Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Experience Portal 6.0, Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet Net-Net 6.2.0 with AT&T IP Toll Free Service using MIS/PNT or AVPN Transport – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Experience Portal, Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Acme Packet Net-Net (models 3800, 4250, or 4500) with the AT&T IP Toll Free service using **MIS/PNT** or **AVPN** transport connection.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Experience Portal is a speech-enabled Interactive Voice Response system that allows enterprises to provide multiple self- and assisted service resources to their customers in a flexible and customizable manner.

An Acme Packet Net-Net 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 signaling for interoperability. 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 at the Avaya Solution and Interoperability Test Lab.

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Experience Portal, Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Acme Packet Net-Net (models 3800, 4250, or 4500) with the AT&T IP Toll Free service using **MIS/PNT** or **AVPN** transport connection. **Note that the configuration steps in these Application Notes are used for this reference configuration and not meant to be prescriptive**.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Experience Portal is a speech-enabled Interactive Voice Response system that allows enterprises to provide multiple self- and assisted service resources to their customers in a flexible and customizable manner.

An Acme Packet Net-Net 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 signaling for interoperability.

Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise site with Experience Portal, Communication Manager, Session Manger, System Manager, Avaya phones, an Acme Session Border Controller, an Apache Tomcat application server, and a speech server (Nuance Recognizer and Nuance Vocalizer).
- A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise site was connected via MIS/PNT or AVPN transport connection.

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

- Inbound calls to various Experience Portal applications.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., music on hold), Automatic Speech Recognition, and Text to Speech.
- Experience Portal applications canvassing of Communication Manager for skilled agent availability before transferring inbound calls to the skills.
- Experience Portal applications transferring of inbound calls to Communication Manager skilled agent regardless of agent's availability.
- Call and two-way talkpath establishment between callers and Communication Manager agents following transfers from Experience Portal.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729a and G.711 codec support.
- Inbound AT&T IP Toll Free calls to Experience Portal destined for agents/stations connected to Communication Manager, if unanswered, are covered to Messaging.
- Experience Portal applications sending DTMF to the AT&T IP Toll Free to invoke AT&T IP Toll Free Legacy Transfer Connect features (only those permitted for Voice Response Units) and processing the resulting DTMF responses from the AT&T IP Toll Free service.
- Inbound calls to a self service Experience Portal application which forwards the call to 8YY or any other PSTN number over AT&T IP Flex Reach network.
- Long duration calls.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2** for sample call flows) between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Acme Packet Net-Net, and the AT&T IP Toll Free service.

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

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

2.2. Known Limitations/Test Results

1. AT&T IP Transfer Connect option of the AT&T IP Toll Free service was not verified with Experience Portal 6.0 and hence not supported.
2. G.726 codec is not supported by Experience Portal 6.0.
3. If Communication Manager receives an SDP offer with multiple codecs, where at least two of the codecs are supported in the codec set provisioned on Communication Manager, then Communication Manager selects a codec according to the priority order specified in the Communication Manager codec set, not the priority order specified in the SDP offer. For example, if the AT&T IP Toll Free service offers G.711, G.729A, and G.729B in that order, but the Communication Manager codec set contains G.729B, G729A, and G.711 in that order, then Communication Manager selects G.729A, not G.711. The practical resolution is to provision the Communication Manager codec set to match the expected codec priority order in AT&T IP Toll Free SDP offers.
4. Although Experience Portal release 6.0 and Communication Manager 6.0.1 support the possibility of using SIP phones as valid telephone extensions, SIP phones were not tested as part of the configuration used to validate this solution.
5. A slight delay in ringback was observed on Calling Party telephone when the call is transferred from Experience Portal to an agent on Communication Manager.
6. For an outcall to an 8YY number from Experience Portal, the Experience Portal application needs to add a Diversion Header otherwise AT&T network will send a 403 Forbidden message back and the call will fail. This diversion header can also be added on the Acme SBC as shown in **Section 9**, and that was the way it was implemented in this reference configuration.

The test objectives stated in **Section 2** with limitations as noted in this section were verified.

2.3. Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (888) 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 sample configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Experience Portal provides interactive voice response services to inbound callers. Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. Single server was used for MPP and EPM for this reference configuration.
- Communication Manager provides the enterprise voice communications services. In this sample configuration, Communication Manager runs on an Avaya S8800 Server.
- Session Manager provides core SIP routing and integration services that enables communications between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- System Manager provides a common administration interface for centralized management of all Session Managers in an enterprise.
- The Avaya G650 Media Gateway provides the physical interfaces and resources for enterprise voice communications. This solution is extensible to other Avaya Media Gateways.
- Avaya phones are represented with Avaya 96xx Series IP Telephones running H.323 software. Additionally Avaya one-X® Agent and Analog and Digital phones were also used.
- The Acme Packet Net-Net Session Director (SD) 3800[1] provides SIP Session Border Controller (Acme SBC) functionality between the AT&T IP Toll Free service and the enterprise internal network[2]. UDP transport protocol is used between the Acme Packet Net-Net SD and the AT&T IP Toll Free service.
- The Apache Tomcat Application Server hosts the VXML and CCXML applications that provide the directives for handling the inbound calls to Experience Portal which are referenced in Experience Portal.
- The Speech Server consists of Nuance Recognizer and Nuance Vocalizer. Experience Portal uses the Speech Server for Automatic Speech Recognition (ASR) and Text-To-Speech (TTS) capabilities.
- Messaging provides the corporate voice messaging capabilities in this reference configuration. The provisioning of Messaging is beyond the scope of this document.

---

[1] Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

[2] The AT&T IP Toll Free service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Acme Packet SBC in this sample configuration. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Acme SBC and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Acme Packet SBC and Communication Manager.

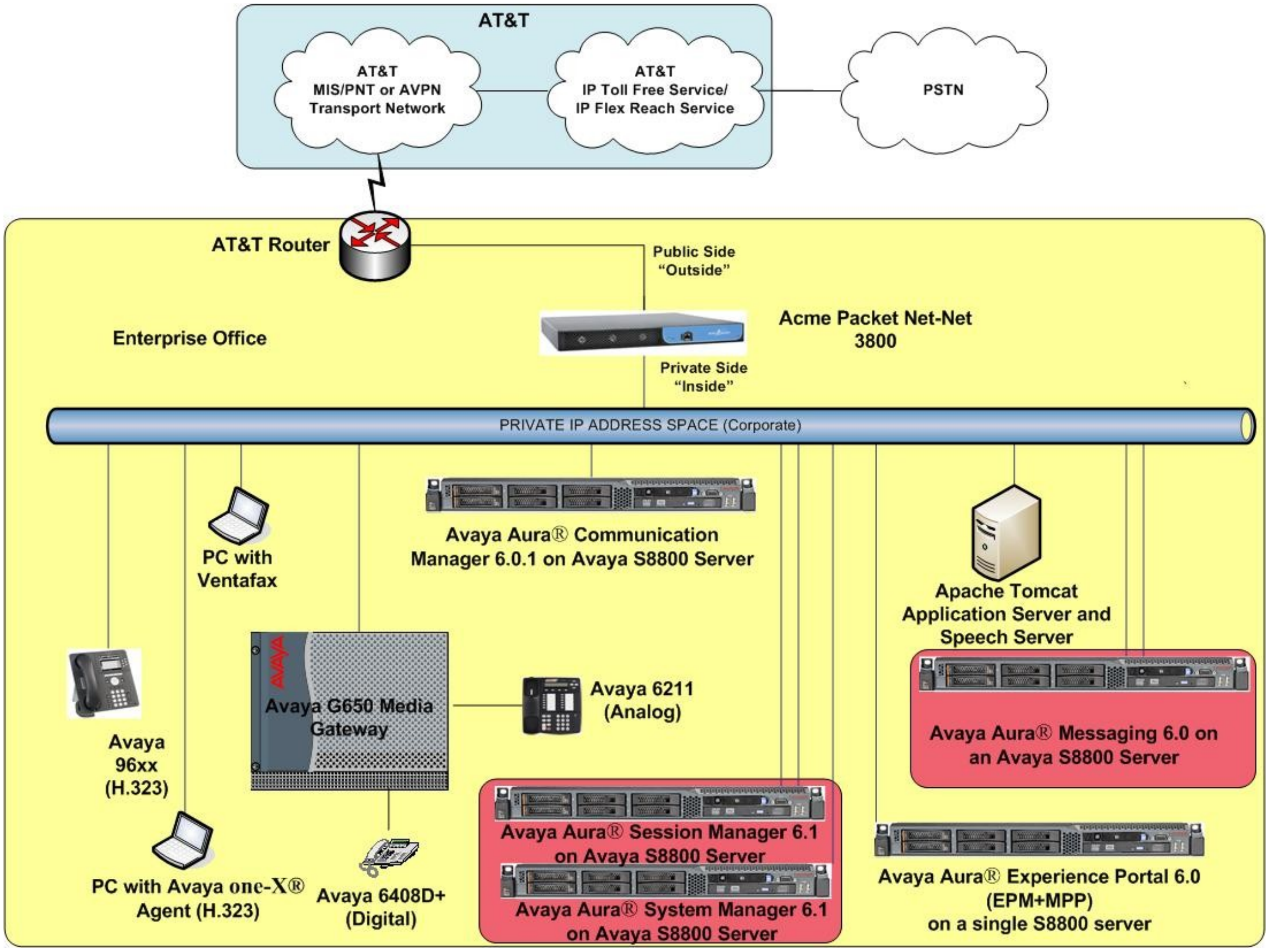


Figure 1: Reference Configuration

3.1. Illustrative Configuration Information

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

Component	Illustrative Value in these Application Notes
Avaya Aura® Experience Portal	
EPM/MPP Servers IP Address	10.80.130.220
Automatic Speech Recognition and Text to Speech server IP Address	10.80.130.153
Avaya Aura® Communication Manager	
C-LAN IP Address	10.8.130.206
Vector Directory Number (VDN) Extensions	666-20xx
Skill (Hunt Group) Extensions	666-40xx
Agent Extensions	666-30xx
Phone Extensions	666-50xx
Announcement Extensions	666-10xx
Avaya Aura® Session Manager/System Manager	
System Manager IP Address	10.80.150.204
Session Manager Management IP Address	10.80.150.205
Session Manager Network IP Address	10.80.150.206
Acme Packet Session Border Controller	
IP Address of "Outside" Interface (connected to AT&T IP Toll Free Service)	192.168.62.50
IP Address of "Inside" Interface (connected to Avaya elements)	10.80.130.250
AT&T IP Toll Free Service	
Border Element IP Address	135.242.225.210
DNIS Passed in Request URI used by Session Manager for routing	00000[1,2,3,4,5]100[1,2,3,4,5]
Digits Passed in SIP "To" Header to Avaya Aura® Experience Portal	800555xxxx

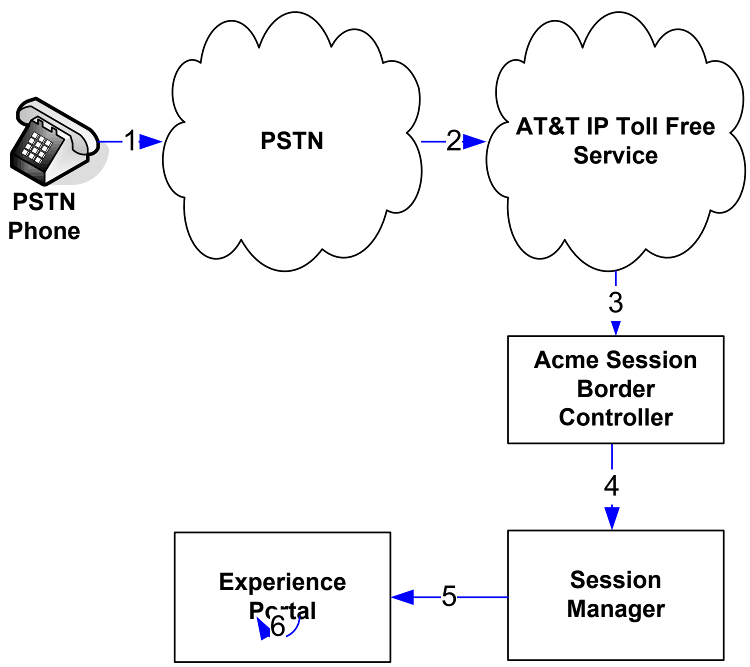
Table 1: Illustrative Values Used in these Application Notes

3.2. Call Flows

To understand how inbound AT&T IP Toll Free calls are handled by Experience Portal, several call flows are described in this section.

The first call scenario illustrated below is an inbound call arriving and remaining on Experience Portal.

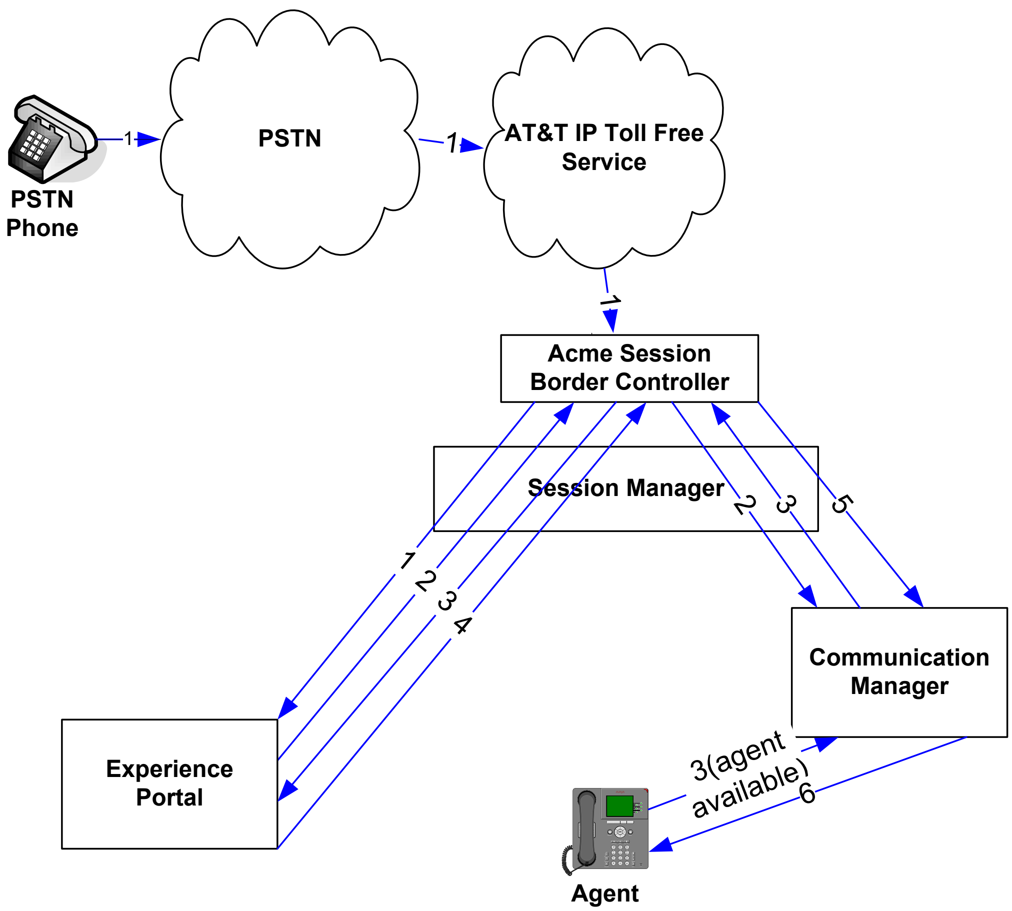
1. A PSTN phone originates a call to an AT&T IP Toll Free service number.
2. The PSTN routes the call to the AT&T IP Toll Free service network.
3. The AT&T IP Toll Free service routes the call to the Acme SBC.
4. Acme SBC performs any necessary SIP header modifications, and routes the call to Session 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 Experience Portal.
6. Experience Portal matches the called party number to a VXML and/or CCXML application, answers the call, and handles the call according to the directives specified in the application. In this scenario, the application sufficiently meets the caller's needs or requests, and thus the call does not need to be transferred to Communication Manager.



Inbound Call Handled Entirely by Experience Portal

The second call scenario illustrated below is an inbound call arriving on Experience Portal and transferred to Communication Manager only after an agent with appropriate skill becomes available on Communication Manager.

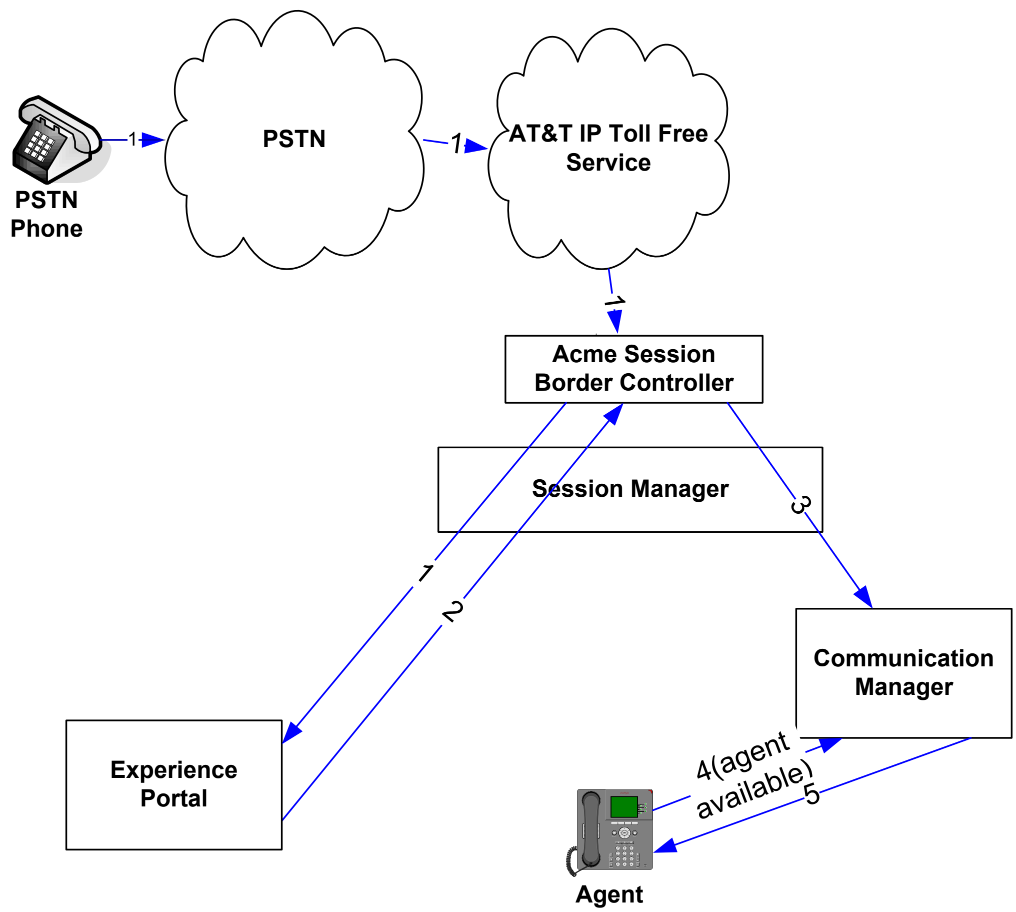
1. Same as the first five steps from the first call scenario.
2. In this scenario, the application is not sufficient to meet the caller's requests, and thus the call needs to be transferred to a Communication Manager agent. Experience Portal then puts the inbound call on hold and places a call to vector/skill for an agent on Communication Manager via Acme SBC/Session Manager. While the inbound call is on hold, Experience Portal may play music to the caller, prompt the caller for additional information, or otherwise interact with the caller.
3. Communication Manager informs Experience Portal when an agent in that skill becomes available.
4. Experience Portal instructs the Acme SBC to transfer the inbound call to that skill.
5. The Acme SBC transfers the inbound call to the aforementioned skill on Communication Manager.
6. Communication Manager routes the call to the agent.



Inbound Call Handled by Experience Portal and Transferred to Communication Manager upon Agent Availability

The third call scenario illustrated below is an inbound call arriving on Experience Portal and transferred to Communication Manager skill without determining whether an agent with required skill is available or not.

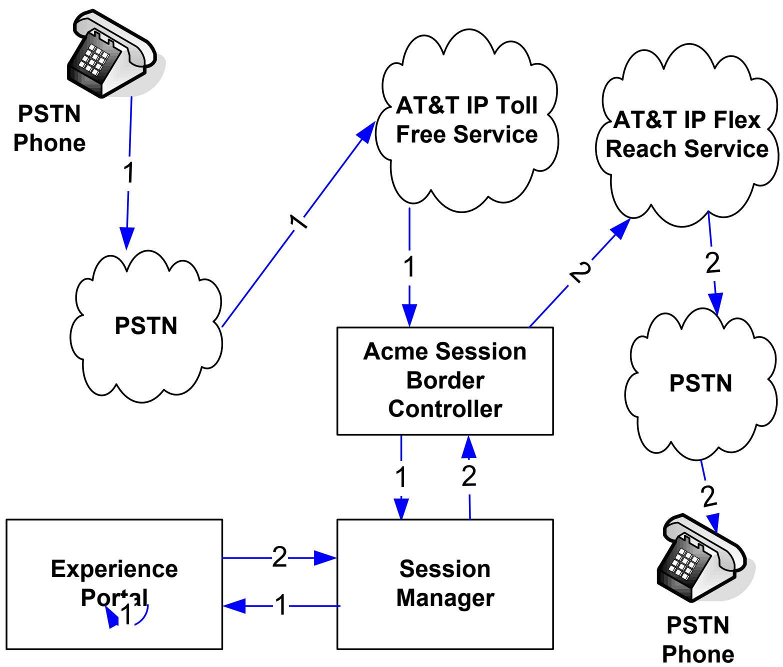
1. Same as the first five steps from the first call scenario.
2. In this scenario, the application on Experience Portal is not sufficient to meet the caller's needs or requests, and thus the call needs to be transferred to an agent/skill on Communication Manager. Experience Portal instructs the Acme SBC via Session Manager to transfer the inbound call to an agent/skill on Communication Manager without verifying that an agent with required skill is available on Communication Manager.
3. The Acme SBC transfers the inbound call to the required skill/agent on Communication Manager.
4. An agent becomes available on Communication Manager.
5. Communication Manager routes the call to the agent.



Inbound Call Transferred by Experience Portal to Communication Manager regardless of Agent Availability

The fourth call scenario illustrated below is an inbound call arriving on Experience Portal and forwarded to an 8YY number or any other PSTN number over AT&T Flex Reach network.

1. Same as the first six steps from the first call scenario.
2. In this scenario, the application is sufficient to meet the caller's requests, and thus the call needs to be forwarded to another PSTN number. Based upon the selection, Experience Portal forwards the call to an appropriate PSTN number which can be a regular PSTN number or an 8YY number.



Inbound Call forwarded by Experience Portal to another PSTN number

4. Equipment and Software Validated

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

Component	Version
Avaya S8800 Server	Avaya Aura® Experience Portal 6.0
Experience Portal Management (EPM)	EPM 6.0.0.0.3306
Media Processing Platform (MPP)	MPP 6.0.0.0.3401
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0.1 with Service Pack 5 (R016x.00.1.510.1)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW06 FW054
TN799DP Control-LAN (C-LAN)	HW01 FW040
TN2602AP IP Media Processor (MedPro)	HW02 FW061
TN2501AP VAL-ANNOUNCEMENT	HW02 FW018
Avaya S8800 Server	Avaya Aura® System Manager 6.1.0 (SP5)
Avaya S8800 Server	Avaya Aura® Session Manager 6.1.0 (SP5)
Avaya 9650 IP Telephone	Avaya one-X® Deskphone Edition H.323 Release 3.110b
Avaya 9611 IP Telephone	Avaya one-X® Deskphone Edition H.323 Release S6.0.0
Avaya one-X® Agent	Release 2.5
Apache Tomcat Application Server	6.0.33
Nuance Recognizer	9.0
Nuance Recognizer English en-US Language Pack	9.0
Nuance Vocalizer	5.0.5
Nuance Vocalizer American English en-US Donna	5.0.2
Nuance MediaServer	5.0.5
Acme Packet Net-Net Session Director 3800	SCX6.2.0 MR-6 Patch 5 (Build 916)
AT&T IP Toll Free Service	VNI 22

Table 1: Equipment and Software Versions

5. Avaya Aura® Session Manager

These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [4] and [5] for further details if necessary. Configuration of Session Manager is performed from System Manager. To invoke the System Manager Common Console, launch a web browser. Enter https://<*IP address of the System Manager server*>/ in the URL field, and log in with the appropriate credentials.

