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>6.2.0. Q48</li> </ul>
Avaya 96x0 IP Telephone	H.323 Version S3.2
Avaya 96x1 IP Telephone	H.323 Version S6 2408 SIP Version 6.2.2.17
Avaya 9601 IP Telephone	SIP version 6.1.5.12
Avaya one-X® Communicator	H323 6.1 SP8 (6.1.8.06)
Avaya 1603 IP Telephone	H323 (ha1603ua1_3200.bin)
Avaya Flare® Experience for A175	SIP A175-IPT-SIP-R1_1_3-021913
Avaya Flare® Experience for Windows	SIP 1.1.2.11
Avaya 6424 Digital telephone	-
Ventafax Home Version (Windows based Fax device)	6.1.59.144

**Table 2: Equipment and Software Versions**

**Note** - Compliance testing of solutions included the Avaya Session Border Controller for Enterprise (Avaya SBCE) version 6.2; also includes those solutions with the Avaya SBCE version 4.0.5 as well.

## 5. Configure Avaya Aura® Session Manager Release 6.3

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

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

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Avaya SBCE. In addition, provisioning for calls to 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. Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely System Manager.

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

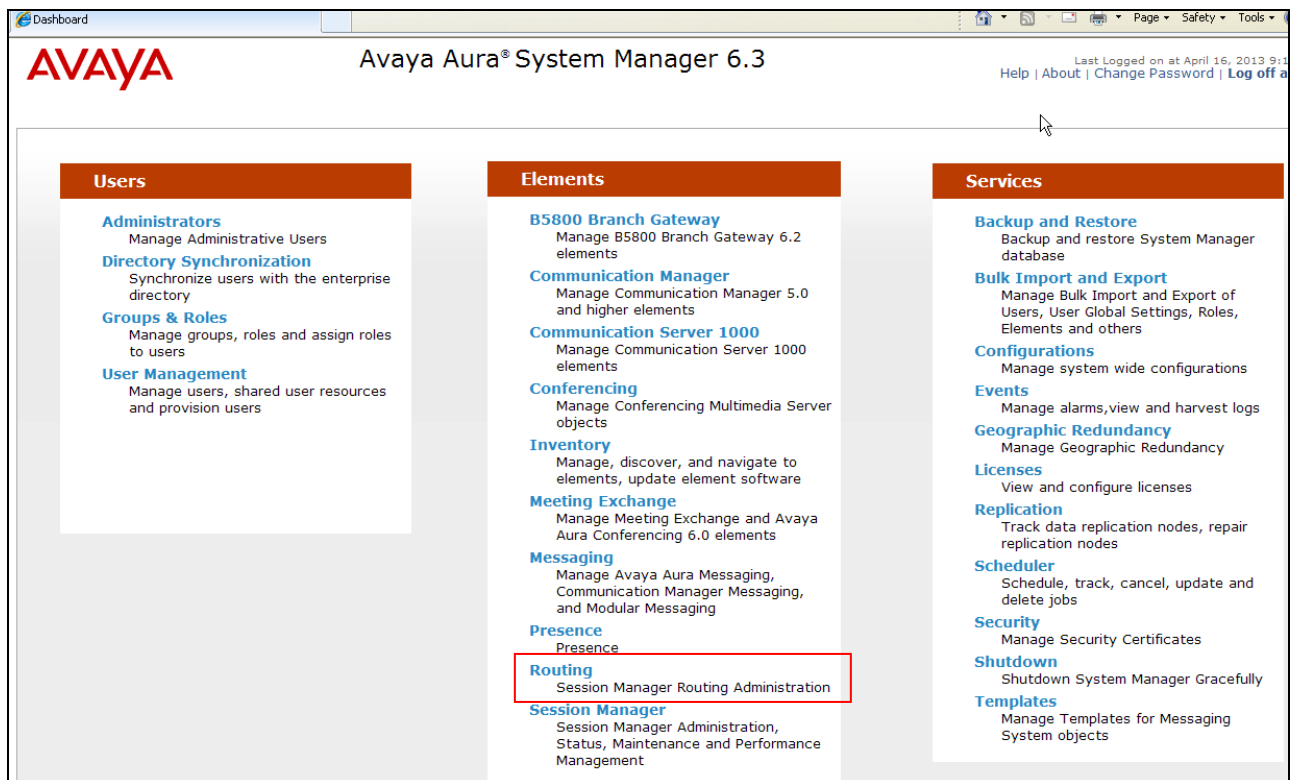
The following administration activities will be described:

- Define SIP Domain
- Define Locations for Communication Manager, the Avaya SBCE, and Aura® Messaging.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Avaya SBCE, and Aura® Messaging.
- Define SIP Entities corresponding to Communication Manager, the Avaya SBCE, and Aura® Messaging.
- Define Entity Links describing the SIP trunk between Communication Manager and Session Manager, the SIP Trunk between Session Manager and the Avaya SBCE, and the SIP trunk between Session manager and Aura® Messaging.

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

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

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



## 5.1. SIP Domain

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

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

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

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

Avaya Aura® System Manager 6.3

Last Logged on at April 16, 2013 9:14 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) × [Home](#)

Home / Elements / Routing / Domains

Domain Management [Commit](#) [Cancel](#) [Help ?](#)

Name	Type	Notes
*customera.com	sip	

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

**Note** – Multiple SIP Domains may be defined if required.

## 5.2. Locations

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

### 5.2.1. Location for CPE Equipment

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

**Step 1** - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location (e.g., **Main**).
- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern:** Enter the IP address of the CPE subnet (e.g., **192.168.67.\***).
- **Notes:** Add a brief description. [Optional]

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



AVAYA

Avaya Aura® System Manager 6.3

Help

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

\* Name:

Main

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

\* Minimum Multimedia Bandwidth:

64

Kbit/Sec

\* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

\* Latency before Overall Alarm Trigger:

5

Minutes

\* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Refresh

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 192.168.67.*	

Select : All, None

Commit Cancel

## 5.3. Configure Adaptations

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

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

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

### 5.3.1. Adaptation for calls to Avaya Aura® Communication Manager

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

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

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

**Step 2** - In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g., **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**).
- In the **Module parameter** field enter **odstd=customera.com osrcd=customera.com**. The **odstd** parameter will replace the IP address of Session Manager (**192.168.67.47**) with **customera.com** in the *inbound* Request URI, and the **osrcd** parameter will replace the AT&T border element IP address (**135.25.29.74**) with **customera.com**, when Session Manager sends the Invite to Communication Manager.

The screenshot shows the Avaya Aura® System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.3", and a user status bar indicating "Last Logged on at April 16, 2013 9:15 AM" with links for "Help", "About", "Change Password", and "Log off admin". The left sidebar contains a tree view with "Routing" selected, and sub-items like "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", and "Regular Expressions". The main content area is titled "Adaptation Details" and includes "Commit" and "Cancel" buttons. Under the "General" tab, the following fields are visible:
 

- \* Adaptation name:** ACM63\_public
- Module name:** DigitConversionAdapter (selected from a dropdown menu)
- Module parameter:** odstd=customera.com osrcd=customera.com
- Egress URI Parameters:** (empty text field)
- Notes:** (empty text field)

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

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

**Step 4** – Repeat **Step 3** for all additional AT&T DNIS numbers.

**Step 5** - Click on **Commit**.

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

**Digit Conversion for Incoming Calls to SM**

Add Remove

0 Items Refresh Filter: Enable

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

**Digit Conversion for Outgoing Calls from SM**

Add Remove

14 Items Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0000001050	*10	*10		*10	44002	destination		IPTF
<input type="checkbox"/>	*0000011051	*10	*10		*10	44003	destination		IPTF
<input type="checkbox"/>	*0000021052	*10	*10		*10	44002	destination		IPTF
<input type="checkbox"/>	*0000031053	*10	*10		*10	19003	destination		IPTF

Select : All, None

Commit Cancel

### 5.3.2. Adaptation for calls to Avaya Aura® Messaging

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

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

**Step 2** - In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g., **AAM\_Digits**).

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

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

- Example: **0000041053** is a DNIS string sent in the Request URI by AT&T Toll Free service that is associated with Avaya Aura® Messaging pilot number 36000.
  - Enter **0000041053** in the **Matching Pattern** column.
  - Enter **10** in the **Min/Max** columns.
  - Enter **10** in the **Delete Digits** column.
  - Enter **36000** in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

**Step 4** - Click on **Commit**.

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

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Adaptations

**Adaptation Details**

Commit Cancel

**General**

\* Adaptation name: AAM\_Digits

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes:

**Digit Conversion for Incoming Calls to SM**

Add Remove

0 Items Refresh

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*0000041053	*10	*10		*10	36000	destination		IPTF

Select : All, None

Commit Cancel

## 5.4. SIP Entities

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

- Session Manager (**Section 5.4.1**).
- Communication Manager for AT&T access (**Section 5.4.2**) – This entity, and its associated Entity Link (using TCP with port 5062, is for calls from AT&T to Communication Manager via the Avaya SBCE.
- Communication Manager for local access (**Section 5.4.3**) – This entity, and 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 IP Toll Free service via the Avaya SBCE.
- Avaya Aura® Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using TCP and port 5060), is for traffic from Avaya Aura® Messaging to Communication Manager.

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

### 5.4.1. Avaya Aura® Session Manager SIP Entity

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

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

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

**Step 3** - In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:

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

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

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

This is for connections to Avaya SBCE and Avaya Aura® Messaging.

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

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

Port	Protocol	Default Domain	Notes
5061	TLS	customera.com	Local traffic
5062	TCP	customera.com	Public traffic

**Step 6** – Enter any notes as desired and leave all other fields on the page blank/default.

**Step 7** - Click on **Commit** (not shown).

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

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

## 5.4.2. Avaya Aura® Communication Manager SIP Entity - Public

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

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

- **Name** – Enter a descriptive name for the Communication Manager public trunk (e.g. **ACM63\_public**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g., **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location **Main** administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page select:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.

