Avaya Solution & Interoperability Test Lab

Applications Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0 and Avaya Aura™ Session Border Controller with AT&T IP Toll Free SIP Trunk Service – Issue 1.1

Abstract

These Application Notes describe the steps for configuring Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and the Avaya Aura™ Session Border Controller with the AT&T IP Toll Free service using MIS/PNT transport connection.

Avaya Aura™ Session Manager 6.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura™ Communication Manager 6.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura™ Session Manager. An Avaya Aura™ Session Border Controller is the point of connection between Avaya Aura™ Session Manager and the AT&T IP Toll Free service and is used not only to secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. Interaction of Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager with the AT&T IP Transfer Connect service option will be addressed in separate Application Notes.

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

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Avaya Aura™ Session Border Controller (SBC) with the AT&T IP Toll Free service using MIS/PNT transport connection.

Avaya Aura™ Session Manager 6.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura™ Communication Manager 6.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura™ Session Manager. An Avaya Aura™ Session Border Controller (SBC) is the point of connection between Avaya Aura™ Session Manager and the AT&T IP Toll Free service and is used not only to secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing MIS/PNT[1] transport. **Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.** Interaction of Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager with the AT&T IP Transfer Connect service option will be addressed in separate Application Notes.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound IP Toll Free call flows (see **Section 2.2** for examples) between Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, Avaya Aura™ Session Border Controller, and the AT&T IP Toll Free service.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the AT&T network. Calls were made to and from the PSTN across the AT&T network (see **Section 2.2** for sample call flows). The following features were tested as part of this effort:

- SIP trunking
- T.38 Fax
- 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

[1] MIS/PNT does not support compressed RTP (cRTP).

1.2. 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.

1.3. Known Limitations

1. If Avaya Aura™ Communication Manager receives an SDP offer with multiple codecs, where at least two of the codecs are supported in the codec set provisioned on Avaya Aura™ Communication Manager, then Avaya Aura™ Communication Manager selects a codec according to the priority order specified in its configured 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 Avaya Aura™ Communication Manager codec set contains G.729B, G729A, and G.711 in that order, then Avaya Aura™ Communication Manager selects G.729A, not G.711. The practical resolution is to provision the Avaya Aura™ Communication Manager codec set to match the expected codec priority order in AT&T IP Toll Free SDP offers.
2. G.726 codec is not supported between Avaya Aura™ Communication Manager and the AT&T IP Toll Free service.
3. G.711 faxing is not supported between Avaya Aura™ Communication Manager and the AT&T IP Toll Free service. Avaya Aura™ Communication Manager does not support the protocol negotiation that AT&T requires to have G.711 fax calls work. T.38 faxing is supported, as is Group 3 and Super Group 3 fax. Fax speeds are limited to 9600 bps in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Avaya Aura™ Communication Manager.
4. Shuffling must be disabled on the SIP trunk between Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager for calls local to the enterprise site due to codec negotiation issues with Avaya SIP telephones.

2. Reference Configuration

The reference configuration used in these Application Notes is shown in the figure below and consists of several components:

- 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 Manager instances in an enterprise.
- Communication Manager provides the voice communications services for a particular enterprise site. In this reference configuration, Communication Manager runs on an Avaya S8800 Server. This solution is extensible to other Avaya S8xxx Servers.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G650 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya “desk” phones are represented with Avaya 4600 and 9600 Series IP Telephones running H.323 software, 9600 Series IP Telephones running SIP software, Avaya 6211 series Analog Telephones, and Avaya one-X® Agent, a PC based Softphone.
- Session Border Controller provides SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network[2]. UDP transport protocol is used between the Session Border Controller and the AT&T IP Toll Free service.
- An existing Avaya Modular Messaging system (in Multi-Site mode in this reference configuration) provides the corporate voice messaging capabilities in the reference configuration and its provisioning is beyond the scope of this document.
- Inbound calls from PSTN were sent from AT&T IP Toll Free service, through the Session Border Controller to the Session Manager which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate agent/phone or fax extension. The H.323 phones on the enterprise side registered to the Communication Manager C-LAN. The SIP phones on the enterprise side registered to the Session Manager.

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

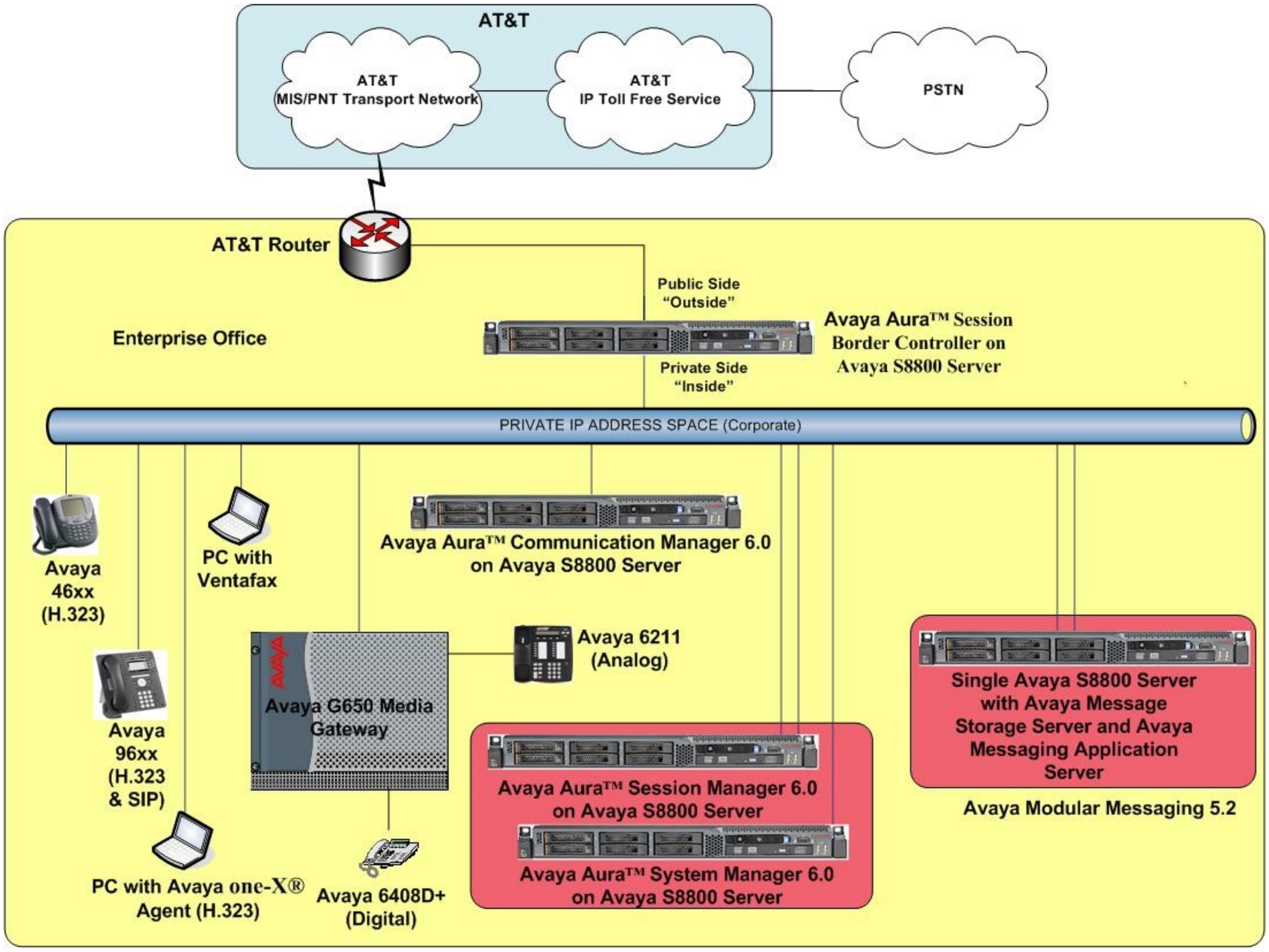

Figure 1: Reference configuration

2.1. Illustrative Configuration Information

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

Note - The AT&T IP Toll Free service border element IP addresses shown in this document are examples. AT&T Customer Care will provide the actual IP addresses as part of the IP Toll Free service provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura™ System Manager	
Management IP Address	10.80.120.21
Avaya Aura™ Session Manager	
Management IP Address	10.80.120.27
Network IP Address	10.80.120.28
Avaya Aura™ Communication Manager	
C-LAN IP Address	10.80.111.31
VDN	6665310 to 6665313
Skill (Hunt Group)	11, 12, 13
Agent login ID's	6665611 to 6665615
Hunt Group Extensions	6665711 (11), 66665712 (12), 6665713 (13)
Phone Extensions	66650xx – H323 Phones 66654xx – SIP Phones 66651xx – Analog Phone 66652xx – Digital Phones
Voice Messaging Pilot Extension	666-4999
Avaya Modular Messaging	
Messaging Application Server (MAS) IP Address	10.80.100.30
Messaging Server (MSS) IP Address	10.80.100.29
Avaya Aura™ Session Border Controller	
IP Address of "Outside" (Public) Interface (connected to AT&T Access Router/IP Toll Free Service)	192.168.62.55 (active)
IP Address of "Inside" (Private) Interface (connected to Avaya Aura™ Session Manager)	10.80.130.12 (active)
AT&T IP Toll Free Service	
Border Element IP Address	135.242.225.200
Digits passed in SIP-URI Request	00000105x, 00000106x

Table 1: Illustrative Values Used in these Application Notes

2.2. Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled by Session Manager and Communication Manager, following call flows are described in this section.

2.2.1. Inbound Call

The first call scenario illustrated in the figure below is an inbound AT&T IP Toll Free service call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a phone, fax, or in some cases, a vector.

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 Session Border Controller.
4. The Session Border Controller 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 to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to
    - A vector, which in turn, routes the call to an agent
    - Directly to an agent or a phone/fax extension.

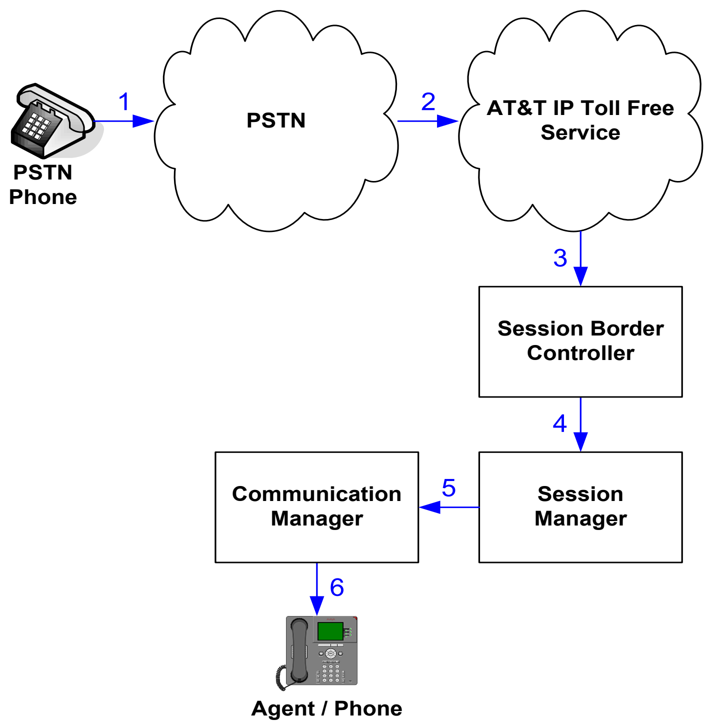

Figure 2: Inbound AT&T IP Toll Free Call to VDN/Agent/Phone

2.2.2. Coverage to Voicemail

The second call scenario illustrated in the figure below is an inbound call that is covered to voicemail. In this scenario, the voicemail system is a Modular Messaging system (MultiSite mode) connected to Session Manager.

1. Same as call scenario in **Section 2.2.1**.
2. The agent or phone on Communication Manager does not answer the call, and the call covers to their voicemail which Communication Manager forwards[3] to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines it needs to route the call to Modular Messaging which answers the call and connects the caller to the called agent/phone voice mailbox. Note that the call[4] continues to go through Communication Manager.

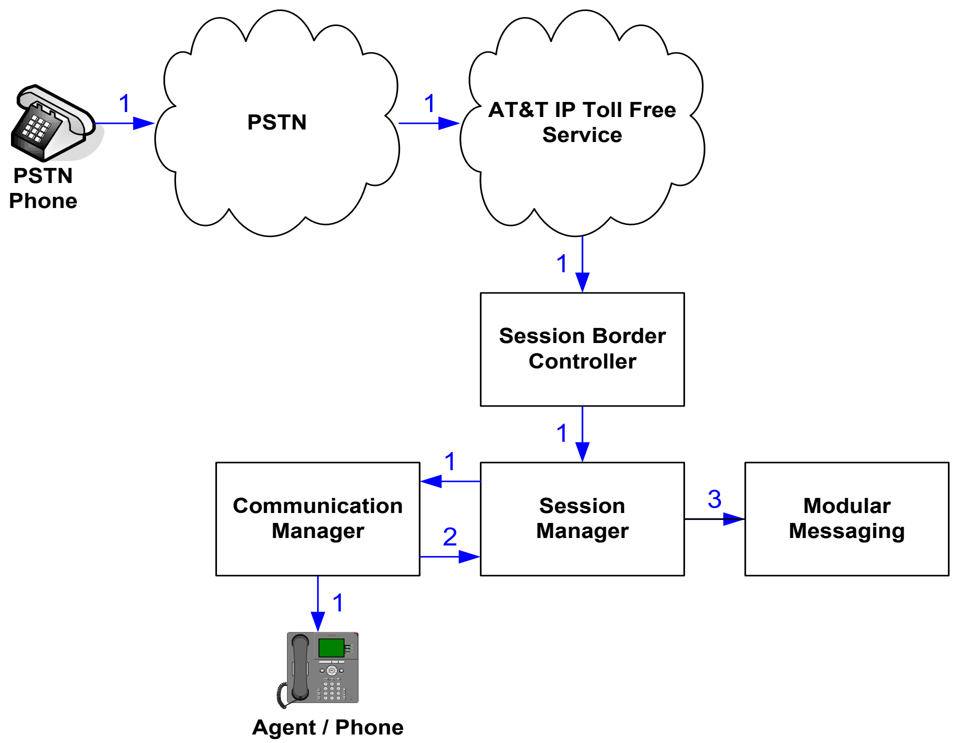

Figure 3: Inbound AT&T IP Toll Free Service Call to Agent/Phone Covered to Avaya Modular Messaging

[3] Communication Manager places a call to Modular Messaging, and then connects the inbound caller to Modular Messaging. SIP redirect methods, e.g., 302, are not used.

[4] The SIP signaling path still goes through Communication Manager. In addition, since the inbound call and Modular Messaging use different codecs (G.729 and G.711, respectively), Communication Manager performs the transcoding, and thus the RTP media path also goes through Communication Manager.

3. Equipment and Software Validated

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

Component	Version
Avaya S8800 Server	Avaya Aura™ System Manager 6.0 (6.0.0.0.556-3.0.6.1)
Avaya S8800 Server	Avaya Aura™ Session Manager 6.0 (6.0.0.0.600020)
Avaya S8800 Server	Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with patch 18246
Avaya S8800 Server	Avaya Aura™ Session Border Controller 6.0 (R6.0.0.3.4), Product Version 36M2, Build Version 3.6.0, Build 46752 on VSP-6.0.1.0.5
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW15 FW050
TN799DP Control-LAN (C-LAN)	HW01 FW037
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW054
TN2501AP VAL-ANNOUNCEMENT	HW03 FW021
TN2224CP Digital Line	HW08 FW015
TN793CP Analog Line	HW04 FW010
Avaya 9630 IP Telephone	Avaya one-X® Deskphone Edition H.323 Version S3.1
Avaya 9620C IP Telephone	Avaya one-X® Deskphone Edition SIP Version 2.6.0 (sip96xx_2_6_0_0.bin)
Avaya one-X® Agent	2.0 with SP3
Avaya 4625SW IP Telephone	a25d01a2_8.bin
Avaya 6408D+ Digital phone	-
Avaya 6211 Analog phone	-
Avaya S8800 Single Server	Avaya Modular Messaging 5.2
Fax device	Ventafax Home Version 6.2
AT&T IP Toll Free Service using MIS/PNT transport service connection	VNI 18

Table 2: Equipment and Software Versions

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session

Manager release 6.1. Avaya agrees to provide service and support for the integration of Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1 with the AT&T IP Toll Free service offer, in compliance with existing support agreements for Avaya Aura® Communication Manager release 6.0 and Avaya Aura® Session Manager 6.0, and in conformance with the integration guidelines as specified in the body of this document.

4. Avaya Aura™ Session Manager

These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1]and [2] 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*>/SMGR in the URL, and log in with the appropriate credentials.

4.1. 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.

4.2. Routing Policies

Routing Policies define how Session Manager routes 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 Manager instances, Communication Manager systems, 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 instances 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[5] 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 to Session Manager, 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 from SM, apply any called party number modifications necessary to conform to the expectations of the next-hop SIP Entity. For example, on egress from Session Manager to Communication Manager, modify the called party number such that the number is consistent with the dial plan on Communication Manager.

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

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

[5] 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.

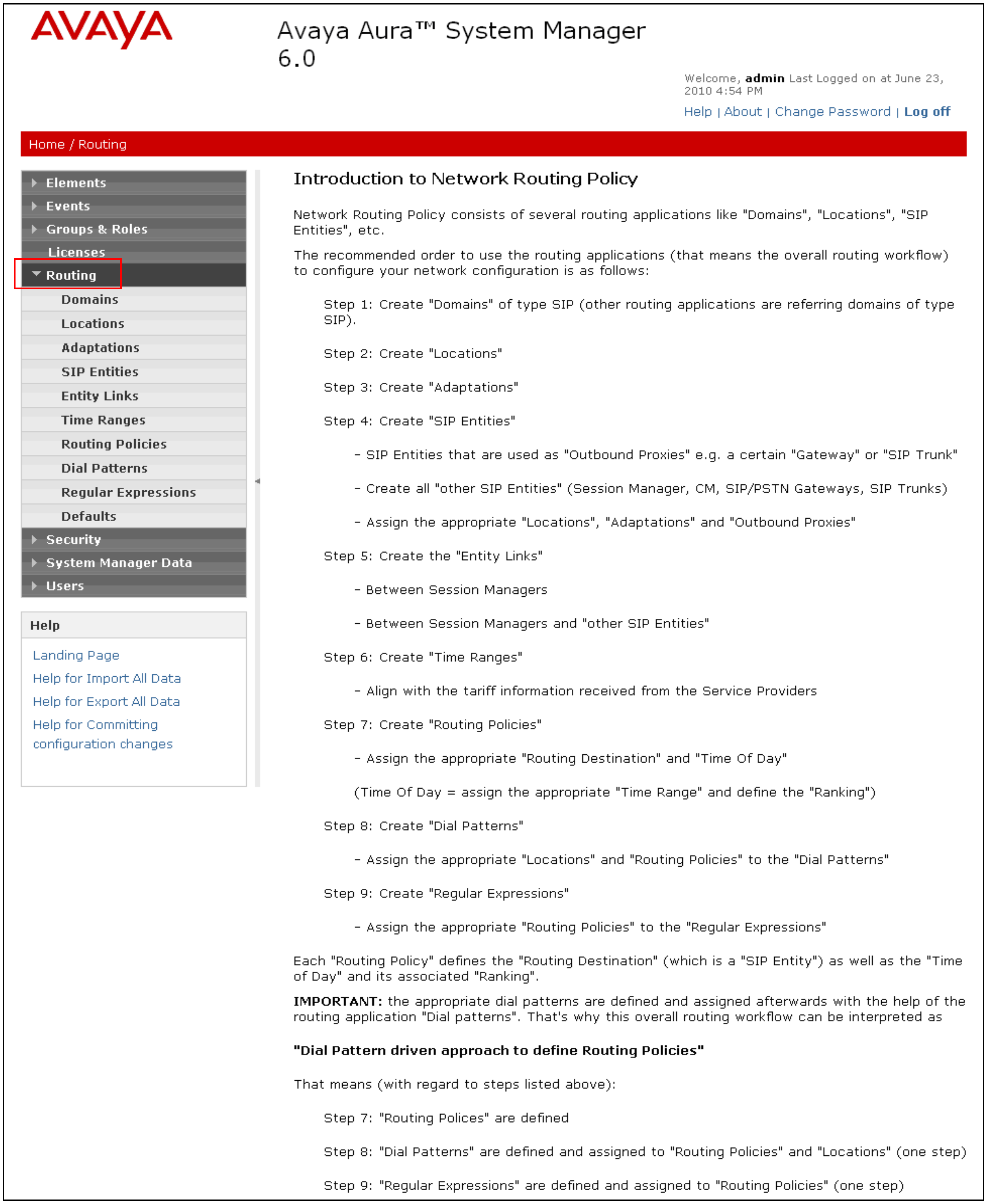

Figure 4: Main Routing Page

4.3. 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 on "**Domains**". In the **Domain Management** page click on "**New**" (not shown) and configure as follows:
    - **Name** –Set to **avaya.com** in this reference configuration
    - **Type –** Set to **sip**
    - Notes – Optional Field
2. Click on "**Commit**"
3. Repeat above steps to add additional domains.

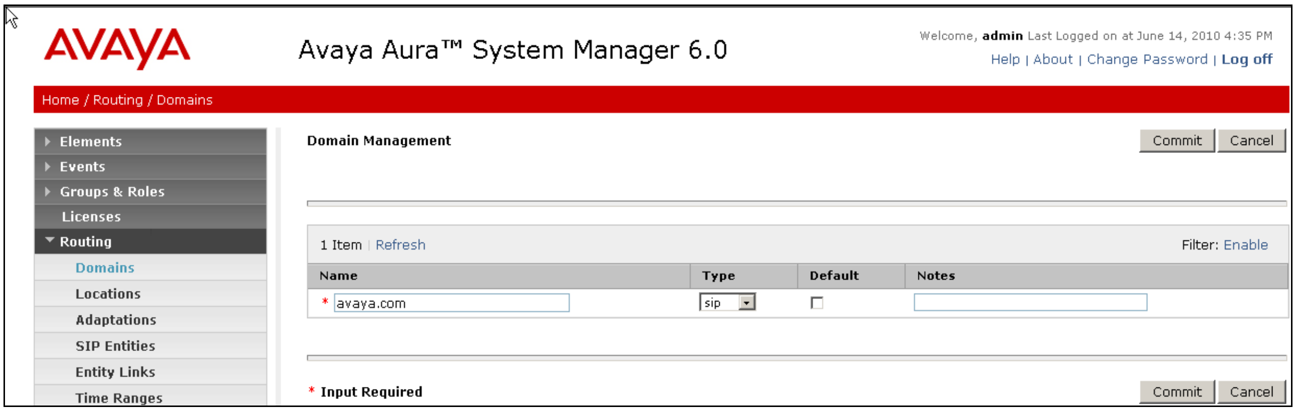

Figure 5: Domain Management Page

4.4. 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**". In the **Location** page [not shown] click on "**New**".
2. In the **Location Details** page, configure as follows:
   - **Name** – Enter any descriptive string.
   - **Notes** – (Optional) Enter a description
   - **Managed Bandwidth** and **Average Bandwidth per Call** – (Optional) To limit the number of calls going to and from this location i.e., apply Call Admission Control.
   - **Location Pattern** - [Optional] To identify IP addresses associated with this Location. In the reference configuration, the IP address of Session Border Controller i.e. **10.80.130.12** was used.
3. Click on "**Commit**".
4. Repeat above steps to add any additional Locations (e.g. **Subnet 10.80.100.x**, **10.80.120.x**, **Subnet 10.80.130.x**, **Subnet 10.80.111.x**) used in this Reference Configuration.