5.1. Background

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.

5.2. Routing Policies

Routing Policies define how Session Manager will route calls between SIP network elements. Routing Policies are dependent on the administration of several inter-related items:

- SIP Entities – SIP Entities represent SIP network elements such as Session Managers, Communication Managers, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- Entity Links – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager and other SIP Entities.
- SIP Domains – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- Locations – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.

- Adaptations – Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities. As another example, basic "Digit Conversion" Adaptations are used in this reference configuration to convert digit strings in **destination** (e.g., Request-URI) and **origination** (e.g. P-Asserted Identity) type headers of SIP messages sent to and received from SIP Entities.
- Dial Patterns – A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one[3] of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed. Note that Dial Patterns are matched after ingress Adaptations have already been applied.
- Time Ranges – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Routing Policy may be associated with one or more Time Ranges during which the Routing Policy is in effect. For example, for a Dial Pattern administered with two Routing Policies, one Routing Policy can be in effect on weekday business hours and the other Routing Policy can be in effect on weekday off-hours and weekends. **In the reference configuration no restrictions were placed on calling times**.

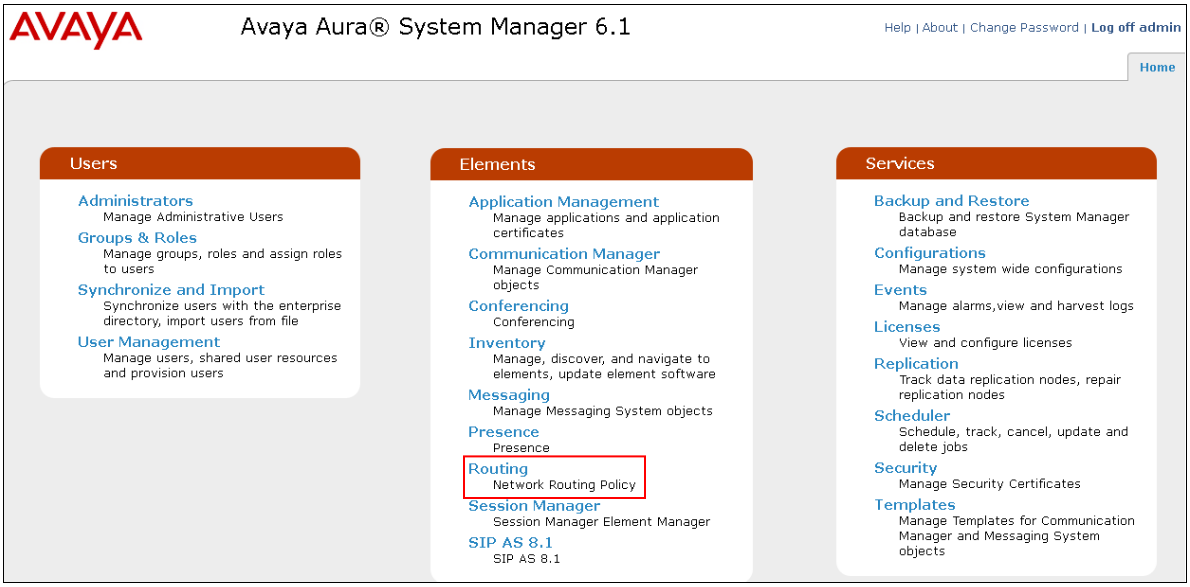
The general strategy employed in this reference configuration with regard to Called Party Number manipulation and matching, and call routing is as follows:

- Use common number formats and uniform numbers in matching called party numbers for routing decisions.
- On ingress, Session Manager may apply any called party number modifications necessary to **normalize** the number to a common format or uniform number as defined in the Dial Patterns.
- On egress, Session Manager may apply any called party number modifications necessary to conform to the expectations of the next-hop SIP Entity.

Of course, the items above are just several of many possible strategies that can be implemented with Session Manager.

[3] The Routing Policy in effect at that time with highest ranking is attempted first. If that Routing Policy fails, then the Routing Policy with the next highest rankings is attempted, and so on.

To view the sequenced steps required for configuring network routing policies, click **Routing** on the System Manager Common Console (see below).

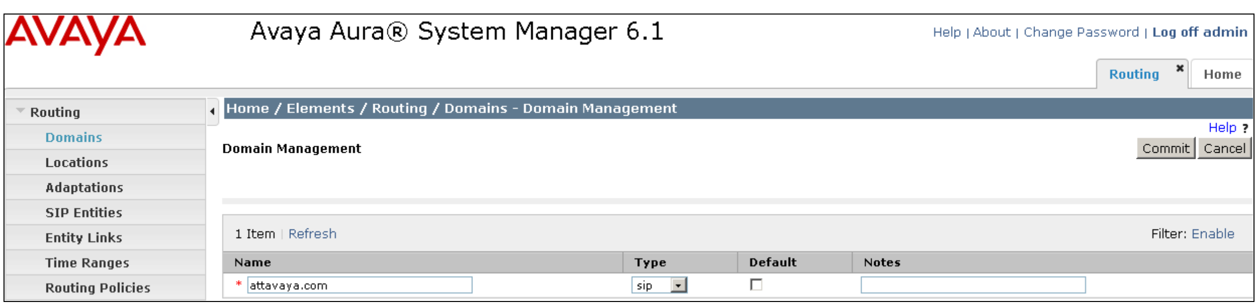


System Manager Common Console Page

5.3. SIP Domains

The steps in this section specify the SIP domains for which Session Manager is authoritative.

1. In the left pane under **Routing**, click **Domains**. On the **Domain Management** page, click on **New** [not shown] and configure as follows:
   - **Name** –Set to **attavaya.com** in this reference configuration. This domain is used in **Section 6.2**, **Step 4** and **Section 7.4**, **Step 1**.
   - **Type** – Set to **sip**.
   - **Notes** – Optional Field.
2. Click **Commit**.
3. Repeat above steps to add additional domains.

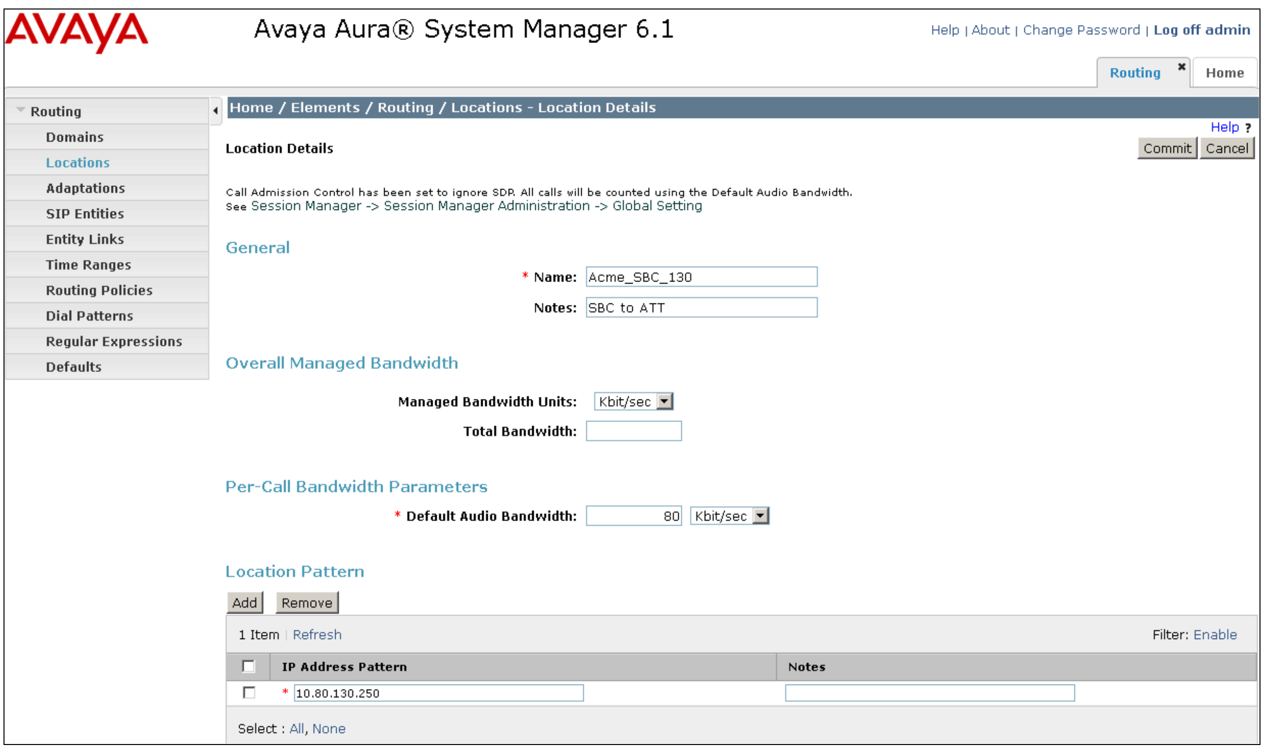


Domain Management Page

5.4. Locations

The steps in this section define the physical and/or logical locations in which SIP Entities reside.

1. In the left pane under **Routing**, click on **Locations**. On the **Location** page [not shown] click **New**.
2. On the **Location Details** page, configure as follows:
   - **Name** – Enter any descriptive string.
   - **Notes** – [Optiona] Enter a description.
   - **Managed Bandwidth** and **Average Bandwidth per Call** – [Optiona] To limit the number of calls going to and from this location i.e., apply Call Admission Control.
   - **Location Pattern** – [Optiona] To identify IP addresses associated with this Location. In the reference configuration, the IP address of Acme SBC i.e. **10.80.130.250** was used.
3. Click **Commit**.
4. Repeat above steps to add any additional Locations (e.g. **Location_130** for **Experience Portal**, **Messaging** and **Communication Manager** matching on **IP Address Pattern** of **10.80.130.***, and **Location_150** for **Session Manager** matching on **IP Address Pattern** of **10.80.150.***) used in this reference configuration.



Location Details Page for Acme SBC

5.5. Adaptations

Adaptations on Session Manager are always between Session Manager and another entity. Adaptations could potentially be applied to both calls coming into Session Manager and going out from the Session Manager. In this section, Adaptations are administered for calls from AT&T to

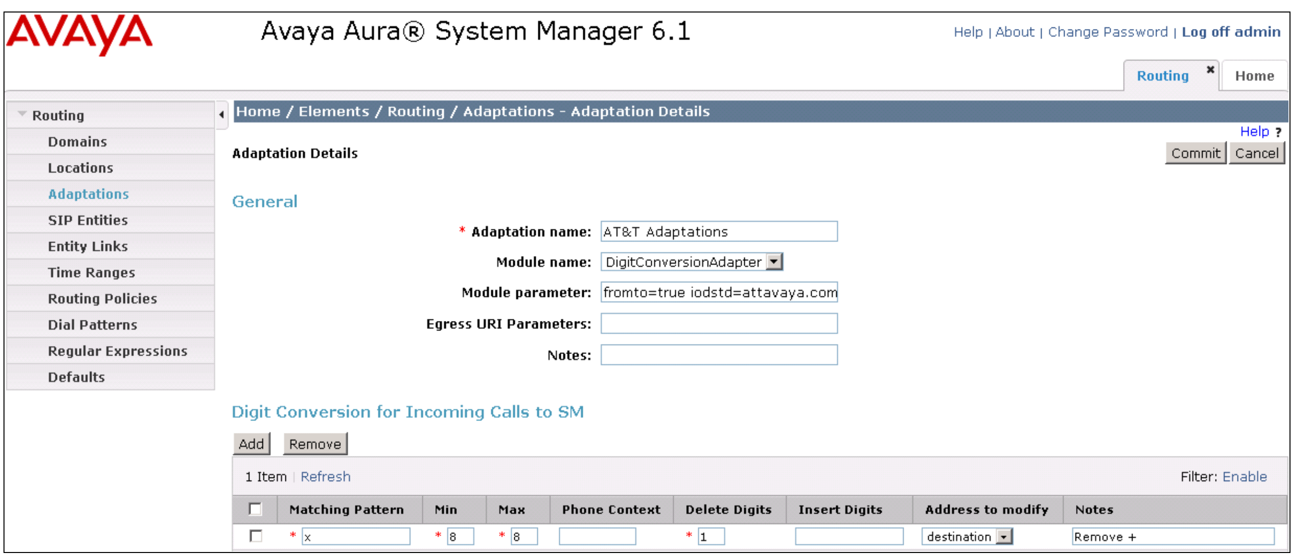
Experience Portal (**Section 5.5.1**) and the calls forwarded from Experience Portal to Communication Manager (**Section 5.5.2**).

5.5.1. Adaptation for Calls to Avaya Aura® Experience Portal

This adaptation replaces the IP address of Session Manager in Request URI and **To** header with the Avaya CPE SIP domain **attavaya.com**.

1. In the left pane under **Routing**, click **Adaptations**. On the **Adaptations** page, click on **New** [not shown].
2. In the **Adaptation Details – General** section, configure as follows:
   - **Adaptation name** – Set to any descriptive string.
   - **Module name** - Select **DigitConversionAdapter** from the drop-down list; if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**.
   - **Module parameter** - Enter **fromto=true iodstd=attavaya.com odstd=135.242.225.210**, which will replace the IP Address/Domain in the Request URI and **To** header with the Avaya CPE domain **attavaya.com** for egress to Experience Portal. Also, it replaces the domain in the calls originating from Experience Portal destined for Acme SBC to the IP Address of the AT&T Border element.
3. In the **Adaptation Detail - Digit Conversion for Incoming Calls to SM** section, configure as follows to remove a leading + sign in the user part of Request URI:
   - **Matching Pattern** – Set to match the first character user part of Request URI.
   - **Min** and **Max** – Set to **8**.
   - **Delete Digits** – Set to **1**.
   - **Address to modify** – Select **destination** from the drop-down list.
4. Click **Commit**.

Note: In the reference configuration no **Digit Conversation for Outgoing Calls from SM** are required.



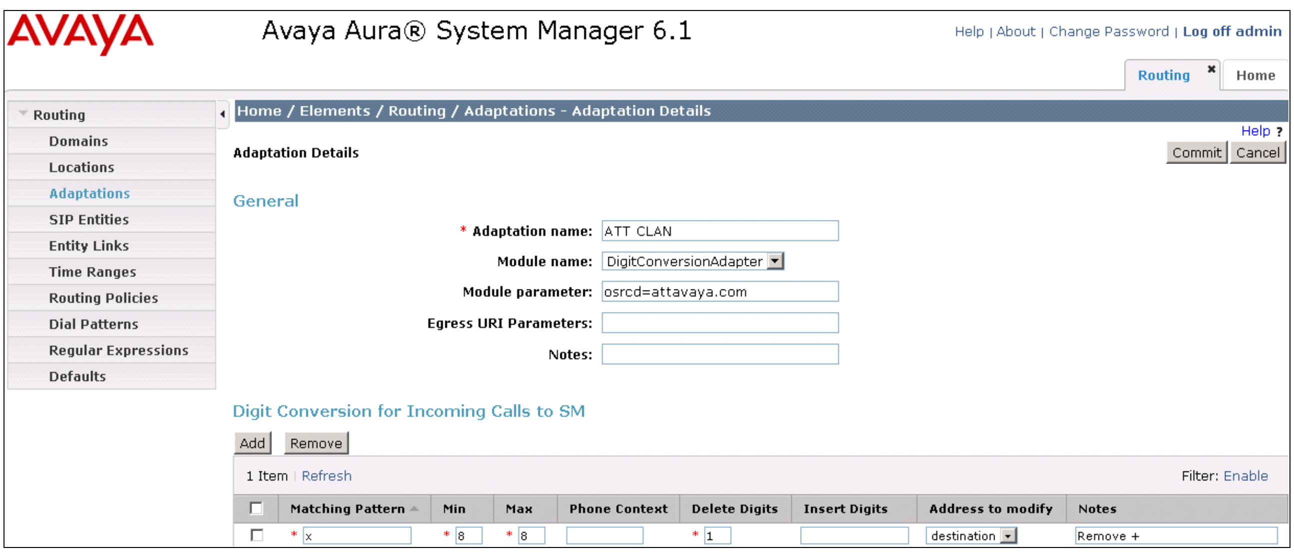
Adaptation Details Page – Adaptation for Acme SBC

5.5.2. Adaptation for Calls to Avaya Aura® Communication Manager

This adaptation replaces the IP address of Session Manager with the Avaya CPE SIP domain **attavaya.com** in the **PAI** header.

1. In the left pane under **Routing**, click **Adaptations**. On the **Adaptations** page, click **New** [not shown].
2. On the **Adaptation Details – General** section, configure as follows:
   - **Adaptation name** – Set to any descriptive string.
   - **Module name** - Select **DigitConversionAdapter** from the drop-down list; if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**.
   - **Module parameter** - Enter **osrcd=attavaya.com**, which will replace the IP Address/Domain in the **PAI** header for egress to Communication Manager.
3. In the **Adaptation Detail - Digit Conversion for Incoming Calls to SM** section, configure as follows to remove a leading + sign in the user part of Request URI:
   a. **Matching Pattern** – Set to match the first character user part of Request URI.
   b. **Min** and **Max** – Set to **8**.
   c. **Delete Digits** – Set to **1**.
   d. **Address to modify** – Select **destination** from the drop-down list.
4. Click **Commit**.

Note: In the reference configuration no **Digit Conversation for Outgoing Calls from SM** are required.



Adaptation Details Page – Adaptation for Communication Manager

5.6. SIP Entities

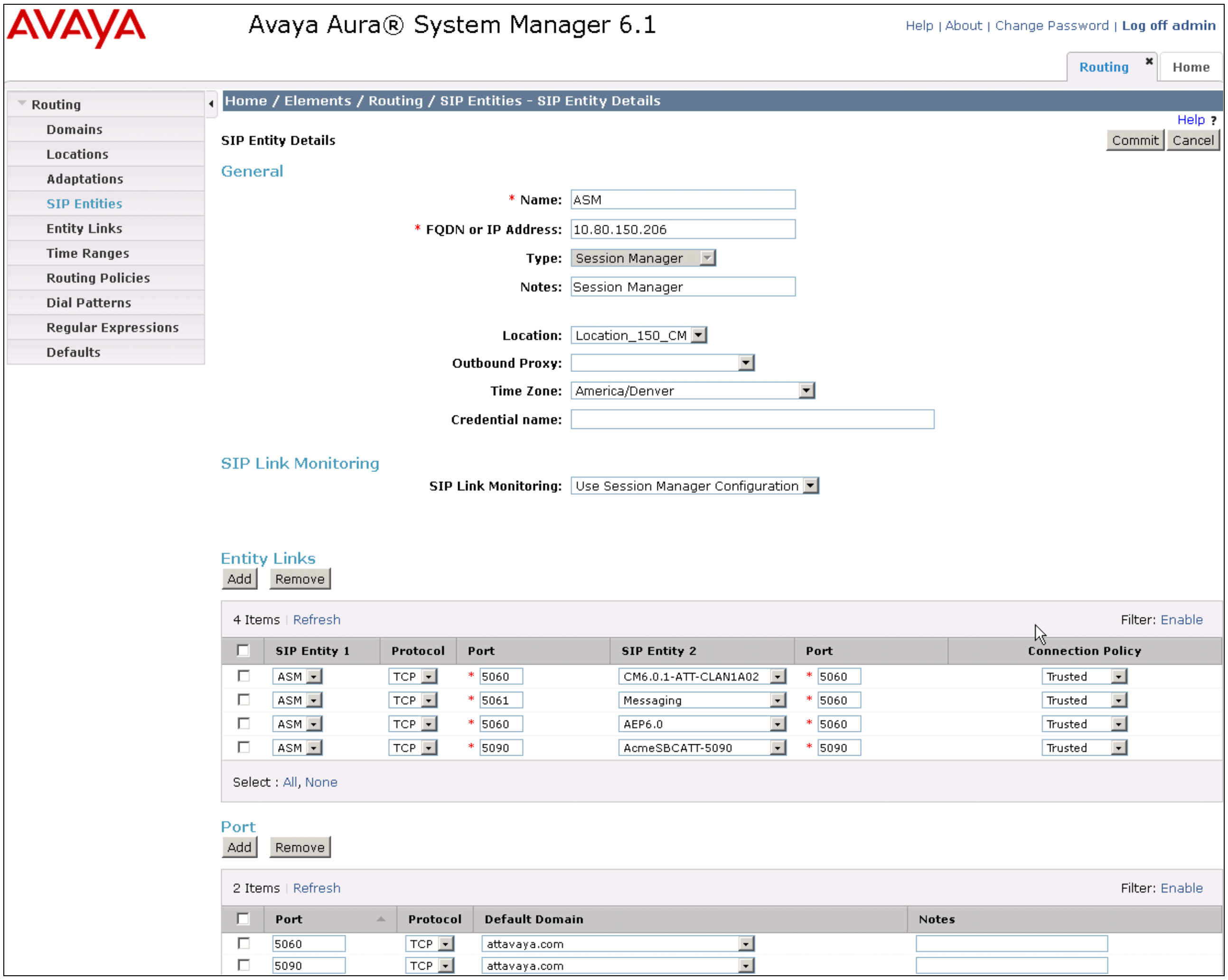
In this section, SIP Entities are administered for the following SIP network elements:

- Avaya Aura® Session Manager
- Avaya Aura® Experience Portal
- Avaya Aura® Communication Manager
- Acme Session Border Controller
- Avaya Aura® Messaging

Note – In this reference configuration TCP (port 5060) is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as transport protocol between Communication Manager and Session Manager in customer environments.