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

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** ACM63\_public
- FQDN or IP Address:** 192.168.67.202
- Type:** CM
- Notes:** (empty)
- Adaptation:** ACM63\_public
- Location:** Main
- Time Zone:** America/New\_York
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty)
- Backup Session Manager Bandwidth Association:** (empty)

Buttons for 'Commit' and 'Cancel' are visible in the top right corner.

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

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

### 5.4.3. Avaya Aura® Communication Manager SIP Entity – Local

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

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** ACM63\_Local
- FQDN or IP Address:** 192.168.67.202
- Type:** CM (dropdown menu)
- Notes:** (empty text box)
- Adaptation:** (empty dropdown menu)
- Location:** Main (dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text box)
- Call Detail Recording:** none (dropdown menu)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty dropdown menu)
- Backup Session Manager Bandwidth Association:** (empty dropdown menu)

At the top right of the form are 'Commit' and 'Cancel' buttons.



#### 5.4.4. Avaya Session Border Controller for Enterprise SIP Entity

To configure the Avaya SBCE SIP entity, repeat the steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of the inside interface of the Avaya SBCE and the **Type** field is set to **SIP Trunk**. See the figure below for the values used in the reference configuration. Note that since the IP Toll Free service is inbound only, no Adaptation was necessary.

**SIP Entity Details**CommitCancel

**General**

**\* Name:** A-SBCE

**\* FQDN or IP Address:** 192.168.67.120

**Type:** SIP Trunk

**Notes:**

**Adaptation:**

**Location:** Main

**Time Zone:** America/New\_York

**Override Port & Transport with DNS SRV:** ☐

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

**Credential name:**

**Call Detail Recording:** none

**CommProfile Type Preference:**

**SIP Link Monitoring**

**SIP Link Monitoring:** Link Monitoring Enabled

**\* Proactive Monitoring Interval (in seconds):** 120

**\* Reactive Monitoring Interval (in seconds):** 60

**\* Number of Retries:** 1

**Supports Call Admission Control:** ☐

**Shared Bandwidth Manager:** ☐

**Primary Session Manager Bandwidth Association:**

**Backup Session Manager Bandwidth Association:**

### 5.4.5. Avaya Aura® Messaging SIP Entity

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

The screenshot shows the 'SIP Entity Details' configuration window. It has a 'Commit' button and a 'Cancel' button in the top right corner. The 'General' tab is selected. The configuration fields are as follows:

- Name:** AA-M
- \* FQDN or IP Address:** 192.168.67.147
- Type:** Modular Messaging (dropdown menu)
- Notes:** (empty text field)
- Adaptation:** AAM\_Digits (dropdown menu)
- Location:** Main (dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- \* SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown menu)

The 'SIP Link Monitoring' section is also visible:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty dropdown menu)
- Backup Session Manager Bandwidth Association:** (empty dropdown menu)

## 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**).
- Avaya Aura® Messaging (**Section 5.5.4**).

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

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

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

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

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

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **ACM63\_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5062** (see **Section 5.4.1**).
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **ACM63\_public**).
- **SIP Entity 2 Port** - Enter **5062**.
- **Connection Policy** – Select **Trusted**.

**Step 3** - Click on **Commit**.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* ACM63_public	* sm63	TCP	* 5062	* ACM63_public	* 5062	Trusted	<input type="checkbox"/>	

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

To configure this entity link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.3** for the Communication Manager local Entity (e.g., **ACM63\_Local**). The **Protocol** is **TLS** and the **Port** is **5061**. See the figure below for the values used in the reference configuration.

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* ACM63_Local	* sm63	TLS	* 5061	* ACM63_local	* 5061	Trusted	<input type="checkbox"/>	

### 5.5.3. Entity Link for the Avaya SBCE

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

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* A-SBCE	* sm63	TCP	* 5060	* A-SBCE	* 5060	Trusted	<input type="checkbox"/>	

### 5.5.4. Entity Link to Avaya Aura® Messaging

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

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* AA-M	* sm63	TCP	* 5060	* AA-M	* 5060	Trusted	<input type="checkbox"/>	

## 5.6. Time Ranges

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

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

**Step 3** - Click on **Commit**.

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

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

## 5.7. Routing Policies

In this section, the following Routing Policies are administered:

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

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

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

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

**Step 2** - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **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.

Routing Policy Details

General

\* Name: ACM63\_Public

Disabled: ☐

\* Retries: 0

Notes: from AT&T

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

**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** (not shown).

SIP Entities			
6 Items   Refresh			
	Name	FQDN or IP Address	Type
<input type="radio"/>	AA-M	192.168.67.147	Modular Messaging
<input type="radio"/>	ACM63_local	192.168.67.202	CM
<input checked="" type="radio"/>	ACM63_public	192.168.67.202	CM
<input type="radio"/>	A-SBCE	192.168.67.120	Other
<input type="radio"/>	sm63	192.168.67.47	Session Manager
Select : None			

- 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, if multiple Time Ranges were selected, user may enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on **Commit**.
- Step 8** - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.
- Step 9** - No **Regular Expressions** were used in the reference configuration.
- Step 10** - Click on **Commit**.

Routing Policy Details
Commit
Cancel

General

\* Name: ACM63\_Public  
Disabled: ☐  
\* Retries: 0  
Notes: from AT&T

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM62_public	192.168.67.202	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	1		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Select : All, None

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes

Commit Cancel

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

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

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing local calls to Communication Manager (e.g. **ACM63\_Local**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local SIP Entity (e.g. **ACM63\_Local**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details

CommitCancel

General

\* Name:ACM63\_Local

Disabled:☐

\* Retries:0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM63_Local	192.168.67.202	CM	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

AddRemove

2 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Select : All, None

Regular Expressions

AddRemove

0 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

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

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

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

Routing Policy Details

CommitCancel

General

\* Name: To\_AAM

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

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

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

AddRemove

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Select : All, None

Regular Expressions

AddRemove

0 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------



## 5.8. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:

- Inbound PSTN calls via the AT&T IP Toll Free service to Communication Manager stations/agents.
- Inbound PSTN calls for message retrieval, via Avaya Aura® Messaging pilot extension defined on Communication Manager.
- Message Wait Indicator (MWI) from Avaya Aura® Messaging to Communication Manager.

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

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

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

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

**Step 2** - In the **General** section of the **Dial Pattern Details** page, provision the following:

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

The screenshot shows the 'Dial Pattern Details' page in the Avaya Aura Communication Manager web interface. The left sidebar is expanded to show the 'Routing' menu, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and has a 'General' tab. The form fields are: Pattern (00000), Min (10), Max (10), Emergency Call (unchecked), Emergency Priority (1), Emergency Type (empty), SIP Domain (customer.com), and Notes (IPTF). There are 'Commit' and 'Cancel' buttons at the top right of the form area.

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

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

**Step 5** - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7.1** (e.g., **ACM63\_Public**).

**Originating Location**
☐ Apply The Selected Routing Policies to All Originating Locations

☐ **Name** **Notes** Filter: Enable

☒ Main

Select : All, None

**Routing Policies**
Filter: Enable

☐ **Name** **Disabled** **Destination** **Notes**

☐ ACM63\_Local ☐ ACM62\_local

☒ ACM63\_Public ☐ ACM62\_public from AT&T

☐ A-SBCE\_to\_ATT ☐ A-SBCE

☐ To\_AAM ☐ AA-M

Select : All, None

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

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

**Originating Locations and Routing Policies**

1 Item  Filter: E

☐ **Originating Location Name** **Originating Location Notes** **Routing Policy Name** **Rank** **Routing Policy Disabled** **Routing Policy Destination** **Routing Po Notes**

☐ Main ACM63\_Public 1 ☐ ACM63\_public from AT&T

Select : All, None

**Denied Originating Locations**

0 Items  Filter: E

☐ **Originating Location** **Notes**

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

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

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

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

**Dial Pattern Details**  
**General**  

\* Pattern:

36000

\* Min:

5

\* Max:

5

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

AA-M Pilot Number

**Originating Locations and Routing Policies**  

Add

Remove

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To_AA-M	0	<input type="checkbox"/>	AA-M	

Select : All, None

**Denied Originating Locations**  

Add

Remove

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

\* Input Required 

Commit

Cancel

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

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

- In the **General** section of the **Dial Pattern Details** page, enter the Communication Manager extension pattern based on the 5 digit dial plan defined in **Section 6.2**. In the reference configuration, station extensions used the pattern **19xxx**.
- Enter a **Min** and **Max** pattern of **5**.
- In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox (not shown) corresponding to the Location defined in **Section 5.2.1** (e.g., **Main**).
- In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox (not shown) corresponding to the Routing Policy administered for routing calls to Communication Manager local trunk in **Section 5.7.2** (e.g., **ACM63\_Local**).

Routing / Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

\* Pattern: 19

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: Station MWI and SIP phones

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		ACM63_Local	0	<input type="checkbox"/>	ACM63_local	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

## 6. Avaya Aura® Communication Manager

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

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

### 6.1. System Parameters

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

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

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

<b>display system-parameters customer-options</b>		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	12000	0	
Maximum Concurrently Registered IP Stations:	18000	4	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	18000	1	
Maximum Video Capable IP Softphones:	18000	2	
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>24</b>	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	522	0	
Maximum TN2501 VAL Boards:	128	0	
Maximum Media Gateway VAL Sources:	250	1	
Maximum TN2602 Boards with 80 VoIP Channels:	128	0	
Maximum TN2602 Boards with 320 VoIP Channels:	128	0	
Maximum Number of Expanded Meet-me Conference Ports:	300	0	
(NOTE: You must logoff & login to effect the permission changes.)			