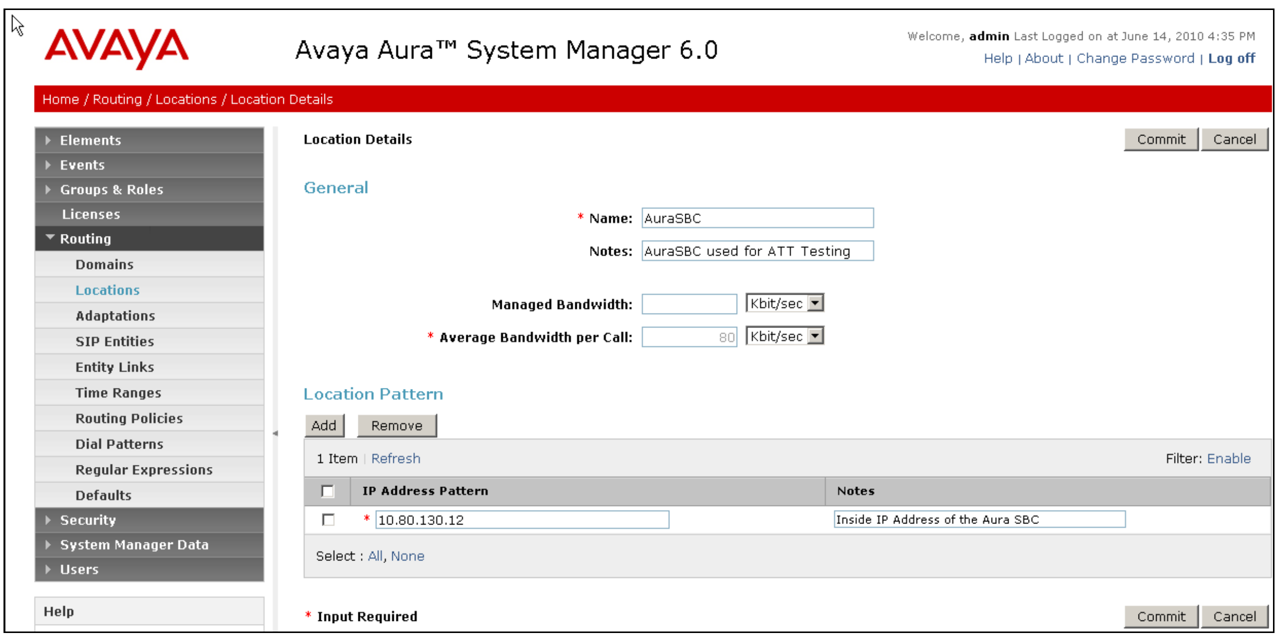

Figure 6: Location Details Page

4.5. 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 Communication Manager (**Section 4.5.1**). Modification of SIP messages sent to Communication Manager are:

- The IP address of Session Manager is replaced with the Avaya CPE SIP domain (**avaya.com**) in the PAI Header.
- The AT&T DNIS in Request URI is replaced with an associated Communication Manager Extension/VDN.

4.5.1. Adaptation for calls to Avaya Aura™ Communication Manager

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager only.

1. In the left pane under **Routing**, click on "**Adaptations**". In the **Adaptations** page, click on "**New**" (not shown).
2. In the **Adaptation Details** page, 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=avaya.com**, which will replace the IP Address/Domain in the PAI header with the Avaya CPE domain (avaya.com) for egress to Communication Manager.
   - Configure **Digit Conversion for Outgoing Calls from SM** section as follows:
     a) Click **Add**.
     b) **Matching Pattern** – Add a matching pattern in the Request URI of the call coming into Session Manager.
     c) **Min** and **Max** – Set the minimum and maximum value of the pattern to be matched.
     d) **Delete Digits** – Set the number of digits to be deleted from the pattern.
     e) **Insert Digits** – Set the number of digits to be added to the number in the Request URI.
     f) **Address to modify** – Set the address to modify i.e. origination/destination or both.
     g) **Notes** – [Optional]
   - Repeat the previous step for additional digit conversions to be configured.
   - The figure below lists the digit conversions done for calls coming from AT&T Toll Free service destined for Communication Manager. Note that the 9-digit DNIS coming from AT&T is converted to a 7-digit Communication Manager extension.
3. Click on "**Commit**".

Note: In the reference configuration no **Digit Conversion for Incoming Calls to SM** are required.

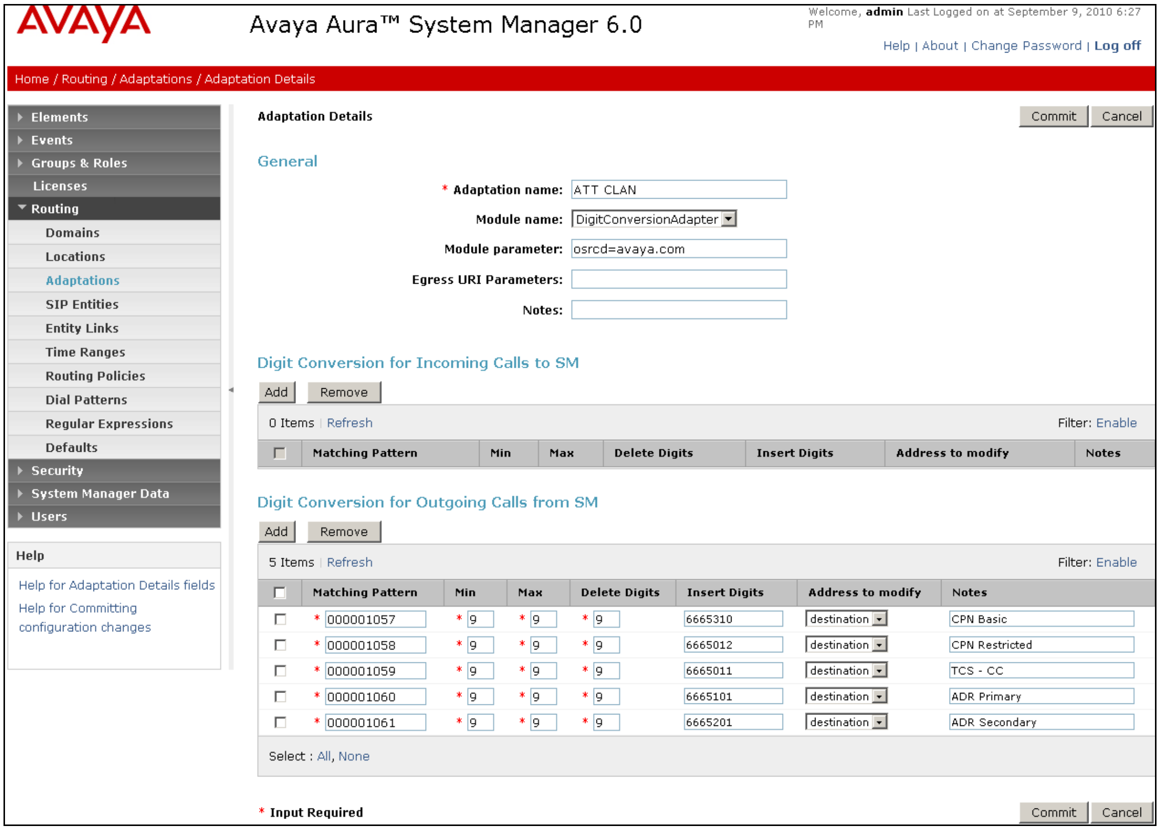

Figure 7: Adaptation Details Page – Adaptation for Communication Manager

4.6. SIP Entities

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

- Avaya Aura™ Session Manager
- Avaya Aura™ Communication Manager
- Avaya Aura™ Session Border Controller
- Avaya SIP Endpoints SIP Entity
- Avaya Modular 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.

4.6.1. Avaya Aura™ Session Manager SIP Entity

1. In the left pane under **Routing**, click on "**SIP Entities**". In the **SIP Entities** page click on "**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 (e.g. **SM1**).
   - **FQDN or IP Address –** Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation. Set to **10.80.120.28** in this reference configuration.
   - **Type –** Select "**Session Manager**".
   - **Location** – Select "**Location 1 Subnet 10.80.120.x**" as configured in **Section 4.4**.
   - **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 **SIP Link Monitoring** field.
4. In the **Port** section of the **SIP Entity Details** page, click on "**Add**" and provision an entry as follows:
   - **Port –** Enter "**5060**" (see note above).
   - **Protocol –** Select "**TCP**" (see note above).
   - **Default Domain –** (Optional) Select a SIP domain administered in **Section 4.3**.
5. Repeat **Step 4** to provision another entry, except with "**5080**" for **Port** and "**TCP**" for **Protocol**. Since a single C-LAN was used in this reference configuration, a separate port was configured to separate the SIP endpoint traffic from other traffic on C-LAN. This was done because of the known limitation noted in **Section 1.3**, **Item 4**.
6. Click on "**Commit**".

These entries enable Session Manager to accept SIP requests on the specified ports/protocols.

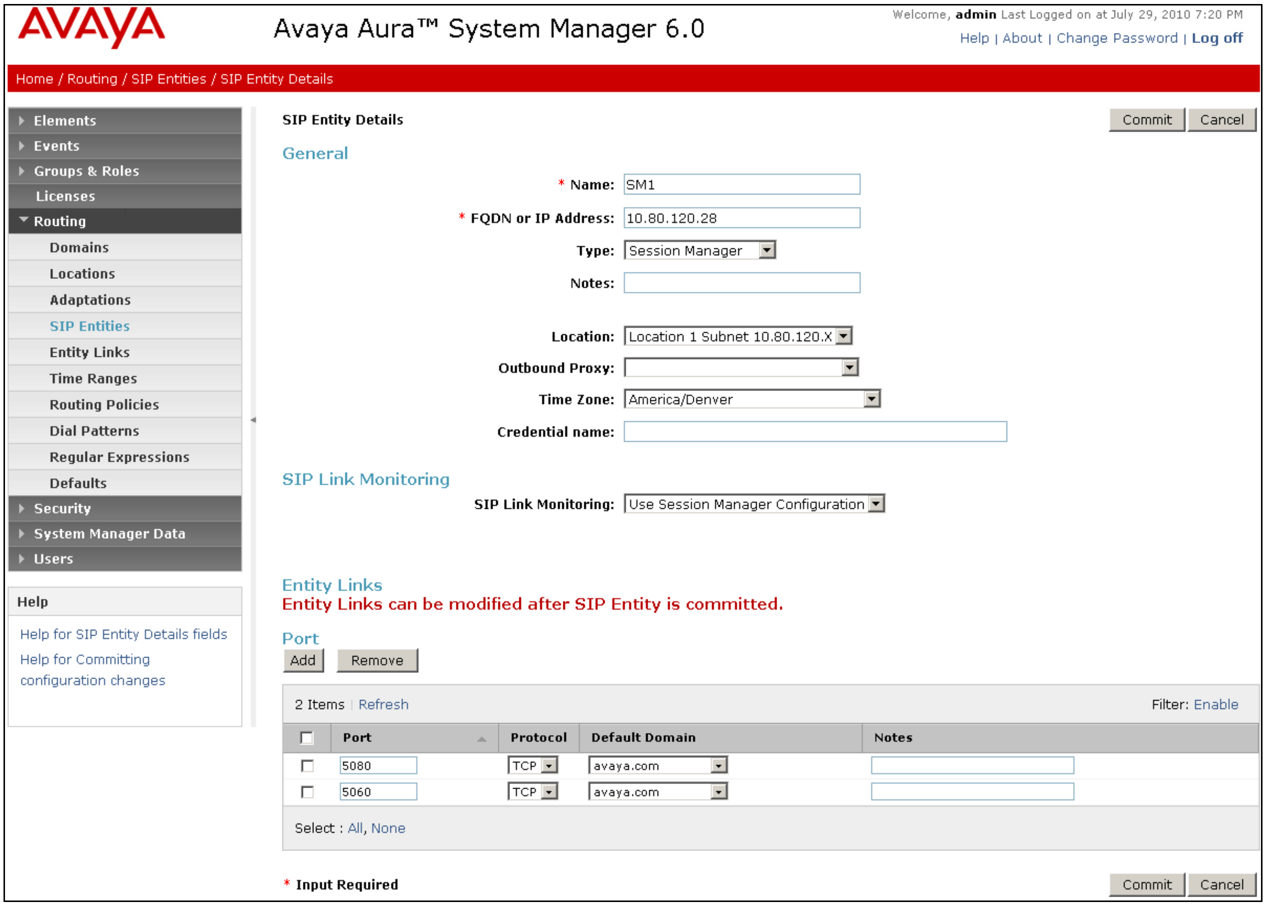

Figure 8: SIP Entity Details Page –Session Manager SIP Entity

4.6.2. Avaya Aura™ Communication Manager SIP Entity

1. In the **SIP Entities** page, click on "**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 in **Section 5.3**, **Step 5**.
   - **Type –** Select "**CM**".
   - **Adaptation –** Select the Adaptation administered in **Section 4.5.1**.
   - **Location** – Select a Location administered in **Section 4.4**.
   - **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. Click on "**Commit**".

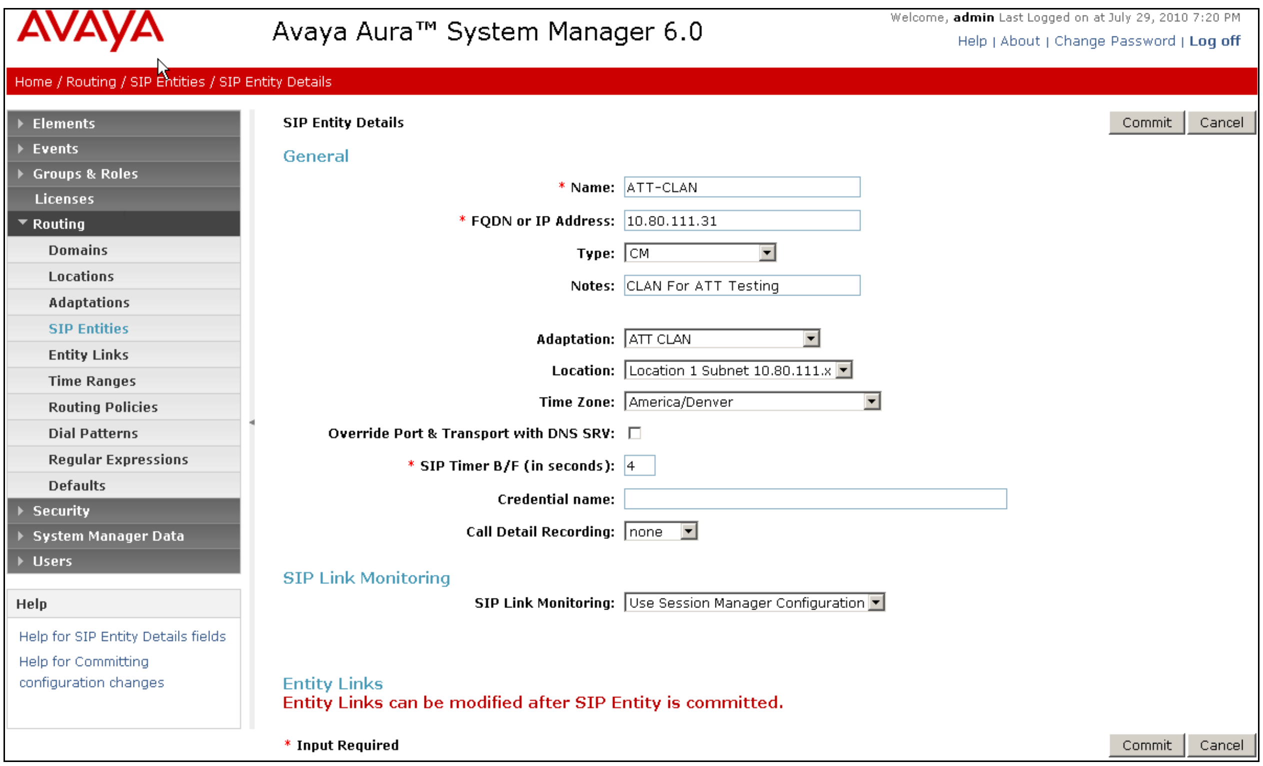

Figure 9: SIP Entity Details Page –Communication Manager SIP Entity

4.6.3. Avaya Aura™ Session Border Controller SIP Entity

To configure the Session Border Controller Entity, repeat the Steps in **Section 4.6.2**. The **FQDN or IP Address** field is populated with the IP address of the private (inside) interface configured in **Section 7.1** and the **Type** field is set to "**Other**". See the figure below for the values used in this reference configuration.

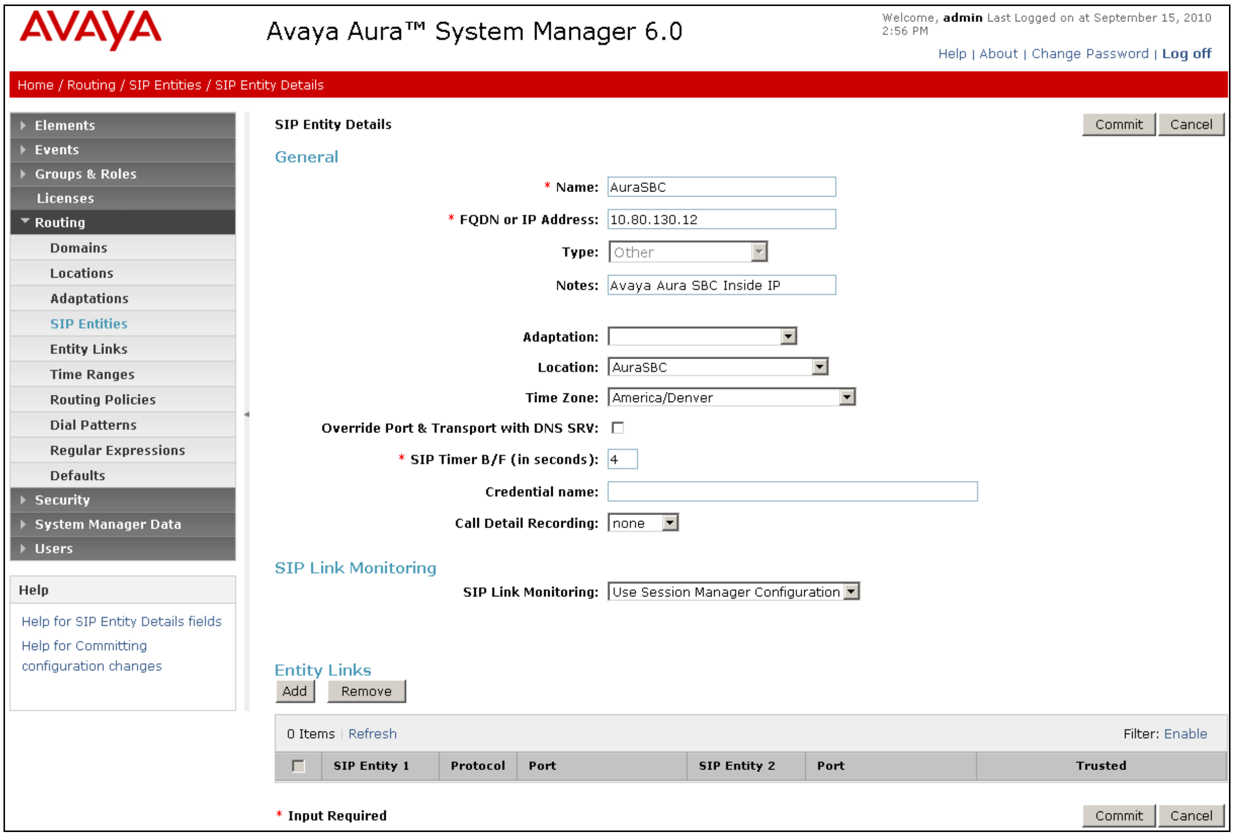

Figure 10: SIP Entity Details Page – Session Border Controller SIP Entity

4.6.4. Avaya SIP Endpoints SIP Entity

Because of the shuffling limitation noted in **Section 1.3**, **Item 4** a separate SIP Entity was created to handle calls to and from SIP endpoints registered with Session Manager. A single CLAN was used in this reference configuration but a different port number was used as configured in **Section 4.6.1**, **Step 5**. Configuration for this Entity is similar to the Entity configured in **Section 4.6.2**.

Note: For routing the calls from SIP Endpoints to Communication Manager, this Entity has to be used in Application Sequence. The configuration of the Application Sequence on Session Manager is beyond the scope of this document.

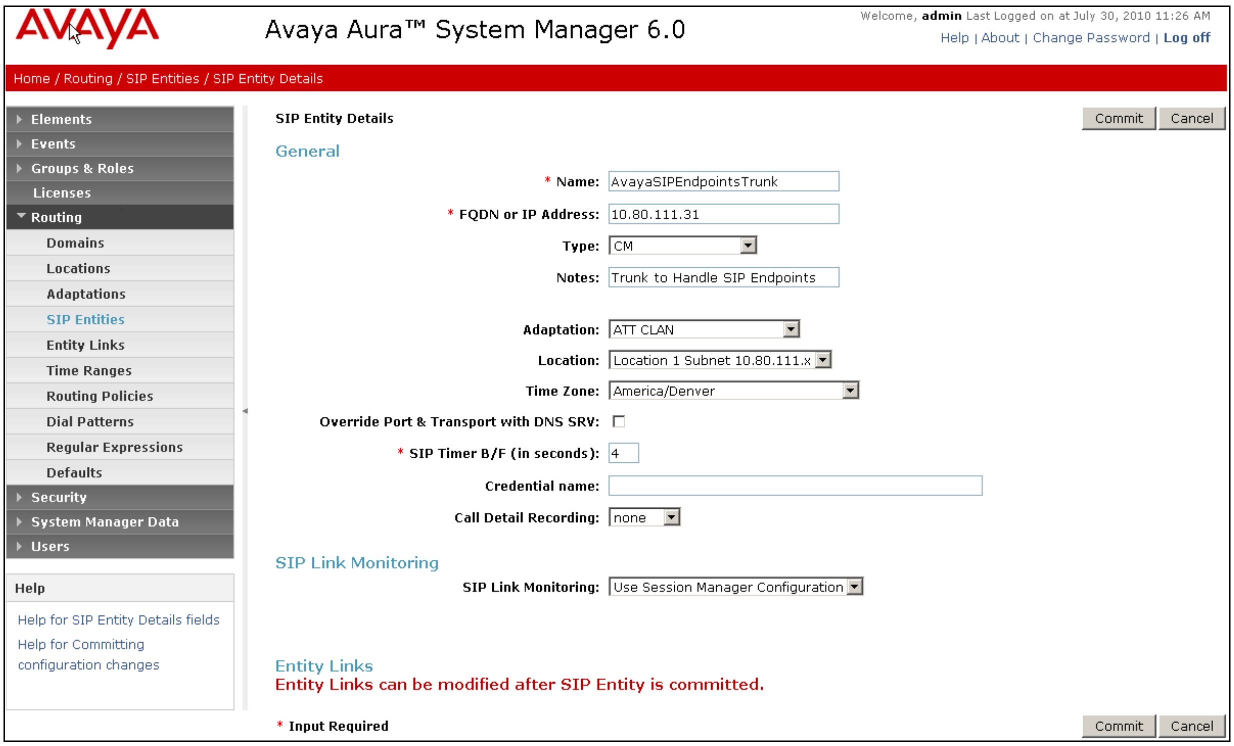

Figure 11: SIP Entity Details Page – Avaya SIP Endpoints

4.6.5. Avaya Modular Messaging SIP Entity

To configure the Modular Messaging SIP Entity, repeat the steps in **Section 4.6.2**. The **FQDN or IP Address** field is populated with the IP address of the Modular Messaging Application Server (MAS) and the **Type** field is set to "**Other**". See the figure below for the values used in this reference configuration.

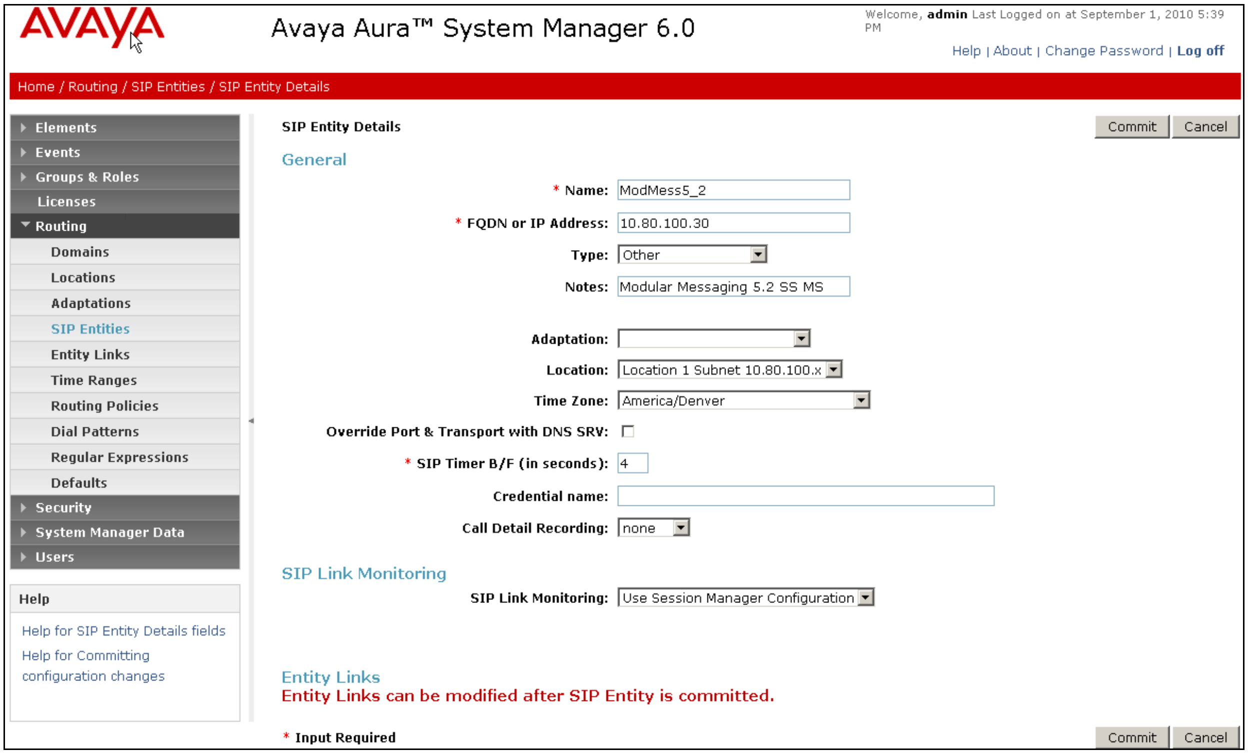

Figure 12: SIP Entity Details Page – Avaya Modular Messaging SIP Entity

4.7. Entity Links

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

- Avaya Aura™ Communication Manager
- Avaya Aura™ Session Border Controller
- Avaya SIP Endpoints SIP Entity
- Avaya Modular 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.