5.6.1. Avaya Aura® Session Manager SIP Entity

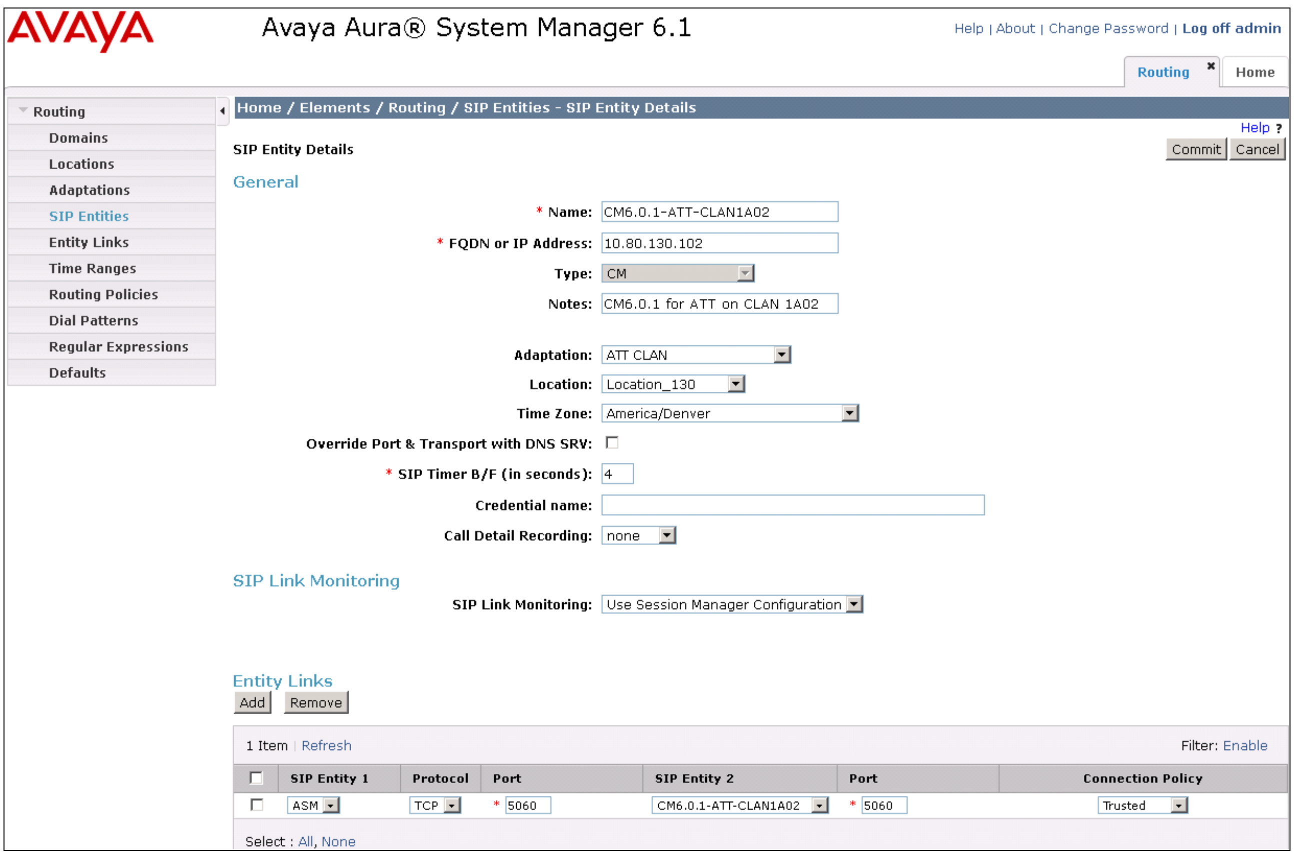
1. In the left pane under **Routing**, click **SIP Entities**. In the **SIP Entities** page click **New** [not shown].
2. In the **General** section of the **SIP Entity Details** page, configure as follows:
   - **Name –** Enter a descriptive name for Session Manager.
   - **FQDN or IP Address –** Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation. Set to **10.80.150.206** in this reference configuration.
   - **Type –** Select **Session Manager**.
   - **Location** – Select **Location_150_SM** as configured in **Section 5.4**.
   - **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.
3. In the **SIP Link Monitoring** section of the **SIP Entity Details** page select **Use Session Manager Configuration** for the **SIP Link Monitoring** field.
4. In the **Port** section of the **SIP Entity Details** page, click on **Add** and provision as follows:
   - **Port –** Enter **5060** (see note above).
   - **Protocol –** Select **TCP** (see note above).
   - **Default Domain –** (Optional) Select a SIP domain administered in **Section 5.3**.
   - Repeat this step to configure additonal port entries.
5. The screen below also shows all the entity links configured for this entity. These Entity links are actually configured/displayed in **Section 5.7**.
6. Click **Commit**.



SIP Entity Details Page –Session Manager SIP Entity

5.6.2. Avaya Aura® Communication Manager SIP Entity

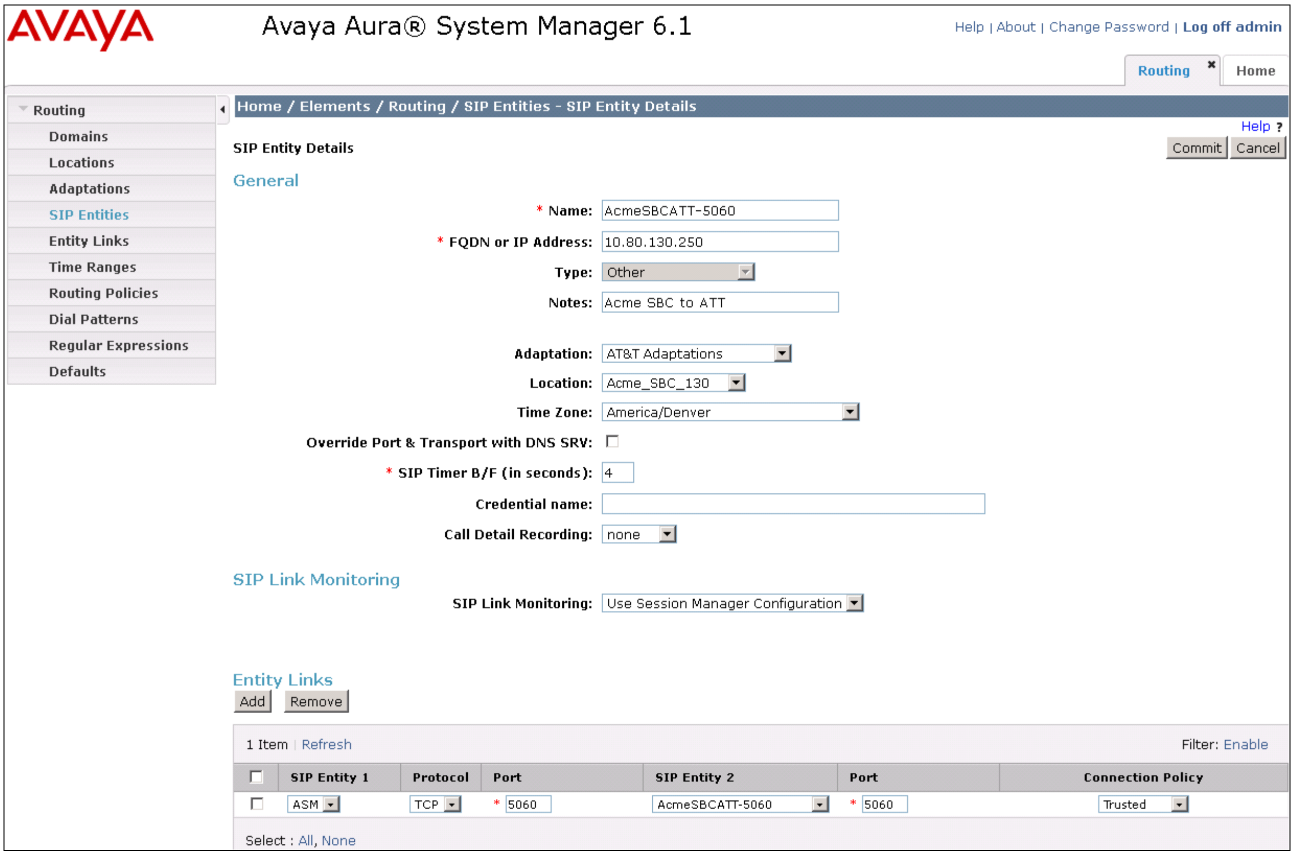
1. In the **SIP Entities** page, click **New** [not shown].
2. In the **General** section of the **SIP Entity Details** page, configure as follows:
   - **Name –** Enter any descriptive name for the Communication Manager Signaling Interface.
   - **FQDN or IP Address –** Enter the IP address of the Communication Manager C-LAN provisioned/displayed in **Section 7.3**, **Step 2**.
   - **Type –** Select **CM**.
   - **Adaptation –** Select the Adaptation administered in **Section 5.5.2**.
   - **Location** – Select a Location administered in **Section 5.4**.
   - **Time Zone** – Select the time zone in which Communication Manager resides.
   - In the **SIP Link Monitoring** section of the **SIP Entity Details** page select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
3. The screen below shows the entity link configured for this entity. This Entity link is actually configured/displayed in **Section 5.7.1**.
4. Click **Commit**.



SIP Entity Details Page –Communication Manager SIP Entity

5.6.3. Acme Session Border Controller SIP Entity

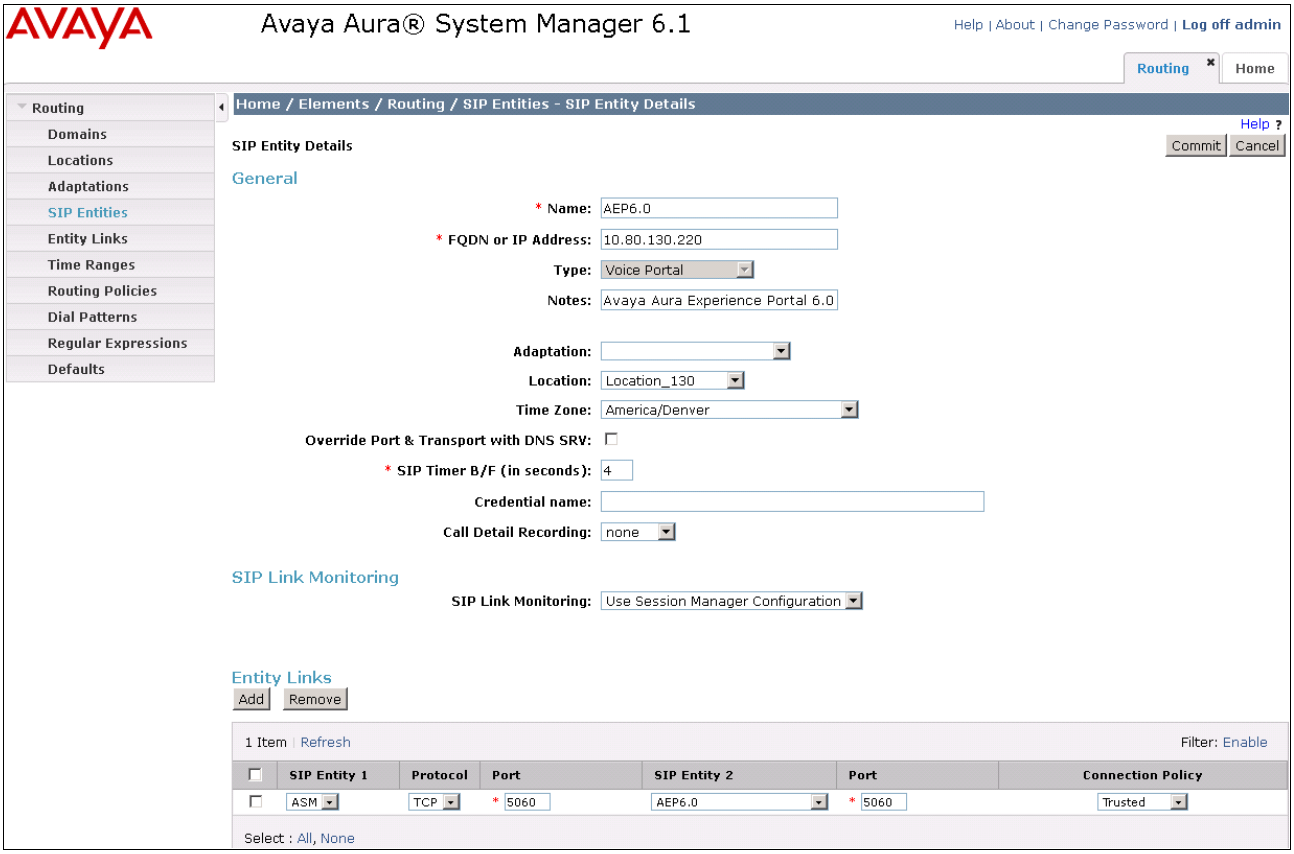
To configure the Session Border Controller Entity, repeat the Steps in **Section 5.6.2**. The **FQDN or IP Address** field is populated with the IP address of the private (inside) interface configured in **Section 9** under **network interface** section and the **Type** field is set to **Other**. The entity link is configured/displayed in **Section 5.7.2**. See the screen below for the values used in this reference configuration.



SIP Entity Details Page – Session Border Controller SIP Entity

5.6.4. Avaya Aura® Experience Portal Entity

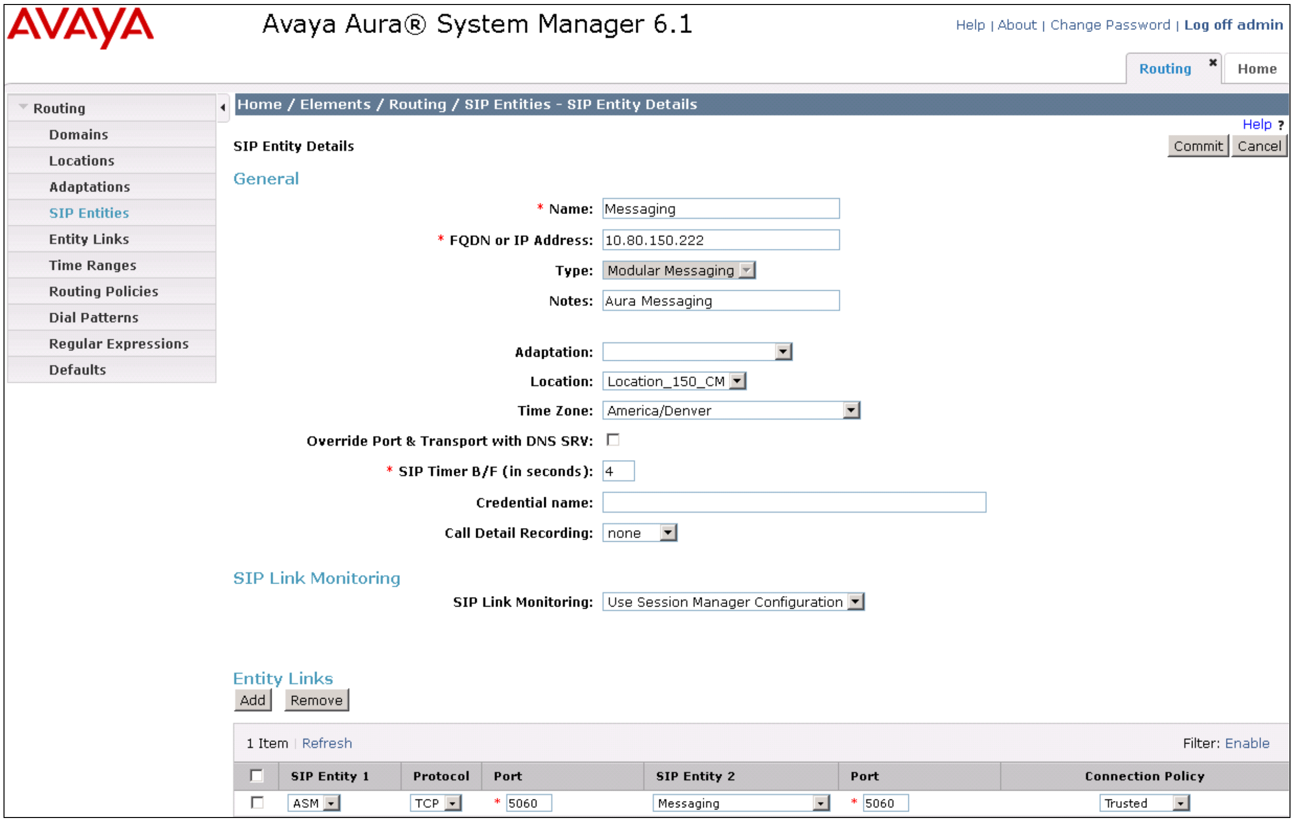
To configure the Experience Portal Entity, repeat the Steps in **Section 5.6.2**. The **FQDN or IP Address** field is populated with the IP address of the Experience Portal and the **Type** field is set to **Voice Portal**. The entity link is configured/displayed in **Section 5.7.3**. See the screen below for the values used in this reference configuration.



SIP Entity Details Page –Experience Portal SIP Entity

5.6.5. Avaya Aura® Messaging SIP Entity

To configure the Messaging SIP Entity, repeat the steps in **Section 5.6.2**. The **FQDN or IP Address** field is populated with the IP address of Messaging and the **Type** field is set to **Modular Messaging**. The entity link is configured/displayed in **Section 5.7.4**. See the screen below for the values used in this reference configuration.



SIP Entity Details Page –Messaging SIP Entity

5.7. Entity Links

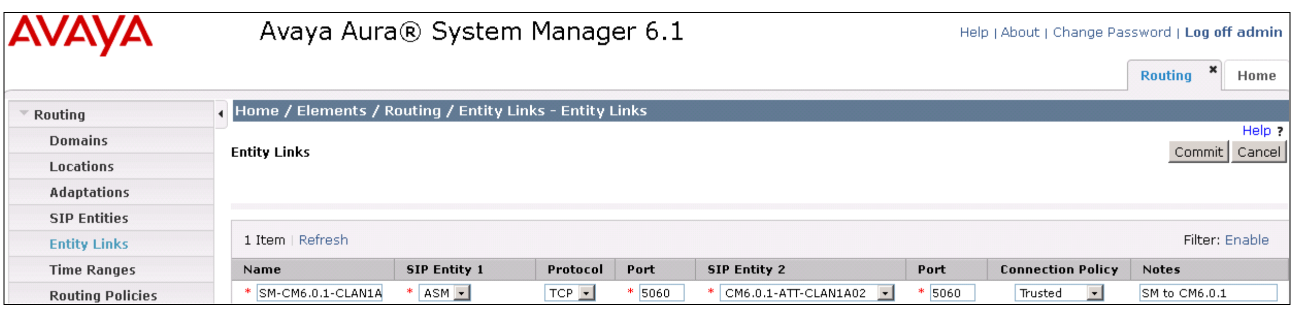
In this section, Entity Links are administered between Avaya Aura® Session Manager and the following SIP Entities:

- Avaya Aura® Communication Manager
- Acme Session Border Controller
- Avaya Aura® Experience Portal
- Avaya Aura® Messaging

Note – In this reference configuration TCP (port 5060) is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as transport protocol between Experience Portal/Communication Manager and Session Manager in customer environments.

5.7.1. Entity Link to Avaya Aura® Communication Manager

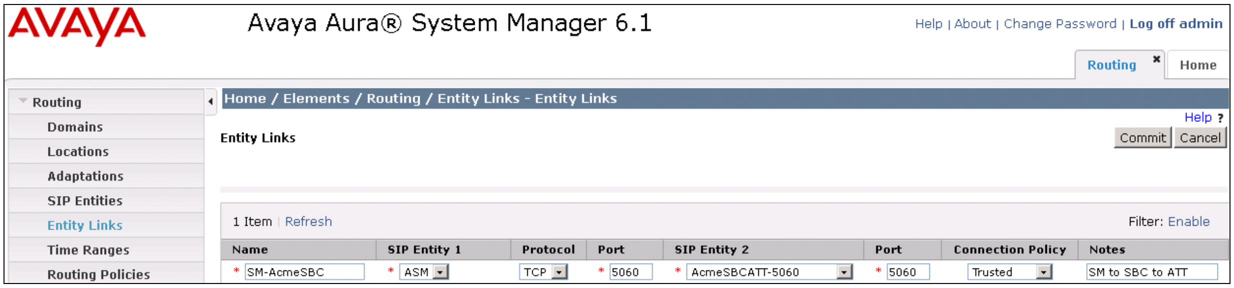
1. In the left pane under **Routing**, click **Entity Links**. In the **Entity Links** page click **New** [not shown].
2. On the **Entity Links** page, provision as follows:
   - **Name** – Enter a descriptive name for this link to Communication Manager.
   - **SIP Entity 1** – Select the SIP Entity administered in **Section 5.6.1** for the Session Manager. SIP Entity 1 must always be the Session Manager instance.
   - **SIP Entity 1 Port** – Enter **5060**.
   - **SIP Entity 2** –Select the SIP Entity administered in **Section 5.6.2** for Communication Manager.
   - **SIP Entity 2 Port** - Enter **5060**.
   - **Connection Policy** – Select **Trusted**.
   - **Protocol** – Select **TCP**.
3. Click **Commit**.



Entity Links Page – Entity Link to Communication Manager

5.7.2. Entity Link to Acme Session Border Controller

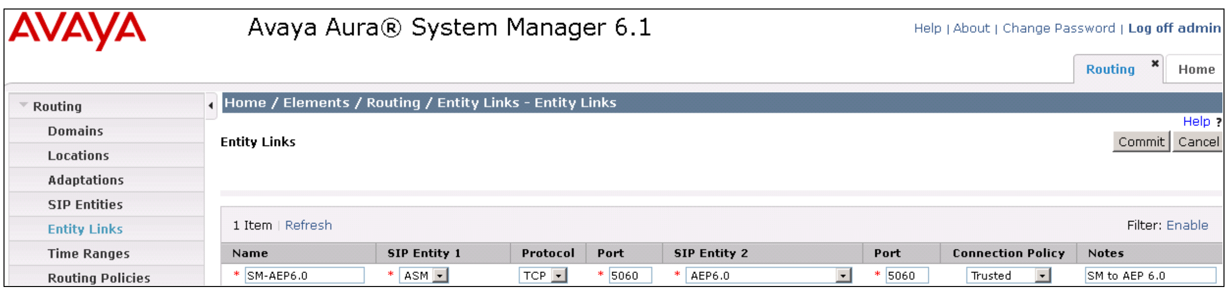
To configure the entity link between the Session Manager and Acme SBC SIP entity, repeat the steps in **Section 5.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.6.3**. See the screem below for the values used in this reference configuration.



Entity Links Page – Entity Link to Acme SBC SIP Entity

5.7.3. Entity Link to Avaya Aura® Experience Portal

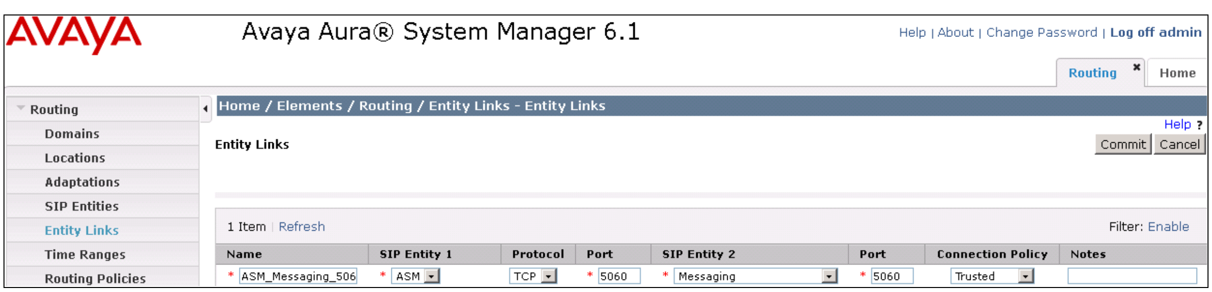
To configure this entity link, repeat the steps in **Section 5.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.6.4**. See the screen below for the values used in this reference configuration.



Entity Links Page – Entity Link to Experience Portal SIP Entity

5.7.4. Entity Link to Avaya Aura® Messaging

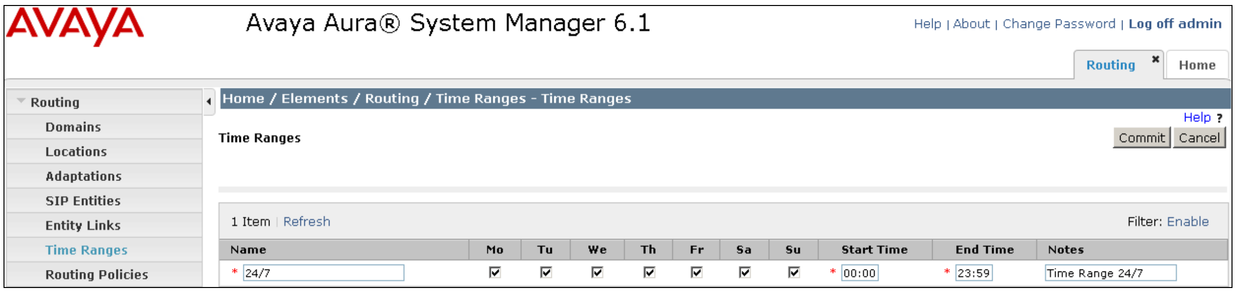
To configure this entity link, repeat the steps in **Section 5.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.6.5**. See the screen below for the values used in the reference configuration.