**Step 3 - On Page 4** of the system-parameters customer-options form:

Verify the **Enhanced EC500?** , **IP Stations?**, **ISDN-PRI?**, and **IP Trunks?** fields are set to **y**.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		<b>IP Stations? y</b>
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? n
<b>Enhanced EC500? y</b>	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		<b>ISDN-PRI? y</b>
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
<b>IP Trunks? y</b>		
IP Attendant Consoles? y		
(NOTE: You must logoff & login to effect the permission changes.)		

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

display system-parameters customer-options		Page 5 of 11
OPTIONAL FEATURES		
Multinational Locations? n		Station and Trunk MSP? y
Multiple Level Precedence & Preemption? y		Station as Virtual Extension? y
Multiple Locations? n		
	System Management Data Transfer? n	
Personal Station Access (PSA)? y	Tenant Partitioning? y	
PNC Duplication? n	Terminal Trans. Init. (TTI)? y	
Port Network Support? y	Time of Day Routing? y	
Posted Messages? y	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
<b>Private Networking? y</b>	Usage Allocation Enhancements? y	
Processor and System MSP? y		
<b>Processor Ethernet? y</b>	Wideband Switching? y	
Remote Office? y	Wireless? n	
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

## 6.2. Dial Plan

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

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

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

change dialplan analysis

Page 1 of 12

DIAL PLAN ANALYSIS TABLE

Location: all

Percent Full: 2

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	5	ext						
3	5	ext						
4	5	ext						
6	3	dac						
8	1	fac						
9	1	fac						
*	3	fac						
#	3	fac						

## 6.3. IP Node Names

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

**Step 1** - Enter the **change node-names ip** command, and add a node name and IP address for the following:

- Session Manager signaling interface (e.g., **SM** and **192.168.67.47**).
- Avaya Aura® Messaging (**AAM** and **192.168.67.147**).
- Avaya SBCE private network interface (**A-SBCE** and **192.168.67.120**).

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

## 6.4. IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the reference configuration.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to **y**.
- Assign a **Network Region** (e.g., **1**).
- Use default values for the remaining parameters.

display ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		
Enable Interface? y	Target socket load: 1700	
Network Region: 1	Allow H.323 Endpoints? y	
	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 192.168.67.202	
Subnet Mask: /24		

## 6.5. IP Network Regions

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

### 6.5.1. IP Network Region 1 – Local Region

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



**Step 1** – Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region 1). This IP network region will be used to represent the local CPE. Populate the form with the following values:

- Enter a descriptive name (e.g., **Local**).
- Enter **customerera.com** in the **Authoritative Domain** field.
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min:** – Set to **16384** (AT&T recommendation).
- **UDP Port Max:** – Set to **32767** (AT&T recommendation).

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

**Step 2** - On **page 2** of the form:

- Verify that RTCP reporting and monitoring are set to **y**.

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

**Step 3 - On page 4 of the form:**

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

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

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

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

**Step 1 – On Page 1 of the form:**

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

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

**Step 2** – On **Page 4** of the form:

- Verify that codec set **2** is listed for **dst rgn 3** and **4**.

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

## 6.6. IP Codec Parameters

### 6.6.1. Codecs for IP Network Region 1 (local calls)

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

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

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

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

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

## 6.6.2. Codecs for IP Network Region 2

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

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

change ip-codec-set 2					Page	1 of	2
IP Codec Set							
Codec Set: 2							
Audio	Silence	Frames	Packet				
Codec	Suppression	Per Pkt	Size(ms)				
1: G.729B	n	3	30				
2: G.729A	n	3	30				
3: G.711MU	n	2	20				

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

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

## 6.7. SIP Trunks

Two SIP trunks are defined on Communication Manager in the reference configuration:

- AT&T access trunk – SIP Trunk 2
  - Note that this trunk will use TCP port 5062 as described in **Section 5.5.1**.
- Local trunk for Avaya Aura® Messaging and Avaya SIP telephone access – SIP Trunk 1
  - Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

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

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

### 6.7.1. SIP Trunk for AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for IPTF calls. This trunk corresponds to the **ACM62\_Public** Entity defined in **Section 5.4.2**.

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

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

add signaling-group 2		Page	1 of	1
SIGNALING GROUP				
Group Number: 2	Group Type: sip			
IMS Enabled? n	Transport Method: tcp			
Q-SIP? n				
IP Video? n	Enforce SIPS URI for SRTP? y			
Peer Detection Enabled? y	Peer Server: SM			
Near-end Node Name: procr	Far-end Node Name: SM63			
Near-end Listen Port: 5062	Far-end Listen Port: 5062			
	Far-end Network Region: 2			
	Far-end Secondary Node Name:			
Far-end Domain: customerera.com				
	Bypass If IP Threshold Exceeded? n			
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n			
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y			
Session Establishment Timer(min): 3	IP Audio Hairpinning? n			
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n			
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6			

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

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

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: ATT	COR: 1	TN: 1	TAC: 602
Direction: incoming	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 2		
	Number of Members: 20		

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

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

add trunk-group 2		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
SCCAN? n		Redirect On OPTIM Failure: 5000	
		Digital Loss Group: 18	
<b>Preferred Minimum Session Refresh Interval(sec): 900</b>			
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 **Numbering Format:** to **private**. Note that 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.

<b>add trunk-group 2</b>	<b>Page 3 of 21</b>
TRUNK FEATURES	
ACA Assignment? n	Measured: none      Maintenance Tests? y
<b>Numbering Format: private</b>	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

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

- Verify **Network Call Redirection** and **Send Diversion Header** are set to **n** (default).
- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPTF service (e.g., **100**).

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

<b>add trunk-group 2</b>	<b>Page 4 of 21</b>
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	Send Transferring Party Information? n
	<b>Network Call Redirection? n</b>
Build Refer-To URI of REFER From Contact For NCR? n	
	<b>Send Diversion Header? n</b>
	<b>Support Request History? y</b>
	<b>Telephone Event Payload Type: 100</b>
	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

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

This section describes the steps for administering the local SIP trunk to Session Manager. This trunk is used for Avaya Aura® Messaging and Avaya SIP station calls. This trunk corresponds to the **ACM62\_Local** Entity defined in **Section 5.4.3**.

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **1**), and repeat the steps in **Section 6.7.1** with the following changes:

- **Transport Method** – Set to **tls** (see the note at the beginning of this section).

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061** (see the note at the beginning of this section).
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.5.1**.

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

**Step 2** - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **1**). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.7.1** with the following changes:

- **Group Name** – Enter a descriptive name (e.g., **Local**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **601**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **1**).

<b>add trunk-group 1</b>		<b>Page 1 of 21</b>
TRUNK GROUP		
<b>Group Number: 1</b>	<b>Group Type: sip</b>	<b>CDR Reports: y</b>
<b>Group Name: Local</b>	<b>COR: 1</b>	<b>TN: 1</b>
<b>Direction: two-way</b>	<b>Outgoing Display? n</b>	<b>TAC: 601</b>
<b>Dial Access? n</b>	<b>Night Service:</b>	
<b>Queue Length: 0</b>		
<b>Service Type: tie</b>	<b>Auth Code? n</b>	
	<b>Member Assignment Method: auto</b>	
	<b>Signaling Group: 1</b>	
	<b>Number of Members: 20</b>	

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

- Configure the same as **Section 6.7.1**.

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



- Configure the same as **Section 6.7.1**.

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

- Set **Telephone Event Payload Type** to the RTP payload type required by the IPTF service (e.g., **100**).
- Use default for all other values.

<b>add trunk-group 1</b>	<b>Page 4 of 21</b>
PROTOCOL VARIATIONS	
Mark Users as Phone? n Prepend '+' to Calling/Alerting/Diverting/Connected Number? n Send Transferring Party Information? n Network Call Redirection? n Build Refer-To URI of REFER From Contact For NCR? n Send Diversion Header? n Support Request History? y <b>Telephone Event Payload Type: 100</b> 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. Private Numbering

In the reference configuration, the private-numbering form is used to:

- Convert Communication Manager local extensions to IPTF DNIS numbers, (previously identified by AT&T), for inclusion in any SIP headers directed to the IPTF service via the public trunk (e.g., 2) defined in **Section 6.7.1**.
- Define local extension ranges to facilitate call coverage to Avaya Aura® Messaging via the local trunk (e.g., 1) defined in **Section 6.7.2**.