4.7.1. Entity Link to Avaya Aura™ Communication Manager

1. In the left pane under **Routing**, click on "**Entity Links**". In the **Entity Links** page click on "**New**" (not shown).
2. Continuing in the **Entity Links** page, provision the following:
   - **Name** – Enter a descriptive name for this link to Communication Manager (e.g. **SM1-ATTClan**).
   - **SIP Entity 1** – Select the SIP Entity administered in **Section 4.6.1** for Session Manager. SIP Entity 1 must always be an Session Manager instance.
   - **SIP Entity 1 Port** – Enter "**5060**"
   - **SIP Entity 2** –Select the SIP Entity administered in **Section 4.6.2** for Communication Manager.
   - **SIP Entity 2 Port** - Enter "**5060**".
   - **Trusted –** Check the checkbox.
   - **Protocol –** Select "**TCP**".
3. Click on "**Commit**".

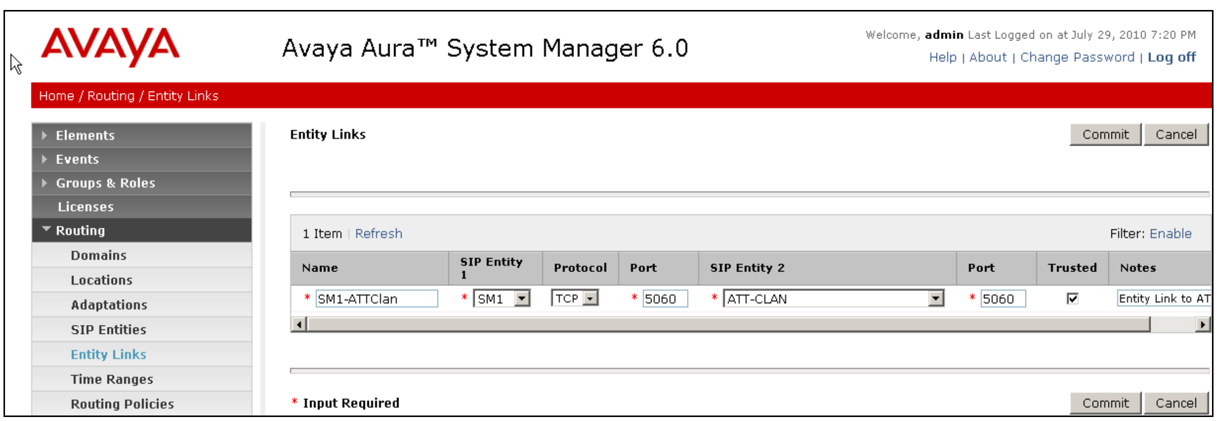

Figure 13: Entity Links Page – Entity Link to Communication Manager

4.7.2. Entity Link to AT&T IP Toll Free Service via Session Border Controller

To configure the entity link between the Session Manager and Session Border Controller entities, repeat the steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.3**. See the figure below for the values used in this reference configuration.

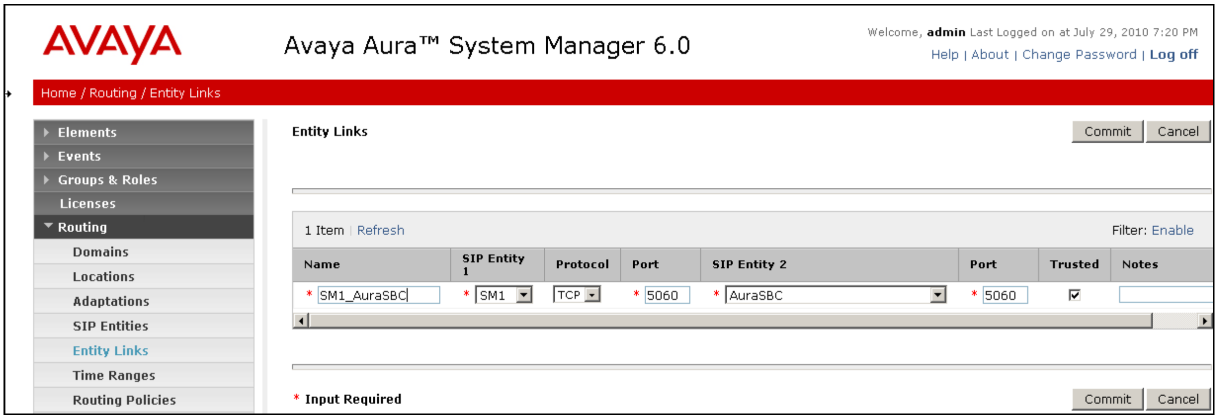

Figure 14: Entity Links Page – Entity Link to AT&T IP Toll Free Service via Session Border Controller

4.7.3. Entity Link to Avaya Aura™ Communication Manager for SIP Endpoints

To configure this entity link, repeat the steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.4**. See the figure below for the values used in this reference configuration.

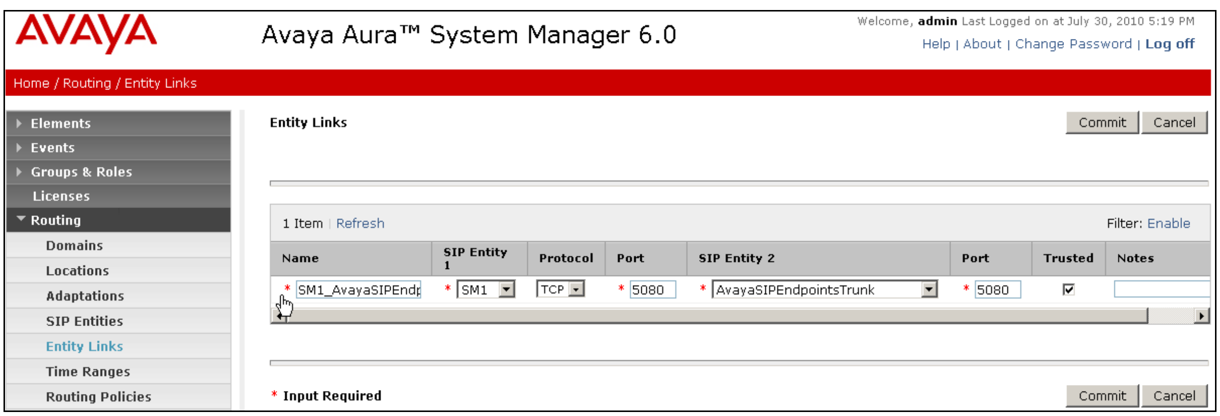

Figure 15: Entity Links Page – Entity Link to AT&T IP Toll Free Service via Session Border Controller

4.7.4. Entity Link to Avaya Modular Messaging

To configure this entity link, repeat the steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.5**. See the figure below for the values used in the reference configuration.

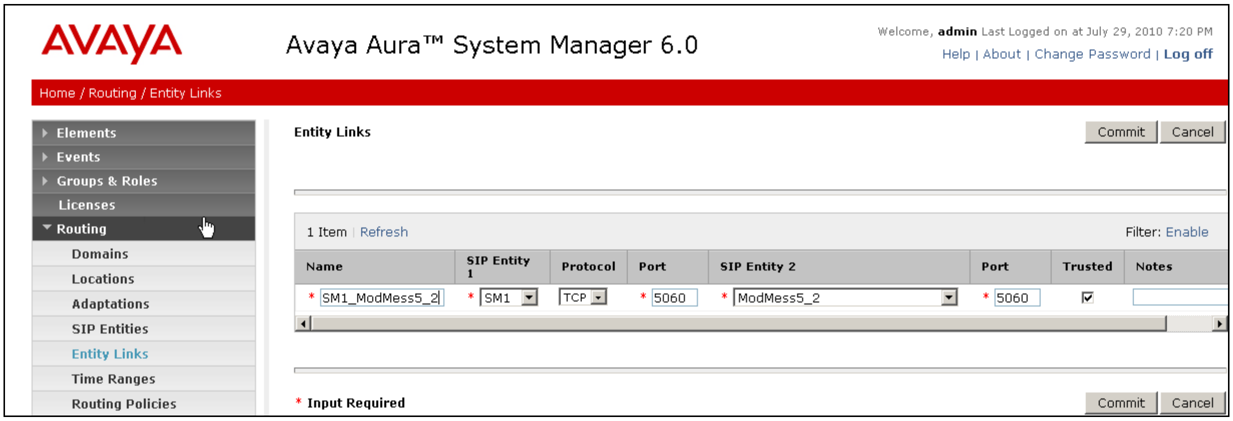

Figure 16: Entity Links Page – Entity Link to Avaya Modular Messaging

4.8. SIP Entity Completed configuration

After the SIP entities and their corresponding links are configured, the SIP Entity Details screens are updated with the Entity Link information. Following figures show all the SIP entities configured in **Section 4.6** after the entity links are added in **Section 4.7**.

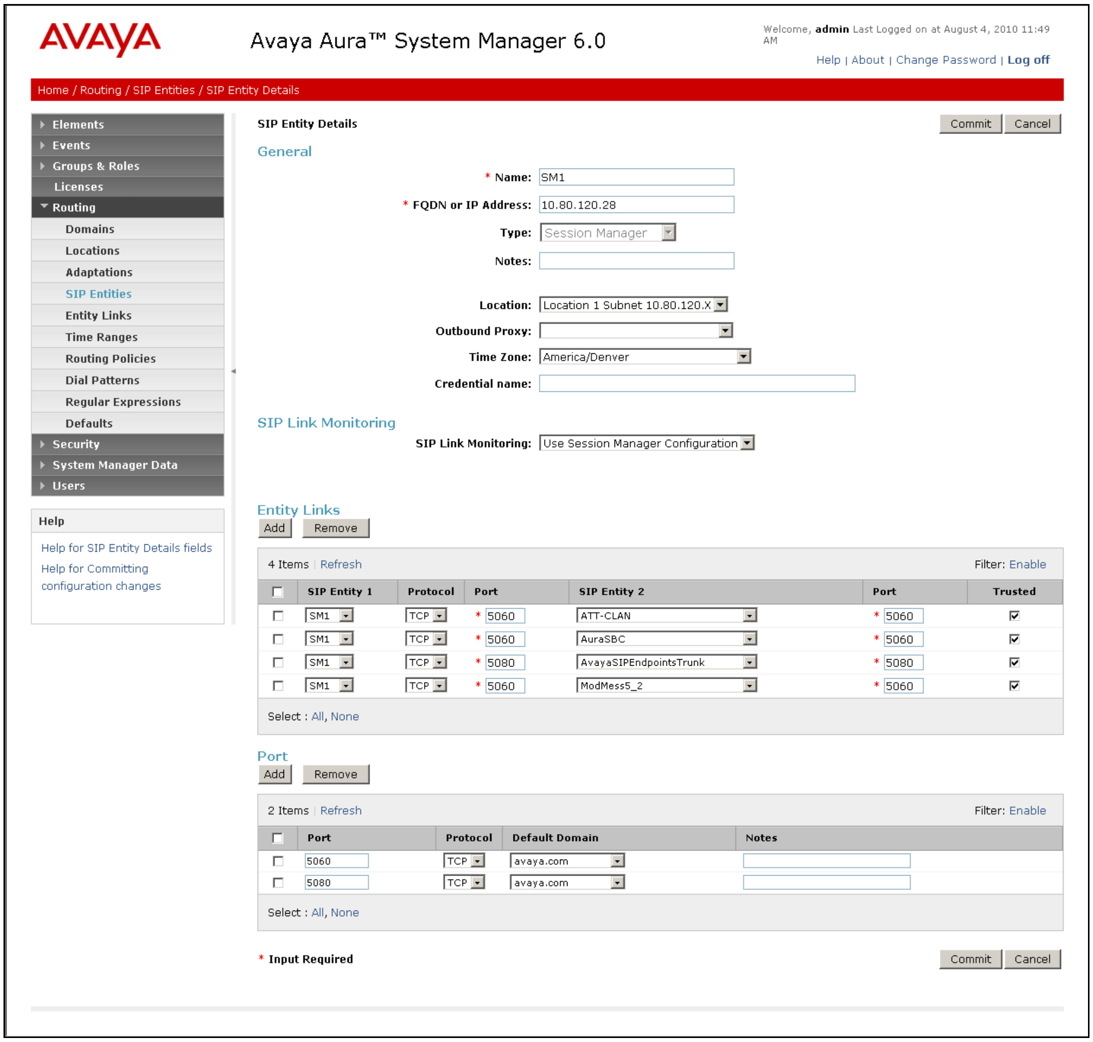

Figure 17: Completed Session Manager Entity configured in Section 4.6.1

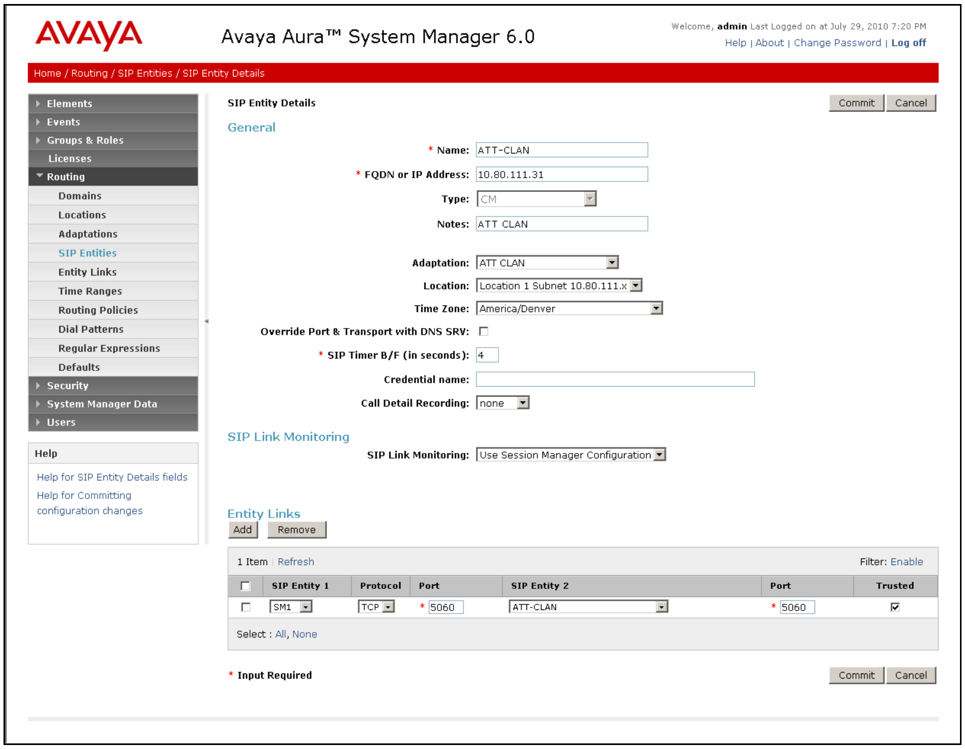

Figure 18: Completed Communication Manager Entity configured in Section 4.6.2

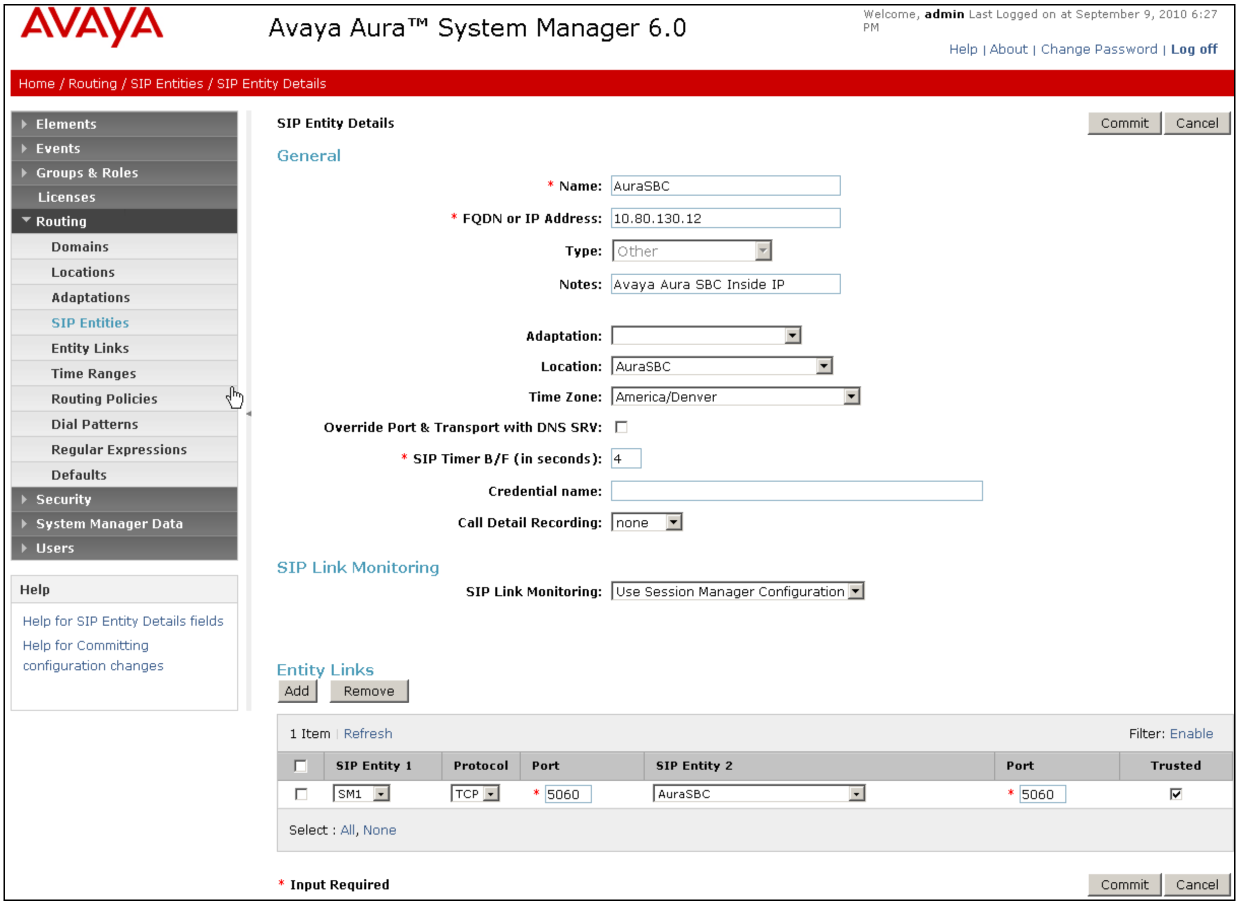

Figure 19: Completed Session Border Controller Entity configured in Section 4.6.3

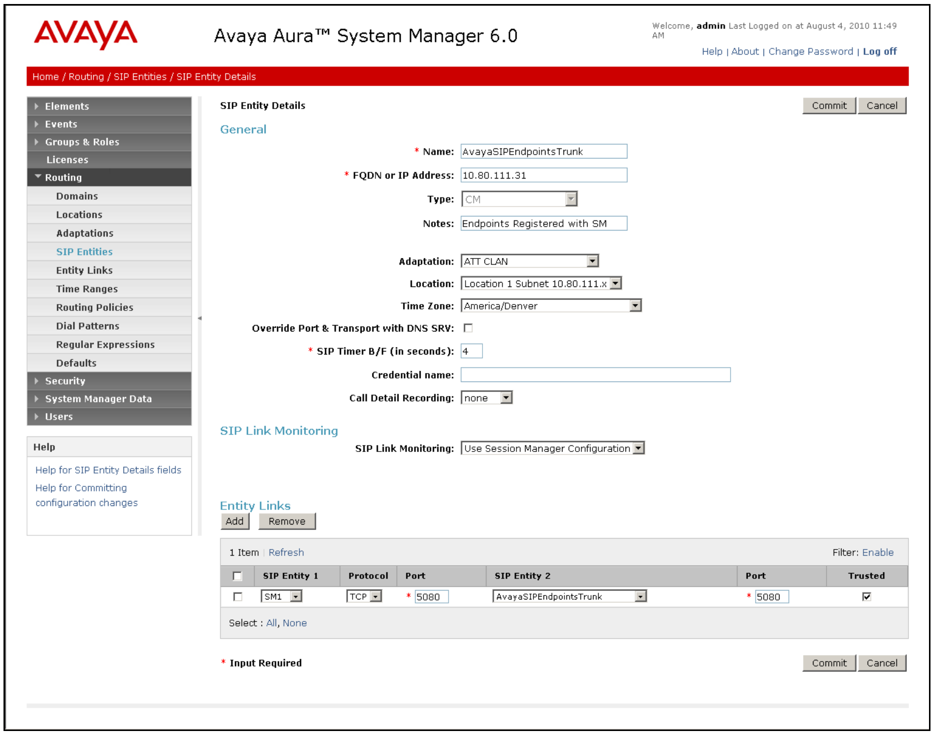

Figure 20: Completed SIP Endpoints Entity configured in Section 4.6.4

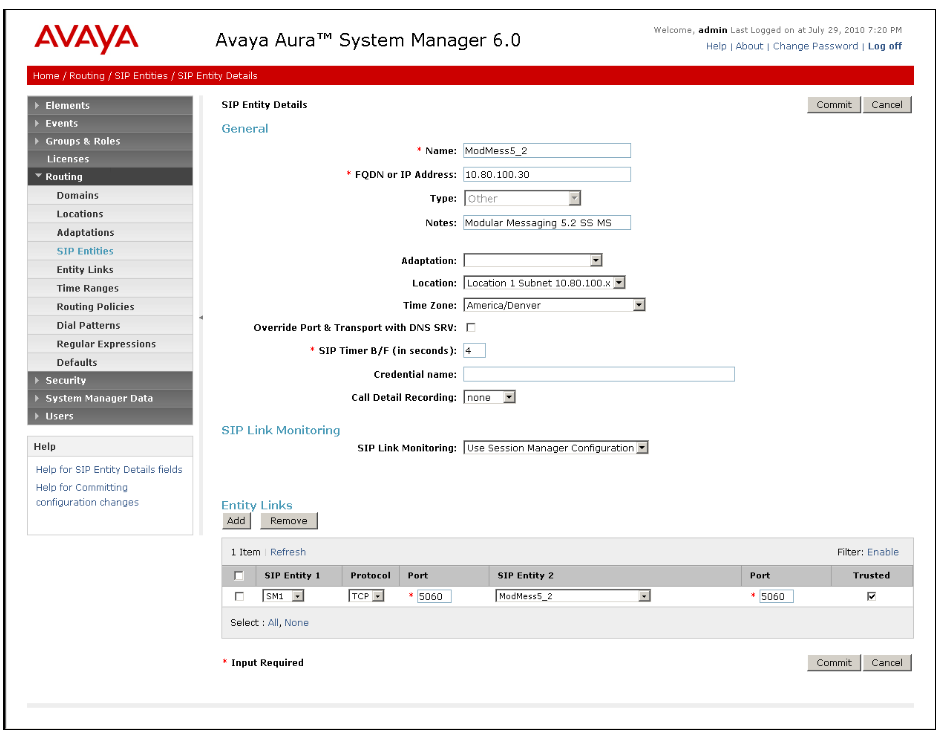

Figure 21: Completed Modular Messaging Entity configured in Section 4.6.5

4.9. Time Ranges

1. In the left pane under **Routing**, click on "**Time Ranges**". In the **Time Ranges** page click on "**New**" (not shown).
2. Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkboxes for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.
3. Click on "**Commit**".
4. Repeat **Steps 1–3** to provision additional time ranges.