Entity Links Page – Entity Link to Messaging SIP Entity

5.8. Time Ranges

1. In the left pane under **Routing**, click **Time Ranges**. In the **Time Ranges** page click **New** [not shown].
2. On 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**.
3. Click **Commit**.
4. Repeat **Steps 1–3** to provision additional time ranges.



Time Ranges Page

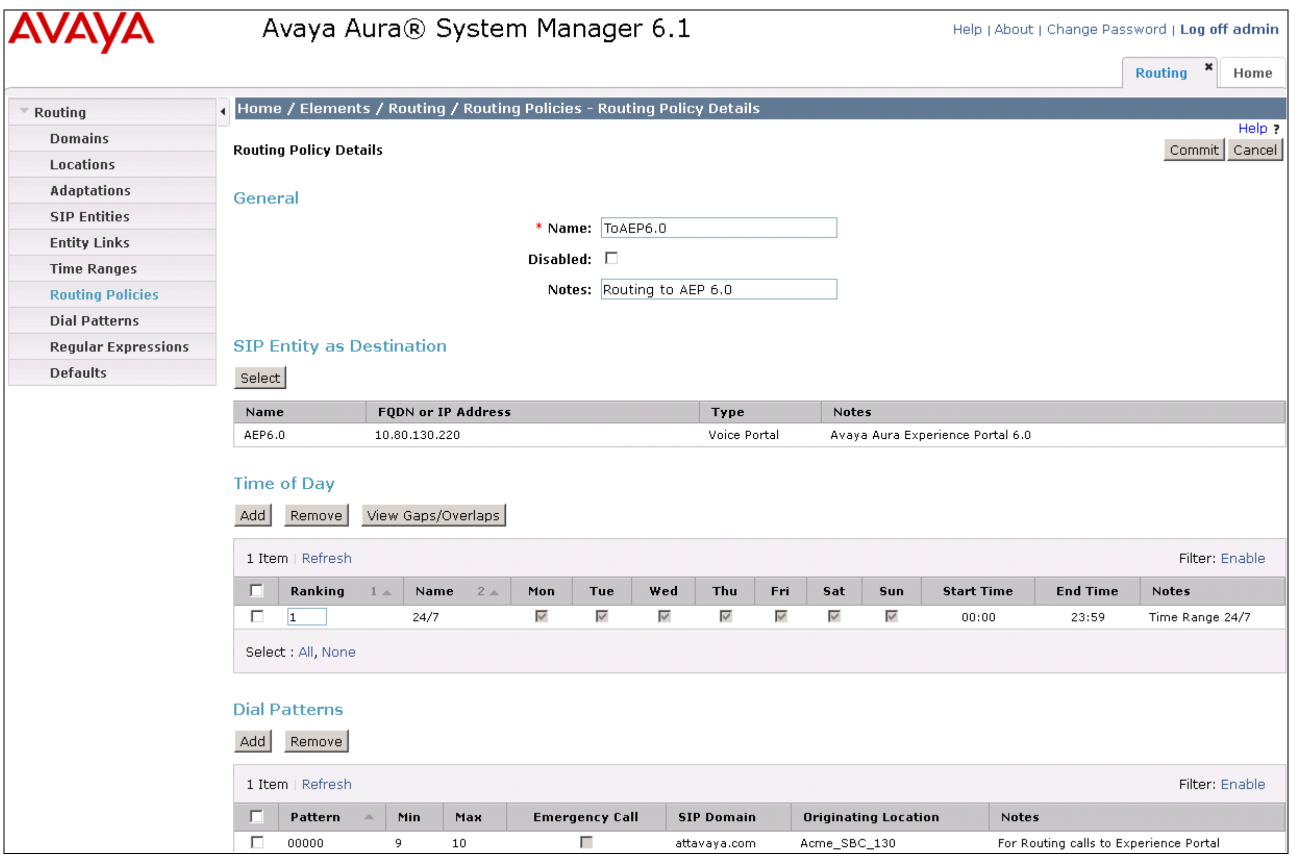
5.9. Routing Policies

In this section, Routing Policies are administered for routing calls to the following SIP Entities:

- Routing Policy to Avaya Aura® Experience Portal
- Routing Policy to Acme Session Border Controller
- Routing Policy to Avaya Aura® Communication Manager for calls from AT&T IP Toll Free service
- Routing Policy to Avaya Aura® Messaging

5.9.1. Routing Policy to Avaya Aura® Experience Portal

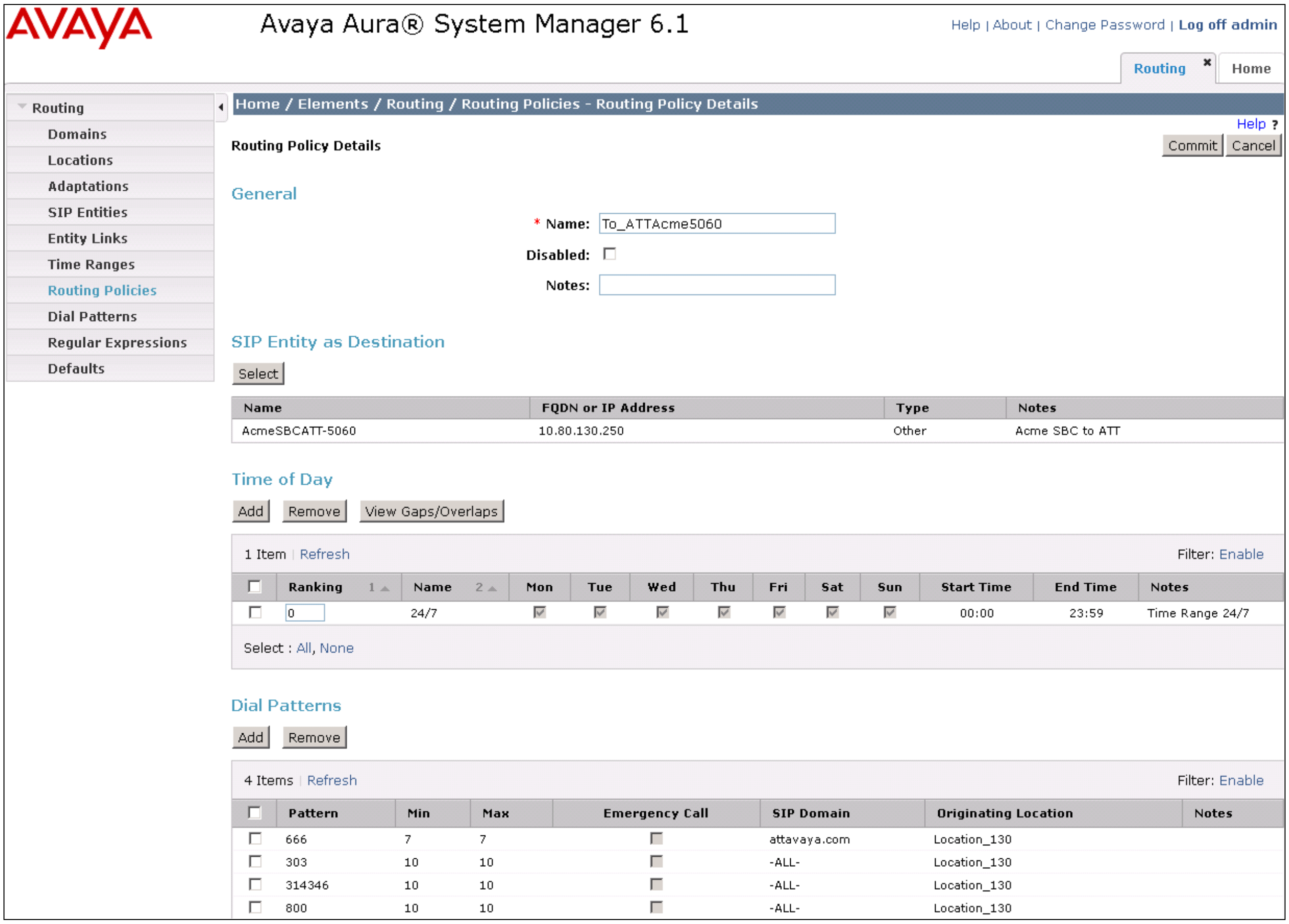
1. In the left pane under **Routing**, click **Routing Policies**. On the **Routing Policies** page click **New** [not shown].
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **ToAEP6.0**) for routing calls from AT&T IP Toll Free service via Acme SBC, and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click **Select**. A pop-up window is displayed [not shown] where Experience Portal entity configured in **Section 5.6.4** is selected. The result is displayed below in the **SIP Entity as Destination** section.
4. On the **Routing Policy Details** page shown below, click **Add** in the **Time of Day** section. In the **Time Range List** page [not shown], check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.8**, and click **Select**. On the **Routing Policy Details** page show below, enter a **Ranking** (the lower the number, the higher the ranking) in the **Time of Day** section for each Time Range.
5. Any **Dial Patterns** that were previously defined will be displayed and entries may be added or removed here. Dial patterns for this reference configuration are provisioned in **Section 5.10.1**.
6. No **Regular Expressions** were used in this reference configuration.
7. Click **Commit**.



Routing Policy Details Page to Experience Portal

5.9.2. Routing Policy to Acme Session Border Controller

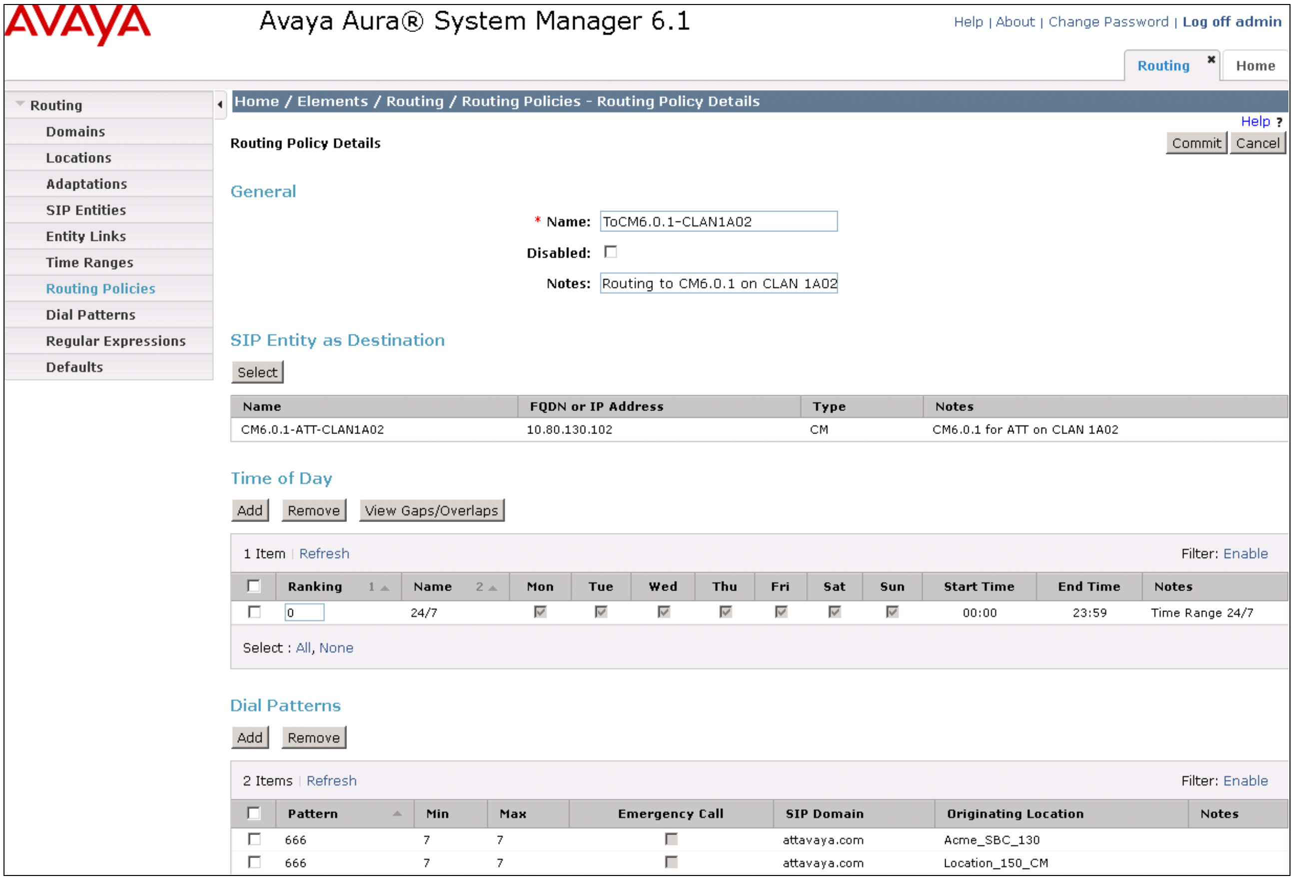
To configure routing policy to Acme SBC, repeat steps in **Section 5.9.1**. The following screen shows the routing policy configured for the calls to be routed to Acme SBC. Dial pattern/s for calls to be routed to Acme SBC are configured/displayed in **Section 5.10.2**.



Routing Policy Details Page to Acme SBC

5.9.3. Routing Policy to Avaya Aura® Communication Manager

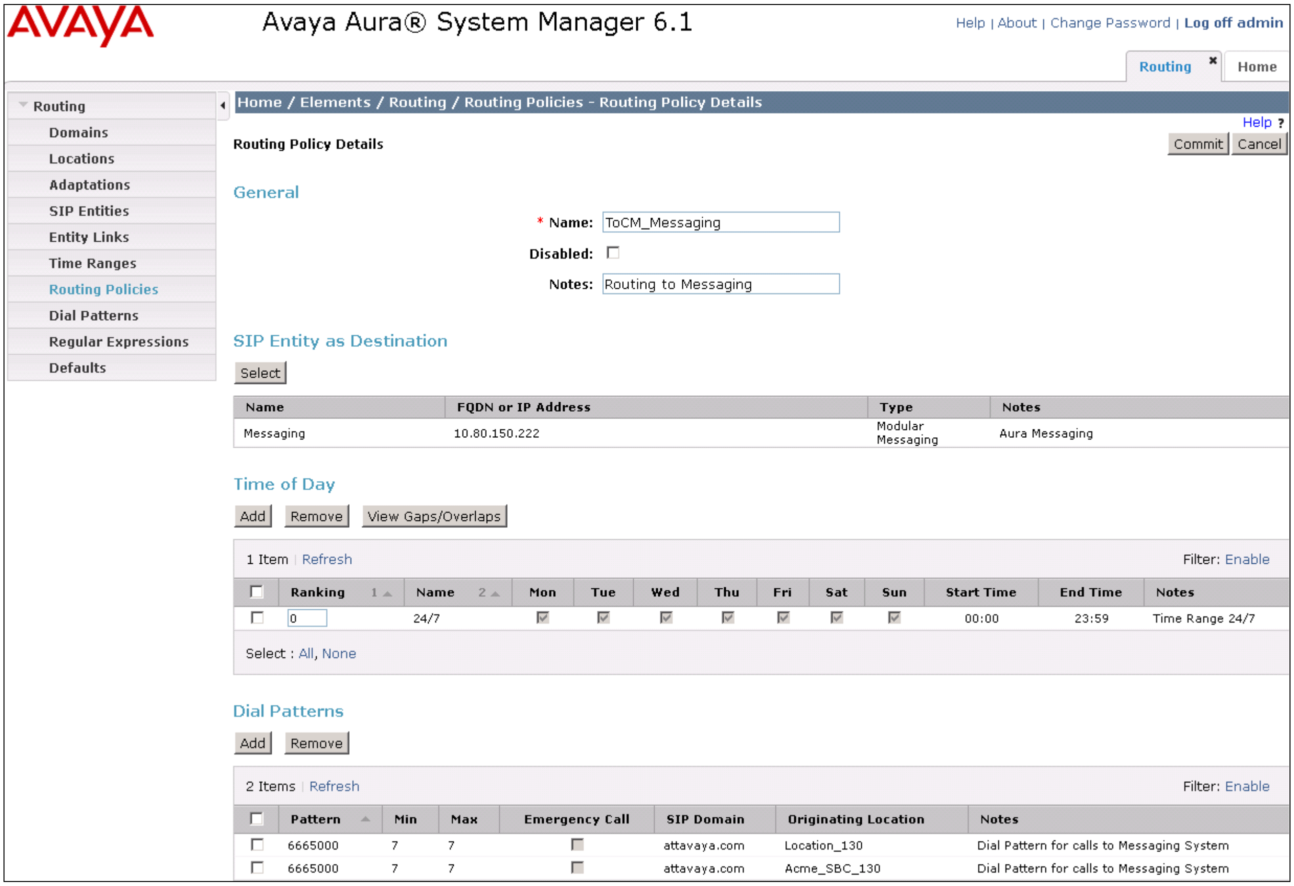
To configure routing policy to Communication Manager, repeat steps in **Section 5.9.1**. The following screen shows the routing policy configured for the calls to be routed to Communication Manager. Dial pattern/s for calls to be routed to Communication Manager are configured/displayed in **Section 5.10.3**.



Routing Policy Details Page to Communication Manager

5.9.4. Routing Policy to Avaya Aura® Messaging

To configure routing policy to Messaging, repeat steps in **Section 5.9.1**. The following screen shows the routing policy configured for the calls to be routed to Messaging. Dial pattern/s for calls to be routed to Messaging, is/are configured/displayed in **Section 5.10.4**.



Routing Policy Details Page to Messaging

5.10. Dial Patterns

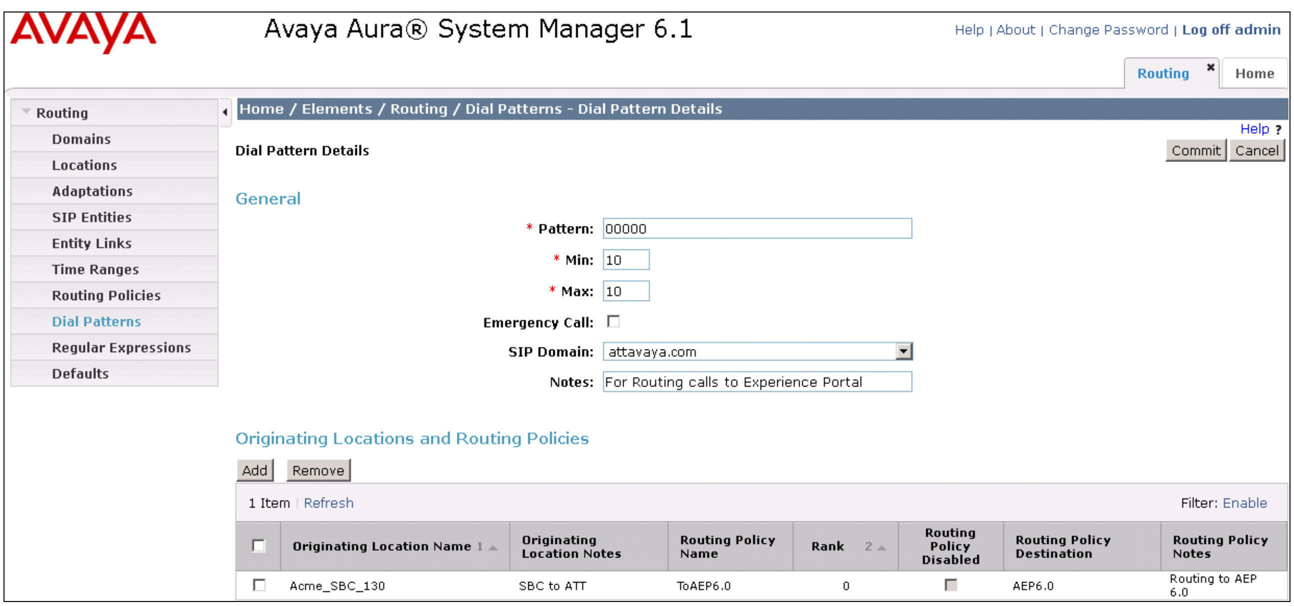
In this section, Dial Patterns are administered matching the following calls:

- Inbound PSTN calls from AT&T IP Toll Free service destined for Avaya Aura® Experience Portal
- Dial Pattern for Acme SBC
- Calls transferred to Avaya Aura® Communication Manager
- Calls to Avaya Aura® Messaging pilot number

5.10.1. Matching Inbound Calls from AT&T IPTF Service to Avaya Aura® Experience Portal

In this example inbound calls from any PSTN number with the pattern 00000xxxxx are defined.

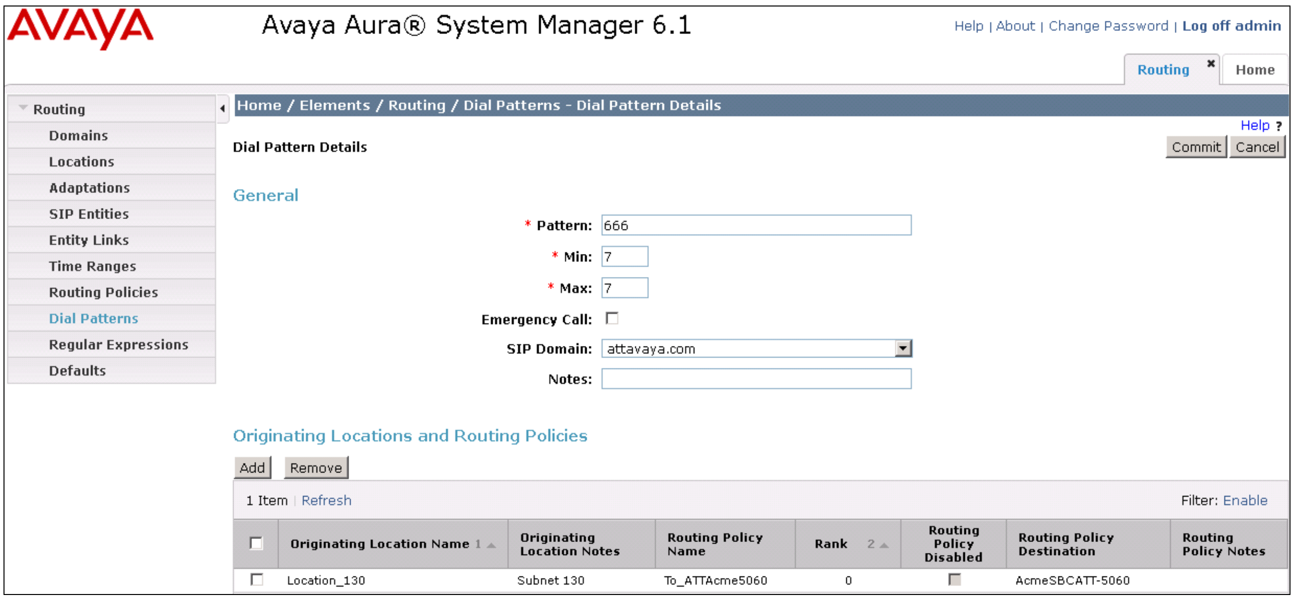
1. In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** [not shown].
2. In the **General** section of the **Dial Pattern Details** page, configure as follows:
   - **Pattern** – Enter matching patterns for inbound dialed digits. Set to **00000** for this reference configuration.
   - **Min** and **Max –** Enter **10**.
   - **SIP Domain** – Select one of the SIP Domains defined in **Section 5.3** or **-ALL-**, to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or any of the administered SIP Domains if **-ALL-** is selected) can match this Dial Pattern. Set to **attavaya.com** in this reference configuration.
   - **Notes** - [Optional] Add any notes if desired.
3. In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click **Add**.
4. In the **Originating Location** section of the **Originating Location and Routing Policy List** page [not shown], select the locations from where calls can originate to be routed to Experience Portal. 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. Originating location **Acme_SBC_130** configured in **Section 5.4** was selected in this reference configuration.
5. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page [not shown], select the Routing Policy administered for routing calls to Experience Portal in **Section 5.9.1**.
6. In the Originating Location and Routing Policy section, the values selected are displayed.
7. Click **Commit** on **Dial Pattern Details** page.