**Step 1** - Using the **change private-numbering 0** command, enter the following for the messaging pilot number (for the local trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager extension assigned to the Avaya Aura® Messaging coverage hunt group defined in **Section 6.11.1** (e.g., **36000**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

**Step 2** – Add all Communication Manager local extension patterns (for the local trunk).

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

**Step 3** – Add a Communication Manager station extension and its corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager station extension (e.g., **19005**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **0000001050**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

**Step 4** – Add a Communication Manager Skill VDN extension and its corresponding IPTF DNIS number (for the public trunk):

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

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

change private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	1	1		5	Total Administered: 10
5	36000	1		5	Maximum Entries: 540
5	4	1		5	
5	19005	2	0000001050	10	
5	19020	2	0000001051	10	
5	19021	2	0000001052	10	
5	19022	2	0000031053	10	
5	44002	2	0000041050	10	
5	44003	2	0000021050	10	
5	44004	2	0000011050	10	

## 6.9. Route Patterns for Local SIP Trunk

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

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

**Step 1** – Enter the **change route-pattern 1** command and enter the following:

- In the **Grp No** column enter 1 for SIP trunk 1 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the Numbering Format column, across from line **1**: enter **unk-unk**.

change route-pattern 1												Page	1	of	3	
Pattern Number: 1												Pattern Name: Local Trunk				
SCCAN? n												Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC			
No				Mrk	Lmt	List	Del	Digits					QSIG			
												Dgts				
1: 1	0											n	user			
2:												n	user			
3:												n	user			
4:												n	user			
5:												n	user			
6:												n	user			
BCC VALUE		TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	No.	Numbering	LAR					
0 1 2 M 4 W		Request									Dgts	Format				
												Subaddress				
1:	y	y	y	y	y	n	n	rest				unk-unk	none			
2:	y	y	y	y	y	n	n	rest					none			
3:	y	y	y	y	y	n	n	rest					none			
4:	y	y	y	y	y	n	n	rest					none			
5:	y	y	y	y	y	n	n	rest					none			

## 6.10. Automatic Alternate Routing (AAR) Dialing

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

**Step 1** – Enter the following:

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

change aar analysis 0							Page	1 of	2
AAR DIGIT ANALYSIS TABLE									
Location: all							Percent Full: 1		
Dialed		Total		Route	Call	Node	ANI		
String		Min	Max	Pattern	Type	Num	Reqd		
1902		5	5	1	aar		n		
36000		5	5	1	aar		n		

## 6.11. Class of Restriction (COR)

As described in **Section 2.2.1, 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 called Agent returns a 180 followed by 181, then the IP Toll Free ADR feature will trigger and the alternate number is called. However, if the Agent only sends 180, then ADR is not triggered. Whether 181 is sent or not is determined by the **Direct Agent Calling** setting in the **Class of Restriction** form. Note that the COR level is applied to the Agent form (see **Section 6.12.3**).

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

change cor 2		Page 1 of 23
CLASS OF RESTRICTION		
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	<b>Direct Agent Calling? y</b>	
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	

## 6.12. Provisioning for Coverage to Aura® Messaging

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

### 6.12.1. Hunt Group for Station Coverage to Avaya Aura® Messaging

**Step 1** – Enter the command **add hunt-group x**, where x is an available hunt group (e.g., 1), and on **Page 1** of the form enter the following:

- **Group Name** – Enter a descriptive name (e.g., AAM).
- **Group Extension** – Enter an available extension (e.g., 36000). Note that the hunt group extension need *not* be the same as the Avaya Aura® Messaging pilot number.
- **ISDN/SIP Caller Display** – Enter **mbr-name**.
- Let all other fields default.

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

**Step 2** – On **Page 2** of the form enter the following:

- **Message Center** – Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Voice Mail Handle** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 6.2** (e.g., **8**).

<b>change hunt-group 1</b>		<b>Page 2 of 60</b>
HUNT GROUP		
Message Center: <b>sip-adjunct</b>		Routing Digits
Voice Mail Number	Voice Mail Handle	(e.g., AAR/ARS Access Code)
<b>36000</b>	<b>36000</b>	<b>8</b>

### 6.12.2. Define Coverage Path for Station Coverage to Avaya Aura® Messaging

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

**Step 1** – Enter the command **add coverage path x**, where **x** is an available coverage path (e.g., **1**), and on **Page 1** of the form enter the following:

- **Point1** – Specify the hunt group defined in the previous section (e.g., **h1**).
- **Rng** – Enter the number of rings before the stations go to coverage (e.g., **4**).
- Let all other fields default.

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

### 6.12.3. Apply Station/Agent Coverage Path to Avaya Aura® Messaging and Agent Class of Restriction.

The coverage path configured in the previous section is defined on the station form or on the agent form. In addition, the Class of Restriction (COR) defined in **Section 6.11** is applied to the Agent.

**Step 1** – Enter the command **change station xxxxx**, where **xxxxx** is a previously defined station (e.g., **19001**), and on **Page 1** of the form enter the following:

- **Coverage path** – Specify the coverage path defined in **Section 6.12.2**. Note that the coverage path field will appear at different positions on the form depending on whether agent or station extensions are being provisioned.

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

**Step 2** – Enter the command **change agent xxxxx**, where **xxxxx** is a previously defined agent (e.g., **47002**), and on **Page 1** of the form enter the following:

- **COR** – Specify the Class of Restriction defined in **Section 6.11**.
- **Coverage path** – Specify the coverage path defined in **Section 6.12.2**.

change agent-loginID 47002		Page 1 of 3
AGENT LOGINID		
Login ID: 47002	AAS? n	
Name: Agent2	AUDIX? n	
TN: 1	LWC Reception: spe	
<b>COR: 2</b>	LWC Log External Calls? n	
<b>Coverage Path: 1</b>	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. Call Center Provisioning

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

- Agent form – Page 1

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

- Agent form – Page 2

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

- Skill 2 Hunt Group form – Page 1

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

- Skill 2 VDN form – **Page 1**

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

- Skill 2 Vector form – **Page 1**

display vector 2		Page 1 of 6
CALL VECTOR		
Number: 2	Name: Skill2	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y	ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y	CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y	
01 wait-time	2 secs	hearing ringback
02 announcement	42002	
03 queue-to	skill 2	pri m
04 wait-time	10 secs	hearing music
05 announcement	42005	
06 goto step	3	if unconditionally
07 stop		
08		

## 7. Avaya Aura® Messaging

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



## 8. Configure Avaya Session Border Controller for Enterprise

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

### 8.1. Initial Installation/Provisioning

**Note:** The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [8] and [9] for additional information.

**IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.**

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

### 8.2. Log into the Avaya SBCE

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

1. Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the login ID and password.



### 8.3. Global Profiles

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

#### 8.3.1. Server Interworking – Avaya Side

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

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

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

**Next**

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

### 8.3.2. Server Interworking – AT&T Side

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

**Step 1** - On the **General** Tab:

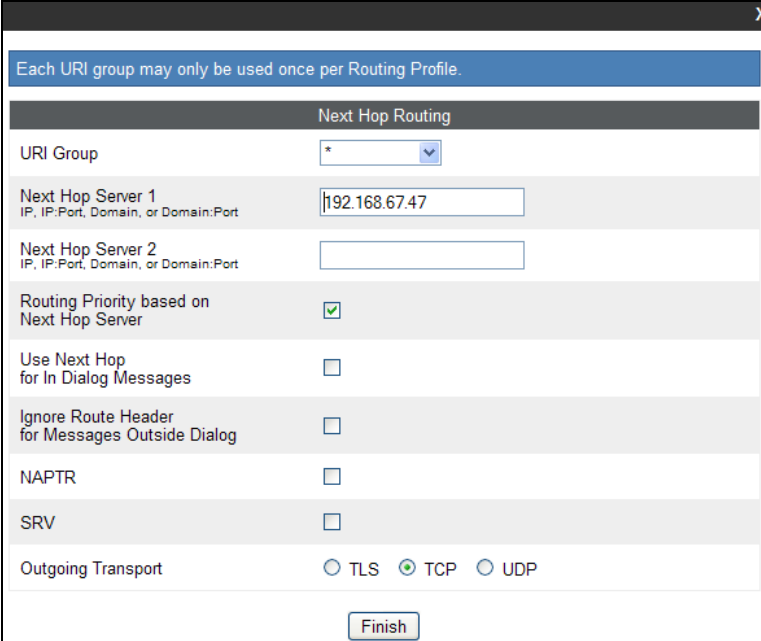
- Enter a profile name: (e.g., **ATT\_Trunk\_SI**).
- Check **T38 Support**.
- All other options on the General Tab can be left at default.
- Select **Next**.

**Step 2** - Accept default values on all remaining tabs, then click **Finish** (not shown).

### 8.3.3. Routing – Avaya Side

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

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



The screenshot shows a configuration window titled "Next Hop Routing". At the top, a blue banner states "Each URI group may only be used once per Routing Profile." Below this, the configuration fields are as follows:

Next Hop Routing	
URI Group	<input type="text" value="*"/>
Next Hop Server 1 <small>IP, IP:Port, Domain, or Domain:Port</small>	<input type="text" value="192.168.67.47"/>
Next Hop Server 2 <small>IP, IP:Port, Domain, or Domain:Port</small>	<input type="text"/>
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input checked="" type="radio"/> TCP <input type="radio"/> UDP
<input type="button" value="Finish"/>	

### 8.3.4. Routing – AT&T Side

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

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

6. Click **Finish**.

Each URI group may only be used once per Routing Profile.

**Next Hop Routing**

URI Group: \*

Next Hop Server 1: 135.25.29.74

Next Hop Server 2:

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☐ TCP ☒ UDP

Finish

### 8.3.5. Server Configuration – To Avaya Aura® Session Manager

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

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**, and select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **SM\_Trunk\_SC**) and select **Next**.
3. The **Add Server Configuration Profile - General** window will open (not shown).
  - a. Select Server Type: **Call Server**
  - b. **IP Address: 192.168.67.47** (Session Manager IP Address)
  - c. **Supported Transports:** Check **UDP** and **TCP**
  - d. **TCP Port: 5060**
  - e. **UDP Port: 5060**
  - f. Select **Next**
4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
  - a. Select **Next** to accept default values.
5. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
  - a. Select **Next** to accept remaining default values.
6. The **Add Server Configuration Profile - Advanced** window will open.
  - a. Select **Enable Grooming**
  - b. For **Interworking Profile** select **Avaya\_Trunk\_SI** created in **Section 8.3.1**.

- c. For the **Signaling Manipulation Script** select the **epv\_parameter\_bandwidth** script defined in **Section 8.3.9**.
- d. Select **Finish**, accepting remaining default values.