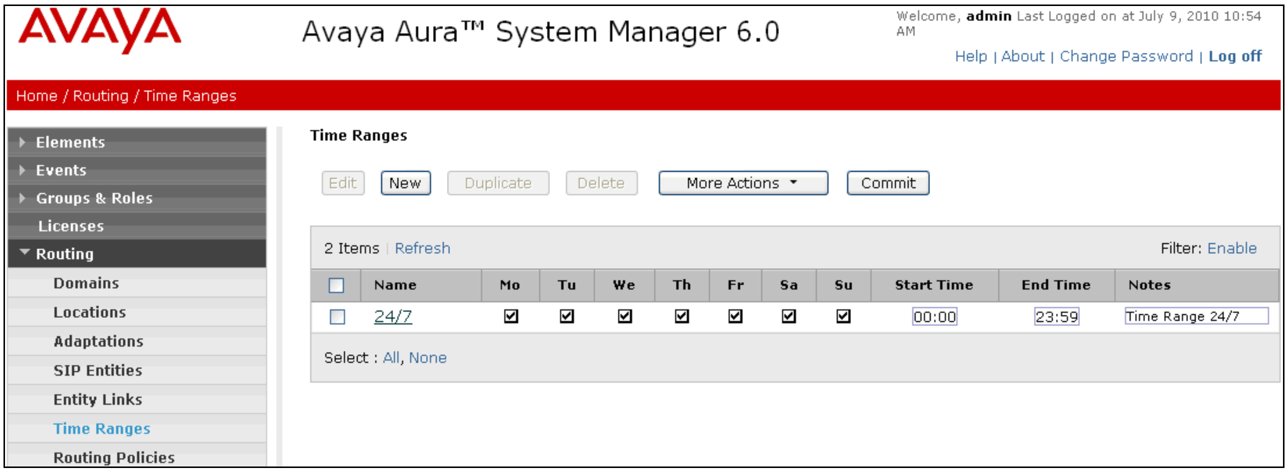

Figure 22: Time Ranges Page

4.10. Routing Policies

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

- Routing Policy to Avaya Aura™ Communication Manager for calls from AT&T
- Routing Policy to Avaya Modular Messaging

4.10.1. Routing Policy to Communication Manager

1. In the left pane under **Routing**, click on "**Routing Policies**". In the **Routing Policies** page click on "**New**" (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **To_ACM**) for routing calls from AT&T, and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

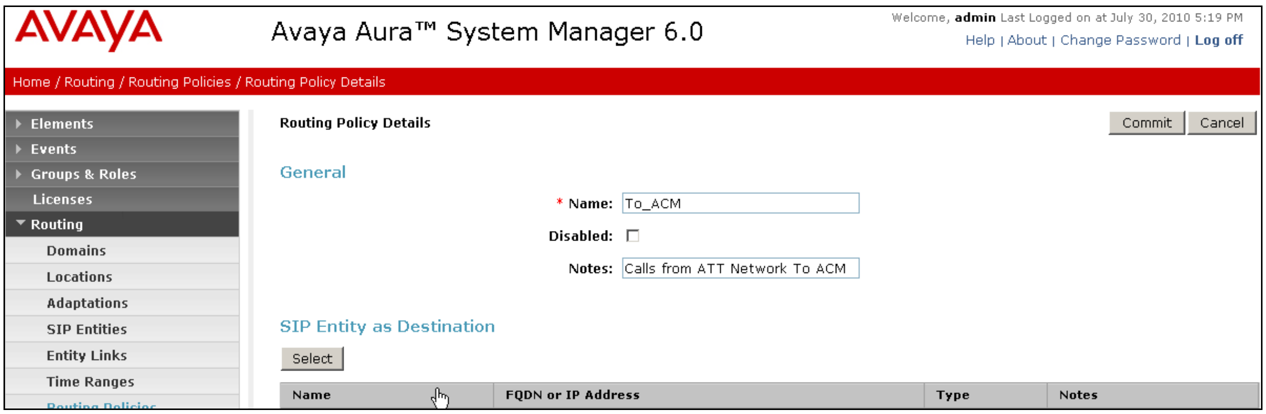

Figure 23: Routing Policy to Communication Manager

3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on "**Select**".
4. In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.6.2** for Communication Manager (**ATT-CLAN**), and click on "**Select**".

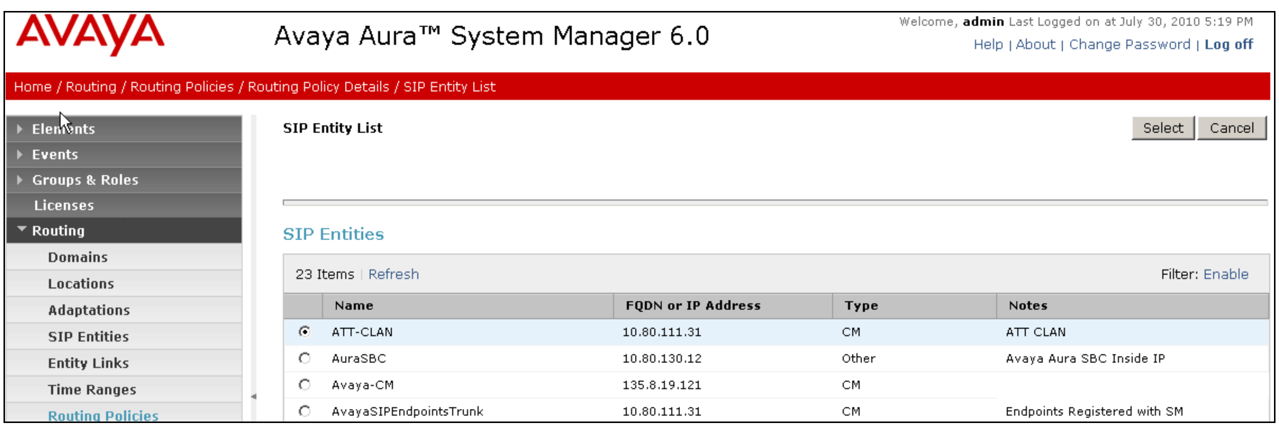

Figure 24: SIP Entity List Page - Routing to Communication Manager

5. Returning to the **Routing Policy Details** page click on "**Add**" in the **Time of Day** section.
6. In the **Time Range List** page [not shown], check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 4.9**, and click on "**Select**".

7. Returning to the **Routing Policy Details** page, enter a **Ranking** (the lower the number, the higher the ranking) in the **Time of Day** section for each Time Range.
8. 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 configured in **Section 4.11**.
9. No **Regular Expressions** were used in this reference configuration.
10. Click **Commit**.

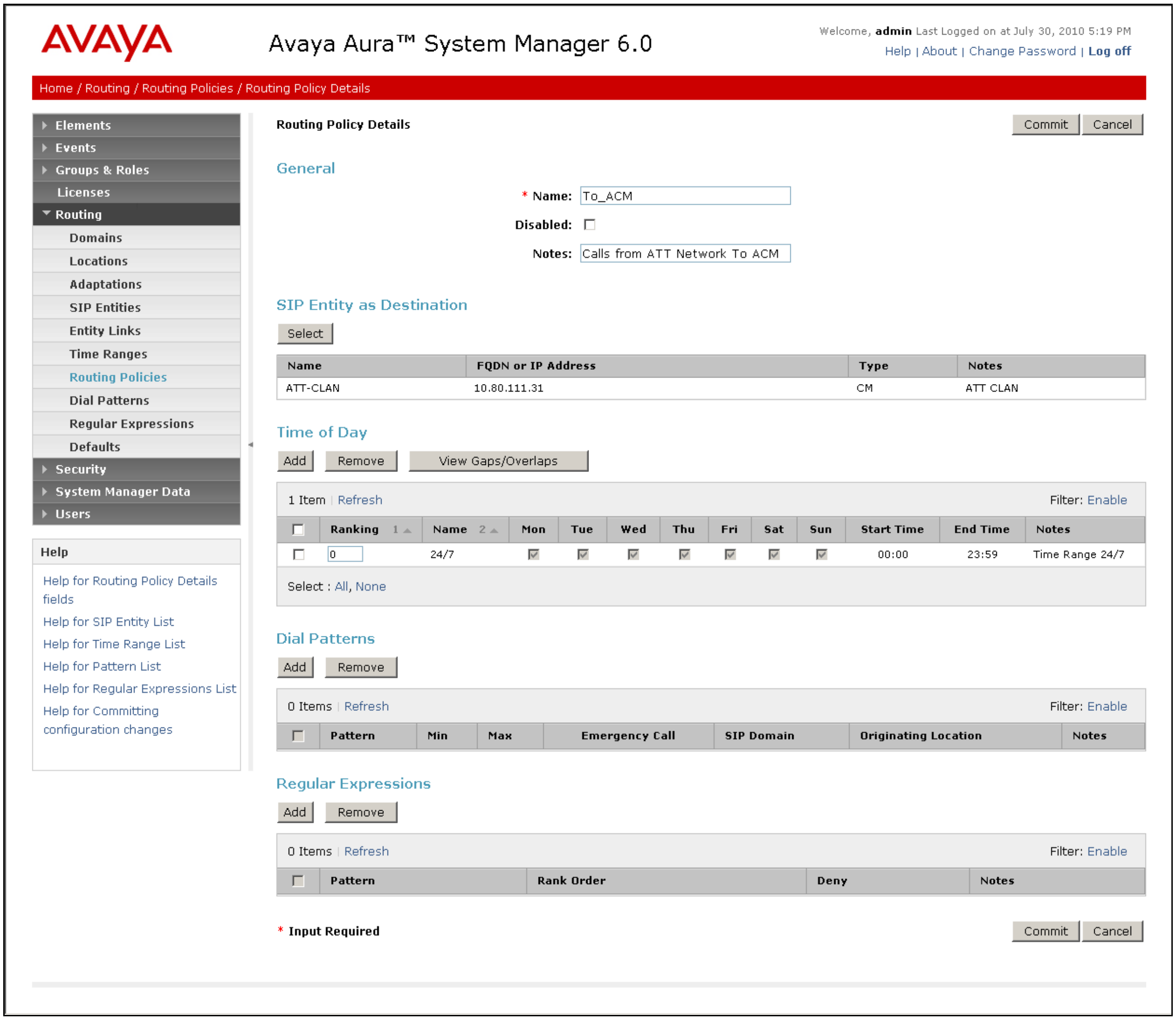

Figure 25: Routing Policy Details Page to Communication Manager

4.10.2. Routing Policy to Avaya Modular Messaging

To configure this routing policy to Modular Messaging, repeat the Steps in **Section 4.10.1**. In the **SIP Entity as Destination** section, select the SIP Entity administered in **Section 4.6.5** for Modular Messaging. See the figure below for the values used in the reference configuration.

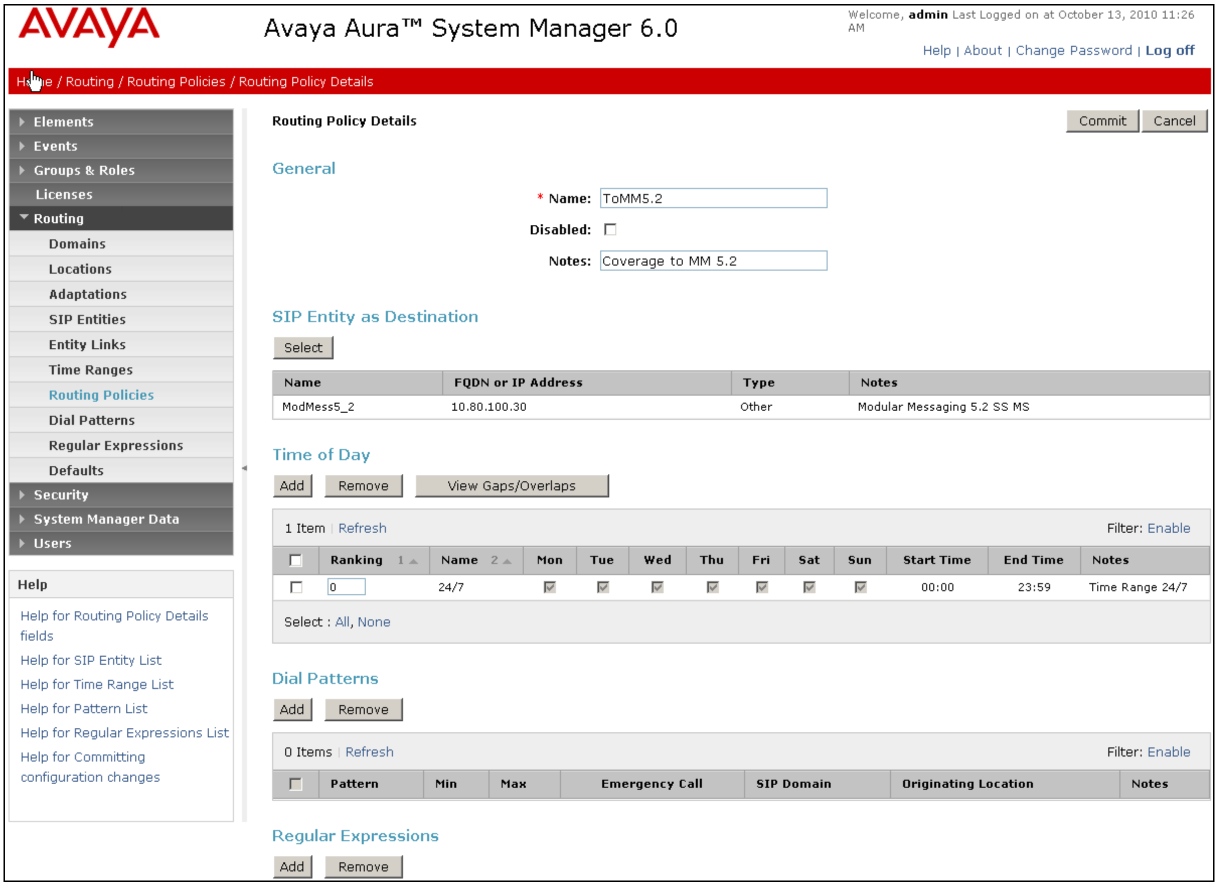

Figure 26: Routing Policy Details Page to Avaya Modular Messaging

4.11. Dial Patterns

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

- Inbound PSTN calls via AT&T IP Toll Free service.
- Calls to Avaya Modular Messaging pilot number.

4.11.1. Matching Inbound Calls from AT&T IPTF to Communication Manager

In this example inbound calls from any PSTN number with the pattern 0000010xx 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 **0000010** in this example.
   - **Min** and **Max** – Enter **9**.
   - **SIP Domain** – Select one of the SIP Domains defined in **Section 4.3** 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 **avaya.com** in this example.
   - (Optional) Add any notes if desired.
3. In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on "**Add**".

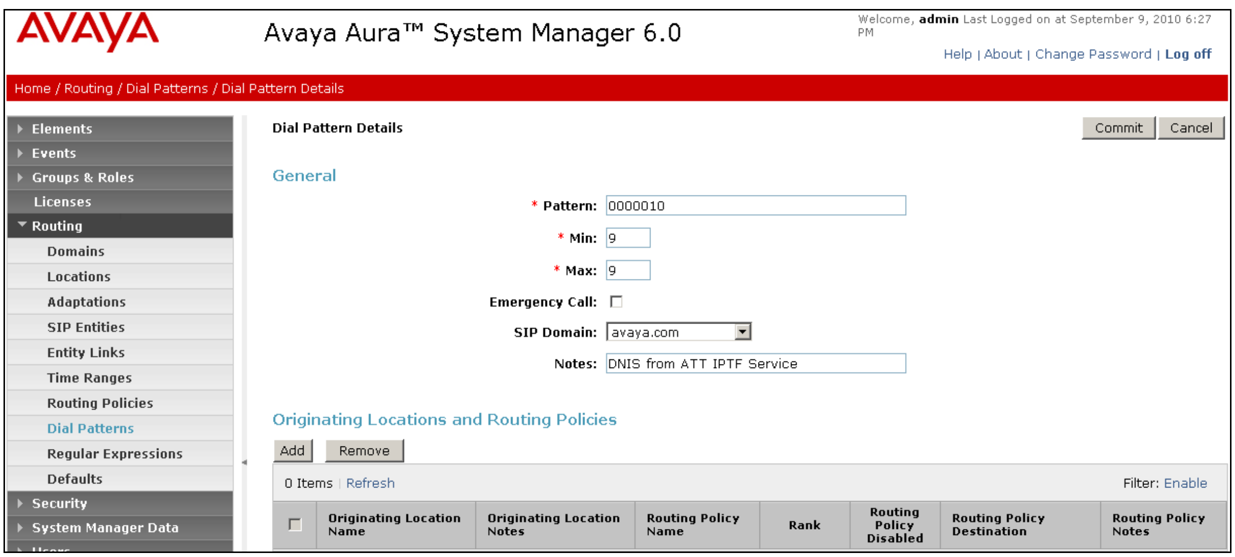

Figure 27: Dial Pattern Details Page - Matching Inbound AT&T IP Toll Free Service Calls

4. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, select the locations from where calls can originate to be routed to Communication Manager. 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 was set to "**AuraSBC**" in this reference configuration.
5. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, select the Routing Policy administered for routing calls to Communication Manager in **Section 4.10.1**.
6. Click on **Select**.

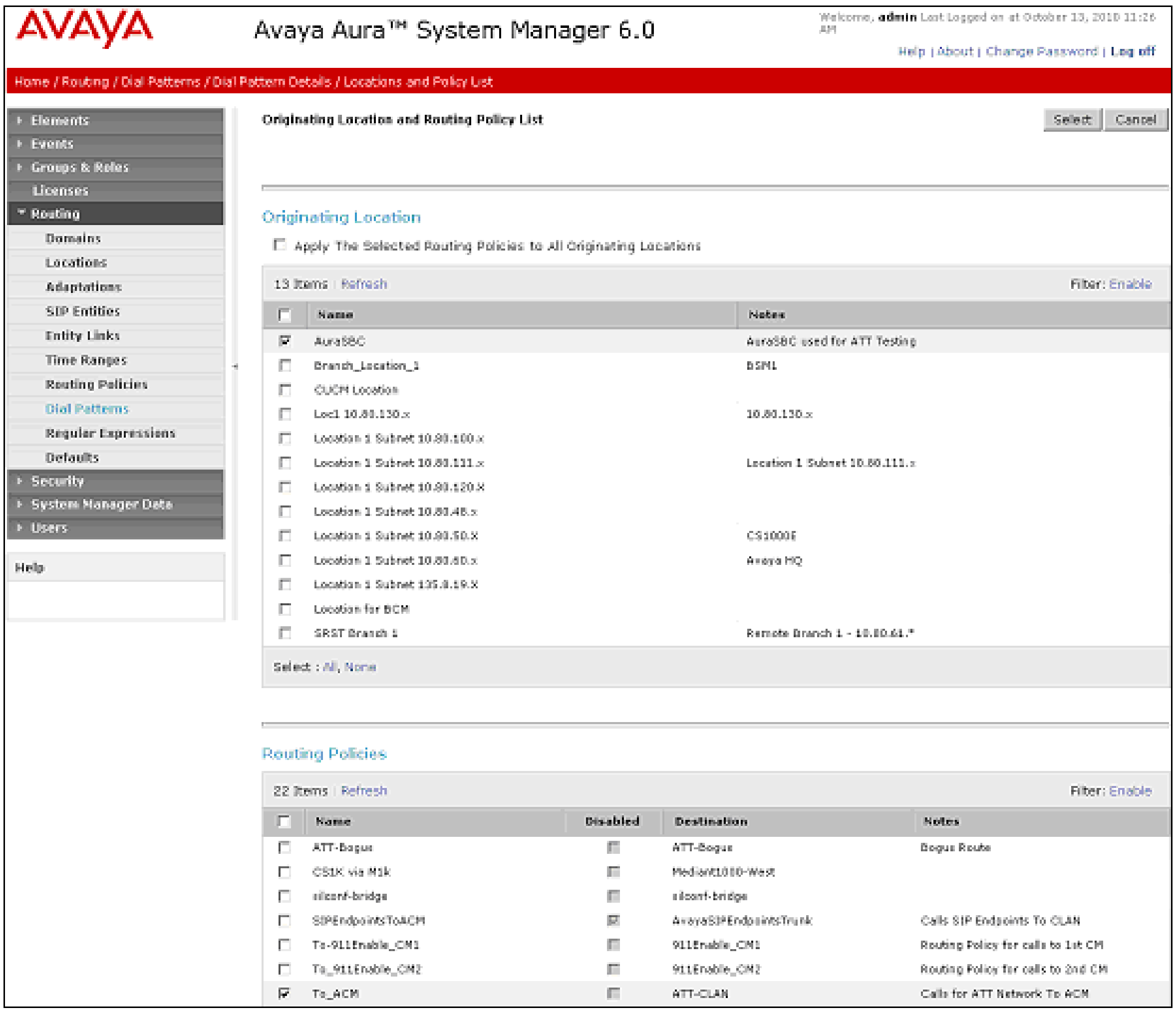

Figure 28: Originating Location and Routing Policy List Page - Matching Inbound Calls from AT&T to Communication Manager

7. Returning to the **Dial Pattern Details** page below, click on "**Commit**".

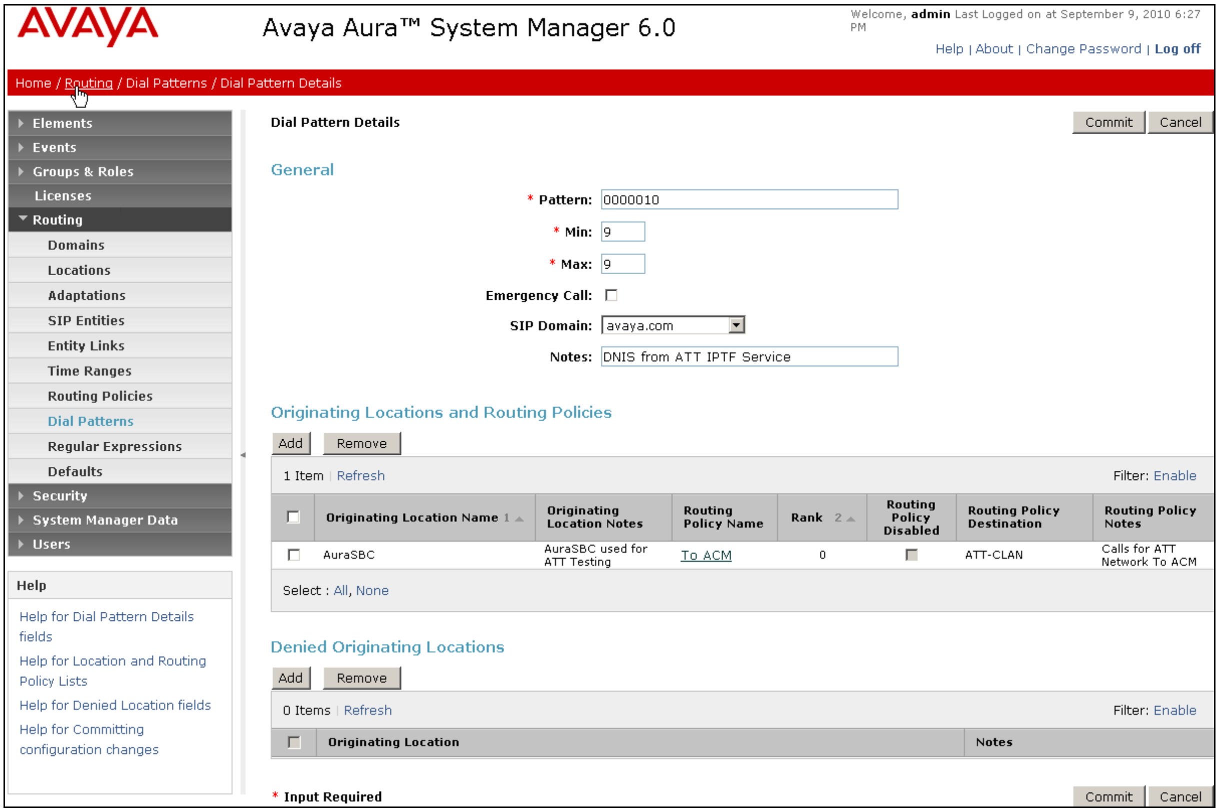

Figure 29: Dial Pattern Details – After adding Originating Locations and Routing Policies

4.11.2. Matching Inbound Calls to Avaya Modular Messaging Pilot Number via Avaya Aura™ Communication Manager

Communication Manager stations cover to Modular Messaging using a pilot extension (6664999 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 Modular Messaging, repeat the Steps in **Section 4.11.1**. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, select the locations from where calls can originate to be routed to Modular Messaging. Note that only those calls that originate from the selected Location(s), or any of the administered Locations if "**-ALL-**" is selected, can match this Dial Pattern. See the figure below for the values used in the reference configuration. See **Section 4.12** for all the Dial Patterns used in this reference configuration.