Dial Pattern Details Page - Matching Inbound Calls from AT&T to Experience Portal

5.10.2. Dial Pattern for Acme SBC

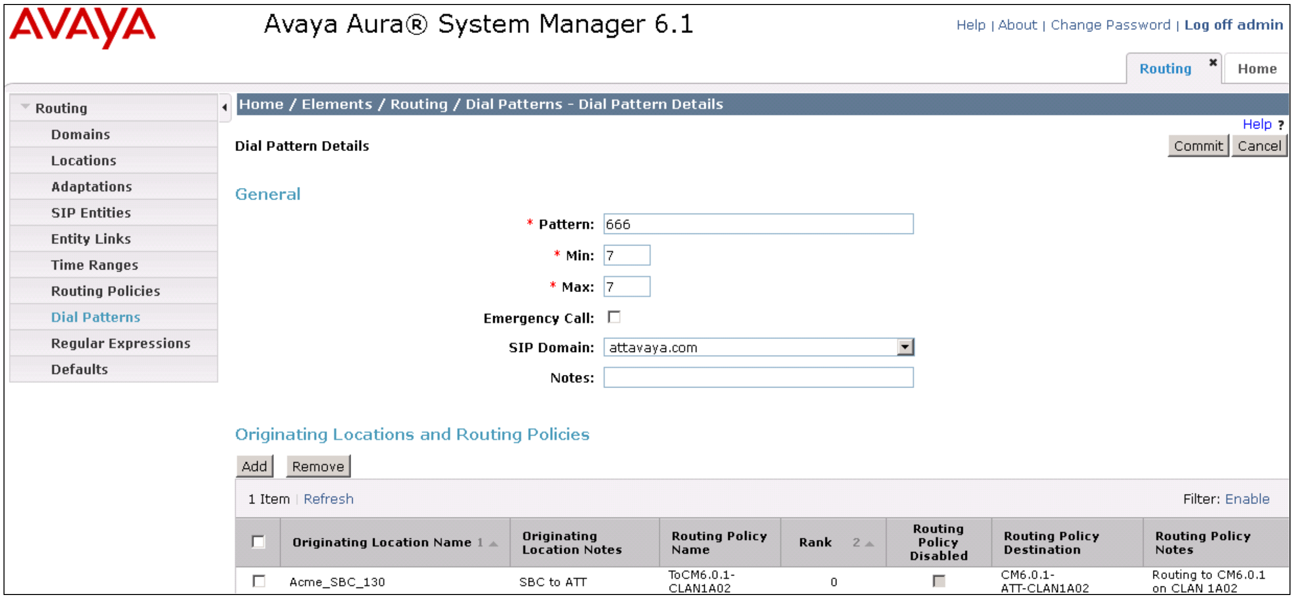
Repeat steps in **Section 5.10.1** to add additional dial patterns. The following screen shows the dial pattern configured for the calls to be routed to Acme SBC from Experience Portal in this reference configuration. Additional dial patterns **303xxxxxxx**, **314xxxxxxxx** and **800xxxxxxx** were also configured. Calls from Experience Portal are always routed to Acme SBC first and Acme SBC then decides based upon the local policy whether to forward the calls to PSTN or send them back to Session Manager for delivery to Communication Manager. In this reference configuration, calls to **800, 314** and **303** were forwarded to PSTN whereas calls to **666xxxx** were sent back to Session Manager for delivery to endpoints on Communication Manager.



Dial Pattern Details Page – Acme SBC

5.10.3. Matching Calls to Avaya Aura® Communication Manager

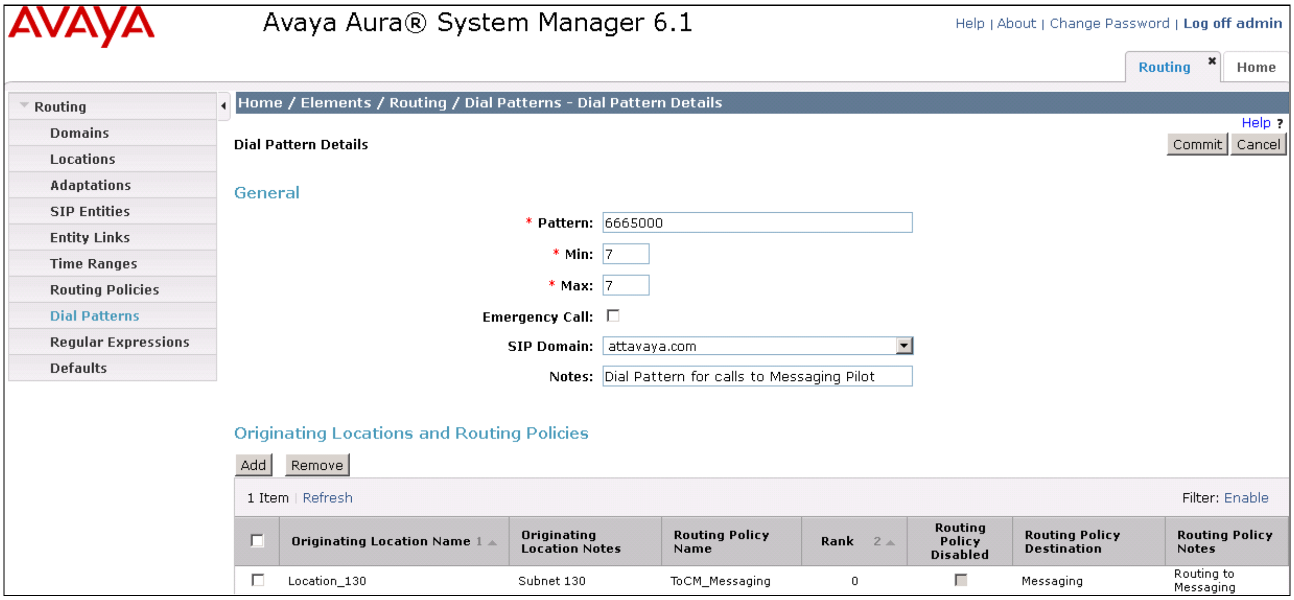
Repeat steps in **Section 5.10.1** to add additional dial patterns. The following screen shows the dial pattern configured for the calls to be routed to Communication Manager via Acme SBC from Experience Portal in this reference configuration. In this example, the calls from Experience Portal to **666xxxx** are routed to Communication Manager via Session Manager.



Dial Pattern Details Page – Matching calls from Experience Portal for Acme SBC

5.10.4. Matching Inbound Calls to Avaya Aura® Messaging Pilot Number

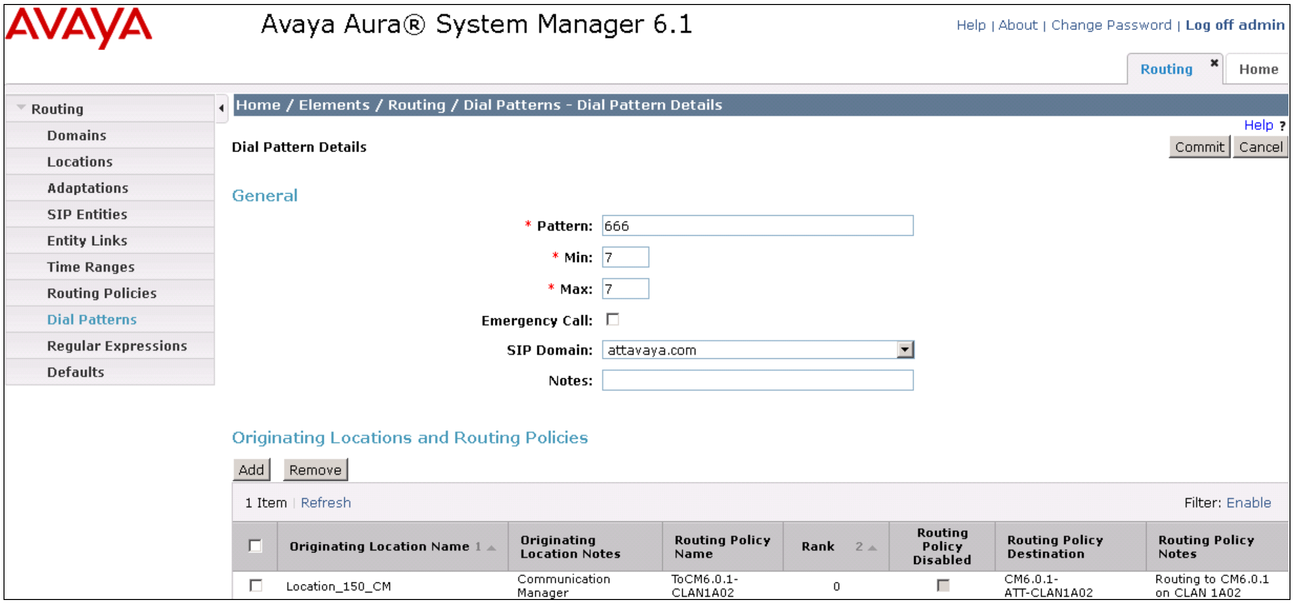
Communication Manager stations cover to Messaging using a pilot extension **6665000** in this reference configuration. Also, stations on Communication Manager may dial this number to retrieve messages or modify mailbox settings. To match dial pattern for the calls covered to Messaging, repeat the Steps in **Section 5.10.1**. Routing Policy configured in **Section 5.9.4** was used to route the call to Messaging.



Dial Pattern Details – Coverage to Messaging

5.10.5. Dial Pattern for MWI (Message Waiting Indicator) for stations on Avaya Aura® Communication Manager

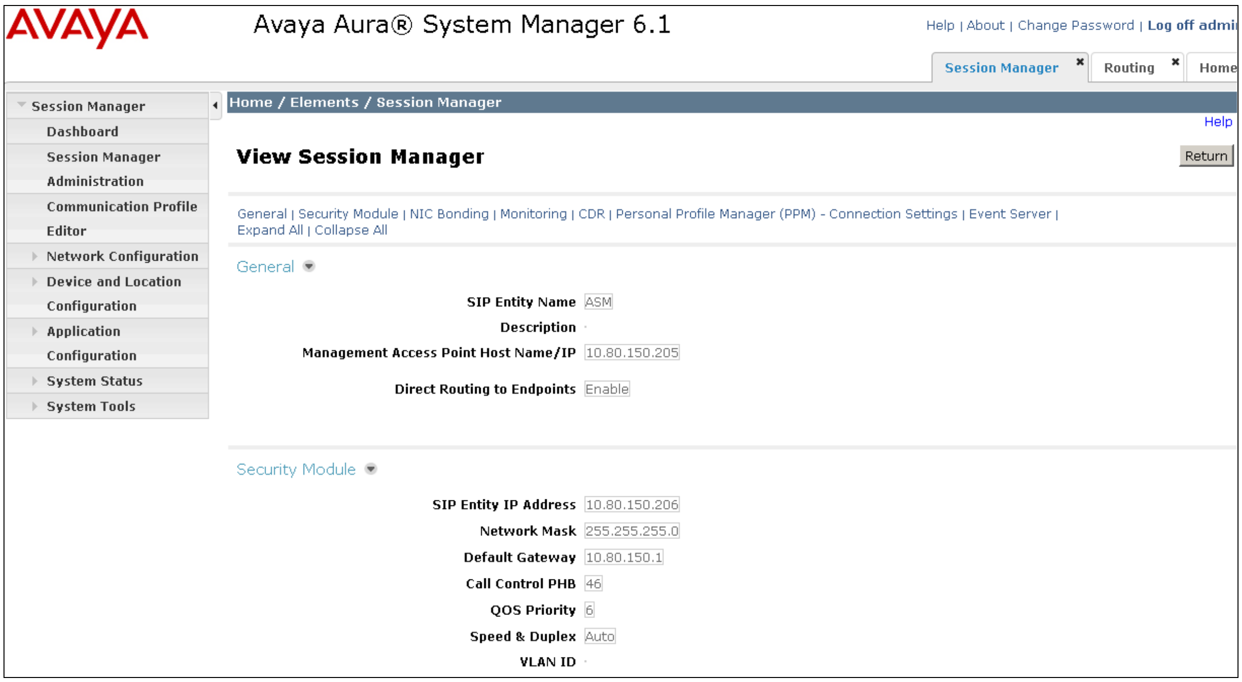
This pattern is used to match the stations on Communication Manager for MWI. Repeat the Steps in **Section 5.10.1**. Routing Policy configured in **Section 5.9.3** was used to route the MWI Notify to Communication Manager.



Dial Pattern Details – MWI for Communication Manager stations

5.11. Avaya Aura® Session Manager Administration

1. On the screen shown in **Section 5.2**, click Session Manager.
2. In the left pane of **Session Manager** page, click **Session Manager Administration**. On the **Session Manager Administration** page [not shown] in the Session Manager Instances, click **Add** [not shown] to add a Session Manager instance.
3. The screen below shows the Session Manager instance configured for this reference configuration.



View Session Manager Page

6. Avaya Aura® Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [1], [2] and [[3] for further details if necessary.

6.1. Background

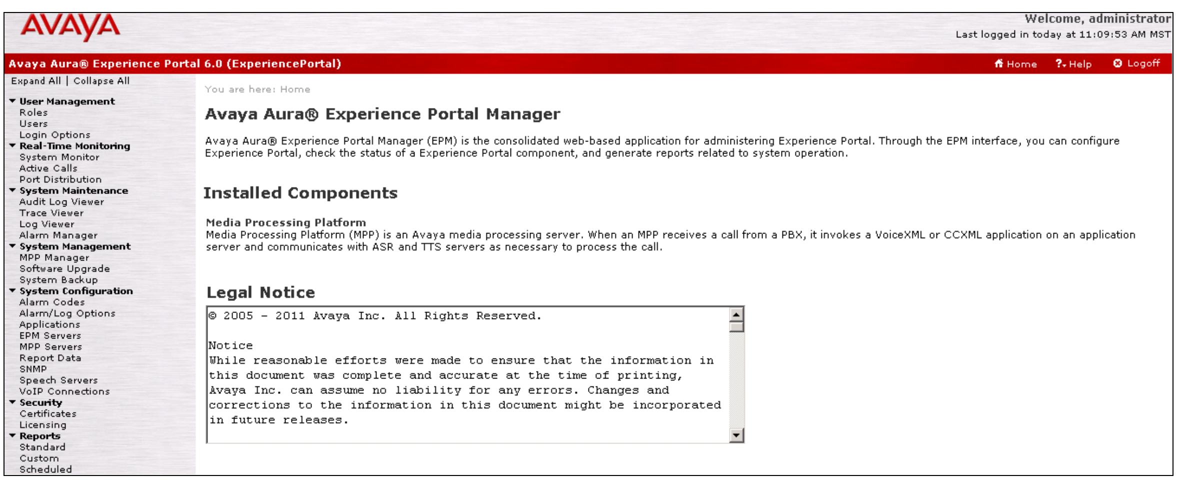
Experience Portal handles inbound calls according to the directives specified by Voice XML (VXML) and/or Call Control XML (CCXML) applications. These applications do not reside on Experience Portal, but on one or more separate application servers. References to these applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match[4] is found, Experience Portal informs the caller that the call can not be handled, and disconnects the call.

For this reference configuration, VXML and CCXML applications were developed specifically to exercise SIP call flow scenarios expected to occur with the AT&T IP Toll Free service. In production, enterprises can develop their own VXML and/or CCXML applications to meet their specific customer self-service needs, or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes.

6.2. VoIP Connection

This section describes the steps on Experience Portal for administering a SIP connection to the Session Manager.

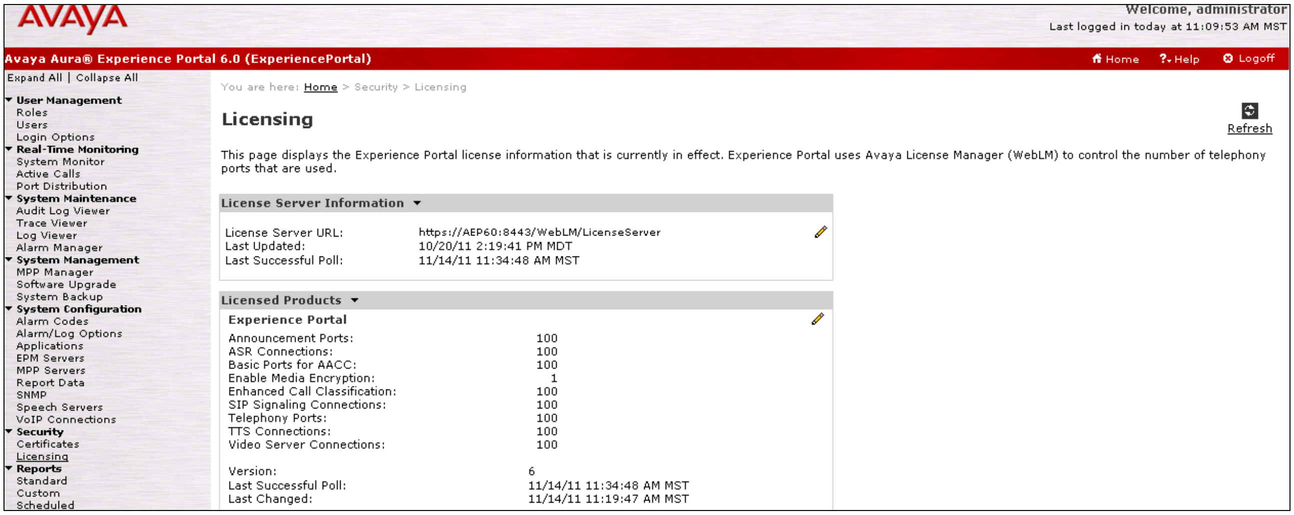
1. Launch a web browser, enter http://<IP address of the Avaya EPM server>/ in the URL, log in with the appropriate credentials and the following screen is displayed.



Experience Portal Home Page

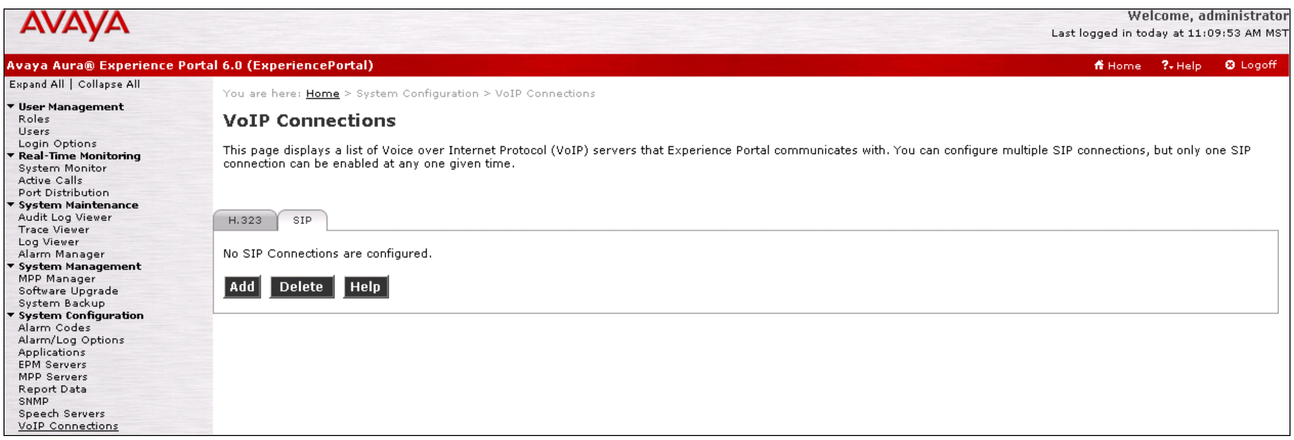
[4] One application reference may be configured with "inbound default" as the called number to handle all inbound calls that do not match any other application references.

2. In the left pane, navigate to **Security→Licensing**. On the **Licensing** page, verify that Experience Portal is properly licensed. For required licenses that are not enabled, contact an authorized Avaya account representative to obtain the licenses



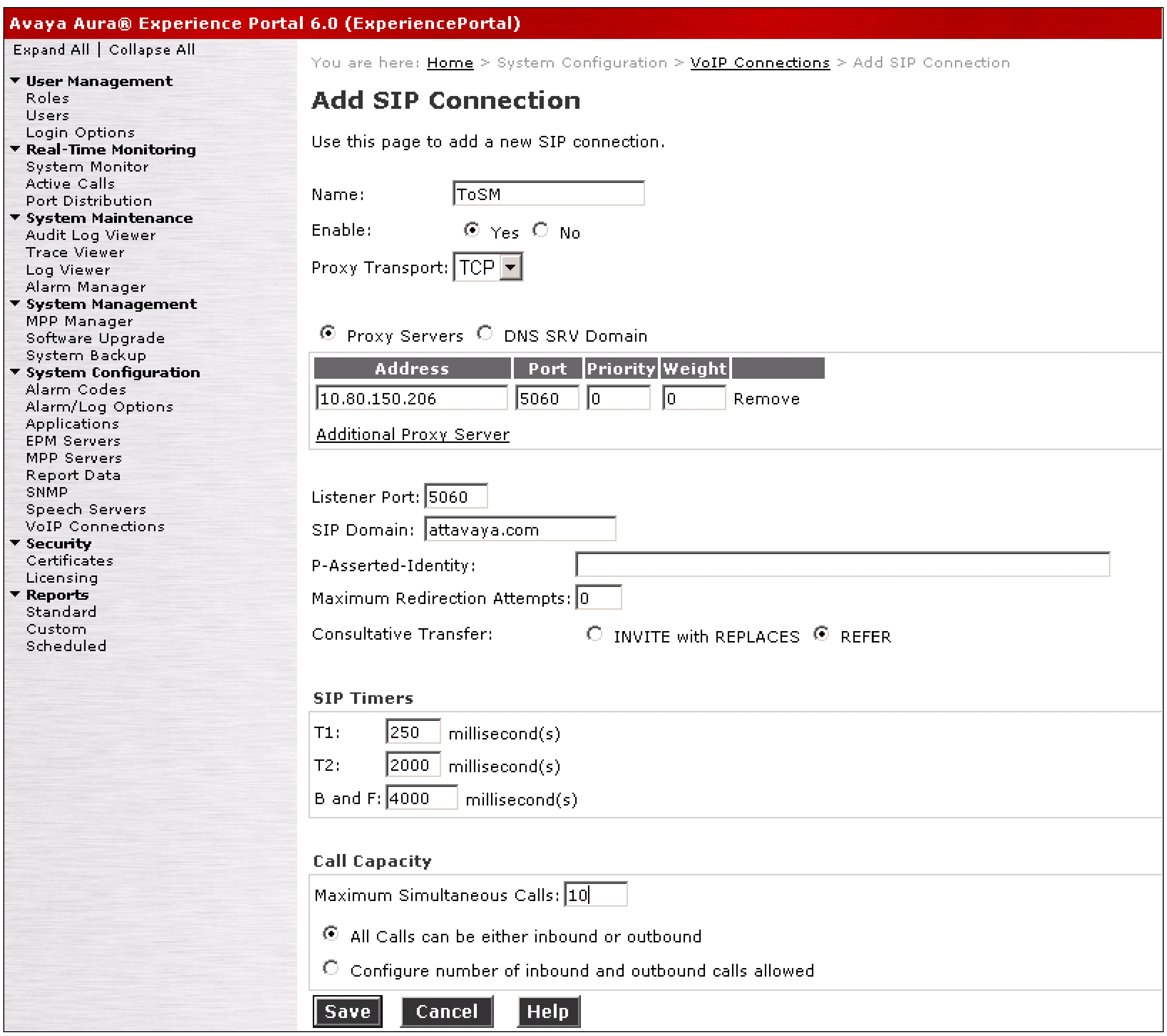
Experience Portal Licensing Page

3. In the left pane, navigate to **System Configuration→VoIP Connections**. On the **VoIP Connections** page, select the **SIP** tab and click **Add** to add a SIP trunk. Note that only **ONE** SIP trunk can be active at any given time on Experience Portal.