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

**Server Configuration: SM\_Trunk\_SC**

Buttons: Add, Rename, Clone, Delete

Server Profiles: SM\_Trunk\_SC

**General** | Authentication | Heartbeat | Advanced

Server Type	Call Server
IP Addresses / FQDNs	192.168.67.47
Supported Transports	TCP, UDP, TLS
TCP Port	5060
UDP Port	5060
TLS Port	5061

Edit

**General** | Authentication | Heartbeat | **Advanced**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya_Trunk_SI
TLS Client Profile	
Signaling Manipulation Script	epv_parameter_bandwidth
TCP Connection Type	SUBID
UDP Connection Type	SUBID
TLS Connection Type	SUBID

Edit

### 8.3.6. Server Configuration – To AT&T Border Element

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

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**.
3. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **ATT\_SC**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will Open (not shown).
  - a. Select Server Type: **Trunk Server**
  - b. **IP Address: 135.25.29.74** (IPTF Border Element IP Address).
  - c. **Supported Transports: Check UDP**
  - d. **UDP Port: 5060**

- e. Select **Next**.
5. The **Add Server Configuration Profile - Authentication** window will open (not shown).
  - a. Select **Next** to accept default values.
6. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
  - a. Select **Next** to accept default values.
7. The **Add Server Configuration Profile - Advanced** window will open.
  - e. Select **ATT\_Trunk\_SI** for **Interworking Profile** (created in **Section 8.3.2**).
  - a. Select **Finish**.

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

The screenshot shows the 'Server Configuration: ATT\_SC' window with the 'General' tab selected. The left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main area shows the 'Server Profiles' list with 'ATT\_SC' and 'SM\_Trunk\_SC'. The 'General' tab displays the following configuration:

General	Authentication	Heartbeat	Advanced
Server Type	Trunk Server		
IP Addresses / FQDNs	135.25.29.74		
Supported Transports	UDP		
UDP Port	5060		

An 'Edit' button is located at the bottom right of the configuration table.

The screenshot shows the 'Server Configuration: ATT\_SC' window with the 'Advanced' tab selected. The configuration is as follows:

General	Authentication	Heartbeat	Advanced
Enable DoS Protection	<input type="checkbox"/>		
Enable Grooming	<input type="checkbox"/>		
Interworking Profile	ATT_Trunk_SI		
Signaling Manipulation Script	None		
UDP Connection Type	SUBID		

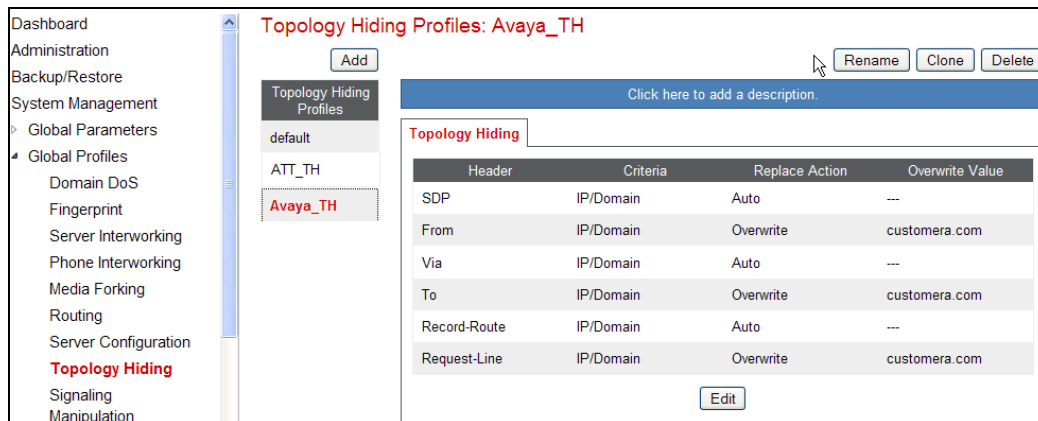
An 'Edit' button is located at the bottom right of the configuration table.

### 8.3.7. Topology Hiding – Avaya Side

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

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.
3. Click **default** profile and select **Clone Profile**.
4. Enter Profile Name: (e.g., **Avaya\_TH**).
5. For the Header **To**,
  - a. In the **Criteria** column select **IP/Domain**

- b. In the **Replace Action** column select: **Overwrite**
  - c. In the **Overwrite Value** column: **customera.com**
6. For the Header **From**,
  - a. In the **Criteria** column select **IP/Domain**
  - b. In the **Replace Action** column select: **Overwrite**
  - c. In the **Overwrite Value** column: **customera.com**
7. For the Header **Request Line**,
  - a. In the **Criteria** column select **IP/Domain**
  - b. In the **Replace Action** column select: **Overwrite**
  - c. In the **Overwrite Value** column: **customera.com**
8. Click **Finish** (not shown).



### 8.3.8. Topology Hiding – AT&T Side

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

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

Topology Hiding Profiles

default
ATT\_TH
Avaya\_TH

Click here to add a description.

**Topology Hiding**

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

Edit

### 8.3.9. Signaling Manipulation

The Avaya SBCE can manipulate inbound and outbound SIP headers. In the reference configuration, one signaling manipulation script is used.

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

**Step 1** - As described in **Section 2.2.1, Item 4**, Avaya SIP endpoints may send requests with Endpoint-View headers containing private network information. These are removed in **Section 8.4.3**. However an “epv” parameter is also inserted into the Contact header of these requests. This parameter also contains private network information. The following signaling manipulation is used to remove this “epv” parameter from the Contact header.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **epv\_parameter\_bandwidth**). The following script is defined:

Title

epv\_parameter\_bandwidth

Save

```

1 // Remove epv paramater from Contact in SIP endpoint Invite
2
3 within session "INVITE"
4 {
5     act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6     {
7         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
8     }
9 }
10

```



**Step 2** - As described in **Section 2.2.1, Item 5**, some Avaya SIP endpoints may send Bandwidth headers that may cause issues with the AT&T network. The following signaling manipulation script is added to the script defined in **Step 1** above, to remove these Bandwidth headers.

1. The following script is added:

Titleepv\_parameter\_bandwidthSave

```
1 // Remove epv paramater from Contact in SIP endpoint Invite
2
3 within session "INVITE"
4 {
5     act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6     {
7         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
8     }
9 }
10
11 // Remove Bandwidth Headers to AT&T
12
13 within session "ALL"
14 {
15     act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
16     {
17         %BODY[1].regex_replace("b=AS:64\r\n","");
18         %BODY[1].regex_replace("b=CT:64\r\n","");
19         %BODY[1].regex_replace("b=TIAS:64000\r\n","");
20     }
21 }
22
```

**Step 3** - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the Avaya Server Configuration in **Section 8.3.5, Step 6**.

## 8.4. Domain Policies

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

### 8.4.1. Application Rules

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Application Rules**
3. Select the **default** Rule
4. Select **Clone Rule** button
  - a. Name: **SIP\_Trunk\_AR**
  - b. Click **Finish**
5. Highlight the rule just created: **SIP\_Trunk\_AR**
  - a. Click the **Edit** button
  - b. In the **Voice** row:
    - i. Change the **Maximum Concurrent Sessions** to an appropriate amount (e.g., **2000**)

- ii. Change the **Maximum Sessions per Endpoint** to an appropriate amount (e.g.,**2000**)

**Application Rules: SIP\_Trunk\_AR**

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Click here to add a description.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

**Miscellaneous**

CDR Support	None
RTCP Keep-Alive	No

Edit

### 8.4.2. Media Rules

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

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

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

Dashboard  
Administration  
Backup/Restore  
System Management  
  > Global Parameters  
  > Global Profiles  
  > SIP Cluster  
  4 Domain Policies  
    Application Rules  
    Border Rules  
    **Media Rules**  
    Security Rules  
    Signaling Rules  
    Time of Day Rules  
    End Point Policy Groups  
    Session Policies  
  > TLS Management  
  > Device Specific Settings

**Media Rules: Avaya\_Trunk\_low\_med**

Add Filter By Device... Rename Clone Delete

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- ATT\_low\_med
- Avaya\_Trunk\_low\_med**

Click here to add a description.

Media NAT Media Encryption Media Anomaly Media Silencing **Media QoS**

Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

Audio DSCP AF11

Video QoS

Video DSCP AF11

Edit

### 8.4.3. Signaling Rules

Signaling Rules may be used to remove various SIP headers.

#### 8.4.3.1 Avaya - Requests

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

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

Use the following steps to remove the **P-Location** header:

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button
  - Enter a name: **Avaya\_with\_SM**
  - Click **Finish**
5. Highlight the **Avaya\_with\_SM** rule created in **Step 4** and enter the Following:
  - Select the **Add In Header Control** button (not shown). The Add Header Control window will open.
  - Select the **Request Headers** tab (not shown).
  - Click the **Edit** button and the **Edit Header Control** window will open.
  - Check the **Proprietary Request Header** box.
  - From the **Header Name** menu select **P-Location**.
  - From the **Method Name** menu select **Invite**.

- For **Header Criteria** select **Forbidden**.
  - From the **Presence Action** menu select **Remove Header**.
6. Click **Finish**

Proprietary Request Header?	<input checked="" type="checkbox"/>
Header Name	P-Location
Method Name	INVITE
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	Remove header
<div>486 Busy Here</div>	
<div>Finish</div>	

7. Repeat **Steps 5** and **6** to create a rule to remove the **Alert-Info** header.
- Click the **Edit** button and the **Edit Header Control** window will open.
  - Verify the **Proprietary Request Header** box is unchecked.
  - From the **Header Name** menu select **Alert-Info**
  - From the **Method Name** menu select **Invite**.
  - For **Header Criteria** select **Forbidden**
  - From the **Presence Action** menu select **Remove Header**.
8. Click **Finish**

Proprietary Request Header?	<input type="checkbox"/>
Header Name	Alert-Info
Method Name	INVITE
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	Remove header
<div>486 Busy Here</div>	
<div>Finish</div>	

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

11. Repeat **Steps 5** through **6** to create a rule to remove the **AV-Correlation-ID** header.

- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- In the **Header Name** field enter **AV-Correlation-ID**
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**
- From the **Presence Action** menu select **Remove Header**.