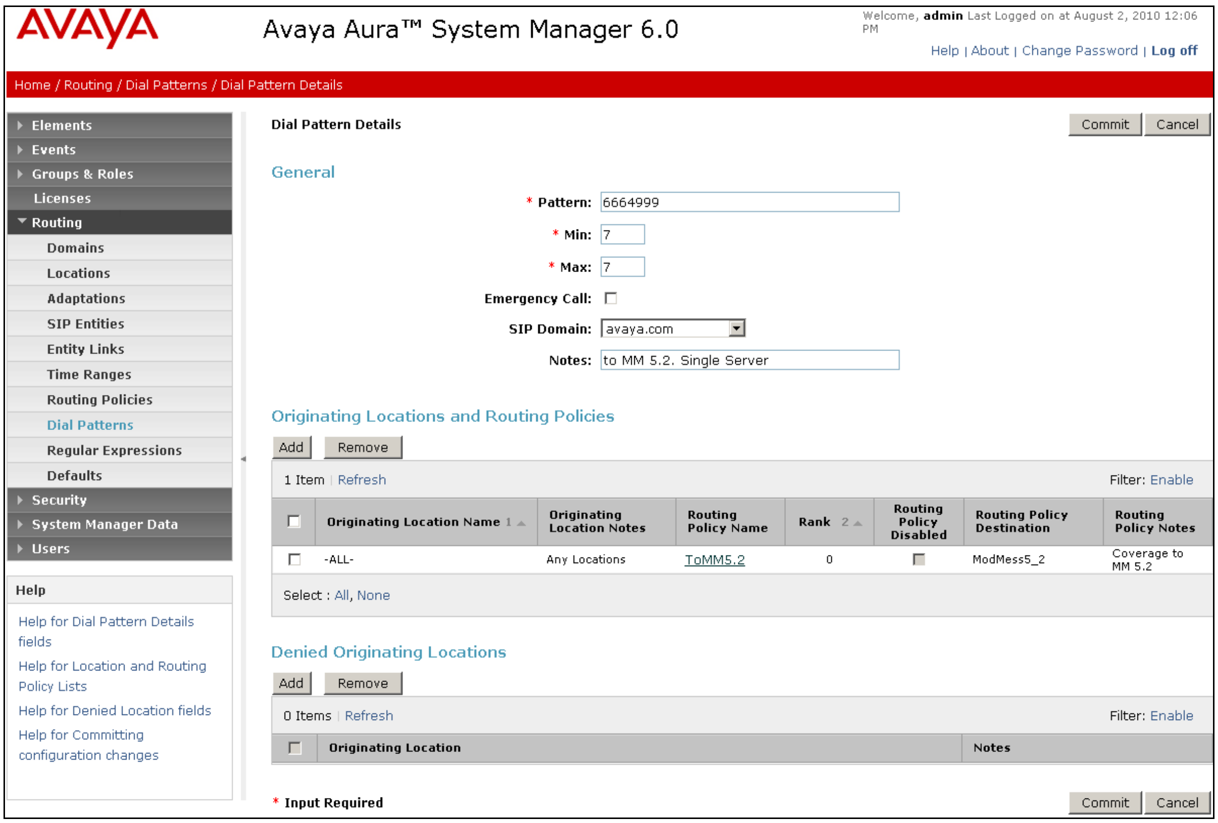

Figure 30: Dial Pattern Details – Coverage to Modular Messaging

4.12. Routing Policy Completed Configuration

After the Routing Policy and various Dial Patterns are configured, the Routing Policy screens change to reflect all the Dial Patterns used to determine where the call needs to be routed. Following figures show all the Routing Policies configured in **Section 4.10** after the Dial Patterns are added in **Section 4.11**.

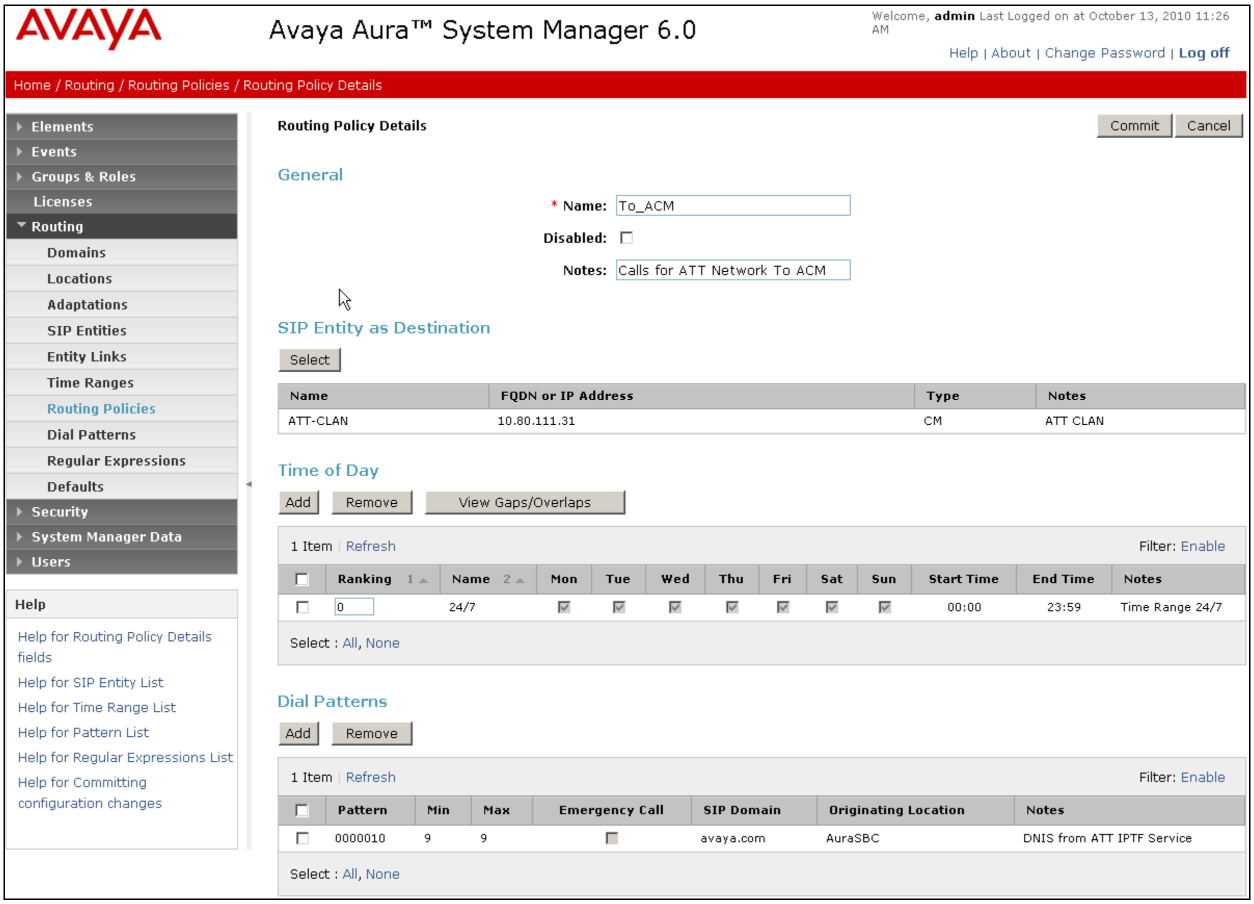

Figure 31: Completed Routing Policy Details to Communication Manager (Section 4.10.1)

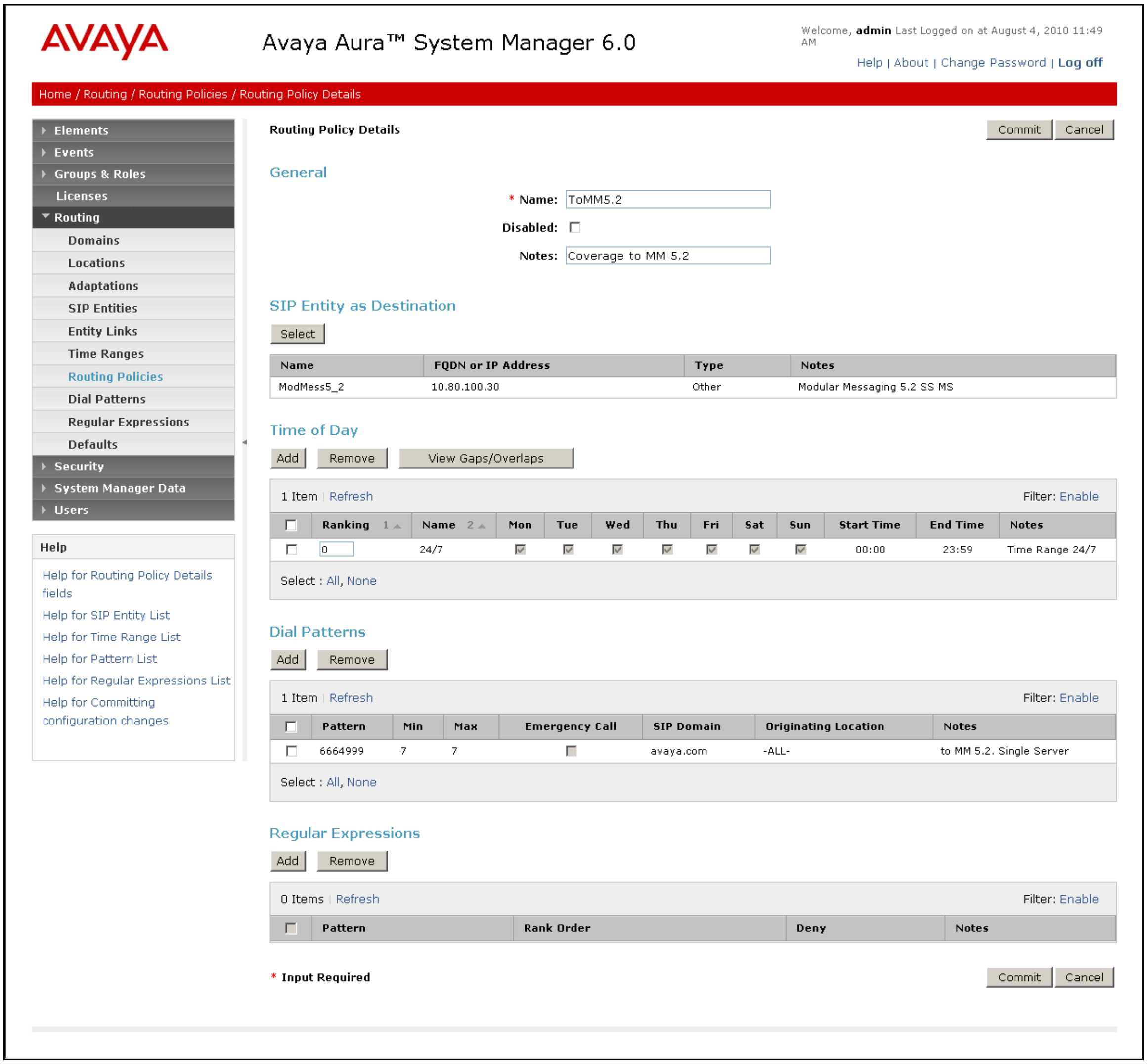

Figure 32: Completed Routing Policy Details to Modular Messaging (Section 4.10.2)

4.13. Session Manager Administration

1. In the left pane under **Elements**, click on **Session Manager → Session Manager Administration**. In the **Session Manager Administration** page click on "**Add**" (not shown).
2. In the **General** section of the **Add Session Manager** page:
   - **SIP Entity Name** – Select the SIP Entity administered for Session Manager in **Section 4.6.1**.
   - **Management Access Point Host Name/IP** – Enter the IP address of the management interface on Session Manager as defined during installation, (*not* the network interface).
3. In the **Security Module** section of the **Add Session Manager** page, enter the **Network Mask** and **Default Gateway** of the Session Manager network interface as defined during installation.
4. Use default values for the remaining fields.
5. Click on "**Commit**".

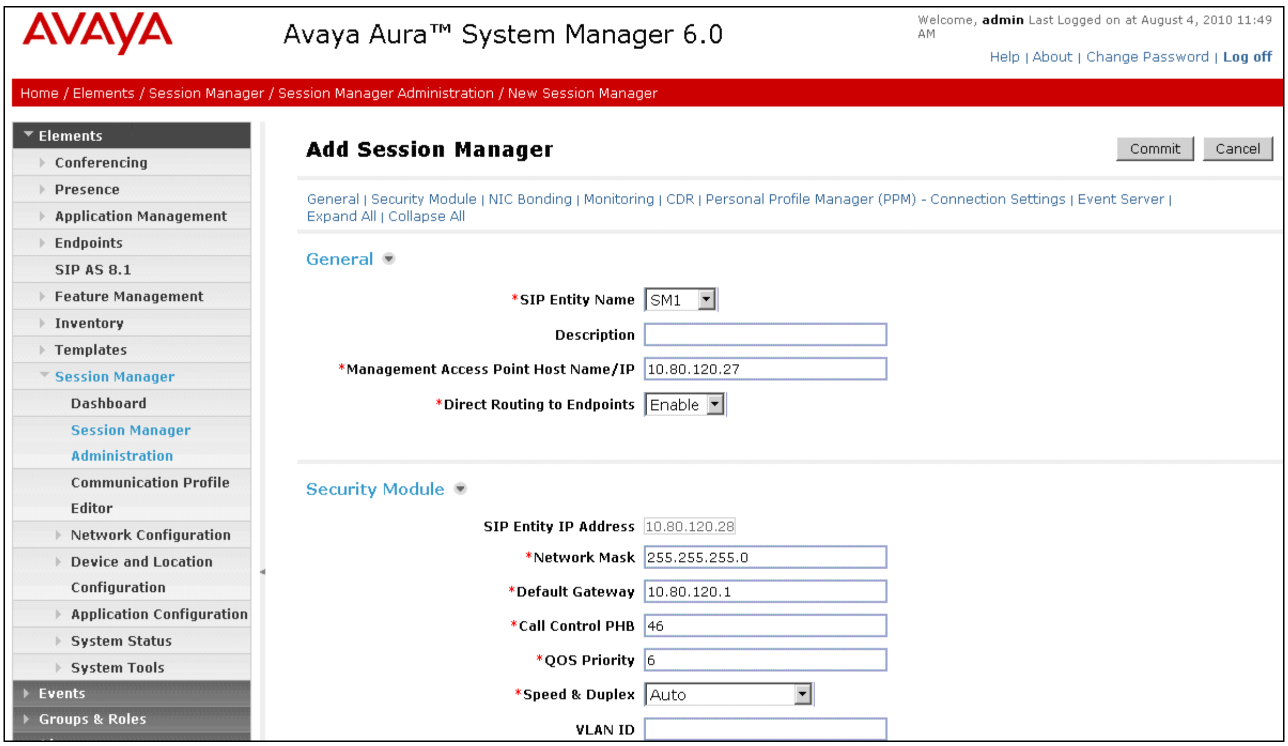

Figure 33: Add Session Manager Page

5. 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 [3] and [4] 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.

5.1. System Parameters

This section reviews the Communication Manager licenses and features that are required for the reference 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: 8000   0
           Maximum Concurrently Registered IP Stations: 18000  4
             Maximum Administered Remote Office Trunks: 0      0
Maximum Concurrently Registered Remote Office Stations: 0      0
              Maximum Concurrently Registered IP eCons: 0      0
  Max Concur Registered Unauthenticated H.323 Stations: 0      0
                 Maximum Video Capable H.323 Stations: 0      0
                  Maximum Video Capable IP Softphones: 0      0
                       Maximum Administered SIP Trunks: 24000  85
  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: 0      0
           Maximum TN2602 Boards with 80 VoIP Channels: 128    0
          Maximum TN2602 Boards with 320 VoIP Channels: 128    2
   Maximum Number of Expanded Meet-me Conference Ports: 0      0

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

Figure 34: System Parameters Customer Options Form – Page 2

2. On **Page 3** of the **system-parameters customer-options** form, verify that the **ARS** feature is enabled.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y              DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

Figure 35: System Parameters Customer Options Form – Page 3

3. On Page 4 of the **system-parameters customer-options** form, verify that the **Enhanced EC500?** , the **IP Stations?**, and the **IP Trunks?** fields are set to "**y**".

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

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

           IP Attendant Consoles? n
```

Figure 36: System Parameters Customer Options Form – Page 4

4. On **Page 5** of the **system-parameters customer-options** form, verify that the **Private Networking** and **Processor Ethernet** fields are set to "**y**".

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

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

Figure 37: System Parameters Customer Options Form – Page 5

5.2. Dial Plan and Feature Access Codes

This section briefly describes the dial plan requirements and feature access codes for the reference configuration described in these Application Notes.

1. Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings administered in the figure below:
   - 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 reference configuration conform to this format.
   - 7-digit extensions with a **Call Type** of "**ext**" beginning with the digits "**6665**". Local extensions for Communication Manager stations, agents, and Vector Directory Numbers (VDNs) in this reference configuration conform to this format.
   - 1-digit facilities access code (indicated with a **Call Type** of "**fac**"), e.g., "**9**" access code for outbound ARS dialing and "**8**" for AAR local dialing.
   - 3-digit facilities access codes, e.g., codes starting with "*" and "#" for Agent logon/logoff).

```
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
   6665        7   ext
   3           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

Figure 38: Dialplan Analysis Form

2. Enter the **change feature-access-codes** command. On Page 1 of the **feature-access-codes** form, set **Auto Alternate Routing (AAR) Access Code** to "**8**" that is valid under the administered dial plan in **Step 1**.

```
change feature-access-codes                                   Page   1 of   8
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
```

Figure 39: Feature Access Codes Form

5.3. 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 Avaya site. For simplicity in this reference configuration, all Communication Manager elements, e.g., stations, C-LAN and MedPro boards, etc., within the Avaya site are assigned to a single IP network region and all internal calls use a single IP codec set. Additionally, this section describes the steps for administering IP network regions and codec sets for external calls between the Avaya site and the AT&T IP Toll Free network.

1. Enter the **change ip-codec-set *ci*** command, where ***ci*** is the number of an IP codec set used only for **internal** calls. In this reference configuration, following codecs were used for internal calls.

```
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.711MU           n          2        20
 2: G.729B            n          2        20
 3: G.729A            n          2        20
```

Figure 40: IP Codec Set Form for Internal Calls – Page 1

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

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

Figure 41: IP Codec Set Form for Internal Calls – Page 2

- Repeat this step as necessary for each IP codec set used only for internal calls.

2. Enter the **change ip-codec-set** ***ce*** command, where ***ce*** is the number of an unused IP codec set. This IP codec set will be used for external calls. On Page 1 of the **ip-codec-set** form, provision the codecs in the order shown in figure below:

Note - The **Frames Per Pkt** and **Packet Size (ms)** values for **G.729A**, **G711MU** and **G.726A-32K** are set according to the requirements of the AT&T IP Toll Free service.

```
change ip-codec-set 3                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 3

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.729A             n         2        20
 2: G.711MU            n         2        20
 3: G.726A-32K         n         2        20
```

Figure 42: IP Codec Set Form for External Calls – Page 1

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

```
change ip-codec-set 3                                          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
```

Figure 43: IP Codec Set Form for External Calls – Page 2

3. Enter the **change ip-network-region nrl**, where **nrl** is the number of an unused IP network region for local Communication Manager Elements within the Avaya site. On **Page 1** of the **ip-network-region** form, set the **UDP Port Min** and **UDP Port Max** to "**16384**" and "**32767**" (this port range is an AT&T IP Toll Free service requirement).

```
change ip-network-region 2                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 2
Location:          Authoritative Domain: avaya.com
    Name: Local
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
```

Figure 44: IP Network Region Form for the Network Region Representing the Local Communication Manager Elements

- On **Page 4** of the **ip-network-region** form, enter codec set **3** in front of dst rgn **3** so that source network region **2** can talk to destination network region **3** using codec set **3**. The settings shown in figure below were used in this reference configuration.

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

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

 2    2                                                                all
 3    3     y    NoLimit                                             n
```

Figure 45: IP Network Region Form for an IP Network Region Administered for Local Communication Manager Elements – Page 4

4. Enter the **change ip-network-region nrp**, where **nrp** is the number of an IP network region administered for the AT&T calls. On **Page 1** of the **ip-network-region** form, set the **UDP Port Min** and **UDP Port Max** to "**16384**" and "**32767**" (this port range is an AT&T IP Toll Free service requirement)

```
change ip-network-region 3                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 3
Location:          Authoritative Domain: avaya.com
    Name: ATT PSTN
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 3              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                     IP Audio Hairpinning? y
   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
```

Figure 46: IP Network Region Form for a Network Region Administered for AT&T – Page 1

- On **Page 4** of the **ip-network-region** form, enter codec set **3** for dst rgn **2** so that source network region **3** can talk to destination network region **2** using codec set **3**.The settings shown in figure below were used in this reference configuration.

```
change ip-network-region 3                                      Page   4 of  20

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

Figure 47: IP Network Region Form for an IP Network Region Administered for AT&T – Page 4

5. Enter the **list node-names** command, and note the node names and IP addresses of the Session Manager server used in **Section 5.5.1** and **Section 5.5.2** as well as of the C-LAN board used in **Section 5.5.1** and **Section 5.5.2**.

```
list node-names

                        NODE NAMES

Type     Name              IP Address
IP       CLAN-1A03         10.80.111.31
IP       Gateway           10.80.111.1
IP       MEDPRO-1A11       10.80.111.32
IP       ASM1              10.80.120.28
IP       procr             10.80.111.73
IP       default           0.0.0.0
```

Figure 48: Node Names Form

5.4. Alternate Automated Routing (AAR) Table

The AAR table is selected based on the caller dialing the AAR access code (e.g. "**8**") as defined in **Section 5.2**. The access code is removed and the AAR table matches the remaining dialed digits and sends them to the designated route pattern (see **Section 5.6**). Configure as follows:

- **Dialed String** – Set to **6665** for calls to SIP endpoints registered with Session Manager.
- **Min** and **Max** - Set to **7**, the minimum and maximum size the dialed string will assume.
- **Route Pattern** – Set to **21** as configured in **Section 5.6**.
- **Call Type** – Set to **aar**.
- Repeat the above steps for calls to Modular Messaging pilot number **6664999**. Note in this case the **Call Type** field is set to **unku**.

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

          Dialed           Total     Route    Call   Node  ANI
          String         Min  Max  Pattern    Type   Num   Reqd
    6665                 7    7      21       aar          n
    6664999              7    7      21       unku         n
```

Figure 49: AAR Analysis Form

5.5. SIP Trunks

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

- Inbound for AT&T access – SIP Trunk 1
- Local for Modular Messaging and Avaya SIP telephone access – SIP Trunk 2

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

Note – In the 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.

5.5.1. SIP Trunk for AT&T Access

This section describes the steps for administering the SIP trunk connecting to Session Manager used for AT&T access. This trunk connects to the **SM1** Entity defined in **Section 4.6.1**.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **20**), and provision the following:
   - **Group Type** – Set to "**sip**".
   - **Transport Method** – Set to "**tcp**". Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Session Border Controller and the AT&T IP Toll Free service is UDP.
   - Verify that **Peer Detection Enabled** is "**y**" and that **Peer Server** is **SM**.
   - **Near-end Node Name** – Set to the node name of the CLAN i.e. **CLAN-1A03** noted in **Section 5.3**, **Step 5**.
   - **Far-end Node Name** – Set to the node name of Session Manager i.e. A**SM1** noted in **Section 5.3**, **Step 5**.
   - **Near-end Listen Port** and **Far-end Listen Port** – set to "**5060**" (see Transport Method note above).
   - **Far-end Network Region** – Set to the IP network region **3**, as defined in **Section 5.3**, **Step 4**.
   - **Far-end Domain** – Enter **avaya.com**. This is the domain inserted by Session Manager in **Section 4.5.1**.
   - **DTMF over IP** – Set to "**rtp-payload**" to enable Communication Manager to use DTMF according to RFC 2833.
   - **Direct IP-IP Audio Connections** – Set to "**y**", indicating that the RTP paths should be optimized to reduce the use of Communication Manager audio resources when possible.
   - **Enable Layer 3 Test** – Set to "**y**". This allows Communication Manager to send SIP OPTIONS "pings" to Session Manager to monitor link status.