VoIP Connections Page

4. Configure the SIP connection as follows:
   - **Name** – Set to a descriptive name.
   - **Enable** – Set to **Yes**.
   - **Proxy Transport** – Set to **TCP**.
   - **Proxy Server Address** – Set to the IP address of the Session Manager signaling interface.
   - **Proxy Server Port** – Set to **5060**.
   - **SIP Domain** – Set to SIP domain configured in **Section 5.3**.
   - **Consultative Transfer** – Select **REFER** radio button.
   - **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In this reference configuration a value of **10** was used for this field.
   - Set to the **All Calls can be either inbound or outbound** radio button.
   - Click **Save**.

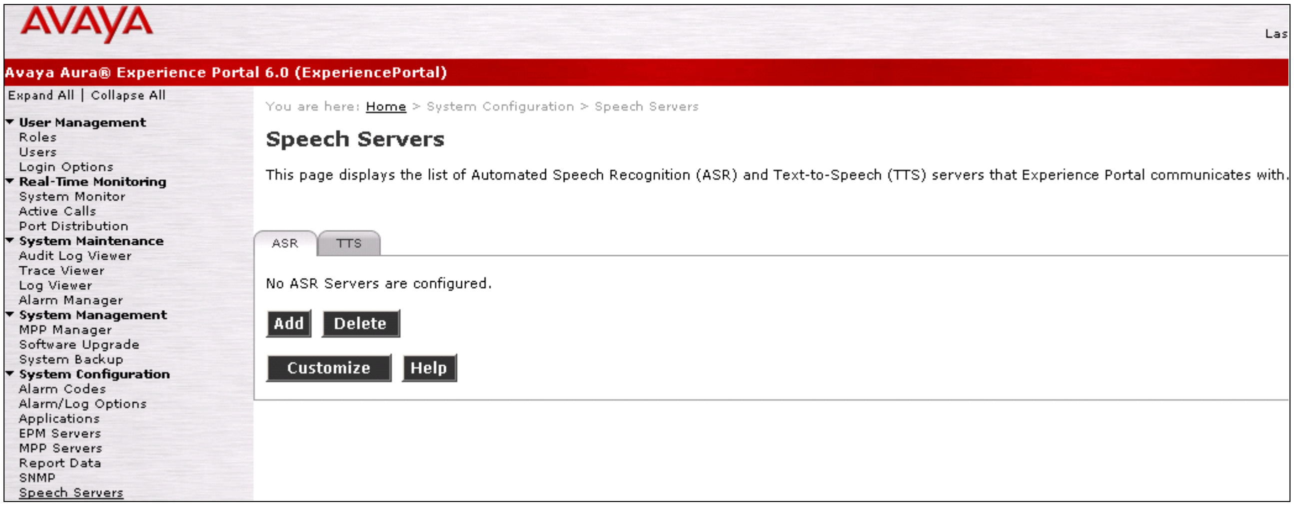


Add SIP Connection Page

6.3. Speech Servers

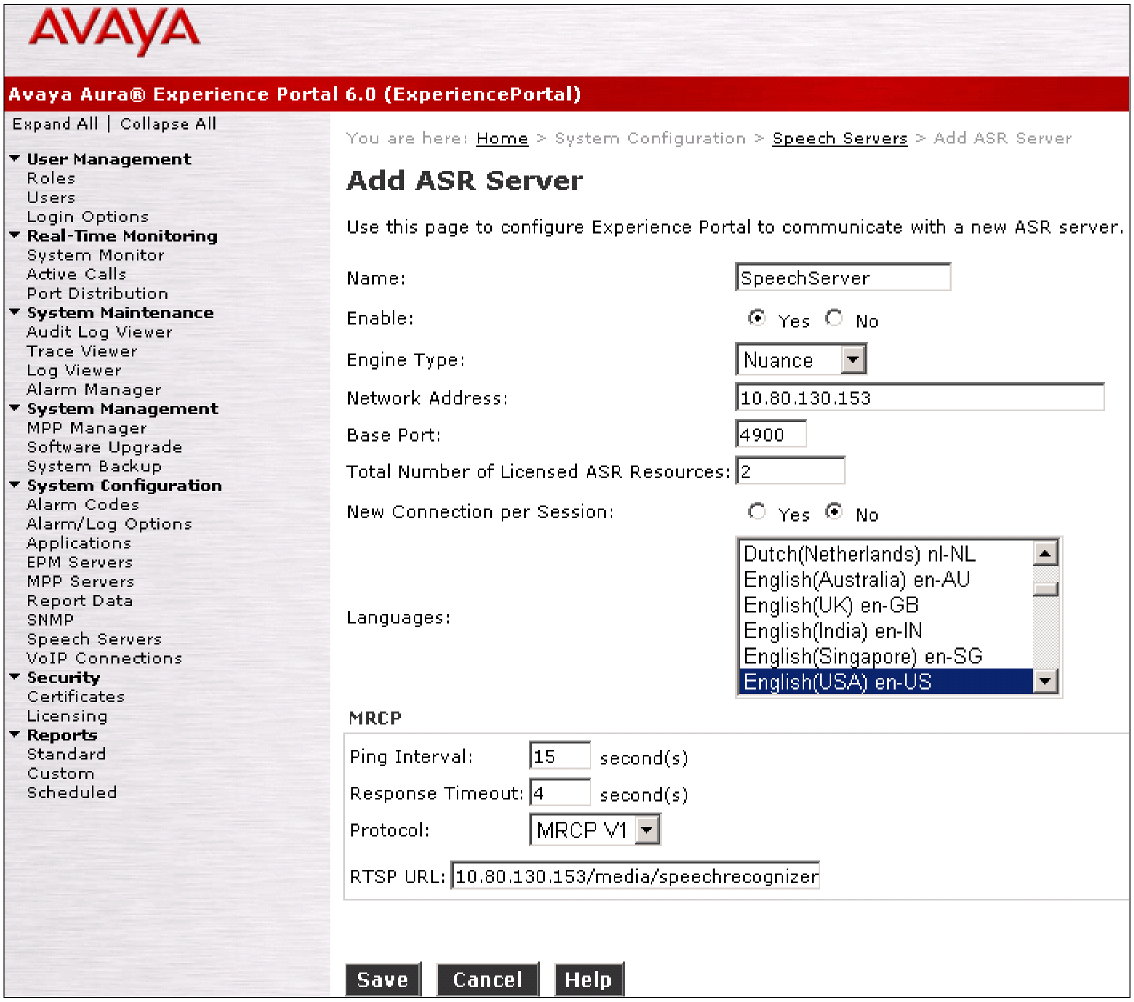
The installation and administration of the Speech Servers is beyond the scope of this document.

1. To configure Experience Portal for communication with Speech Server, navigate to **System Configuration→Speech Servers** and the following screen is displayed. Click **ASR** and **Add** to add an ASR server.



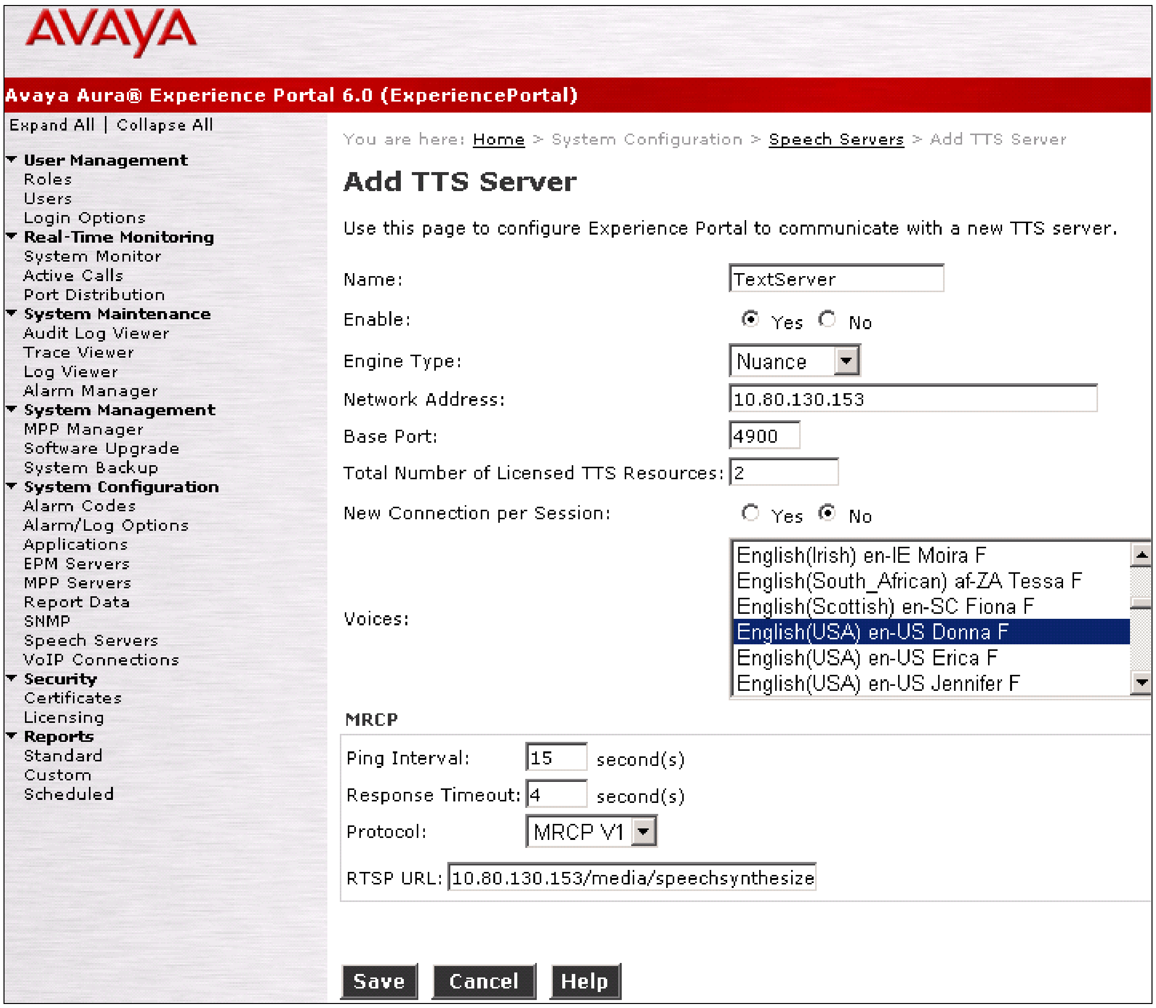
Speech Server Page

2. On the **Add ASR Server** page, configure as follows:
   - **Name** – Set to any descriptive name.
   - **Enable** – Select the **Yes** radio button.
   - **Engine Type** – Select **Nuance**.
   - **Nework Address** – Set to the IP address of the ASR Server.
   - **Languages** – Select the appropriate value.
   - Click **Save**.



Add ASR Server Page

3. Click **TTS** and **Add** on the screen shown in Step 1. On the **Add TTS Server** page, configure as follows:
    - **Name** – Set to any descriptive name.
    - **Enable** – Select the **Yes** radio button.
    - **Engine Type** – Select **Nuance**.
    - **Nework Address** – Set to the IP address of the ASR Server.
    - **Languages** – Select the appropriate value.
    - Click **Save**.



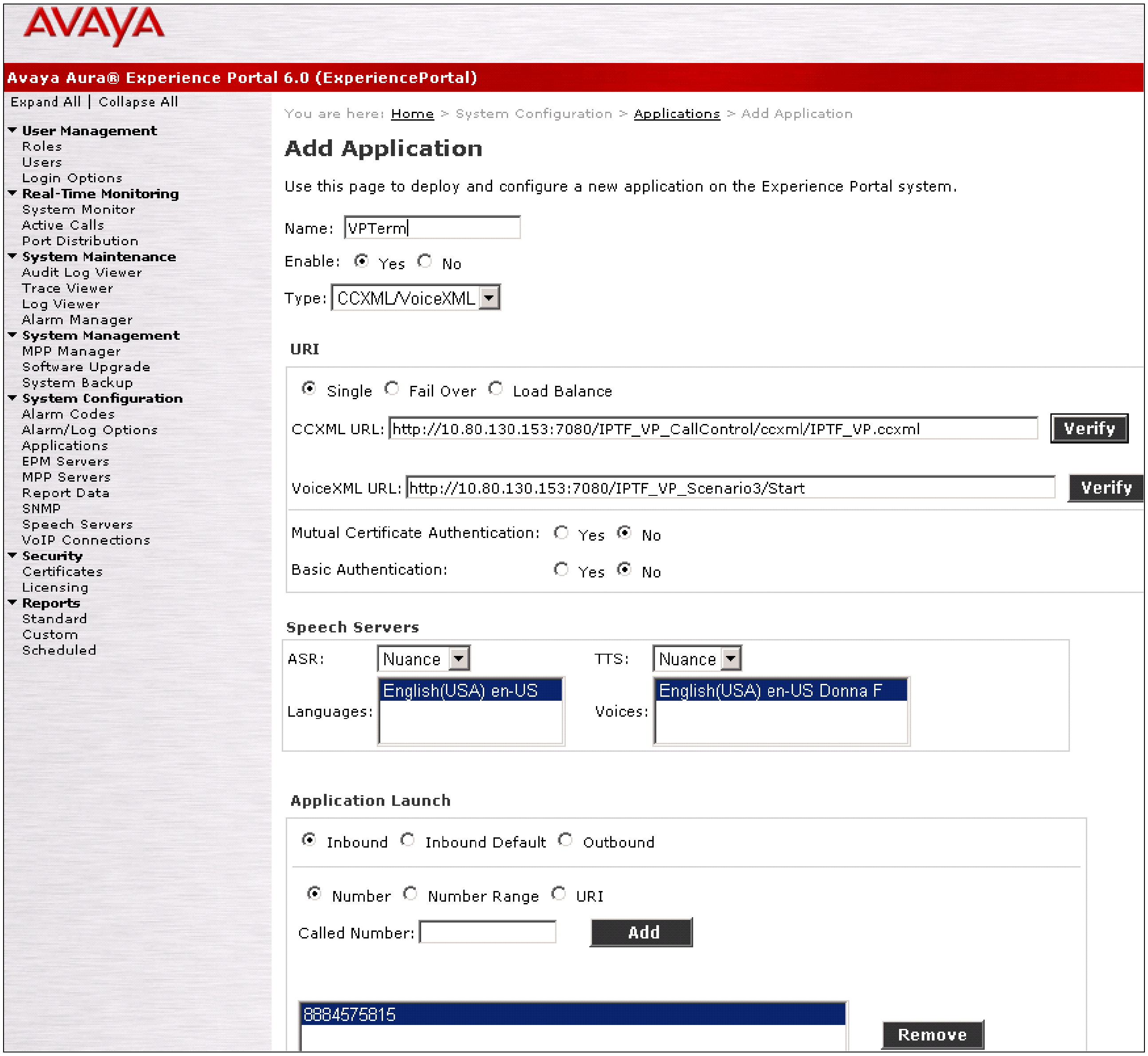
Add TTS Server Page

6.4. Application References

This section describes the steps on Experience Portal for administering a reference to a VXML and/or CCXML application residing on an application server.

1. In the left pane, navigate to **System Configuration→Applications**. On the **Applications** page [not shown], click on **Add** to add an application and configure as follows:
   - **Name** – Set to a descriptive name.
   - **Enable** – Set to **Yes**.
   - **MIME Type** – Set **CCXML/VoiceXML** for the application used in this reference configuration.
   - **VoiceXML** and/or **CCXML URL** – Set to the URL(s) to access the VXML and/or CCXML application(s) on the application server.
   - **Speech Servers ASR** and **TTS** – Set to **Nuance**.
   - **Languages** is set to **English (USA) en-US and Voices** is set to **English(USA) en-US Donna F**. This is as per Speech server settings in **Section 6.3**.
   - **Application Launch –** Set to **Inbound**.

   Inbound AT&T IP Toll Free service calls with these called party numbers will be handled by this application defined in the following steps.
   - Select the **Number** or **URI** radio button. URI is used where the called party number is a mix of numbers and characters.
   - **Called Number –** Set to an inbound AT&T IP Toll Free service called party number specified in the **To** header of the inbound SIP INVITE message. Repeat to define additional AT&T IP Toll Free service called party numbers if necessary.

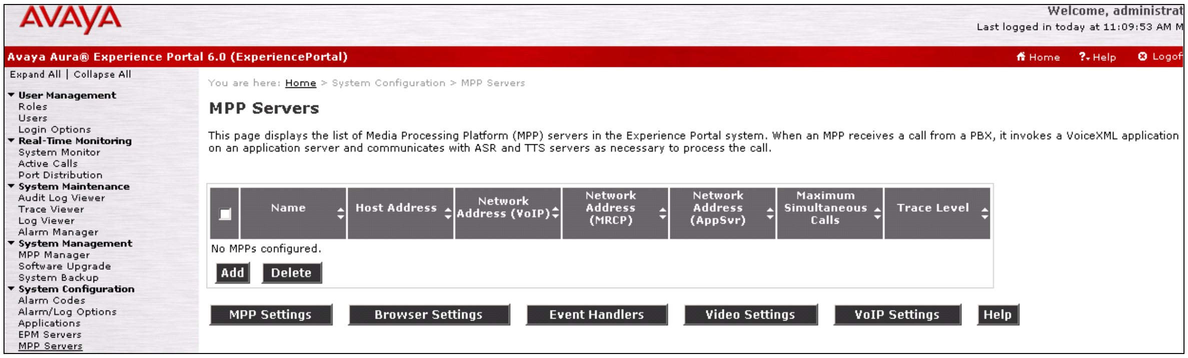


Add Application Page

2. Repeat above step/s to administer additional applications.

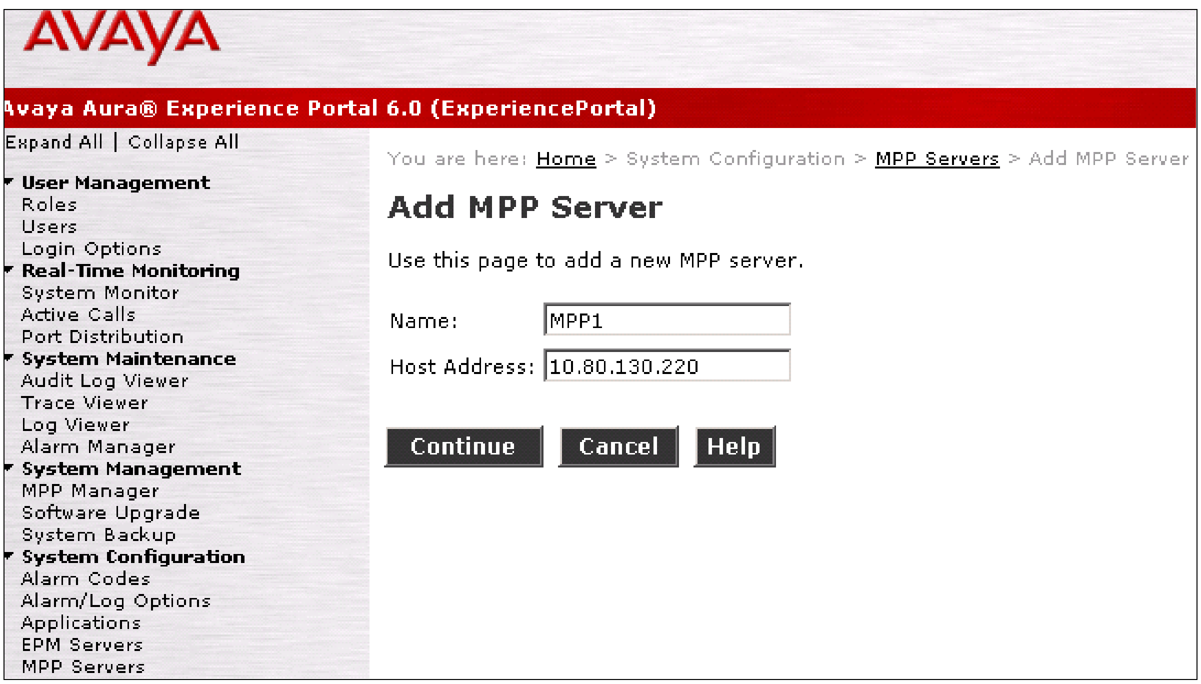
6.5. Add MPP Server

1. In the left pane, navigate to **System Configuration→MPP Servers** and the following screen is displayed. Click **Add**.



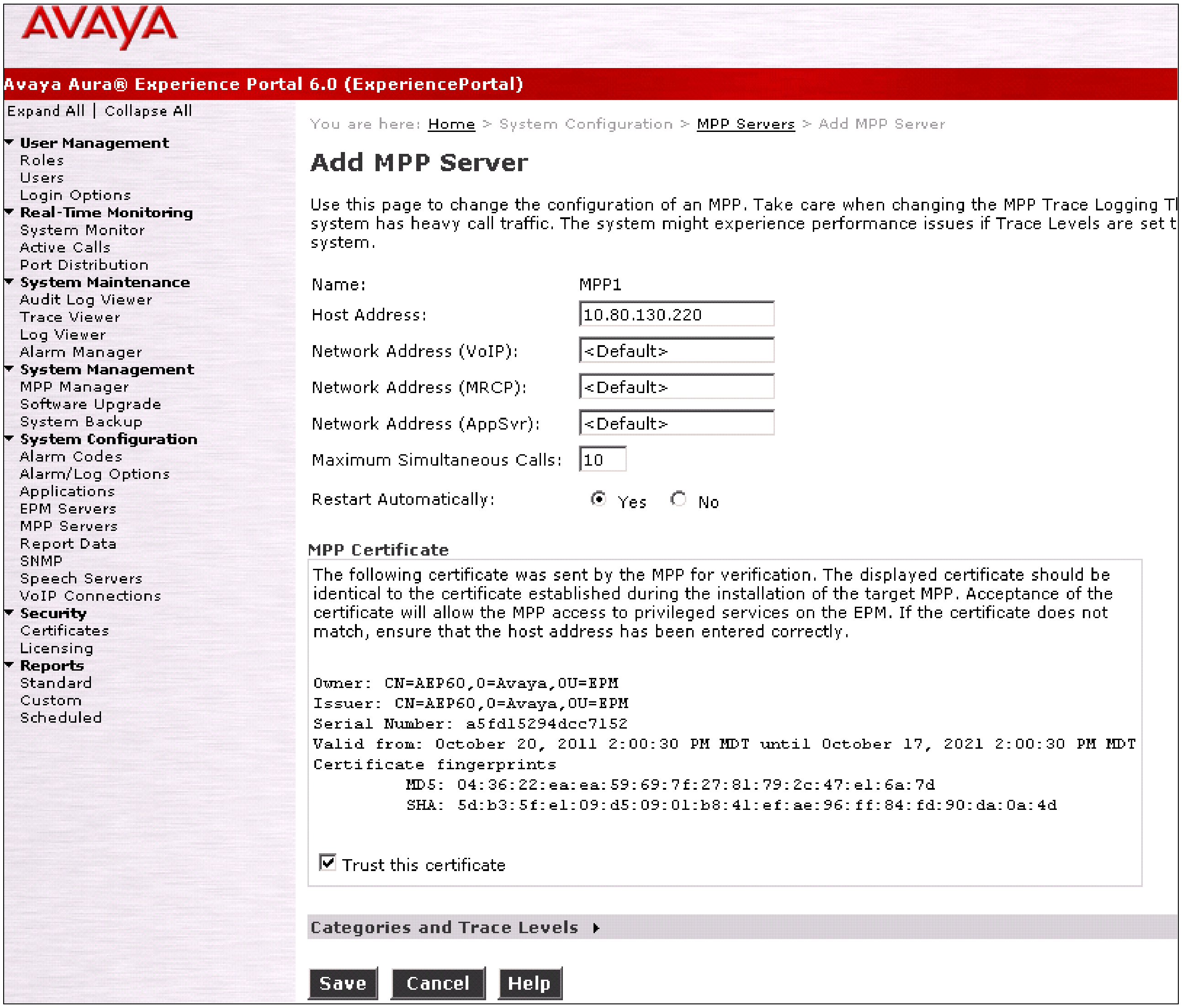
MPP Servers Page

2. Enter any descriptive name in the **Name** field and IP address of the MPP server in the **Host Address** field and click **Continue**.