12. Click **Finish**

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

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

SIP Cluster

Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Signaling Rules: Avaya\_with\_SM

Add

Filter By Device...

Rename

Clone

Delete

Signaling Rules

default

No-Content-Type-Ch...

ATT\_SR

Avaya\_with\_SM

Click here to add a description.

GeneralRequestsResponsesRequest HeadersResponse HeadersSignaling QoS

Add In Header Control

Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	P-Location	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	INVITE	Forbidden	Remove Header	No	IN	Edit	Delete
4	Endpoint-View	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

### 8.4.3.2 Avaya - Responses

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

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

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

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS				
<div>Add In Header ControlAdd Out Header Control</div>									
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	200	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

### 8.4.3.3 AT&T Signaling Rule

Although no AT&T headers needed to be removed, a signaling rule was still created for QOS purposes below.

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button
  - o Enter a name: **ATT\_SR**
  - o Click **Finish**

### 8.4.3.4 Avaya – Signaling QOS

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

Signaling QoS

Signaling QoS

Enabled

☒

ToS

Precedence

999

ToS

1000

DCSP

Value

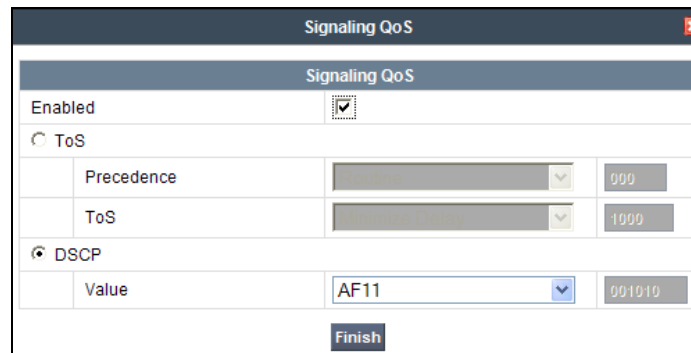
AF11

001010

Finish

### 8.4.3.5 AT&T – Signaling QoS

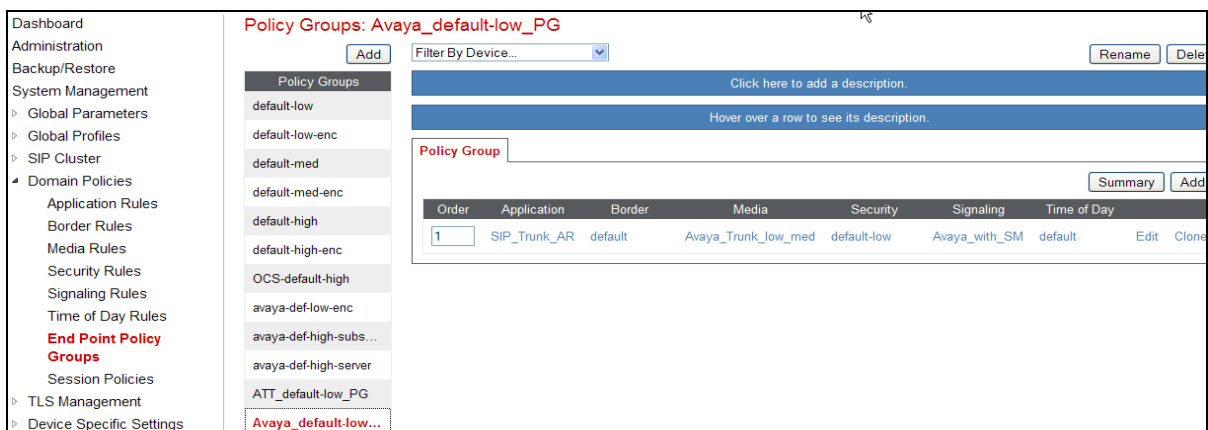
1. Highlight the **ATT\_SR** rule created in **Section 8.4.3.3** and enter the following:
  - Select the **Signaling QoS** tab (not shown).
  - Click the **Edit** button and the **Signaling QoS** window will open.
  - Select **DCSP**.
  - Select **Value = AF11**.
2. Click **Finish**



The image shows a 'Signaling QoS' configuration window. It has a title bar 'Signaling QoS' with a close button. Inside, there's a section 'Signaling QoS' with a checkbox 'Enabled' which is checked. Below this, there are two radio buttons: 'ToS' and 'DSCP'. The 'DSCP' radio button is selected. Under 'DSCP', there is a 'Value' dropdown menu set to 'AF11' and a corresponding display field showing '001010'. At the bottom right, there is a 'Finish' button.

### 8.4.4. Endpoint Policy Groups – Avaya

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
  - a) **Name:** Avaya\_default-low\_PG
  - b) **Application Rule:** SIP\_Trunk\_AR
  - c) **Border Rule:** default
  - d) **Media Rule:** Avaya\_trunk\_low\_med
  - e) **Security Rule:** default-low
  - f) **Signaling Rule:** Avaya\_with\_SM
  - g) **Time of Day:** default
4. Select **Finish** (not shown)



The image shows a web interface for configuring 'Policy Groups: Avaya\_default-low\_PG'. On the left is a navigation menu with 'Domain Policies' expanded, showing 'End Point Policy Groups' in red. The main area has a table of policy groups. The 'Avaya\_default-low...' group is highlighted. Below the table, there's a detailed view for the selected group, showing a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The first row shows: 1, SIP\_Trunk\_AR, default, Avaya\_Trunk\_low\_med, default-low, Avaya\_with\_SM, default. There are 'Edit' and 'Clone' buttons for this row. At the top right of the main area are 'Rename' and 'Delete' buttons. Below the table is a 'Policy Group' section with a 'Summary' button and an 'Add' button.



### 8.4.5. Endpoint Policy Groups – AT&T

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
  - a. **Name:** ATT\_default-low\_PG
  - b. **Application Rule:** SIP\_Trunk\_AR
  - c. **Border Rule:** default
  - d. **Media Rule:** ATT\_low\_med
  - e. **Security Rule:** default-low
  - f. **Signaling Rule:** ATT\_SR
  - g. **Time of Day:** default
4. Select Finish (not shown)

Dashboard  
Administration  
Backup/Restore  
System Management  
  > Global Parameters  
  > Global Profiles  
  > SIP Cluster  
  4 Domain Policies  
    Application Rules  
    Border Rules  
    Media Rules  
    Security Rules  
    Signaling Rules  
    Time of Day Rules  
    **End Point Policy Groups**  
    Session Policies  
  > TLS Management  
  > Device Specific Settings

Policy Groups: ATT\_default-low\_PG

Add Filter By Device... Rename Delete

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-server
- ATT\_default-low\_PG**
- Avaya\_default-low\_PG

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary Add

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	SIP_Trunk_AR	default	ATT_low_med	default-low	ATT_SR	default	Edit Clone

## 8.5. Device Specific Settings

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

### 8.5.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
  - a) The network interfaces were provisioned during installation. However if these values need to be modified, do so via this tab.

Signaling Rules  
Time of Day Rules  
End Point Policy  
Groups  
Session Policies  
TLS Management  
Device Specific Settings  
**Network Management**  
Media Interface  
Signaling Interface  
Signaling Forking  
End Point Flows  
Session Flows  
Relay Services

**Network Management: SBCE**

Devices  
SBCE

**Network Configuration** **Interface Configuration**

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask: 255.255.255.0  
A2 Netmask:   
B1 Netmask: 255.255.255.0  
B2 Netmask:

IP Address	Public IP	Gateway	Interface	
192.168.67.120	<input type="text"/>	192.168.67.1	A1	<input type="button" value="Delete"/>
192.168.64.130	<input type="text"/>	192.168.64.254	B1	<input type="button" value="Delete"/>

3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab.
  - a) Toggle the State of the physical interfaces being used.

Network Configuration	Interface Configuration
Name	
Administrative Status	
A1	Enabled <input type="button" value="Toggle"/>
A2	Disabled <input type="button" value="Toggle"/>
B1	Enabled <input type="button" value="Toggle"/>
B2	Disabled <input type="button" value="Toggle"/>

### 8.5.2. Media Interfaces

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

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

**Media Interface: SBCE**

Devices  
SBCE

**Media Interface**

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP	Port Range	Edit	Delete
Inside_Trunk_MI	192.168.67.120	16384 - 32767	Edit	Delete
Outside_Trunk_MI	192.168.64.130	16384 - 32767	Edit	Delete

### 8.5.3. Signaling Interface

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

**Signaling Interface: SBCE**

Devices  
SBCE

**Signaling Interface**

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Inside_Trunk_SI	192.168.67.120	5060	5060	---	None	Edit	Delete
Outside_Trunk_SI	192.168.64.130	---	5060	---	None	Edit	Delete

### 8.5.4. Endpoint Flows – To Avaya (Session Manager)

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add Flow**, and enter the following:

- a) **Name:** Avaya\_Trunk
  - b) **Server Configuration:** SM\_Trunk\_SC (Section 8.3.5)
  - c) **URI Group:** \*
  - d) **Transport:** \*
  - e) **Remote Subnet:** \*
  - f) **Received Interface:** Outside\_Trunk\_SI (Section 8.5.3)
  - g) **Signaling Interface:** Inside\_Trunk\_SI (Section 8.5.3)
  - h) **Media Interface:** Inside\_Trunk\_MI (Section 8.5.2)
  - i) **End Point Policy Group:** Avaya\_default-low\_PG (Section 8.4.4)
  - j) **Routing Profile:** To\_ATT\_RP (Section 8.3.4)
  - k) **Topology Hiding Profile:** Avaya\_TH (Section 8.3.7)
  - l) **File Transfer Profile:** None
5. Click **Finish** (not shown)