```
add signaling-group 20                                          Page   1 of   1
                                SIGNALING GROUP
 Group Number: 20             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                              SIP Enabled LSP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: CLAN-1A03            Far-end Node Name: ASM1
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 3
Far-end Domain: avaya.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

Figure 50: Signaling Group 1 Form for AT&T IP Toll Free Calls

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **20**). On **Page 1** of the **trunk-group** form, provision the following:
   - **Group Type** – Set to "**sip**".
   - **Group Name** – Enter any descriptive name.
   - **TAC** – Enter a trunk access code that is consistent with the dial plan.
   - **Direction** – Set to "**incoming**".
   - **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 (e.g. **20**).

```
add trunk-group 20                                              Page   1 of  21
                                TRUNK GROUP
Group Number: 20                   Group Type: sip           CDR Reports: y
  Group Name: ATT Testing                 COR: 1        TN: 1        TAC: 120
   Direction: incoming       Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk         Auth Code? N
                                                Member Assignment Method: auto
                                                         Signaling Group: 20
                                                       Number of Members: 20
```

Figure 51: Trunk-Group Form for AT&T IP Toll Free Calls – Page 1

3. On **Page 2** of the **trunk-group** form, set the **Preferred Minimum Session Refresh Interval(sec)** field to "**900**". This entry will actually cause a value of 1800 to be generated in the SIP header which is the value required by AT&T IP Toll Free service.

```
add trunk-group 20                                           Page   2 of  21
      Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 5000
            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
                                     Delay Call Setup When Accessed Via IGAR? n
```

Figure 52: Trunk Group Form for AT&T IP Toll Free Calls – Page 2

4. On **Page 3** of the **trunk-group** form, set **Numbering Format** field to **private**

```
add trunk-group 20                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y
                     Numbering Format: private
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y
                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
```

Figure 53: Trunk Group Form for AT&T IP Toll Free Calls – Page 3

5. On **Page 4** of the **trunk-group** form set **Telephone Event Payload Type** field to the RTP payload type required by the AT&T IP Toll Free service (e.g. **100**). Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Toll Free service to determine this value.

```
add trunk-group 20                                           Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 100

       Convert 180 to 183 for Early Media? y
 Always Use re-INVITE for Display Updates? n
                           Enable Q-SIP? n
```

Figure 54: Trunk Group Form for AT&T IP Toll Free Calls – Page 4

5.5.2. Local SIP Trunk (Modular Messaging and SIP Telephones)

This section describes the steps for administering the local SIP trunk for Avaya Modular Messaging and SIP Telephone traffic.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **21**), and follow the same procedures described in **Section 5.5.1**, **Step 1**, except:
   - **Far-end Network Region** – Set to the IP network region **2**, as defined in **Section 5.3**.
   - **Near-end Listen Port** and **Far-end Listen Port** – set to "**5080**" (see **Section 4.6.1**, **Step 5** for using a different port number).
   - **Direct IP-IP Audio Connections** – Set to "**n**". In an AT&T IP Toll Free environment, shuffling needs to be disabled for Avaya SIP telephones as noted in **Section 1.3**, **Item 4**.
   - **Enable Layer 3 Test** – Set to "**n**".

```
add signaling-group 21                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 2             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                             SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

   Near-end Node Name: CLAN-1A03            Far-end Node Name: ASM1
 Near-end Listen Port: 5080               Far-end Listen Port: 5080
                                       Far-end Network Region: 2

Far-end Domain: avaya.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? n
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                  Alternate Route Timer(sec): 6
```

Figure 55: Signaling Group Form for Local Calls

2. Enter the **add trunk-group x** command, where **x** 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 any descriptive name.
   - **TAC** – Enter a trunk access code that is consistent with the dial plan.
   - **Direction** – Set to "**two-way**".
   - **Service Type** – Set to "**tie**".
   - **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.

```
change trunk-group 21                                           Page   1 of  21
                                TRUNK GROUP
Group Number: 21                   Group Type: sip          CDR Reports: y
  Group Name: MM_and_SIP_Phones            COR: 1        TN: 1        TAC: 121
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 21
                                                     Number of Members: 20
```

Figure 56: Trunk Group Form for Local Calls – Page 1

3. Repeat **Section 5.5.1**, **Steps 3** and **4** for pages 2 and 3 of the form.

```
add trunk-group 21                                           Page   2 of  21
      Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 5000
            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
                                     Delay Call Setup When Accessed Via IGAR? n
```

Figure 57: Trunk Group Form for Local Calls – Page 2

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

Figure 58: Trunk Group Form for Local Calls – Page 3

- On **Page 4** of the **Trunk Group** form set "**Telephone Event Payload Type**" to the RTP payload type required by the AT&T IP Toll Free service (e.g. **100**).

```
add trunk-group 21                                          Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 100

       Convert 180 to 183 for Early Media? y
 Always Use re-INVITE for Display Updates? n
                             Enable Q-SIP? n
```

Figure 59: Trunk Group Form for Local Calls – Page 4

5.6. Route Pattern

5.6.1. Local Calls

This form defines the SIP trunk to be used based on the route pattern selected by the AAR table for local calls (see **Sections 5.4**).

- **Grp No** – Set to **21** i.e. the trunk group configured for Local Access.
- **FRL** – Set to **0** (zero).

```
change route-pattern 21                                         Page   1 of   3
                    Pattern Number: 2   Pattern Name: MM_&_SIP_phones
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 21   0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                          next
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
```

Figure 60: Route pattern form

5.7. Optional Features

5.7.1. 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.

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. Consult[3], [4], [5], and [6] for further details if necessary. The samples that follow are provided for reference purposes only.

```
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.)
```

Figure 61: Call Center Optional Features Form

In the reference configuration below, an inbound call from AT&I IP Toll Free service is handled using the VDN 6665310 (**Figure 66**) which routes the call to Vector 10 (**Figure 67**) and based upon the digit inputted by the caller, the call is directed to an appropriate skill. Skill 11 (**Figure 68**) is shown for reference purposes and additional skills can be similarly added.

```
display agent-loginID 6665611                            Page   1 of   2
                                 AGENT LOGINID

                Login ID: 6665611                                 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
```

Figure 62: Agent Form – Page 1

```
display agent-loginID 6665611                             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:
```

Figure 63: Agent Form – Page 2

```
display hunt-group 11                                          Page   1 of   3
                                  HUNT GROUP

            Group Number: 11                                    ACD? y
              Group Name: Skill-11                            Queue? y
         Group Extension: 666-5711                           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:
```

Figure 64: Skill (Hunt Group) Form – Page 1

```
display hunt-group 11                                         Page   2 of   3
                                  HUNT GROUP

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

      Controlling Adjunct: none

Interruptible Aux Threshold: none
                                 Redirect on No Answer (rings):
                                               Redirect to VDN:
                   Forced Entry of Stroke Counts or Call Work Codes? n
```

Figure 65: Skill (Hunt Group) Form – Page 2

```
display vdn 6665310                                          Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 666-5310
                                  Name: To SelectSkill
                           Destination: Vector Number        10

                  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
```

Figure 66: VDN (Vector Directory Number) Form

```
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 33002    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
```

Figure 67: Vector (RouteToSkill) Form

```
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 33003
03 queue-to     skill 11   pri m
04 announcement 33006
05 goto step    3             if unconditionally
06
```

Figure 68: Vector (Skill 11) Form

5.7.2. Modular Messaging Coverage Path and Hunt Group

Hunt group 1 is used in the reference configuration to verify Modular Messaging coverage functionality. This hunt group is defined with the 7 digit Modular Messaging pilot number **6664999**. The hunt group is associated with call **coverage path 1** in **Figure 69** and the coverage path is assigned to a station (e.g., **6665011** in **Figure 72**). Communication Manager will use the AAR access code "**8**" (defined in **Section 5.4**) to dial Modular Messaging (e.g. **86664999**) as shown in **Figure 71**.

```
display coverage path 1                                         Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage
COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
         Don't Answer?           y               y        Number of Rings: 4
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n
COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1            Rng: 4  Point2:
  Point3:                       Point4:
  Point5:                       Point6:
```

Figure 69: Coverage Path Form

```
display hunt-group 1                                            Page   1 of   60
                                  HUNT GROUP

            Group Number: 1                                ACD? n
              Group Name: MM                             Queue? n
         Group Extension: 6664999                       Vector? n
              Group Type: ucd-mia                Coverage Path:
                      TN: 1        Night Service Destination:
                     COR: 1                  MM Early Answer? n
           Security Code:             Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

Figure 70: Hunt Group Form – Page 1

```
display hunt-group 1                                            Page   2 of   60
                                  HUNT GROUP
                        Message Center: sip-adjunct
     Voice Mail Number        Voice Mail Handle          Routing Digits
                                                  (e.g., AAR/ARS Access Code)
     6664999                  6664999                    8
```

Figure 71: Hunt Group Form – Page 2