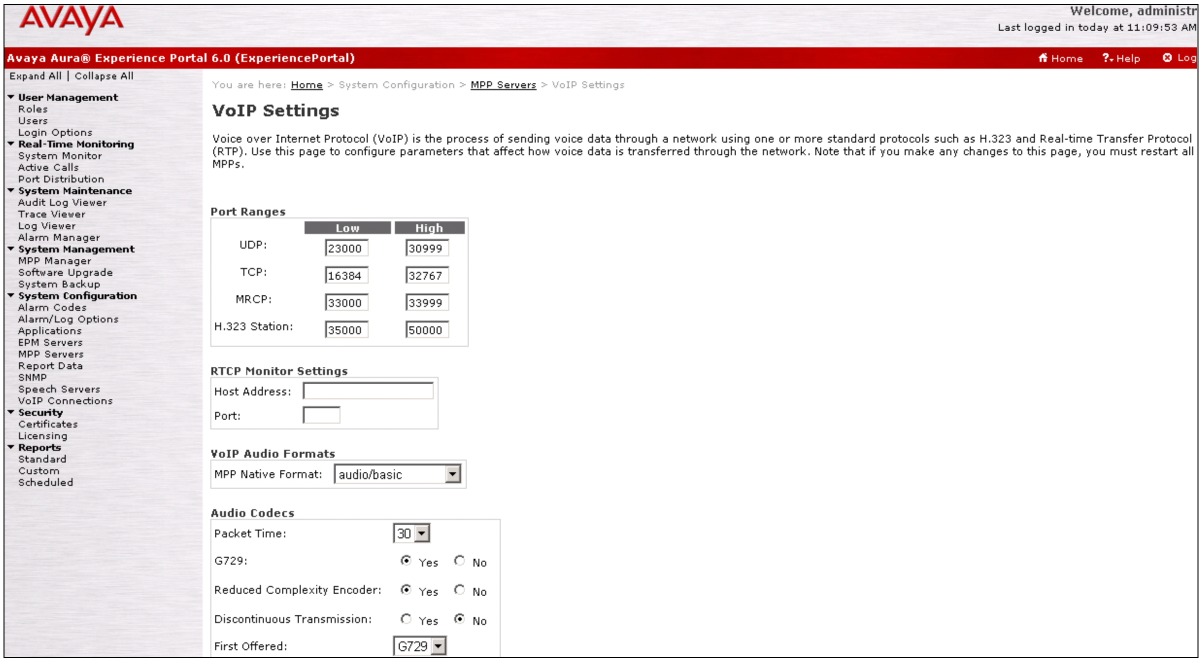
Add MPP Servers Page

3. Check the **Trust this certificate** box and click **Save**.



Add MPP Server Page - Continued

4. Click **VoIP Settings** tab on the screen displayed in **Step 1** and the following screen is displayed. Verify that TCP ports are in the range of **16384** and **32767** as required AT&T IP Toll Free service. Additionally set **Discontinuous Transmission** field under **Audio Codecs** to **No**.



VoIP Settings Page

6.6. Configuring RFC2833 Event Value Offered by Avaya Aura® Experience Portal

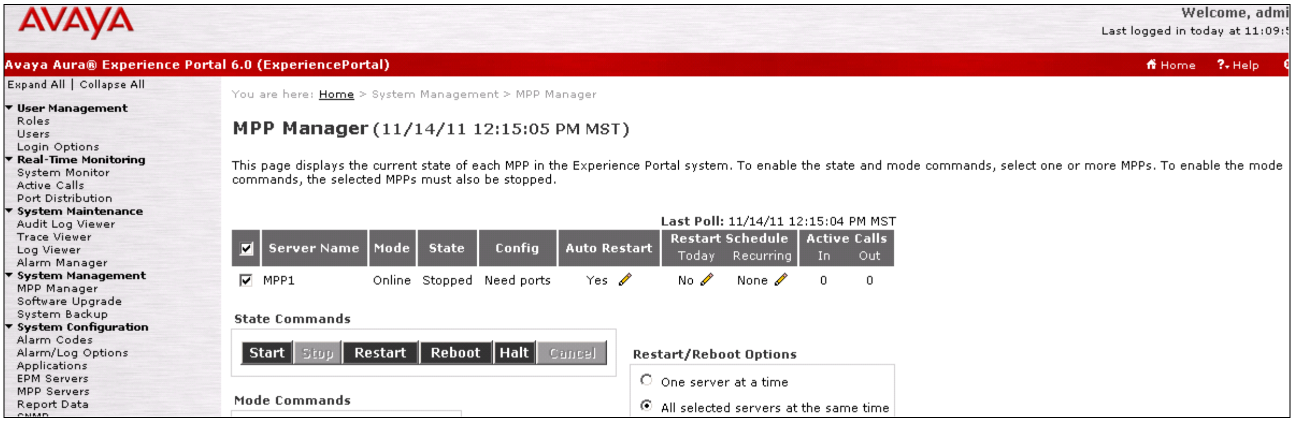
The configuration change example noted in this section is not required for any of the call flows illustrated in these Application Notes. For incoming calls from AT&T IP Toll Free service to Experience Portal, AT&T specifies the value 100 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience Portal answers, the SDP from Experience Portal matches this AT&T offered value. When Experience Portal sends an INVITE with SDP as part of an INVITE-based transfer (e.g., bridged transfer), Experience Portal offers the SDP. By default, Experience Portal specifies the value 127 for the RFC2833 telephone-events. Optionally, the value that is offered by Experience Portal can be changed, and this section outlines the procedure that can be performed by an Avaya authorized representative.

- Access the Experience Portal via the command line interface and navigate to the /opt/Avaya/Experience Portal/MPP/config directory.
- Edit the file mppconfig.xml.
- Search for the parameter **mpp.sip.rfc2833.payload**.
- If the parameter is already specified in the file, simply edit the value assigned to the parameter. If there is no such parameter specified, add a line such as the following to the file, where 100 is the value to be used for the RFC2833 events.
    - **<parameter name=”mpp.sip.rfc2833.payload”>100</parameter>**

After saving the file with the change, restart the MPP server for the change to take effect as shown in **Section 6.7**.

6.7. MPP Manager

In the left pane, navigate to **System Maintenance→MPP Manager** and select the **MPP1**. Click **Restart** to make sure that the changes made in the above steps are effected. Note that all the configuration changes do not require restart of the MPP Manager.



MPP Manager Page

7. 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. For any values not configured, defaults are used in this reference configuration. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [6] and [7] for further details if necessary.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to this reference configuration. Other parameter values may or may not match specific local configurations.

7.1. System Parameters

This section reviews the Communication Manager licenses and features that are required for the sample configuration described in these Application Notes. For required licenses that are not enabled in the steps that follow, contact an authorized Avaya account representative to obtain the licenses.

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

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 100   30
           Maximum Concurrently Registered IP Stations: 12000 6
             Maximum Administered Remote Office Trunks: 8000  0
Maximum Concurrently Registered Remote Office Stations: 12000 0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 20    0
                  Maximum Video Capable H.323 Stations: 20    0
                   Maximum Video Capable IP Softphones: 20    0
                       Maximum Administered SIP Trunks: 5000  30
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                            Maximum TN2501 VAL Boards: 10     1
                     Maximum Media Gateway VAL Sources: 5     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 200   0
      NOTE: You must logoff & login to effect the permission changes.)
```

System-Parameters Customer-Options Form – Page 2

2. On **Page 4** of the **system-parameters customer-options** form, verify that the bolded field in the following screenshot is set to **y**.

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

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

System-Parameters Customer-Options Form – Page 4

7.2. Dial Plan

Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings were administered for this sample configuration:

- 3-digit dial access codes (indicated with a **Call Type** of **dac**) beginning with the digit **1** – Trunk Access Codes (TACs) defined for trunk groups in this sample configuration.
- 7-digit extensions with a **Call Type** of **ext** beginning with the digit **6661** – used for announcements, beginning with the digit **6662** – used for Vector Directory Numbers (VDN), beginning with the digit **6663** – used for agent login ids, beginning with the digit **6664** – used for hunt group extensions, and beginning with the digit **6665** – used for telephone extensions.

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all         Percent Full:    1

       Dialed   Total  Call     Dialed   Total  Call      Dialed   Total  Call
       String   Length Type     String   Length Type      String   Length Type
     1            3    dac
     6662         7    ext
     6663         7    ext
     6664         7    ext
     6665         7    ext
     8            1    fac
     9            1    fac
     *            3    fac
     #            3    fac
```

Dialplan Analysis Form

7.3. IP Network Parameters

These Application Notes assume that the appropriate IP network regions and IP codec sets have already been administered to support internal calls, i.e., calls within the enterprise. For simplicity in this sample configuration, all Communication Manager elements, e.g., stations, C-LAN and MedPro boards, etc., within are assigned to a single IP network region. This section describes the steps for administering an additional IP network region and IP codec set to represent inbound calls from the AT&T IP Toll Free service to Experience Portal that are subsequently transferred to Communication Manager via Session Manager and Acme SBC. Note that the configuration steps in these application notes are used for this reference configuration and not meant to be prescriptive in nature.

1. Enter the **change ip-codec-set n** command, where **n** is the number of an unused IP codec set to be used for inbound calls. On **Page 1** of the **ip-codec-set** form, provision following codecs. AT&T IP Toll Free service uses **G.729A** as its preferred codec but also supports **G.711MU** and **G.726A-32K**. G.726 is supported by Communication Manager but not by Experience Portal.

```
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.729A        n            3         30
 2: G.711MU       n            2         20
 3: G.726A-32K    n            2         20
```

IP-Codec-Set Form for Inbound Calls – Page 1

On **Page 2** of the ip-codec-set form, set the **Fax – Mode** field to **t.38 standard**.

```
change ip-codec-set 2                                          Page   2 of   2

                          IP Codec Set
                              Allow Direct-IP Multimedia? n

                      Mode                    Redundancy
 FAX                  t.38 standard            0
 Modem                off                      0
 TDD/TTY              US                       3
 Clear-channel        n                        0
```

IP-Codec-Set Form for Inbound Calls – Page 2

2. Enter the **change node-names ip** command, and add a node name and the IP address for the Session Manager. Also note the node name and IP address of a C-LAN board that is assigned to one of the IP network regions administered for local Communication Manager elements within the Avaya site. This C-LAN board will be used in **Section 7.4**, **Step 1** for administering a SIP trunk to the Session Manager.

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM                  10.80.150.206
CLAN-1A02            10.80.130.102
```

Change Node-Names IP Form

3. Enter the **change ip-network-region n**, where **n** is the number of an unused IP network region. This IP network region will be used to represent the AT&T IP Toll Free service. Note that the **Code Set** field is set to **2** which is configured in **Step 1**. Also, the port range is set between **16384** and **32767** as required by AT&T.

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

IP-Network-Region Form for the Network Region Representing the Avaya IP Toll Free Service – Page 1

On **Page 4** of the **ip-network-region** form, for each IP network region pair consisting of this IP network region as the **src rgn** and another IP network region as the **dst rgn**, provision the following:

- **codec set** – Set to the codec set administered in **Step 1**.
- **direct WAN** – Set to **y**.
- **WAN-BW-limits** – Set to the maximum number of calls or bandwidth allowed between the two IP network regions. The setting shown below was used in this reference configuration.

In the example below, for all calls to elements in IP network region 1 will use codec set 2.

```
change ip-network-region 2                                    Page   4 of  19

                  Inter Network Region Connection Management

 src dst codec direct   WAN-BW-limits   Video      Intervening   Dyn
 rgn rgn  set   WAN  Units    Total Norm  Prio Shr Regions       CAC IGAR AGL
 2   1    2     y    NoLimit                                         n   all
 2   2
 2   3
 2   4
```

IP-Network-Region Form for an IP Network Region Representing the AT&T IP Toll Free Service– Page 4

7.4. Inbound Calls

This section describes the steps for administering the SIP trunk from Communication Manager to Session Manager.

1. Enter the **add signaling-group s** command, where **s** is the number of an unused signaling group, and provision the following:
   - **Group Type** – Set to **sip**.
   - **Transport Method** – Set to **tcp**. Note that this is only the transport protocol used between Communication Manager and the Session Manager.
   - **Near-end Node Name** – Set to the node name of the C-LAN board noted in **Section 7.3**, **Step 2**.
   - **Far-end Node Name** – Set to the node name of the Session Manager as administered in **Section 7.3**, **Step 2**.
   - **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**.
   - **Far-end Network Region** – Set to the IP network region administered in **Section 7.3**, **Step 3** to represent the PSTN.
   - **Far-end Domain** – Set to **attavaya.com**. This domain matches the domain configured in **Section 5.3**.
   - **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF as per RFC 2833.
   - **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible.

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

 Group Number: 2             Group Type: sip
                       Transport Method: tcp


   Near-end Node Name: CLAN_1A02            Far-end Node Name: ASM
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 2
       Far-end Domain: attavaya.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? n                    Direct IP-IP Early Media? n
 H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Signaling-Group Form for Transferred Inbound Calls

2. Enter the **add trunk-group t** command, where **t** is the number of an unused trunk group. On Page 1 of the **trunk-group** form, provision the following:
   - **Group Type** – Set to **sip**.
   - **Group Name** – Enter a descriptive name.
   - **TAC** – Enter a trunk access code that is consistent with the dial plan.
   - **Direction** – Set to **two-way**.
   - **Service Type** – Set to **public-ntwrk**.
   - **Signaling Group** – Set to the number of the signaling group administered in **Step 1**.
   - **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group.

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

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: ATT IPTF                    COR: 1        TN: 1        TAC: 102
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                                Night Service:
Queue Length: 0
Service Type: public-ntwrk         Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 10
```

Trunk-Group Form for Transferred Inbound Calls – Page 1

3. Enter the **change public-unknown-numbering 0** command to specify the connected party numbers sent on transferred inbound calls. In the **public-unknown-numbering** form, for each local extension range assigned to Communication Manager phones, agents, skills (hunt groups), and VDNs, provision an entry as follows:
   - **Ext Len** – Enter the total number of digits in the local extension range.
   - **Ext Code –** Enter enough leading digits to identify the local extension range.
   - **Trk Grp(s)** – Enter the number of the trunk group administered in **Step 2**.
   - **CPN Prefix** – If necessary, enter enough prefix digits to form the desired connected party number.
   - **CPN Len** – Enter the total length of the connected party number to be sent.

```
change public-unknown-numbering 0                              Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                            Total
Ext Ext             Trk       CPN            CPN
Len Code            Grp(s)    Prefix         Len
                                                      Total Administered: 2
 7  666             2                        7           Maximum Entries: 9999
 10 303            2                        10
```

Public-Unknown-Numbering Form

7.5. Optional Features

The reference configuration uses hunt groups, vectors, and Vector Directory Numbers (VDNs), to provide additional functionality during testing:

- Hunt Group 1 –Messaging coverage for Communication Manager extensions
- VDN 6662010/Vector 10 – VDN and vectors used to select the agent skill

Following VDN/Vectors were used for calls transferred to an agent/skill on Communication Manager without verifying the availability of an agent as described in third call scenario in **Section 3.2**.

- VDN 6662011/Vector 11/Hunt Group 11 – Route call to Agent with Skill 11
- VDN 6662012/Vector 12/Hunt Group 12 – Route call to Agent with Skill 12
- VDN 6662013/Vector 13/Hunt Group 13 – Route call to Agent with Skill 13

Followng VDN/Vectors were used for calls anchored on Experience Portal and only transferred to an agent on Communication Manager once agent becomes available as described in second call scenario in **Section 3.2**.

- VDN 6662031/Vector 31/Hunt Group 31 – Route call to Agent with Skill 11
- VDN 6662032/Vector 32/Hunt Group 32 – Route call to Agent with Skill 12
- VDN 6662033/Vector 33/Hunt Group 33 – Route call to Agent with Skill 13

Note - The administration of Communication Manager Call Center elements – hunt groups, vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Additional licensing may be required for some of these features. Refer to **[8]** and **[9]** for further details if necessary. The samples that follow are provided for reference purposes only.

7.5.1. Hunt Group for Station Coverage to Messaging

Hunt group **2** is used in the reference configuration to verify the coverage to voicemail. The hunt group **2** is defined with the 7 digit Messaging pilot number **666-5000**.

```
display hunt-group 2                                            Page   1 of  60
                                  HUNT GROUP
            Group Number: 2                               ACD? n
              Group Name: Messaging                     Queue? n
         Group Extension: 666-5000                       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:
```

Hunt Group Form – Page 1

```
display hunt-group 2                                            Page   2 of  60
                                  HUNT GROUP
                      Message Center: sip-adjunct
     Voice Mail Number        Voice Mail Handle         Routing Digits
                                                  (e.g., AAR/ARS Access Code)
     6665000                   6665000                  8
```

Hunt Group Form – Page 2

The hunt group is associated with a coverage path **h2** and this coverage path is assigned to a station/agent.

```
display coverage path 2
                                 COVERAGE PATH
                   Coverage Path Number: 2
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage
COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n              n
               Busy?             y              y
        Don't Answer?            y              y         Number of Rings: 3
                All?             n              n
 DND/SAC/Goto Cover?             y              y
   Holiday Coverage?             n              n
COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h2            Rng: 4  Point2:
  Point3:                       Point4:
  Point5:                       Point6:
```

Coverage Path Form

7.5.2. Call Center Provisioning

For provisioning the call center functionality, verify that the call center parameters are enabled as shown below. Verify that an agent login id is created with an appropriate skill. Verify the skill (hunt group) for that agent is in place. Make sure that a VDN as per the dial plan is in place along with the vector which lists the steps to be executed when an inbound call is received from AT&T IP Toll Free service via Experience Portal.

In this reference configuration, an inbound call from AT&T IP Toll Free service is handled using the routing policy configured in **Section 5.9.3** and dial pattern configured in **Section 5.10.1**.

```
display system-parameters customer-options                        Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 5.0

                                ACD? y                        Reason Codes? n
                       BCMS (Basic)? y             Service Level Maximizer? n
         BCMS/VuStats Service Level? y           Service Observing (Basic)? n
  BSR Local Treatment for IP & ISDN? n   Service Observing (Remote/By FAC)? n
                  Business Advocate? n           Service Observing (VDNs)? n
                    Call Work Codes? n                          Timed ACW? n
      DTMF Feedback Signals For VRU? n                 Vectoring (Basic)? y
                  Dynamic Advocate? n              Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y           Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y            Vectoring (3.0 Enhanced)? y
                   Forced ACD Calls? n    Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? n    Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? n                 Vectoring (CINFO)? n
Multiple Call Handling (On Request)? n     Vectoring (Best Service Routing)? n
    Multiple Call Handling (Forced)? n              Vectoring (Holidays)? n
  PASTE (Display PBX Data on Phone)? n             Vectoring (Variables)? n

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

Call Center Optional Features Form

```
display agent-loginID 6663011                               Page   1 of   3
                                 AGENT LOGINID

                Login ID: 6663011                            AAS? n
                    Name: Agent1                           AUDIX? n
                      TN: 1                         LWC Reception: spe
                     COR: 1                LWC Log External Calls? n
           Coverage Path: 2              AUDIX Name for Messaging:
           Security Code:
                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                              Password (enter again):
                                                         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:   :
     WARNING:  Agent must log in again before changes take effect
```

Agent Form – Page 1

```
display agent-loginID 6663011                                Page   2 of   2
                                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: 11      1       16:                 31:                 46:
 2:                 17:                 32:                 47:
 3:                 18:                 33:                 48:
```

Agent Form Page 2

```
display hunt-group 11                                        Page   1 of   4
                                 HUNT GROUP

            Group Number: 11                              ACD? y
              Group Name: Skill-11                      Queue? y
         Group Extension: 6664011                      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 (Hunt Group) Form – Page 1

```
display hunt-group 11                                        Page   2 of   4
                                 HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:

      Controlling Adjunct: none

   Multiple Call Handling: none
 Timed ACW Interval (sec):     After Xfer or Held Call Drops:  n
```

Skill (Hunt Group) Form – Page 2

```
display vdn 6662010                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 666-2010
                                  Name: To SelectSkill
                           Destination: Vector Number        10
                   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
```

SelectSkill VDN

```
display vector 10                                               Page   1 of   6
                                  CALL VECTOR
    Number: 10               Name: RouteToSkill
                                             Meet-me Conf? n           Lock? n
     Basic? y   EAS? n   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? n
01 wait-time    2   secs hearing ringback
02 collect      1    digits after announcement 661002    for none
03 goto vector  11   @step 2 if digits           =      1
04 goto vector  12   @step 2 if digits           =      2
05 goto vector  13   @step 2 if digits           =      3
06 goto step    2            if unconditionally
```

RouteToSkill Vector[5]

```
display vector 11                                               Page   1 of   6
                                  CALL VECTOR
    Number: 11               Name: Skill 11
                                             Meet-me Conf? n           Lock? n
     Basic? y   EAS? n   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? n   CINFO? n   BSR? n   Holidays? n
 Variables? n   3.0 Enhanced? n
01 wait-time    2   secs hearing ringback
02 announcement 6661003
03 queue-to     skill 11   pri m
04 announcement 6661006
05 goto step    3             if unconditionally
06
```

Skill-11 Vector

[5] This vector was used for the call flow scenario where Experience Portal transfers the inbound call to an Communication Manager skill without checking whether an agent in that skill is available.

```
display vector 31                                             Page   1 of   6
                                  CALL VECTOR

    Number: 31              Name: VP Test Vector
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 queue-to     skill 11  pri m
02 stop
03
```

Sample Vector[6]

8. Avaya Aura® Messaging

The administration for Messaging is beyond the scope of these Application Notes. Refer to **[10]** and **[11]** for further details.

[6] This vector was used for the call flow scenario where Experience Portal checks a Communication Manager skill for agent availability before transferring the inbound call to the skill.

9. Configure Acme Session Border Controller

The Acme SBC configuration used in the sample configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Consult with Acme Packet Support [**12**] for further details and explanations on the configuration below.