View Flow: Avaya_Trunk			
Criteria		Profile	
Flow Name	Avaya_Trunk	Signaling Interface	Inside_Trunk_SI
Server Configuration	SM_Trunk_SC	Media Interface	Inside_Trunk_MI
URI Group	*	End Point Policy Group	Avaya_default-low_PG
Transport	*	Routing Profile	To_ATT_RP
Remote Subnet	*	Topology Hiding Profile	Avaya_TH
Received Interface	Outside_Trunk_SI	File Transfer Profile	None

### 8.5.5. Endpoint Flows – To AT&T

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add Flow**, and enter the following:
  - a) **Name:** ATT
  - b) **Server Configuration:** ATT\_SC (Section 8.3.6)
  - c) **URI Group:** \*
  - d) **Transport:** \*
  - e) **Remote Subnet:** \*
  - f) **Received Interface:** Inside\_Trunk\_SI (Section 8.5.3)
  - g) **Signaling Interface:** Outside\_Trunk\_SI (Section 8.5.3)
  - h) **Media Interface:** Outside\_Trunk\_MI (Section 8.5.2)
  - i) **End Point Policy Group:** ATT\_default-low\_PG (Section 8.4.5)
  - j) **Routing Profile:** To\_SM\_RP (Section 8.3.3)
  - k) **Topology Hiding Profile:** ATT\_TH (Section 8.3.8)

- 1) **File Transfer Profile: None**
5. Click **Finish** (not shown)

View Flow: ATT X

<b>Criteria</b> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Flow Name</td><td>ATT</td></tr> <tr><td>Server Configuration</td><td>ATT_SC</td></tr> <tr><td>URI Group</td><td>*</td></tr> <tr><td>Transport</td><td>*</td></tr> <tr><td>Remote Subnet</td><td>*</td></tr> <tr><td>Received Interface</td><td>Inside_Trunk_SI</td></tr> </table>	Flow Name	ATT	Server Configuration	ATT_SC	URI Group	*	Transport	*	Remote Subnet	*	Received Interface	Inside_Trunk_SI	<b>Profile</b> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Signaling Interface</td><td>Outside_Trunk_SI</td></tr> <tr><td>Media Interface</td><td>Outside_Trunk_MI</td></tr> <tr><td>End Point Policy Group</td><td>ATT_default-low_PG</td></tr> <tr><td>Routing Profile</td><td>To_SM_RP</td></tr> <tr><td>Topology Hiding Profile</td><td>ATT_TH</td></tr> <tr><td>File Transfer Profile</td><td>None</td></tr> </table>	Signaling Interface	Outside_Trunk_SI	Media Interface	Outside_Trunk_MI	End Point Policy Group	ATT_default-low_PG	Routing Profile	To_SM_RP	Topology Hiding Profile	ATT_TH	File Transfer Profile	None
Flow Name	ATT																								
Server Configuration	ATT_SC																								
URI Group	*																								
Transport	*																								
Remote Subnet	*																								
Received Interface	Inside_Trunk_SI																								
Signaling Interface	Outside_Trunk_SI																								
Media Interface	Outside_Trunk_MI																								
End Point Policy Group	ATT_default-low_PG																								
Routing Profile	To_SM_RP																								
Topology Hiding Profile	ATT_TH																								
File Transfer Profile	None																								

- Signaling Rules
- Time of Day Rules
- End Point Policy Groups
- Session Policies
- TLS Management
- Device Specific Settings
  - Network Management
  - Media Interface
  - Signaling Interface
  - Signaling Forking
  - End Point Flows
  - Session Flows
  - Relay Services

End Point Flows: SBCE

Devices

SBCE

Subscriber Flows

Server Flows

Server Configuration: ATT\_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	To_SM_RP	View Clone Edit Delete

Server Configuration: SM\_Trunk\_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default-low_PG	To_ATT_VIT	View Clone Edit Delete

## 9. Verification Steps

The following steps may be used to verify the configuration:

### 9.1. AT&T IP Toll Free Service

1. Place an inbound call, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.
4. Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to Avaya Aura® Messaging voicemail. Retrieve the message from Avaya Aura® Messaging either locally or from PSTN.
5. Using the appropriate IPTF access numbers and DTMF codes, verify that the following IPTF features are successful:

JF; Reviewed:  
SPOC 11/5/2013

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

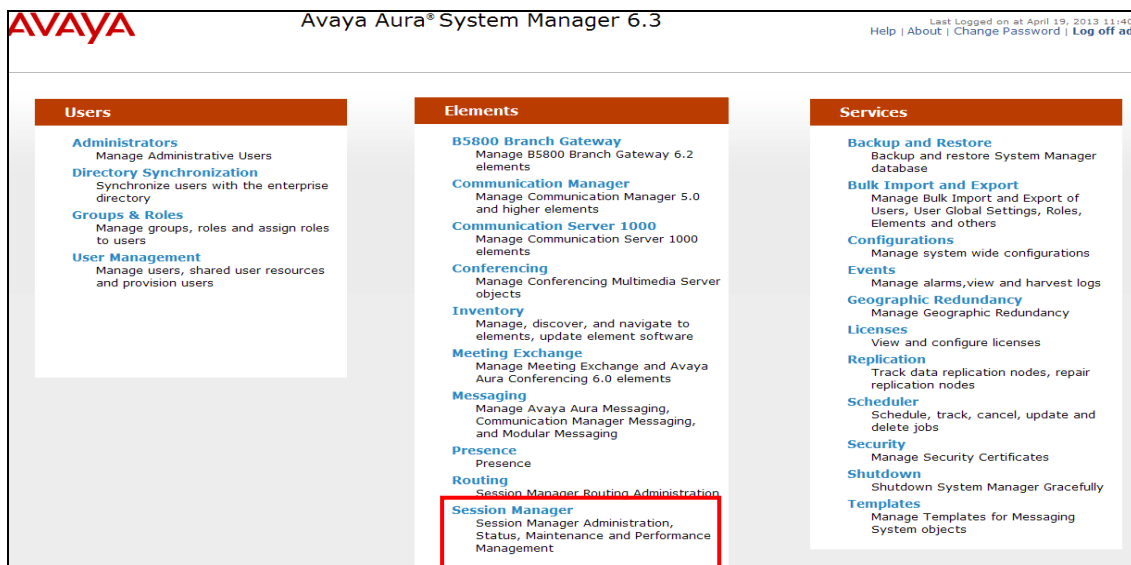
77 of 90  
SM63CM63SBCETF

- a. Legacy Transfer Connect DTMF triggered Agent Hold, Conference and Transfer capabilities
- b. Alternate Destination Routing call redirection capabilities based on Busy, Ring-No-Answer, and other SIP error codes.

## 9.2. Avaya Aura® Session Manager

Session Manager configurations may be verified via System Manager.

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



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

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System Tools

Home / Elements / Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State

Shutdown System

As of 4:05 PM

1 Item

Refresh

Show ALL

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations
<input type="checkbox"/>	<a href="#">sm63</a>	Core	✓	0/0/0	Up	Accept New Service	0/4	0	3/3

Select : All, None

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

Session Manager Entity Link Connection Status

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

All Entity Links for Session Manager: [sm63](#)

Summary View

Status Details for the selected Session Manager:

Refresh

Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">ACM63_local</a>	192.168.67.202	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">ACM63_public</a>	192.168.67.202	5062	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">AA-M</a>	192.168.67.147	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">A-SBCE</a>	192.168.67.120	5060	TCP	FALSE	UP	405 Method Not	UP

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

### 9.2.1. Call Routing Test

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

**Step 1** – **Called Party URI** field = the information passed in the Request URI sent by the Avaya SBCE (e.g., **0000001050@ customera.com**)

**Step 2** – **Calling Party Address** field = the IP address of the inside interface of the Avaya SBCE (e.g., **192.168.67.120**).

**Step 3** – **Calling Party URI** field = The contents of the From header (e.g., **7325551000@192.168.67.120**).

**Step 4** – **Session Manager Listening Port** = **5060** and **Transport protocol** = **TCP** (see the note in **Section 5.4** regarding the use of TCP).

**Step 5** – Populate the **Day of Week** and **Time (UTC)** fields, or let them default to current.

**Step 6** – Verify that the **Called Session Manager** instance is correct (e.g., sm63).

**Step 7** - Click on **Execute Test**.

### Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

#### SIP INVITE Parameters

<b>Called Party URI</b> <input type="text" value="0000001050@customera.com"/>	<b>Calling Party Address</b> <input type="text" value="192.168.67.120"/>
<b>Calling Party URI</b> <input type="text" value="7325551000"/>	<b>Session Manager Listen Port</b> <input type="text" value="5060"/>
<b>Day Of Week</b> <input type="text" value="Monday"/> <b>Time (UTC)</b> <input type="text" value="19:52"/>	<b>Transport Protocol</b> <input type="text" value="TCP"/>
<b>Called Session Manager Instance</b> <input type="text" value="sm63"/>	<input type="button" value="Execute Test"/>

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



## Routing Decisions

Route < sip:44002@customera.com > to SIP Entity ACM63\_public (192.168.67.202). Terminating Location is Main.

## Routing Decision Process

3

NRP Adaptations: ATT\_Production\_via\_SBCE applied.  
BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.  
Conference Factory Well-Known URIs: No matches for uri < 0000001050@customera.com >.  
Originating Location is Main. Using digits < 0000001050 > and host < customera.com > for routing.  
NRP Dial Patterns: Found a Dial Pattern match for pattern < 00000 > Min/Max length 9/10 and domain < customera.com >.  
NRP Routing Policies: Ranked destination NRP SIP Entities: ACM521\_public, ACM63\_public.  
NRP Routing Policies: Removing disabled routes.  
NRP Routing Policies: Ranked destination NRP SIP Entities: ACM63\_public.  
NRP Dial Patterns: Checking NRP Dial Patterns that specify -ALL- NRP Locations.  
NRP Dial Patterns: No matches for digits < 0000001050 > and domain < customera.com >.  
NRP Dial Patterns: No matches for digits < 0000001050 > and domain < null >.  
NRP Dial Patterns: Chose route matching pattern 00000  
END EMERGENCY CALL CHECK: This is not an emergency call.  
Adapting and proxying for SIP Entity ACM63\_public.  
NRP Entity Links: Found direct link to destination. Link uses TCP to port 5062.  
NRP Adaptations: ACM63\_public applied.  
NRP Adaptations: P-Asserted-Identity set to < sip:customera.com >  
NRP Adaptations: Request-URI set to sip:44002@customera.com  
NRP Adaptations: Request URI set to sip:44002@customera.com  
Route < sip:44002@customera.com > to SIP Entity ACM63\_public (192.168.67.202). Terminating Location is Main.