```
display station 6665011                                          Page   1 of   5
                                     STATION
Extension: 6665011                       Lock Messages? n               BCC: 0
     Type: 9620                          Security Code: 123456           TN: 1
     Port: S00000                      Coverage Path 1: 1               COR: 1
     Name: H323-96XX-5011              Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 6665011
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n
                                                         IP Video? n
                              Short/Prefixed Registration Allowed: default
                                              Customizable Labels? y
```

Figure 72: Station Form

6. Avaya Modular Messaging

In this reference configuration, Avaya Modular Messaging is used to verify DTMF, Message Wait Indicator (MWI), as well as basic call coverage functionality. The Avaya Modular Messaging used in the reference configuration is provisioned for Multi-Site mode. Multi-Site mode allows Avaya Modular Messaging to serve subscribers in multiple locations. The administration for Modular Messaging is beyond the scope of these Application Notes. Consult [7], [8], [9], and [10] for further details.

7. Avaya Aura™ Session Border Controller

This section illustrates an example of installation and configuration of the Session Border Controller. Similar to Communication Manager Release 6.0, the Session Border Controller runs on its own S8800 Server as an application template using Avaya Aura™ System Platform. The installation of the System Platform is assumed to have been previously completed.

The Session Border Controller includes a configuration wizard that can be used as part of the installation of the Session Border Controller template on System Platform. As such, screens from the installation of the SBC template are presented in **Section 7.1**. The wizard pre-configures the underlying Session Border Controller for much of the required provisioning. After the installation wizard is completed, subsequent configuration can be performed through the GUI as shown in **Section 7.2**.

In the Reference Configuration, the Avaya S8800 Server has four physical network interfaces, labeled 1 through 4. The port labeled "1" (virtual "eth0") is used for the management and private (inside) network interface of the SBC. The port labeled "4" (virtual "eth2") is used for the public (outside) network interface of the SBC.

Note: If using an Acme Packet Net-Net OS-E / Net-Net 2600 rather than an Avaya Aura™ Session Border Controller (SBC), the configuration can be obtained from the following Acme Packet website: https://support.acmepacket.com. Please note that an Acme Packet ID and Password are required.

7.1. Avaya Aura™ SBC Installation

To begin the SBC Template installation, log in to the System Platform console domain by entering https://<ip-addr>/webconsole as shown in the example screen below. In the Reference Configuration, the console domain uses the IP Address **10.80.130.11**, and the system domain uses the IP Address **10.80.130.10**. Enter an appropriate **User Id** and click **Continue**.

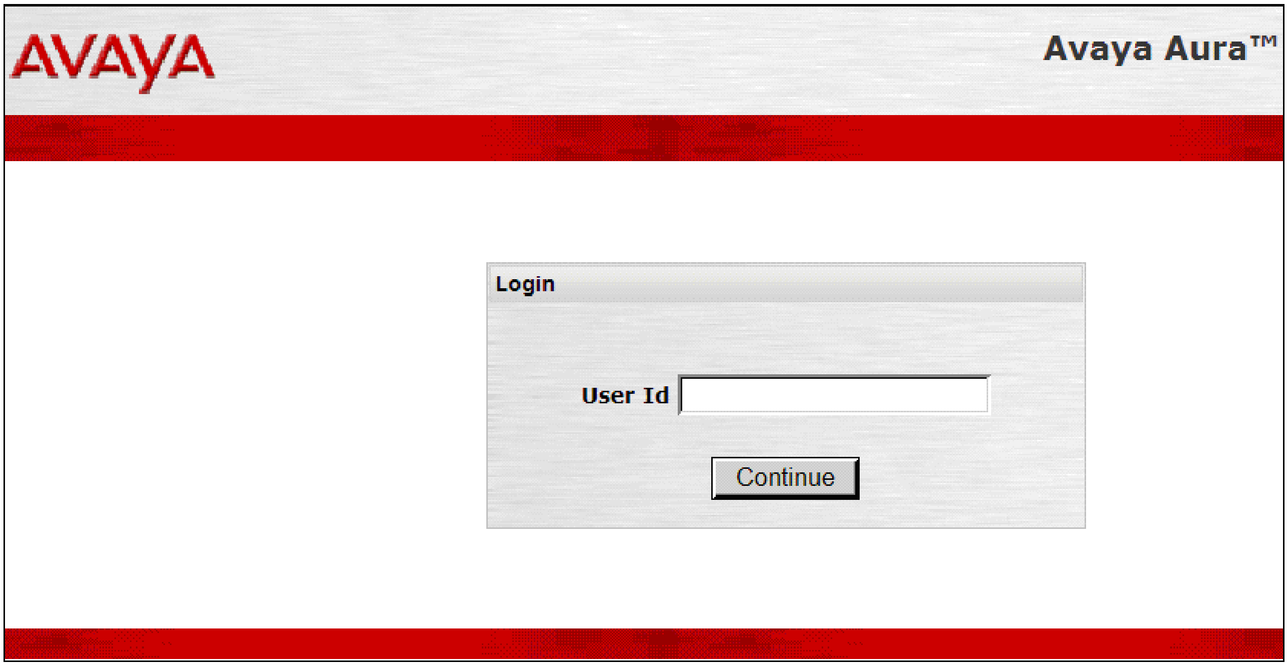

Figure 73: System Platform Console Domain Login screen

On the subsequent screen (not shown), enter the appropriate **Password** and click the **Log On** button.

Select **Virtual Machine Management → Solution Template**. In the **Install Template From** area, choose where the template files are located. In the sample configuration, the template was copied to the to USB drive. Click **Search**.

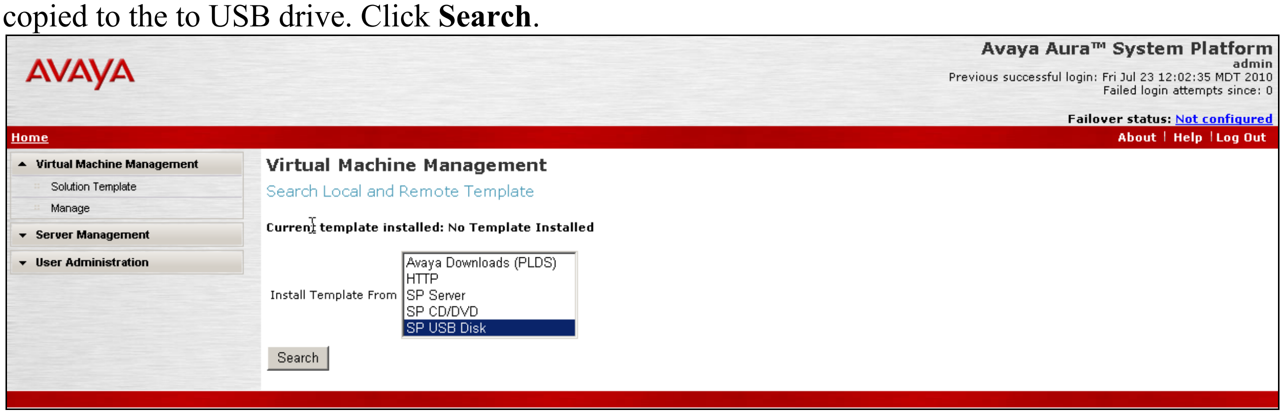

Figure 74: SBC Installation Template Search screen

Select the appropriate file, such as "SBCT.ovf". Click the **Select** button.

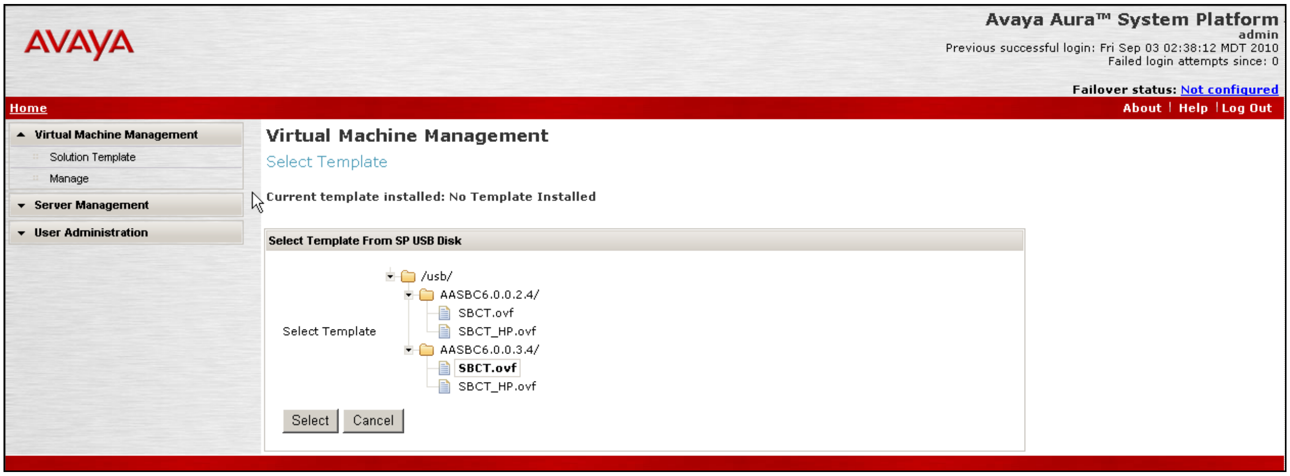

Figure 75: SBC Installation Template Selection screen

In the resultant screen shown below, the **Selected Template** can be observed. If an EPW file is available, it may be uploaded and used. In the sample configuration, the **Continue without EPW file** button was used.

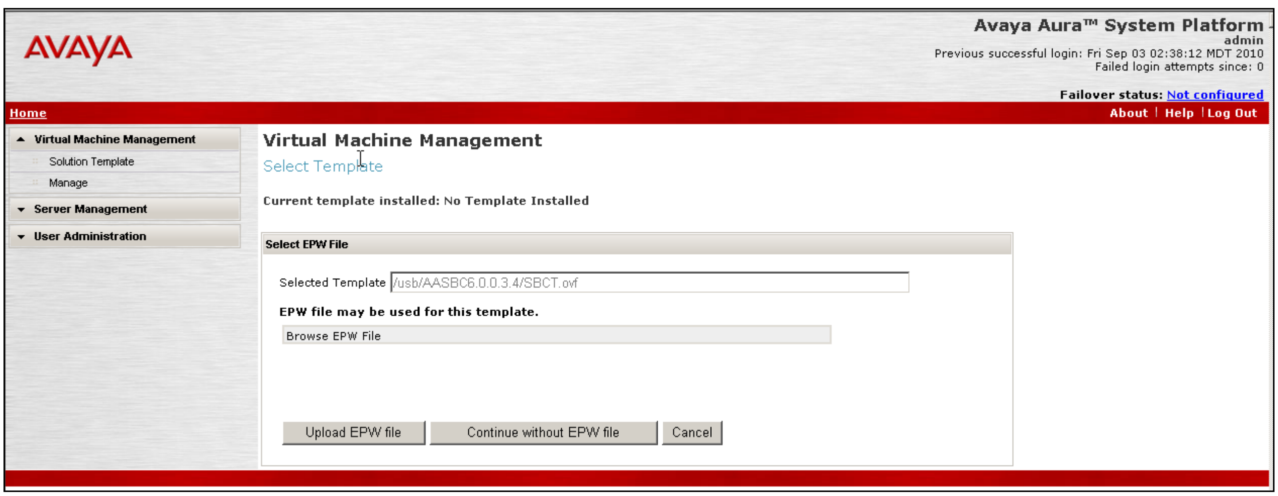

Figure 76: SBC Installation EPW screen

The **Template Details** screen is presented. If satisfied that the information is correct, click the **Install** button.

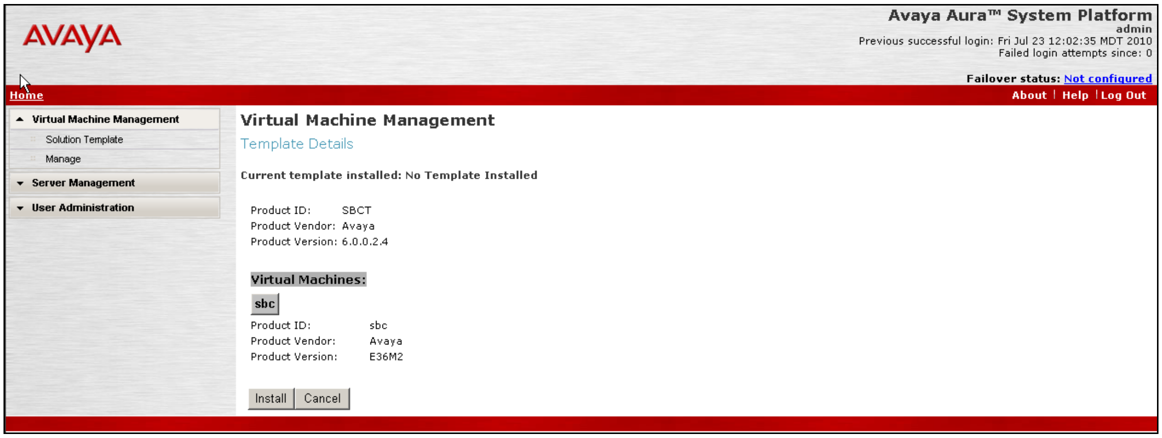

Figure 77: SBC Installation Template Details screen

The installation will proceed until user input is expected, as shown below. The following shows the first screen in a series, beginning with **Network Settings**. The SystemDomain Domain-0 IP Address, Console Domain CDom IP Address, Gateway IP Address, a Network Mask and Primary DNS and Secondary DNS (if configured) are pre-populated. This information was supplied during the System Platform installation. Enter the **IP Address** to be assigned to the SBC (e.g. **10.80.130.12**) and **Hostname** and click on **Next Step**. This IP Address becomes the private, inside IP Address as well as the management address for the Session Border Controller.

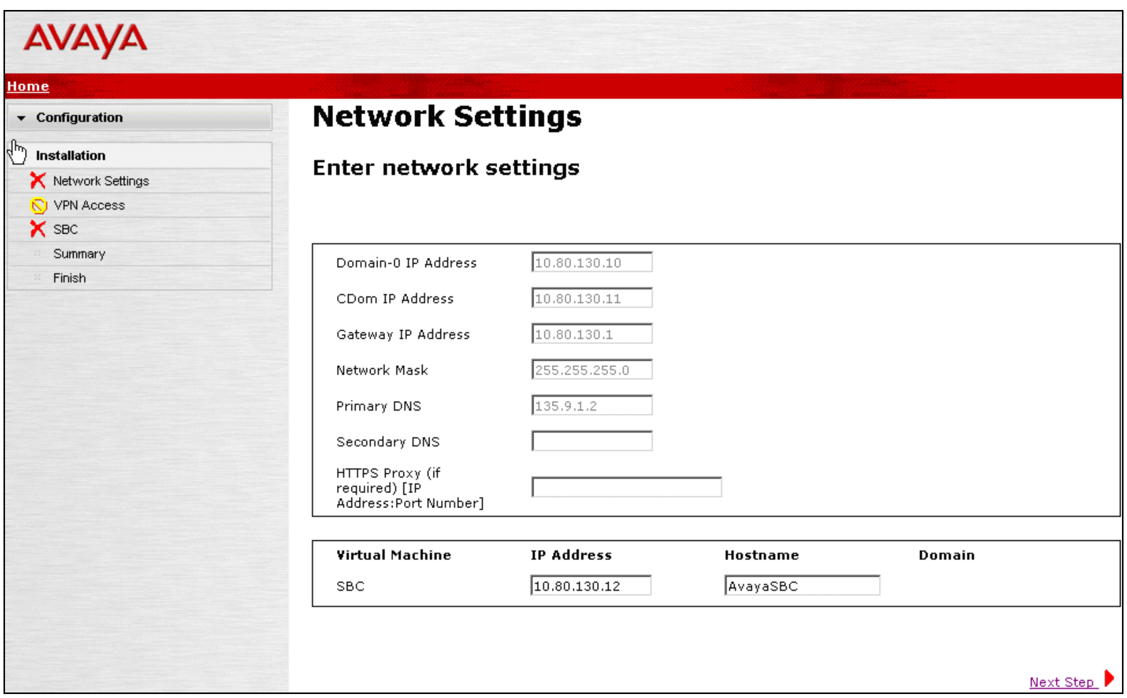

Figure 78: SBC Installation Network Settings screen

The resulting screen (not shown) allows VPN Access parameters to be configured. Configure as appropriate, or skip, and click **Next Step**. In this reference configuration, this step was skipped.

The following screen shows the Session Border Controller Data entry screen. Note that the Private (Management) Interface information has already been completed with the IP Address (10.80.130.12) provided as the **Virtual Machine IP Address** on the first screen of the series. Configure the **SIP Service Provider Data** section as follows:

- **Service Provider** – Set to **AT&T**
- **IP Address** – Set to the AT&T Border Element IP Address
- **Port** – Port number for the SIP Signaling port
- **Media Network** – Set to the AT&T Media Network
- **Media Netmask** – Set to the AT&T Media Netmask

Configure the **SBC Network Data** (Public section) as follows:

- **IP Address** – IP Address of the public interface of the Session Border Controller
- **NetMask** – Netmask for the public IP interface of the Session Border Controller
- **Gateway** – IP Address of the Gateway for the public side of the Session Border Controller

Configure the **Enterprise SIP Server** section as follows:

- **IP Address** – Set to IP Address of the Session Manager network Interface configured in Section 4.6.1.
- **Transport** – Set to **TCP** in Reference Configuration; **TLS** may be used in production environment.
- **SIP Domain** – Set to **avaya.com**
- Click **Next Step**

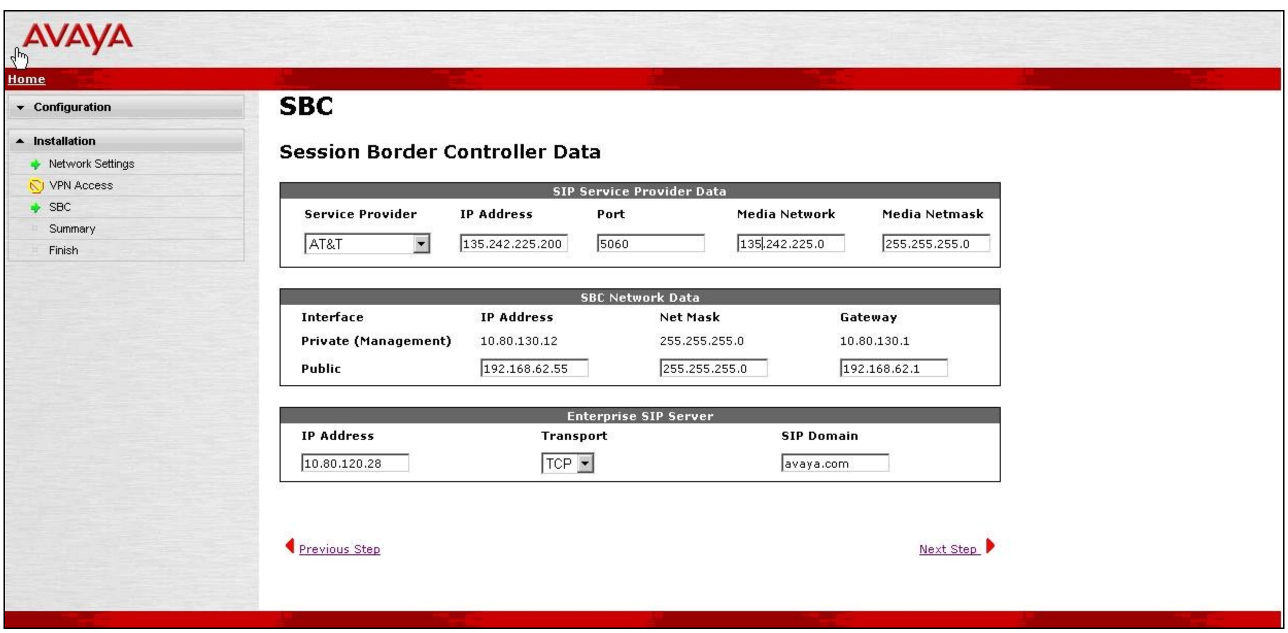

Figure 79: SBC Installation Session Border Controller Data

A summary screen will be presented. The sample configuration is shown in the lower portion of the summary screen.

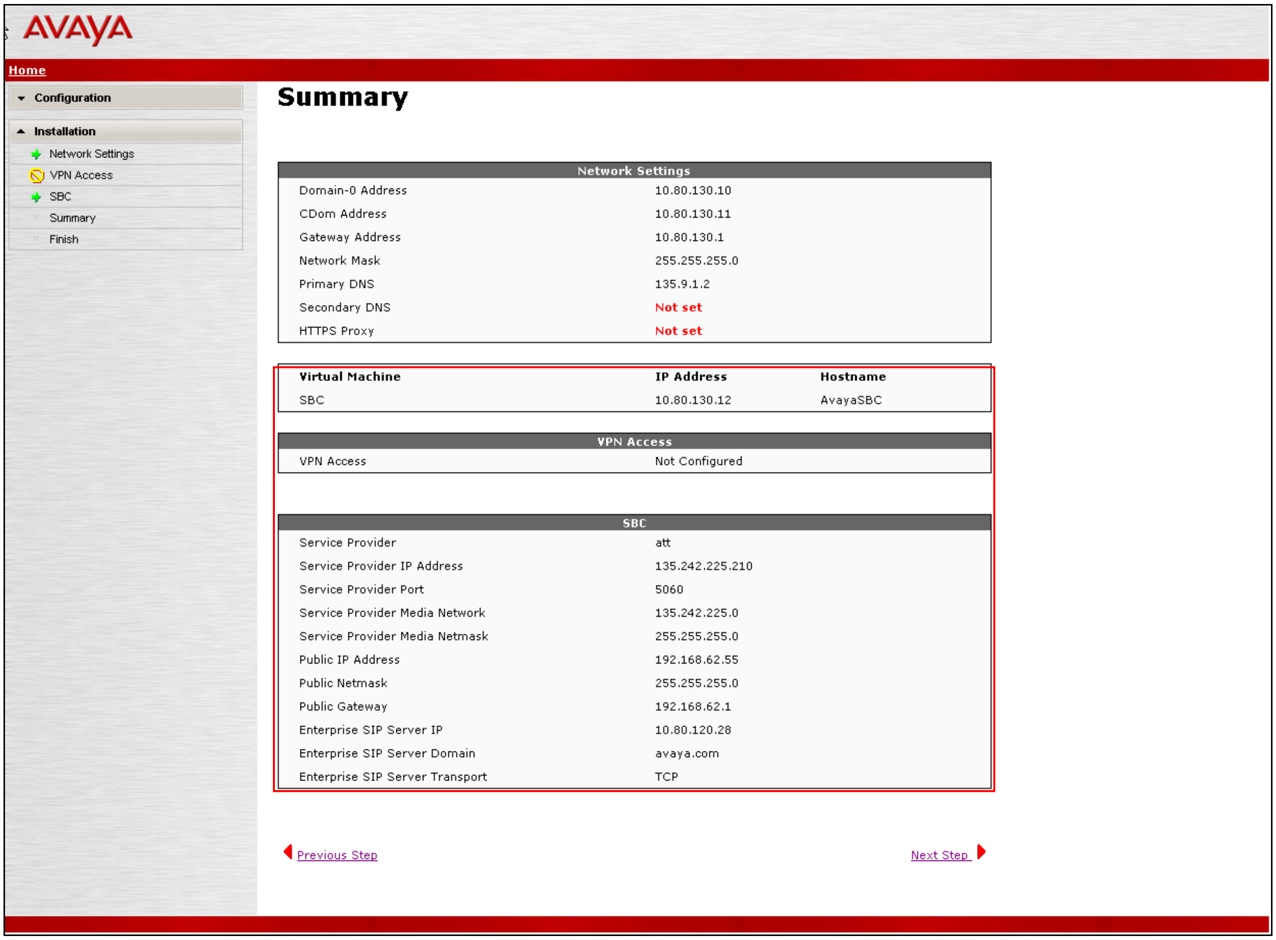

Figure 80: SBC Installation Summary

Click **Next Step** and the **Confirm Installation** screen is presented. After reading and heeding the Warning, click the **Accept** button if satisfied. Click **Install** button to proceed at the screen shown below.

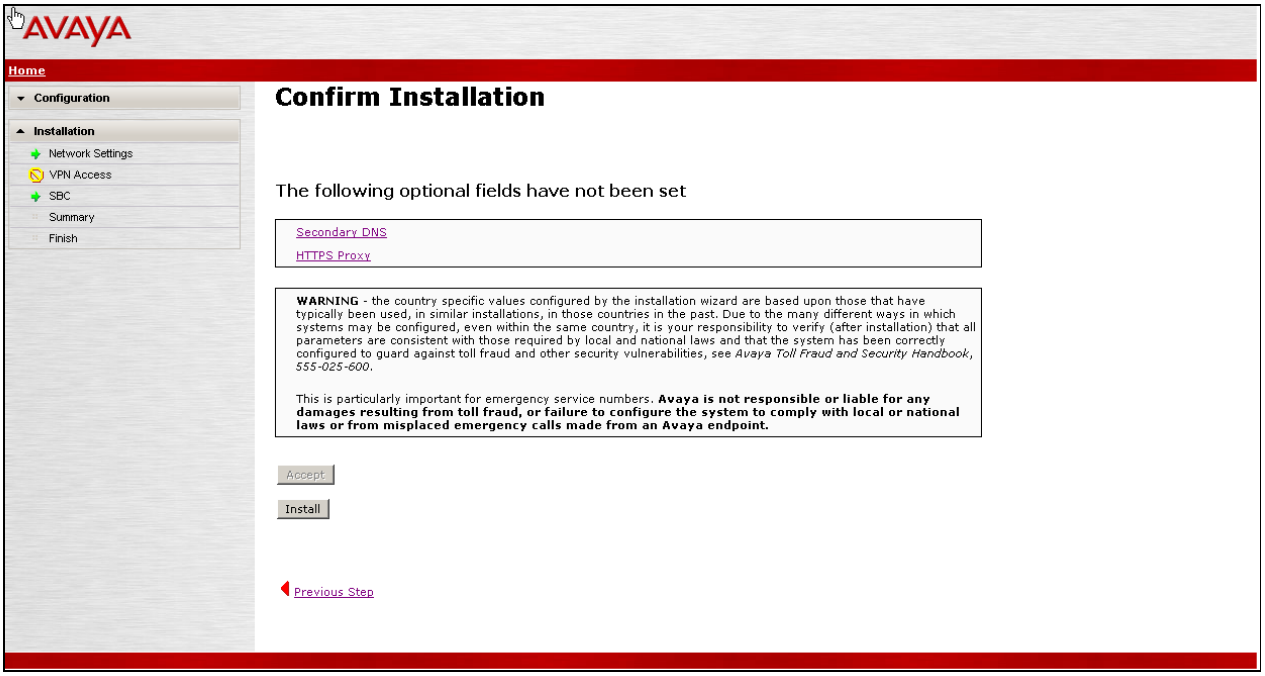

Figure 81: SBC Installation Confirm Installation

The Virtual Machine Management window, which had previously been at the "Wait for User to Complete Data Entry" step, is now proceeding with other aspects of the installation, as shown below.

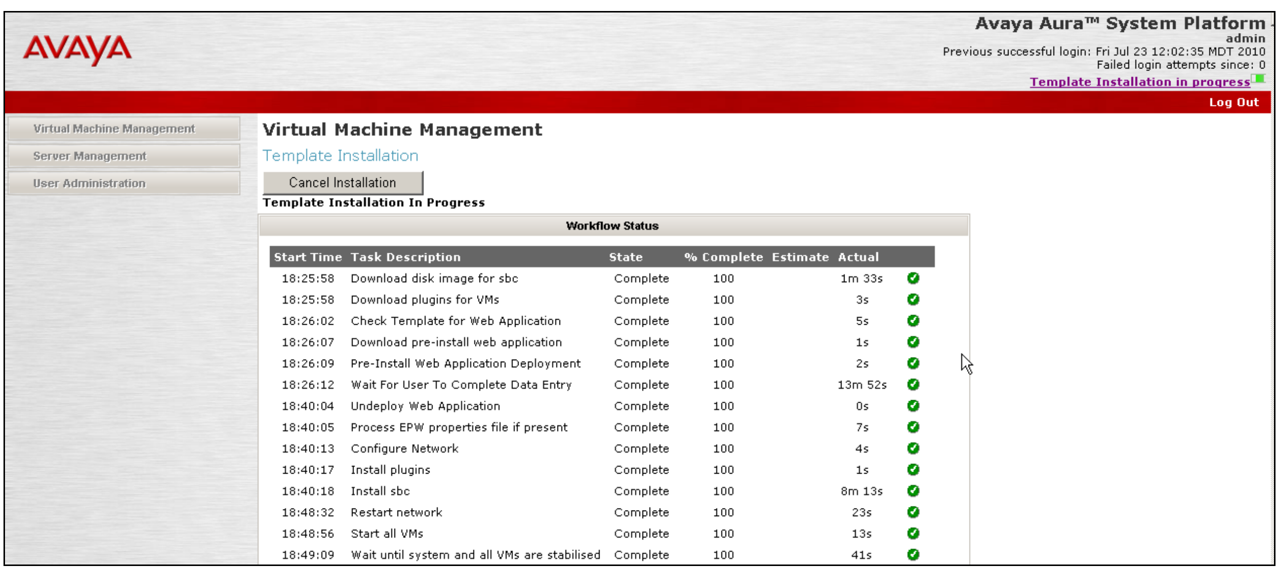

Figure 82: SBC Installation Template Installation Progress

Wait for the “Finalize Installation” task to reach the Complete State, as shown below. This same information is available via the **View Install/Upgrade Log** link on the left.

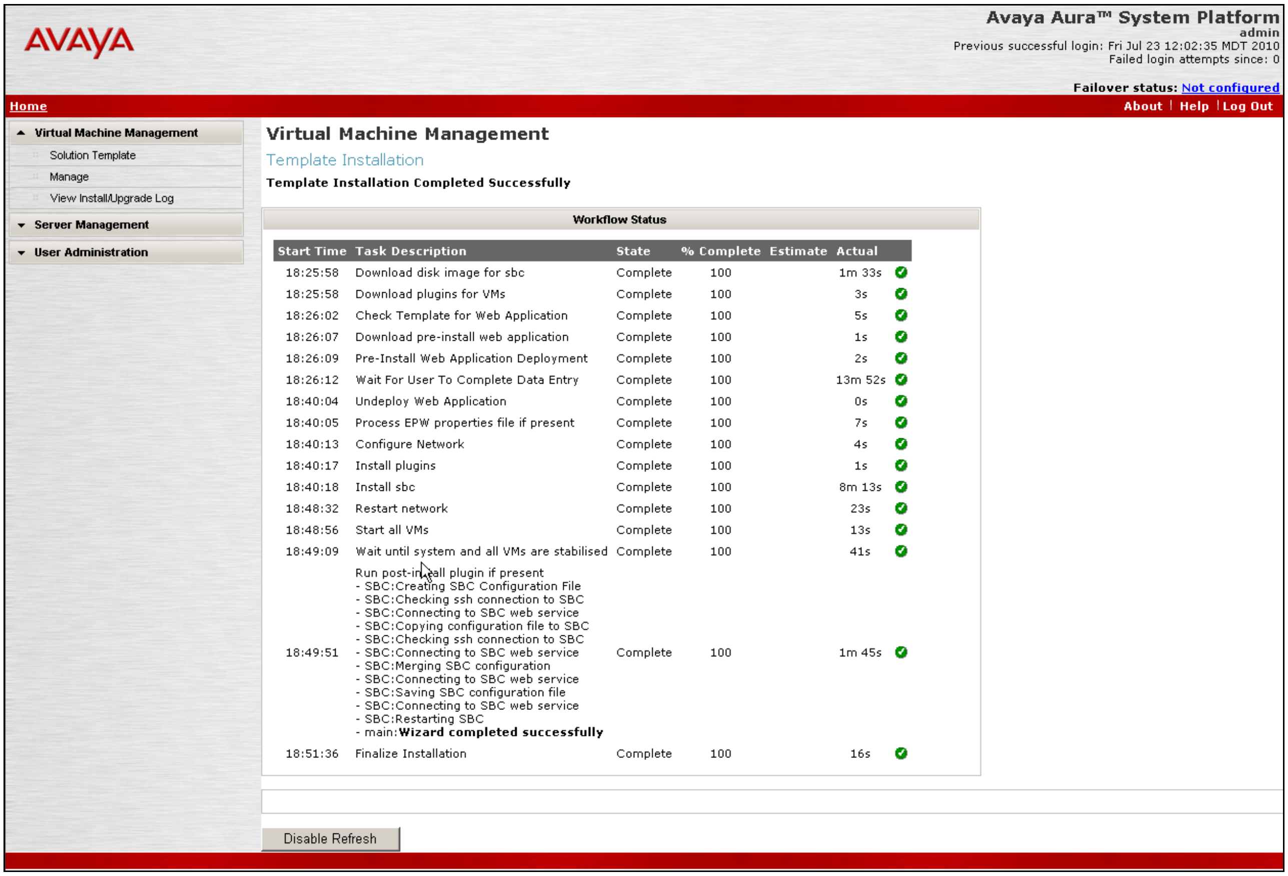

Figure 83: SBC Installation Template Installation Completed

Once the SBC template install has completed, select **Virtual Machine Management** on the left. Now, the Virtual Machine List shows that the SBC Template is installed.

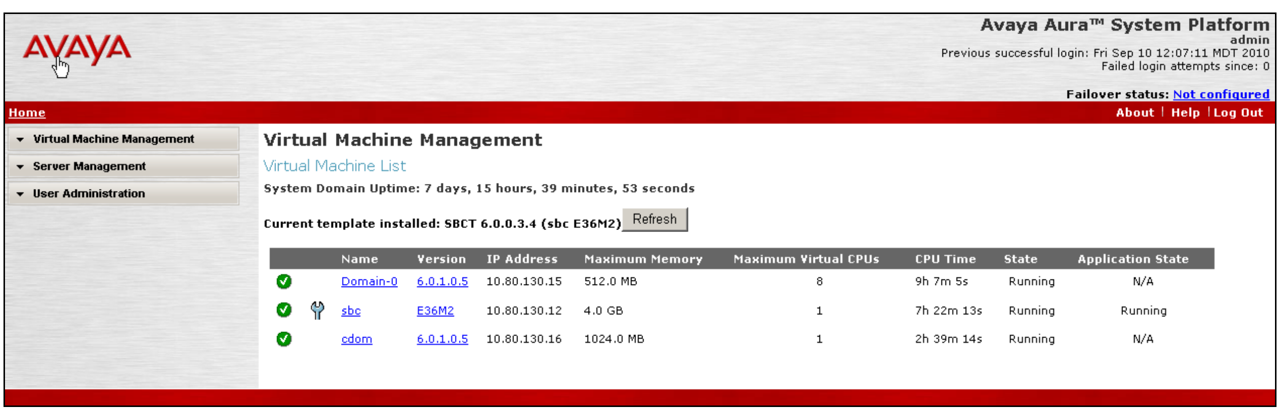

Figure 84: System Platform Virtual Management Screen with SBC installed

7.2. Avaya Aura™ Session Border Controller Configuration

After the installation wizard is completed, and proper service provider (i.e. AT&T) is selected, there would be no need to do any further configuration in future releases. However, in the current release of the Session Border Controller, some additional configuration needs to be performed through the GUI on the SBC. The configuration screens will be familiar to the reader experienced with the Acme Packet Net-Net OS-E.

7.2.1. Login and License Installation

To log in, either select the wrench 

icon shown in the prior screen, or enter the https://<ip-addr> where <ip-addr> is the management IP Address of the SBC. Enter appropriate **Username** and **Password** and click **Login**.

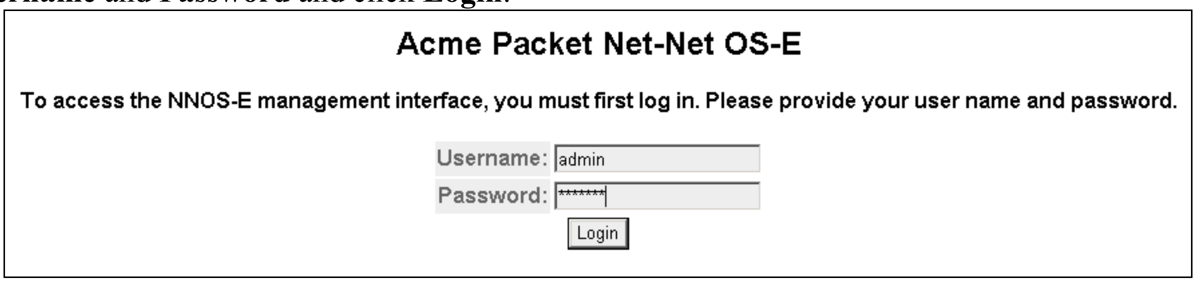

Figure 85: SBC Configuration Login screen

Following **Home** screen appears. Note the box-identifier field. This is required for obtaining the license. **Please acquire licenses prior to proceeding with other configuration steps**.

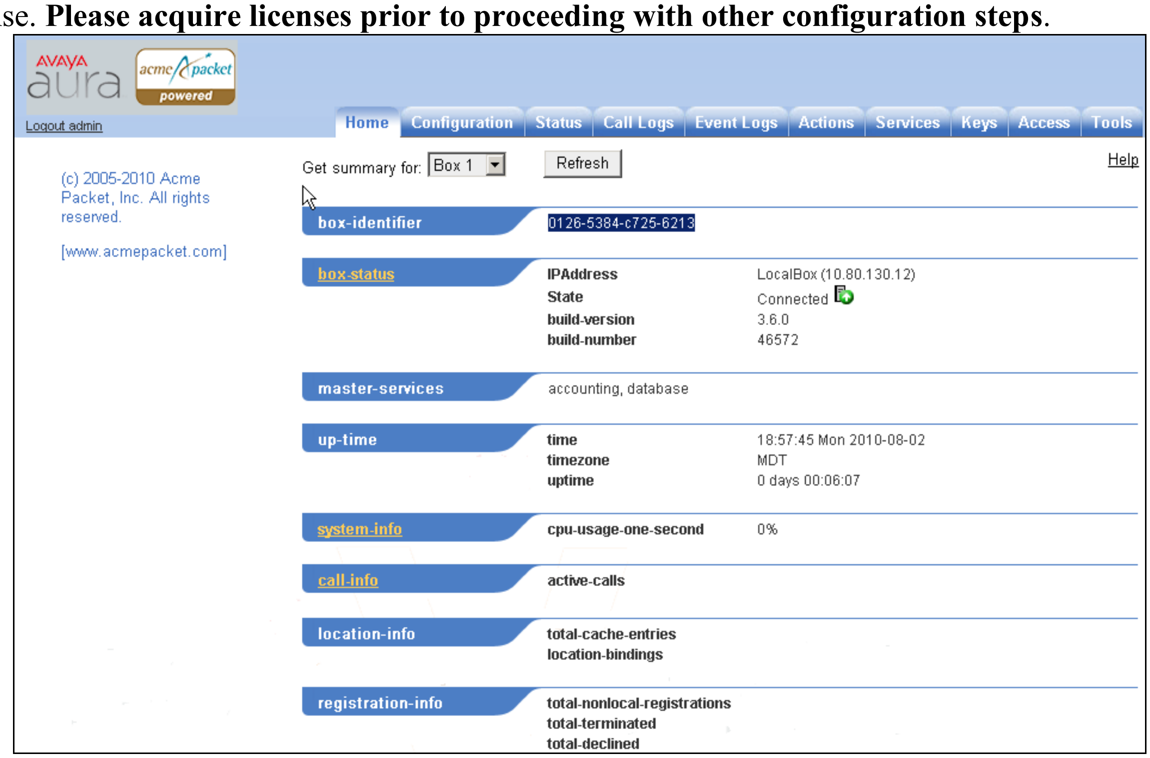

Figure 86: SBC Configuration Home screen

- Click the **Tools** tab and select the **Upload license file** from the left pane.
- Select the location where the license file is located.
- Check the **Apply License** box.
- Click **Upload.**
- If the license install is successful, a message is displayed.
- Click the **Configuration** tab.
- On the Configuration screen (not shown), click on **Configuration** in the left pane and select **Update and save configuration.**
- Click the **Actions** tab and select **restart** from the left pane to reboot SBC.
- After the reboot the SBC, the license is enabled.

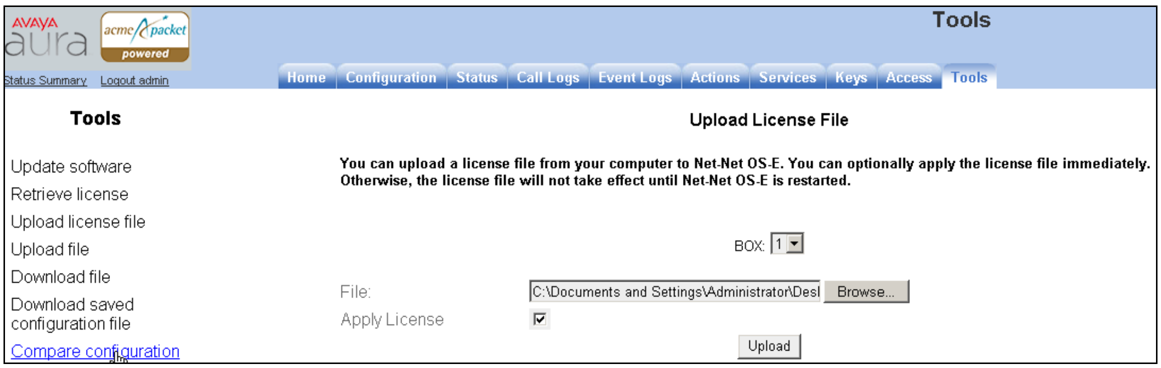

Figure 87: SBC Upload License File screen

7.2.2. Stripping SIP Headers

Session Border Controller can be used to strip SIP headers. For headers that have relevance only within the enterprise, it may be desirable to prevent these header from being sent to the public SIP Service Provider. For example, Session Manager Release 6 inserts the P-Site header and the following procedures may be used to strip it.

- Select the **Configuration** tab. Using the menu on the left hand side, select **vsp → default-session-config**, then locate **header-settings** under the **header:** section as shown in the screen below. Select the **Configure** link on the right.

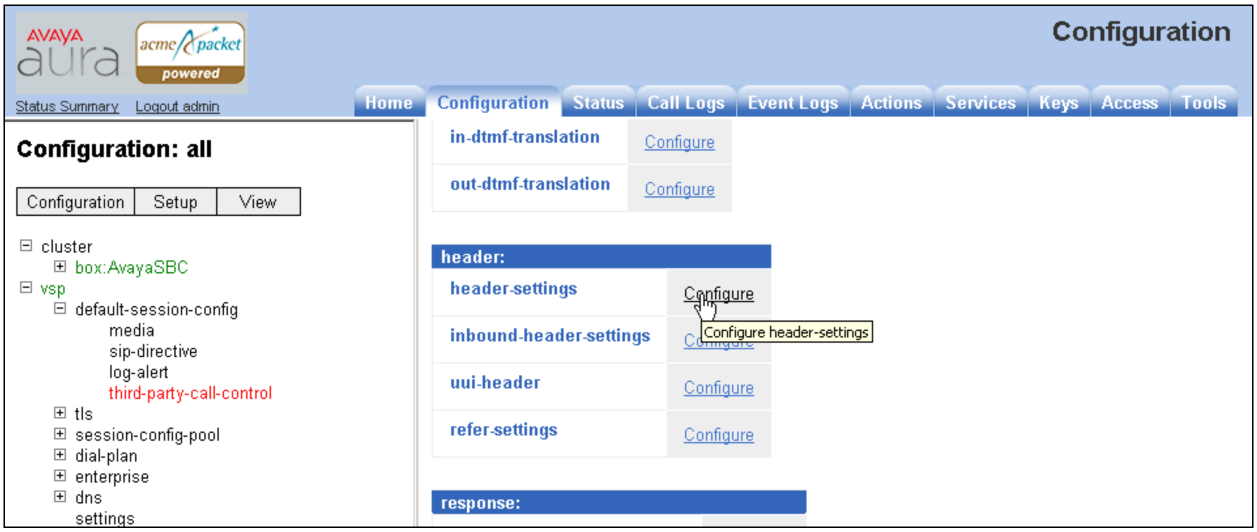

Figure 88: SBC Configuration header-settings

- In the subsequent screen (not shown) click **Edit blocked-header** and the following screen is displayed. Enter the header **P-Site** to be blocked and click **OK**.

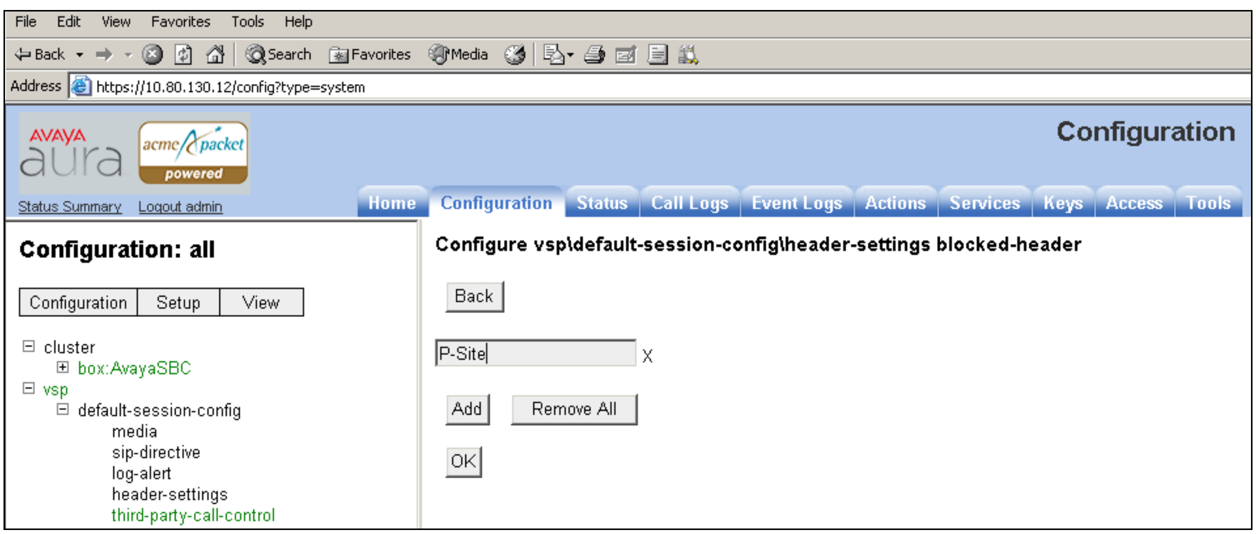

Figure 89: SBC Configuration blocked-header Entry

- The following screen is displayed indicating that P-Site header is configured to be blocked. Click **Set**.

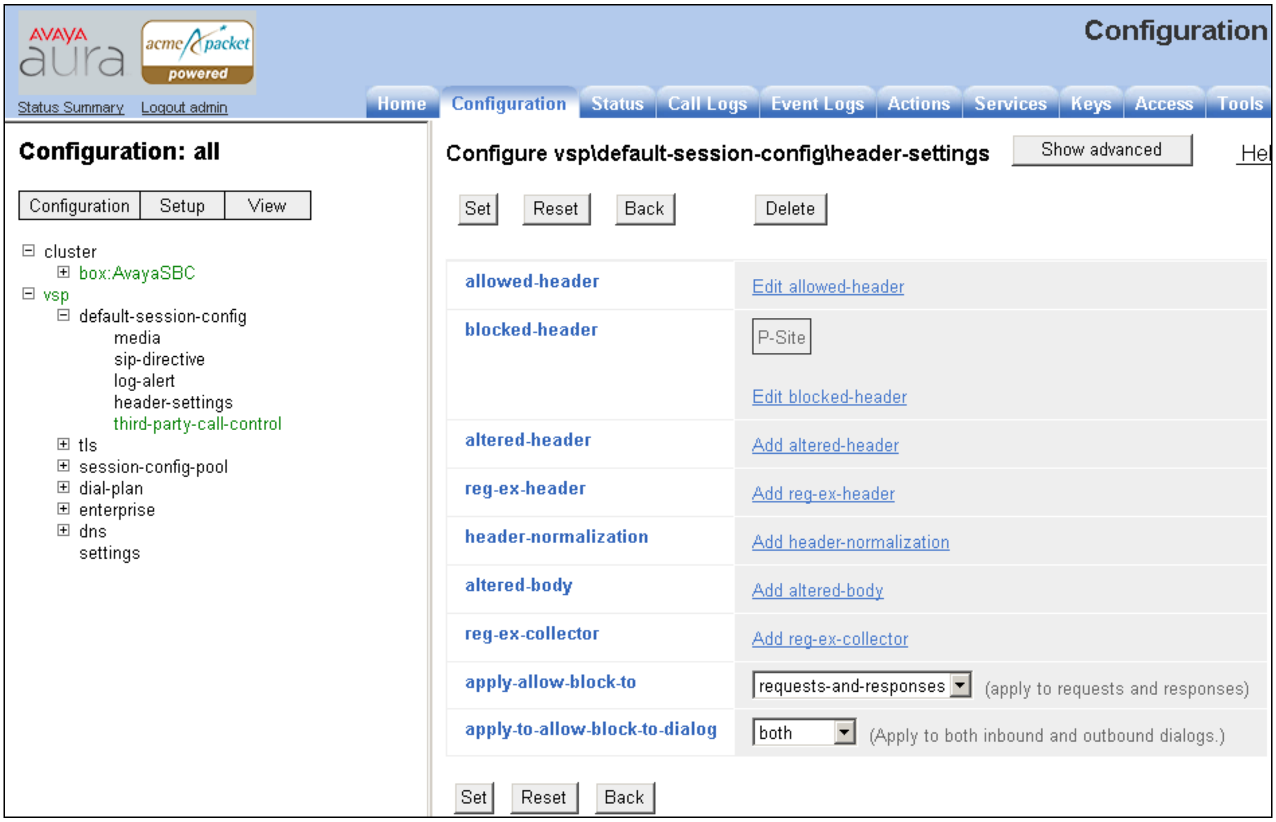

Figure 90: SBC Configuration blocked-header

7.2.3. ICMP Configuration For AT&T OPTIONS Message Response

Navigate to **cluster→box:AvayaSBC→interface eth2→ip outside** and click on **Configure** for **icmp** to allow Session Border Controller to respond to OPTIONS messages from AT&T Border Element.

Figure 91: SBC Configuration ICMP

- Select **enabled** in the **admin** field and click **Set**.

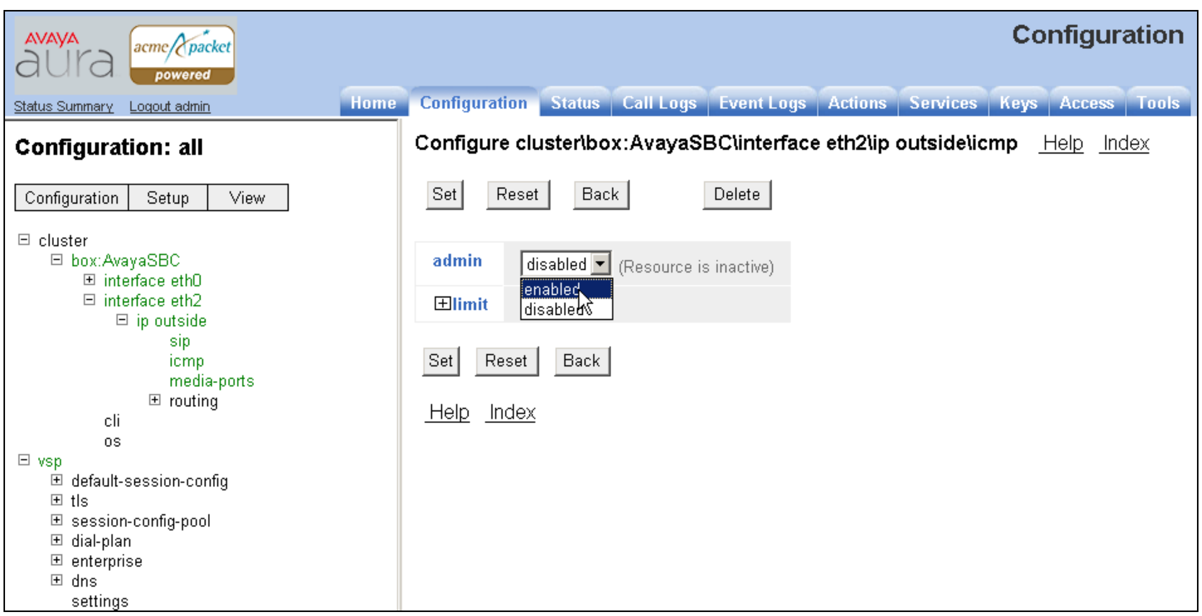

Figure 92: SBC Configuration Enable ICMP Admin

7.2.4. Contact Header Update

To enable the contact header to be updated after calls are transferred for both inbound and outbound calls, following configuration needs to be done:

1. Disable Third Party Call Control
    - To disable third party call control, navigate to **vsp → default-session-config → third-party-call-control** and select **disabled** in the **admin** field. Click **Set**.

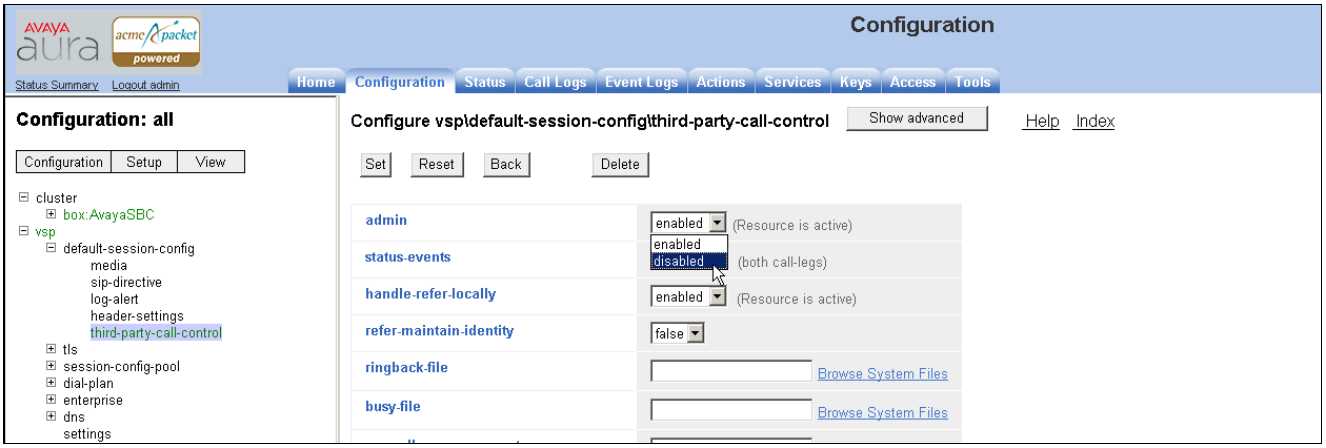

Figure 93: SBC Configuration Disabling Third Party Call Control

2. Enable Use Incoming Contact for both inside and outside leg for calls coming into PBX from AT&T IP Toll Free service.
    - Navigate to **vsp → enterprise→servers→sip-gateway PBX→vsp\session-config-pool\entry ToPBX** and click **Configure** for **contact-uri-settting-in-leg**.

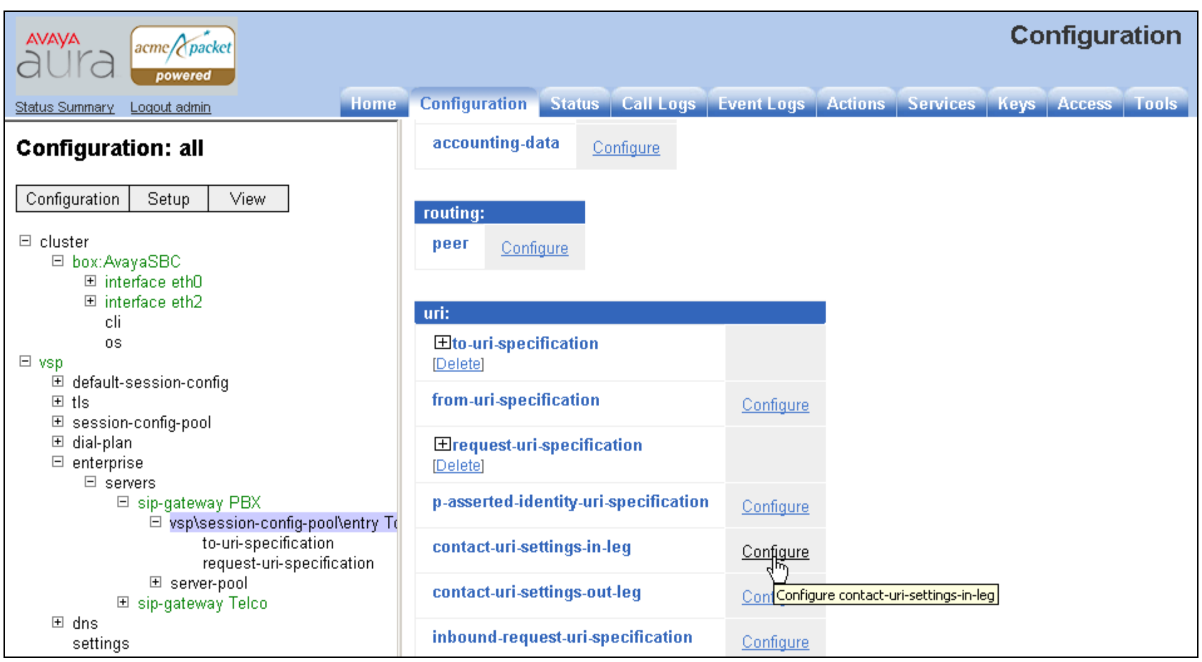

Figure 94: SBC Configuration Contact URI Settings

- Set **add-maddr** field to **disabled** and **use-incoming-contact** to **enabled** and click **Set**.

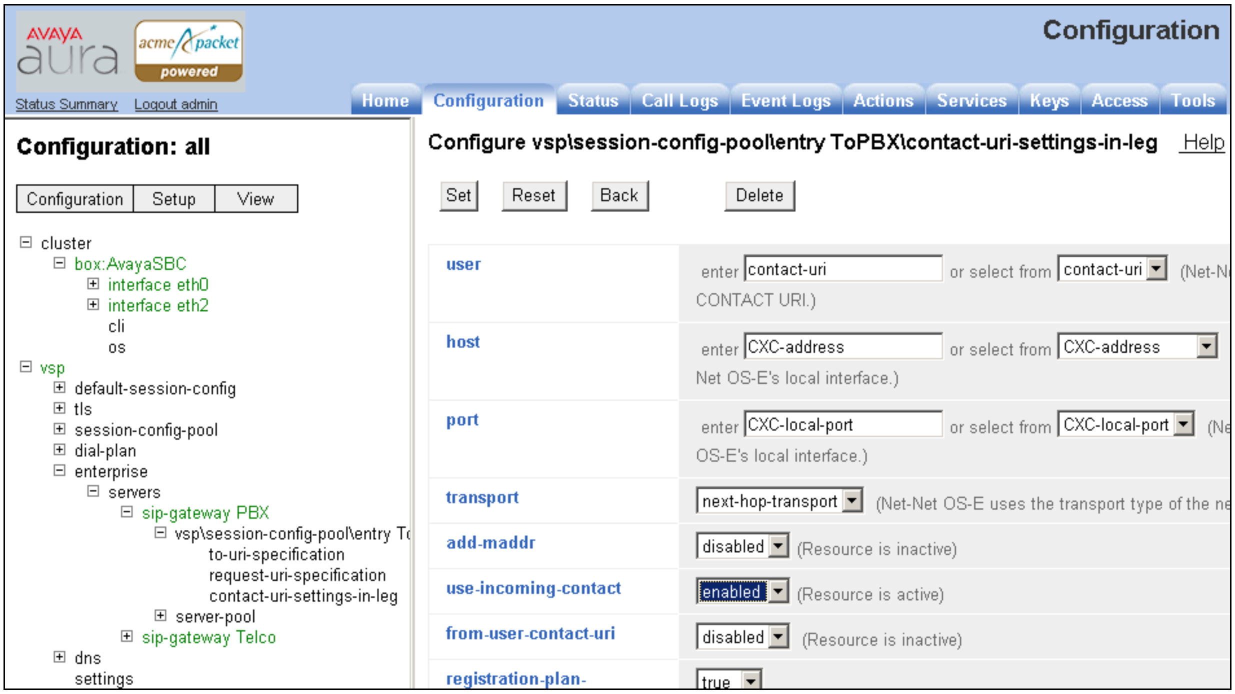

Figure 95: SBC Configuration Enabling Use Incoming Contact

- Repeat above steps to configure **contact-uri-setting-out-leg** by navigating to **vsp → enterprise→servers→sip-gateway PBX→vsp\session-config-pool\entry ToPBX**. Screen displays are not shown since they are similar to the above two figures.

7.2.5. Saving Configuration

To save and activate configuration changes, select **Configuration→Update and save configuration** from the upper left hand side of the user interface, as shown below.

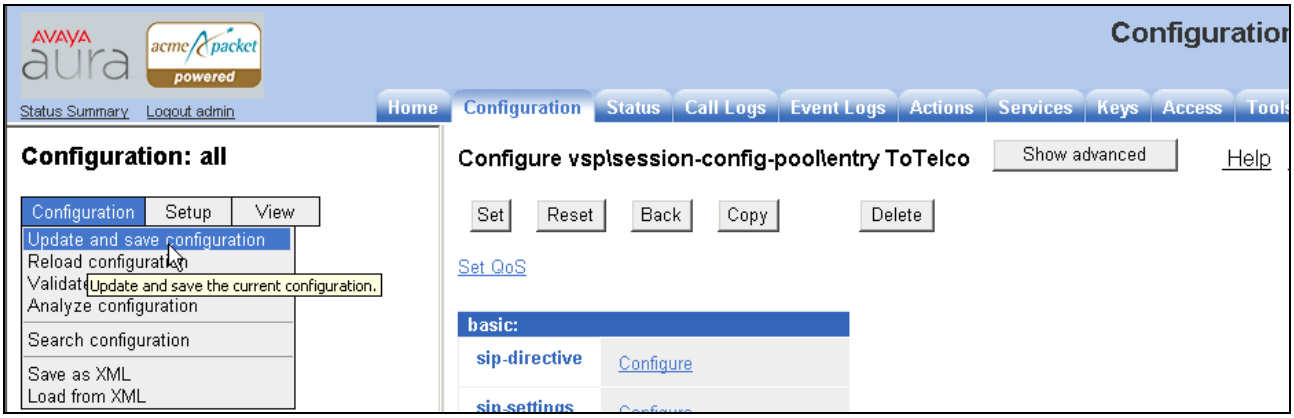

Figure 96: SBC Configuration Update and Save Configuration

The following screen indicates that the configuration was updated and saved.

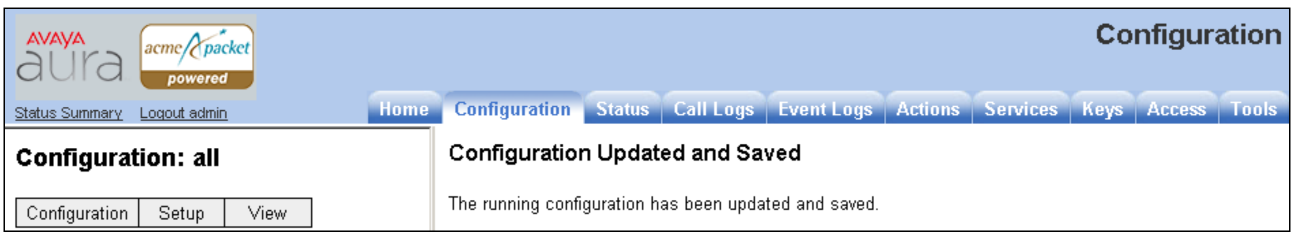

Figure 97: SBC Configuration Saved Confirmation

7.3. Avaya Aura™ Session Border Controller Element Manager Configuration

The notable settings are highlighted in bold on the pertinent settings done during installation in **Section 7.1** and further configuration in **Section 7.2**.