ANNOTATION: The local policy below governs the routing of SIP messages from elements on the network on which the Avaya elements, e.g., Experience Portal, Communication Manager, etc., reside to the AT&T IP Toll Free service.

```
local-policy
      from-address
                              *
      to-address
                              *
      source-realm
                              IPTF-Enterprise
      description
      activate-time           N/A
      deactivate-time         N/A
      state                   enabled
      policy-priority         none
      last-modified-by        admin@console
      last-modified-date      2011-08-12 10:25:23
      policy-attribute
            next-hop                192.168.62.50
            realm                   ATT
            action                  none
            terminate-recursion     disabled
            carrier
            start-time              0000
            end-time                2400
            days-of-week            U-S
            cost                    0
            app-protocol            SIP
            state                   enabled
            methods
            media-profiles
```

ANNOTATION: The local policy below governs the routing of SIP messages from the AT&T IP Toll Free service to Experience Portal via Session Manager.

```
local-policy
      from-address
                              *
      to-address
                              00000
                              666
                              +666
      source-realm
                              ATT
      description
      activate-time           N/A
      deactivate-time         N/A
```

```
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-08-12 10:25:23
        policy-attribute
              next-hop                       10.80.150.206
              realm                          IPTF-Enterprise
              action                         none
              terminate-recursion            disabled
              carrier
              start-time                     0000
              end-time                       2400
              days-of-week                   U-S
              cost                           0
              app-protocol                   SIP
              state                          enabled
              methods
              media-profiles
```

ANNOTATION: The local policy below governs the routing of SIP messages from the Experience Portal to Communication Manager via Session Manager

```
local-policy
        from-address
                                       *
        to-address
                                       666
        source-realm
                                       IPTF-Enterprise
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-08-12 10:25:23
        policy-attribute
              next-hop                       10.80.150.206
              realm                          IPTF-Enterprise
              action                         none
              terminate-recursion            disabled
              carrier
              start-time                     0000
              end-time                       2400
              days-of-week                   U-S
              cost                           0
              app-protocol                   SIP
              state                          enabled
              methods
              media-profiles

media-manager
        state                          enabled
        latching                       enabled
        flow-time-limit                86400
        initial-guard-timer            300
        subsq-guard-timer              300
```

```
      tcp-flow-time-limit            86400
      tcp-initial-guard-timer        300
      tcp-subsq-guard-timer          300
      tcp-number-of-ports-per-flow   2
      hnt-rtcp                       disabled
      algd-log-level                 NOTICE
      mbcd-log-level                 NOTICE
      red-flow-port                  1985
      red-mgcp-port                  1986
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      media-policing                 enabled
      max-signaling-bandwidth        7752190
      max-untrusted-signaling        80
      min-untrusted-signaling        20
      app-signaling-bandwidth        0
      tolerance-window               30
      rtcp-rate-limit                0
      min-media-allocation           32000
      min-trusted-allocation         60000
      deny-allocation                32000
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      dnsalg-server-failover         disabled
      last-modified-by               admin@console
      last-modified-date             2010-09-08 10:22:03

network-interface
      name                           wancom0
      sub-port-id                    0
      description
      hostname
      ip-address                     135.9.230.221
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        135.9.230.254
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list
      ftp-address
```

```
  icmp-address
snmp-address
telnet-address
last-modified-by              admin@console
last-modified-date            2011-08-12 10:21:39
```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.

```
network-interface
      name                          s0p0
      sub-port-id                   0
      description
      hostname
      ip-address                    10.80.130.250
      pri-utility-addr
      sec-utility-addr
      netmask                       255.255.255.0
      gateway                       10.80.130.1
      sec-gateway
      gw-heartbeat
            state                         disabled
            heartbeat                     0
            retry-count                   0
            retry-timeout                 1
            health-score                  0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain                    attavaya.com
      dns-timeout                   11
      hip-ip-list                   10.80.130.250
      ftp-address
      icmp-address                  10.80.130.250
      snmp-address
      telnet-address
      last-modified-by              admin@console
      last-modified-date            2011-08-12 14:58:25
```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the AT&T IP Toll Free service resides.

```
network-interface
      name                          s1p0
      sub-port-id                   0
      description
      hostname
      ip-address                    192.168.62.50
      pri-utility-addr
      sec-utility-addr
      netmask                       255.255.255.128
      gateway                       192.168.62.1
      sec-gateway
      gw-heartbeat
            state                         disabled
            heartbeat                     0
```

```
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
      hip-ip-list                    192.168.62.50
      ftp-address
      icmp-address                   192.168.62.50
      snmp-address
      telnet-address
      last-modified-by               admin@console
      last-modified-date             2011-08-12 10:24:07
ntp-config
      server                         192.9.1.2
      last-modified-by               admin@console
      last-modified-date             2009-03-12 10:20:46

phy-interface
      name                           wancom0
      operation-type                 Control
      port                           2
      slot                           0
      virtual-mac
      wancom-health-score            9
      last-modified-by               admin@console
      last-modified-date             2011-08-12 10:21:30

phy-interface
      name                           s0p0
      operation-type                 Media
      port                           0
      slot                           0
      virtual-mac                    00:08:25:a0:f3:68
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      last-modified-by               admin@console
      last-modified-date             2011-08-13 15:29:00
phy-interface
      name                           s1p0
      operation-type                 Media
      port                           0
      slot                           1
      virtual-mac                    00:08:25:a0:f3:6e
      admin-state                    enabled
      auto-negotiation               enabled
      duplex-mode                    FULL
      speed                          100
      last-modified-by               admin@console
      last-modified-date             2011-08-13 15:29:23
```

ANNOTATION: The realm configuration **ATT** below represents the external network on which the AT&T IP Toll Free service resides, and applies SIP manipulations **RemoveUPDATE.**

```
realm-config
      identifier                    ATT
      description
      addr-prefix                   0.0.0.0
      network-interfaces
                                    s1p0:0
      mm-in-realm                   enabled
      mm-in-network                 enabled
      mm-same-ip                    enabled
      mm-in-system                  enabled
      bw-cac-non-mm                 disabled
      msm-release                   disabled
      generate-UDP-checksum         disabled
      max-bandwidth                 0
      fallback-bandwidth            0
      max-priority-bandwidth        0
      max-latency                   0
      max-jitter                    0
      max-packet-loss               0
      observ-window-size            0
      parent-realm
      dns-realm
      media-policy
      in-translationid
      out-translationid
      in-manipulationid             removeUpdAndmodifyPtime
      out-manipulationid            NAT_IP
      manipulation-string
      class-profile
      average-rate-limit            0
      access-control-trust-level    none
      invalid-signal-threshold      4
      maximum-signal-threshold      3000
      untrusted-signal-threshold    10
      nat-trust-threshold           0
      deny-period                   60
      ext-policy-svr
      symmetric-latching            disabled
      pai-strip                     disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching           none
      restriction-mask              32
      accounting-enable             enabled
      user-cac-mode                 none
      user-cac-bandwidth            0
      user-cac-sessions             0
      icmp-detect-multiplier        0
      icmp-advertisement-interval   0
      icmp-target-ip
      monthly-minutes               0
```

```
      net-management-control         disabled
      delay-media-update             disabled
      refer-call-transfer            disabled
      codec-policy
      codec-manip-in-realm           disabled
      constraint-name
      call-recording-server-id
      stun-enable                    disabled
      stun-server-ip                 0.0.0.0
      stun-server-port               3478
      stun-changed-ip                0.0.0.0
      stun-changed-port              3479
      match-media-profiles
      qos-constraint
      last-modified-by               admin@console
      last-modified-date             2009-04-22 19:26:23
```

ANNOTATION: The realm configuration **IPTF-Enterprise** below represents the internal network on which the Avaya elements reside.

```
realm-config
      identifier                     IPTF-Enterprise
      description
      addr-prefix                    0.0.0.0
      network-interfaces             s0p0:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      generate-UDP-checksum          disabled
      max-bandwidth                  0
      fallback-bandwidth             0
      max-priority-bandwidth         0
      max-latency                    0
      max-jitter                     0
      max-packet-loss                0
      observ-window-size             0
      parent-realm
      dns-realm
      media-policy
      in-translationid
      out-translationid
      in-manipulationid              AddDiversion
      out-manipulationid
      manipulation-string
      class-profile
      average-rate-limit             0
      access-control-trust-level     high
      invalid-signal-threshold       0
      maximum-signal-threshold       0
      untrusted-signal-threshold     0
      nat-trust-threshold            0
      deny-period                    30
      ext-policy-svr
      symmetric-latching             disabled
```

```
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            enabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
last-modified-by               admin@console
last-modified-date             2011-08-12 19:50:37
```

ANNOTATION: The session agent below represents Session Manager used in this reference configuration.

```
session-agent
      hostname                       Enterprise-IPTF
      ip-address                     10.80.150.206
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP+TCP
      realm-id                       IPTF-Enterprise
      egress-realm-id
      description                    Session Manager
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
```

```
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=0
      ping-interval                  180
      ping-send-mode                 keep-alive
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                       disabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                    disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
      p-asserted-id
      trunk-group
      max-register-sustain-rate      0
      early-media-allow
      invalidate-registrations       disabled
      rfc2833-mode                   none
      rfc2833-payload                0
      codec-policy
      enforcement-profile
      refer-call-transfer            enabled
      reuse-connections              TCP
      tcp-keepalive                  enabled
      tcp-reconn-interval            0
      max-register-burst-rate        0
      register-burst-window          0
      last-modified-by               admin@console
      last-modified-date             2011-08-17 17:36:26
```

ANNOTATION: The session agent below represents the AT&T IP Toll Free service border element.

```
session-agent
      hostname                       135.242.225.200
      ip-address                     135.242.225.200
      port                           5060
```

```
state                         enabled
app-protocol                  SIP
app-type
transport-method              UDP
realm-id                      ATT
egress-realm-id
description                   AT&T Border Element
carriers
allow-next-hop-lp             enabled
constraints                   disabled
max-sessions                  0
max-inbound-sessions          0
max-outbound-sessions         0
max-burst-rate                0
max-inbound-burst-rate        0
max-outbound-burst-rate       0
max-sustain-rate              0
max-inbound-sustain-rate      0
max-outbound-sustain-rate     0
min-seizures                  5
min-asr                       0
time-to-resume                0
ttr-no-response               0
in-service-period             0
burst-rate-window             0
sustain-rate-window           0
req-uri-carrier-mode          None
proxy-mode
redirect-action
loose-routing                 enabled
send-media-session            enabled
response-map
ping-method                   OPTIONS;hops=70
ping-interval                 180
ping-send-mode                keep-alive
ping-all-addresses            disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                      disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                   disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate     0
early-media-allow
invalidate-registrations      disabled
rfc2833-mode                  none
```

```
rfc2833-payload               0
codec-policy
enforcement-profile
refer-call-transfer           disabled
reuse-connections             NONE
tcp-keepalive                 none
tcp-reconn-interval           0
max-register-burst-rate       0
register-burst-window         0
last-modified-by              admin@console
last-modified-date            2011-08-17 17:36:20
```

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

```
sip-config
      state                          enabled
      operation-mode                 dialog
      dialog-transparency            enabled
      home-realm-id                  IPTF-Enterprise
      egress-realm-id                IPTF-Enterprise
      nat-mode                       None
      registrar-domain
      registrar-host
      registrar-port                 0
      register-service-route         always
      init-timer                     500
      max-timer                      4000
      trans-expire                   32
      invite-expire                  180
      inactive-dynamic-conn          32
      enforcement-profile
      pac-method
      pac-interval                   10
      pac-strategy                   PropDist
      pac-load-weight                1
      pac-session-weight             1
      pac-route-weight               1
      pac-callid-lifetime            600
      pac-user-lifetime              3600
      red-sip-port                   1988
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      add-reason-header              disabled
      sip-message-len                4096
      enum-sag-match                 disabled
      extra-method-stats             enabled
      registration-cache-limit       0
      register-use-to-for-lp         disabled
      options                        max-udp-length=0
                                       set-inv-exp-at-100-resp
      add-ucid-header                disabled
      last-modified-by               admin@console
      last-modified-date             2011-08-12 10:22:04
```

ANNOTATION: The SIP interface below is used to communicate with the AT&T IP Toll Free service.

```
sip-interface
      state                         enabled
      realm-id                      ATT
      description
      sip-port
            address                       192.168.62.50
            port                          5060
            transport-protocol            UDP
            tls-profile
            allow-anonymous               all
            ims-aka-profile
      carriers
      trans-expire                  0
      invite-expire                 0
      max-redirect-contacts         0
      proxy-mode
      redirect-action
      contact-mode                  none
      nat-traversal                 none
      nat-interval                  30
      tcp-nat-interval              90
      registration-caching          disabled
      min-reg-expire                300
      registration-interval         3600
      route-to-registrar            disabled
      secured-network               disabled
      teluri-scheme                 disabled
      uri-fqdn-domain
      trust-mode                    all
      max-nat-interval              3600
      nat-int-increment             10
      nat-test-increment            30
      sip-dynamic-hnt               disabled
      stop-recurse                  401,407
      port-map-start                0
      port-map-end                  0
      in-manipulationid
      out-manipulationid
      manipulation-string
      sip-ims-feature               disabled
      operator-identifier
      anonymous-priority            none
      max-incoming-conns            0
      per-src-ip-max-incoming-conns 0
      inactive-conn-timeout         0
      untrusted-conn-timeout        0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode          pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                none
```

```
     implicit-service-route        disabled
     rfc2833-payload               101
     rfc2833-mode                  transparent
     constraint-name
     response-map
     local-response-map
     ims-aka-feature               disabled
     enforcement-profile
     route-unauthorized-calls
     tcp-keepalive                 none
     add-sdp-invite                disabled
     add-sdp-profiles
     last-modified-by              admin@console
     last-modified-date            2009-04-22 18:14:23
```

ANNOTATION: The SIP interface below is used to communicate with the Avaya elements.

```
sip-interface
     state                         enabled
     realm-id                      IPTF-Enterprise
     description
     sip-port
          address                       10.80.130.250
          port                          5060
          transport-protocol            TCP
          tls-profile
          allow-anonymous               all
          ims-aka-profile
     carriers
     trans-expire                  30
     invite-expire                 0
     max-redirect-contacts         0
     proxy-mode
     redirect-action
     contact-mode                  none
     nat-traversal                 none
     nat-interval                  30
     tcp-nat-interval              90
     registration-caching          disabled
     min-reg-expire                300
     registration-interval         3600
     route-to-registrar            disabled
     secured-network               disabled
     teluri-scheme                 disabled
     uri-fqdn-domain
     trust-mode                    all
     max-nat-interval              3600
     nat-int-increment             10
     nat-test-increment            30
     sip-dynamic-hnt               disabled
     stop-recurse                  401,407
     port-map-start                0
     port-map-end                  0
     in-manipulationid
     out-manipulationid
     manipulation-string
```

```
      sip-ims-feature                  disabled
      operator-identifier
      anonymous-priority               none
      max-incoming-conns               0
      per-src-ip-max-incoming-conns    0
      inactive-conn-timeout            0
      untrusted-conn-timeout           0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode             pass
      charging-function-address-mode   pass
      ccf-address
      ecf-address
      term-tgrp-mode                   none
      implicit-service-route           disabled
      rfc2833-payload                  101
      rfc2833-mode                     transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                  disabled
      enforcement-profile
      route-unauthorized-calls
      tcp-keepalive                    none
      add-sdp-invite                   disabled
      add-sdp-profiles
      last-modified-by                 admin@console
      last-modified-date               2009-04-16 18:07:58
```

ANNOTATION: The SIP manipulation below removes **UPDATE** from the Allow header in SIP messages from the AT&T IP Toll Free service as **UPDATE** is not supported by Experience Portal. It also modifies the **maxptime** attribute to **ptime** as Experience Portal does not recognize **maxptime** attribute.

```
sip-manipulation
      name                             removeUpdateAndModifyMaxptime
      description                      Strip Update from Allow list, modify Ptime
      header-rule
            name                             ReplaceMaxptime
            header-name                      Content-Type
            action                           manipulate
            comparison-type                  case-sensitive
            msg-type                         any
            methods                          INVITE
            match-value
            new-value
            element-rule
                  name                             modmline
                  parameter-name                   application/sdp
                  type                             mime
                  action                           find-replace-all
                  match-val-type                   any
                  comparison-type                  case-sensitive
                  match-value                      maxptime
                  new-value                        ptime
```

```
header-rule
      name                                  EditAllow
      header-name                           Allow
      action                                manipulate
      comparison-type                       pattern-rule
      match-value
      msg-type                              any
      new-value
      methods
      element-rule
            name                                  StripUPDATE
            parameter-name
            type                                  header-value
            action                                find-replace-all
            match-val-type                        any
            comparison-type                       pattern-rule
            match-value                           (,\s*UPDATE|UPDATE\s*,)
            new-value
last-modified-by                      admin@console
last-modified-date                    2011-10-22 19:25:08
```

ANNOTATION: The SIP manipulation below adds a **Diversion** header in SIP messages from the Experience Portal to AT&T Flex Reach service as **Diversion** header is not generated by Experience Portal. A valid DID is required for calls 8YY numbers otherwise the calls will fail. See **Section 2.2, Item 6** for further information. This manipulation rule was used in this reference configuration and is not intended to be prescriptive.

```
sip-manipulation
      name                                  AddDiverions
      description                           Add Diversion Header for 8YY calls
      header-rule
            name                                  AddDiversionHdr
            header-name                           Diversion
            action                                add
            comparison-type                       boolean
            match-value
            msg-type                              request
            methods
            new-value                       "sip:7323204084@10.80.130.220"
      last-modified-by                      admin@console
      last-modified-date                    2011-08-22 19:25:08
```

ANNOTATION: The steering pools below define the RTP port range on the respective realms.

```
steering-pool
      ip-address                            192.168.62.50
      start-port                            16384
      end-port                              32767
      realm-id                              ATT
      network-interface
      last-modified-by                      admin@console
      last-modified-date                    2011-08-25 19:11:47
steering-pool
```

```
        ip-address                     10.80.130.250
        start-port                     16384
        end-port                       32767
        realm-id                       IPTF-Enterprise
        network-interface
        last-modified-by               admin@console
        last-modified-date             2011-08-12 10:25:12
system-config
        hostname                       Enterprise-Acme
        description
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                   enabled
        enable-snmp-auth-traps         disabled
        enable-snmp-syslog-notify      disabled
        enable-snmp-monitor-traps      disabled
        enable-env-monitor-traps       disabled
        snmp-syslog-his-table-length   1
        snmp-syslog-level              WARNING
        system-log-level               WARNING
        process-log-level              NOTICE
        process-log-ip-address         0.0.0.0
        process-log-port               0
        collect
                sample-interval                5
                push-interval                  15
                boot-state                     disabled
                start-time                     now
                end-time                       never
                red-collect-state              disabled
                red-max-trans                  1000
                red-sync-start-time            5000
                red-sync-comp-time             1000
                push-success-trap-state        disabled
        call-trace                     disabled
        internal-trace                 disabled
        log-filter                     all
        default-gateway                172.16.253.4
        restart                        enabled
        exceptions
        telnet-timeout                 0
        console-timeout                0
        remote-control                 enabled
        cli-audit-trail                enabled
        link-redundancy-state          disabled
        source-routing                 enabled
        cli-more                       disabled
        terminal-height                24
        debug-timeout                  0
        trap-event-lifetime            0
        last-modified-by               admin@console
        last-modified-date             2011-08-12 10:20:46
```

10. Verification Steps

10.1. General

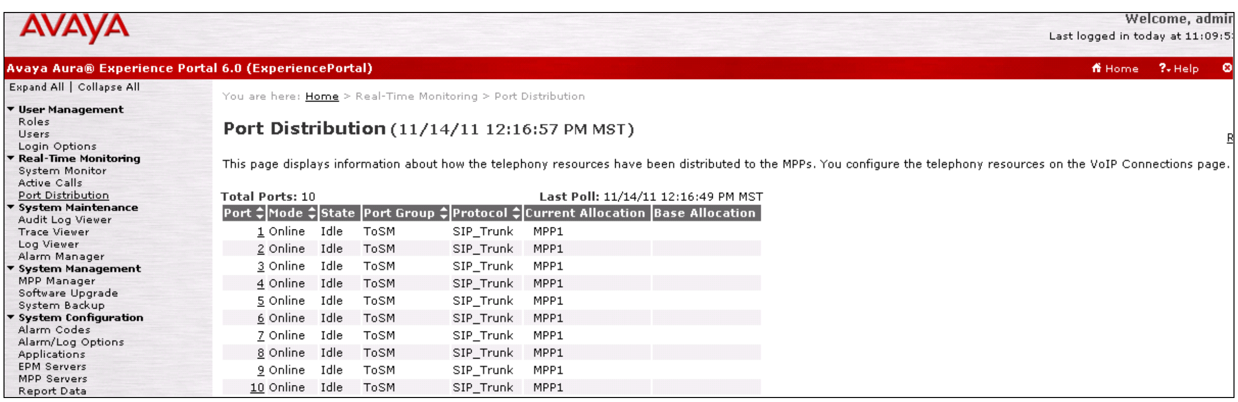
The following steps may be used to verify the configuration:

- Place an inbound call to Experience Portal application, and verify that two-way talkpath exists. Interact with the Experience Portal prompts and verify that the call remains stable for several minutes and disconnect properly.
- Place an inbound call to Experience Portal application that can canvass Communication Manager for skilled agent availability, and select the appropriate prompt(s) to request a transfer to an agent. Verify that when no agent in the skill is available, the caller hears wait treatment from the Experience Portal application while waiting to be transferred. Verify that when an agent in the skill becomes available, the call is successfully transferred to the agent and two-way talkpath exists between the caller and the agent.
- Place an inbound call to Experience Portal application that can transfer an inbound call to Communication Manager regardless of skilled agent availability, and select the appropriate prompt(s) to request a transfer to an agent. Verify that the transfer completes successfully. Verify that when no agent in the skill is available, the caller hears wait treatment from Communication Manager. Verify that when an agent in the skill becomes available, the call is successfully routed to the agent and two-way talkpath exists between the caller and the agent.

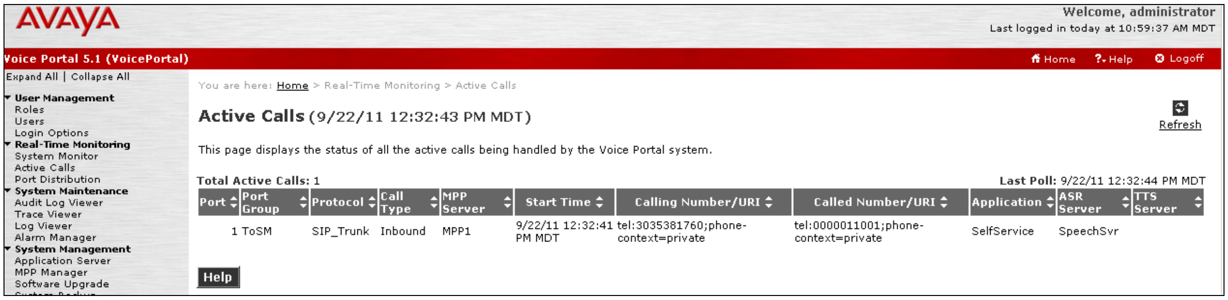
10.2. Avaya Aura® Experience Portal

The following commands are issued from the System Manager console.

1. Navigate to **Real-Time Monitoring→Port Distribution** to verify the SIP trunk on Experience Portal SIP Trunk has been properly configured as shown below:



2. Navigate to **Real-Time Monitoring→Active Calls** to verify the number of active calls, the trunk being used and the application running on Experience Portal:



10.3. Troubleshooting Tools

The logging and reporting functions within the Experience Portal web interface may be used to examine the details of Experience Portal calls.

The Communication Manager **list trace vector**, **list trace vdn**, **list trace tac**, and/or **status trunk *trunk-group-no*** commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. MST (Message Sequence Trace) diagnostic traces (performed by Avaya Support) can be helpful in understanding the specific interoperability issues.

The **traceSM** function within the Session Manager may be used to capture SIP traces between Session Manager and the AT&T IP Toll Free service. In addition, if port monitoring is available, a SIP protocol analyzer such as Wireshark (a.k.a. Ethereal) can be used to capture SIP traces at the various interfaces. SIP traces can be instrumental in understanding SIP protocol issues resulting from configuration problems.

11. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal and the Acme Packet Net-Net can be configured to interoperate successfully with the AT&T IP Toll Free service. This solution provides users of Avaya Aura® Experience Portal the ability to support inbound toll free calls over an AT&T IP Toll Free SIP trunk service connection. The test objectives stated in **Section 2** with limitations noted in **Section 2.2** were verified.

The sample 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.

12. References

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

[1] *Planning for Avaya Aura® Experience Portal*, August 2011
[2] *Implementing Avaya Aura® Experience Portal on a single server*, August 2011
[3] *Administering Aura® Experience Portal*, January 2011
[4] *Installing and Configuring Avaya Aura® Session Manager,* April 2011.
[5] *Administering Avaya Aura® Session Manager*, October 2011.
[6] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, August 2010
[7] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document Id 555-245-205, August 2010
[8] *Administering Avaya Aura® Call Center Features*, November 2010
[9] *Programming Call Vectors in Avaya Aura® Call Center*, June 2010
[10] *Administering Avaya Aura® Messaging*, December 2011
[11] *Implementing Aura® Messaging*, October 2011

Acme Packet Support (login required):
[12] http://support.acmepacket.com

AT&T IP Toll Free Service Descriptions:
[13] *AT&T IP Toll Free*
http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-toll-free-enterprise/

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.