## 9.3. Avaya Aura® Communication Manager

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

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

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

Note that Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 19001, before sending the INVITE to Communication Manager.

list trace tac 602
Page 1

LIST TRACE

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

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

## 9.4. Protocol Traces

Using a SIP protocol analyzer (e.g., Wireshark), monitor the SIP traffic at the Avaya SBCE public outside interface connection to the AT&T IP Toll Free service.

The following is an example of an inbound call filtering on the SIP protocol.

No.	Time	Source	Destination	Protocol	Info
25	18.493	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:0000011051@192.168.64.130:5060, with
26	18.495	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying
27	18.573	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
168	20.562	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
170	20.572	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description
178	20.672	135.25.29.74	192.168.64.130	SIP	Request: ACK sip:192.168.64.130:5060;transport=udp
433	24.398	192.168.64.130	135.25.29.74	SIP	Request: INVITE sip:7325552438@135.25.29.74:5060;transport=
436	24.433	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
441	24.484	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
442	24.495	192.168.64.130	135.25.29.74	SIP/SDP	Request: ACK sip:7325552438@135.25.29.74:5060;transport=u

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

No.	Time	Source	Destination	Protocol	Info
766	29.236	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star *
768	29.265	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star *
770	29.295	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star *
772	29.316	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star * (end)
773	29.316	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star * (end)
774	29.316	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star * (end)
782	29.455	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8
783	29.455	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8
784	29.455	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8
786	29.486	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8

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

No.	Time	Source	Destination	Protocol	Info
901	31.115	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=83, Time=19920
902	31.141	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=416, Time=99840
903	31.146	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=84, Time=20160
904	31.171	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=417, Time=100080
905	31.176	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=85, Time=20400
906	31.201	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=418, Time=100320
907	31.206	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=86, Time=20640
908	31.231	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=419, Time=100560
909	31.236	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=87, Time=20880
910	31.261	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=420, Time=100800

## 9.5. Avaya Session Border Controller for Enterprise Verification

### 9.5.1. Internal Tracing

**Step 1** – Using the left hand column menu described in **Section 7**, 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. If “**All**” is selected, then the Avaya SBCE will trace traffic from both the A1 and B1 interfaces.
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**)
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Click **Start Capture** to begin the trace.

Trace: SBCE

Domain Policies  
TLS Management  
Device Specific Settings  
Network Management  
Media Interface  
Signaling Interface  
Signaling Forking  
End Point Flows  
Session Flows  
Relay Services  
SNMP  
Syslog Management  
Advanced Options  
Troubleshooting  
Debugging  
**Trace**  
DoS Learning

Devices

SBCE

Call Trace

Packet Capture

Captures

Packet Capture Configuration

Status: Ready  
Interface: Any  
Local Address: All :  
Remote Address: \*  
Protocol: All  
Maximum Number of Packets to Capture: 5000  
Capture Filename: TEST.pcap  
Start Capture Clear

The capture process will initialize, (“Please wait while your settings are saved and the capture is started”), and then display will say “**In Progress**”.

Trace: SBCE

Devices  
SBCE

Call Trace

Packet Capture

Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status: In Progress  
Interface: Any  
Local Address: All :  
Remote Address: \*  
Protocol: All  
Maximum Number of Packets to Capture: 5000  
Capture Filename: TEST.pcap  
Stop Capture

**Step 3** – Run the test. Then click on the **Stop Capture** button.

**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.

**Step 6** - Click on the file name link to download the file and use an application such as Wireshark to open the trace.

Trace: SBCE

Devices	Call Trace	Packet Capture	Captures	
SBCE	Last Modified	Descending	Sort	Reset
				Refresh
File Name	File Size (bytes)	Last Modified		
TEST_20130925093634.pcap	147,456	September 25, 2013 9:36:53 AM EDT	Delete	

## 10. Conclusion

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

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

## 11. References

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

### **Avaya Aura® Session Manager/System Manager**

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

### **Avaya Aura® Communication Manager**

5. *Administering Avaya Aura® Communication Manager*, Release 6.3 03-300509, Issue 8, May 2013
6. *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

### **Avaya Aura® Messaging**

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

### **Avaya Session Border Controller for Enterprise**

8. *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2013
9. *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, March 2013

### **AT&T IP Toll Free Service Descriptions:**

AT&T IP Toll Free Service description -

<http://www.business.att.com/enterprise/Service/voice-services/contact-center-solutions/ip-toll-free/#>

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

AT&T may provide multiple network border elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to **135.25.29.75** (the primary AT&T trunk connection to **135.25.29.74** is defined in Sections 8.3.4 and 8.3.6).

### 12.1.1. Configure the Secondary Border Element Server Configuration

Repeat the steps in Section 8.3.6 to create a Server Configuration for the connection to the AT&T secondary Border Element, using the following entries:

**Step 1** - In the **Profile Name** window enter a Profile Name (e.g., **ATT\_Secondary\_SC**) and select **Next**.

**Step 2** – In the **Add Server Configuration Profile - General** window for **Server Type**: select **Trunk Server**.

- Enter **IP Address: 135.25.29.75**.
- For **Supported Transports**: check **UDP**
- For **UDP Port**: enter **5060**
- Select **Next**

**Step 3** - Accept default values for the **Add Server Configuration Profile - Authentication** and **Heartbeat** windows (not shown).

**Step 4** – The **Add Server Configuration Profile - Advanced** window will open.

- Select **ATT\_SI** for **Interworking Profile** (created in Section 7.3.2).

**Step 5** - Select **Finish**.

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

The screenshot displays the Avaya SBCE configuration interface. On the left is a navigation menu with categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main area is titled 'Server Configuration: ATT\_Secondary\_SC' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a 'Server Profiles' list with 'ATT\_SC', 'SM\_Trunk\_SC', and 'ATT\_Secondary\_SC' (highlighted in red). The 'General' tab is selected, showing a table of configuration details:

General	Authentication	Heartbeat	Advanced
Server Type	Trunk Server		
IP Addresses / FQDNs	135.25.29.75		
Supported Transports	UDP		
UDP Port	5060		

An 'Edit' button is located at the bottom right of the configuration table.

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration

### Server Configuration: ATT\_Secondary\_SC

Add
Rename
Clone
Delete

Server Profiles
ATT\_SC
SM\_Trunk\_SC
ATT\_Secondary\_SC

General
Authentication
Heartbeat
Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	
UDP Connection Type	SUBID

Edit

### 12.1.2. Add Secondary Border Element IP Address to Routing

Repeat the steps in **Section 7.3.4** to add a Routing Profile for the AT&T secondary Border Element.

**Step 1** – Select the profile created in **Section 8.3.4** (e.g., To\_ATT\_RP).

**Step 2** - Click **Next**, then enter the following:

- Set **Next Hop Server 2:** to **135.25.29.75**.

**Step 3** - Click **Finish**.

Edit Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group
\*

Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port
135.25.29.74

Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port
135.25.29.75

Routing Priority based on Next Hop Server
☒

Use Next Hop for In Dialog Messages
☐

Ignore Route Header for Messages Outside Dialog
☐

NAPTR
☐

SRV
☐

Outgoing Transport
☐ TLS
☐ TCP
☒ UDP

Finish



### 12.1.3. Configure Secondary AT&T Border Element End Point Flow

**Step 1** – Repeat the steps in **Section 8.5.5**, with the following changes, to add an Endpoint Flow for the AT&T secondary Border Element:

- For **Name**: enter **ATT\_Secondary**

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

The screenshot displays the 'Server Flows' configuration page in the Avaya SBC interface. It is divided into three sections, each for a different server configuration:

- Server Configuration: ATT\_SC**: Contains a table with one flow named 'ATT' with priority 1. The URI Group is '\*', Received Interface is 'Inside\_Trunk\_SI', Signaling Interface is 'Outside\_Trunk\_SI', End Point Policy Group is 'ATT\_default-low\_PG', and Routing Profile is 'To\_SM\_RP'.
- Server Configuration: ATT\_Secondary\_SC**: Contains a table with one flow named 'ATT\_Secondary' with priority 1. The URI Group is '\*', Received Interface is 'Inside\_Trunk\_SI', Signaling Interface is 'Outside\_Trunk\_SI', End Point Policy Group is 'ATT\_default-low\_PG', and Routing Profile is 'To\_SM\_RP'.
- Server Configuration: SM\_Trunk\_SC**: Contains an 'Update' button and a table with one flow named 'Avaya\_Trunk' with priority 1. The URI Group is '\*', Received Interface is 'Outside\_Trunk\_SI', Signaling Interface is 'Inside\_Trunk\_SI', End Point Policy Group is 'Avaya\_default-low\_PG', and Routing Profile is 'To\_ATT\_RP'.

Each table has columns: Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. Action links (View, Clone, Edit, Delete) are present for each flow.

When completed the Avaya SBC-E will issue OPTIONS messages to the primary (**135.25.29.74**) and secondary (**135.25.29.74**) border elements.

---

©2013 Avaya Inc. All Rights Reserved.

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

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

---