```
cat cxc.cfg
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#
config cluster
 config box 1
  set hostname AvayaSBC
  set timezone America/Denver
  set name AvayaSBC

  set identifier 00:ca:fe:42:98:08

  config interface eth0
   config ip inside
    set ip-address static 10.80.130.12/24
    config ssh
    return

    config snmp
     set trap-target 10.80.130.16 162
     set trap-filter generic
     set trap-filter dos
     set trap-filter sip
     set trap-filter system
    return
    config web
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return

    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
```

```
  set tls-port 5061 "" "" any 0
 return
```

config icmp
return

```
config media-ports
return
```

config routing
config route Default
set gateway 10.80.130.1
return

```
  config route Static0
   set destination network 192.11.13.4/30
   set gateway 10.80.130.15
  return
  config route Static1
   set admin disabled
  return
  config route Static2
   set admin disabled
  return
  config route Static3
   set admin disabled
  return
  config route Static4
   set admin disabled
  return
  config route Static5
   set admin disabled
  return
  config route Static6
   set admin disabled
  return
  config route Static7
   set admin disabled
  return
```

config route internal-sip-media
set destination host 10.80.120.28
set gateway 10.80.130.1
return

```
 return
return
```

```
  return

  config interface eth2
   config ip outside
    set ip-address static 192.168.62.55/25
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" any 0
    return
    config icmp
    return
    config media-ports
    return
    config routing
     config route Default
      set admin disabled
     return
     config route external-sip-media
      set destination network 135.242.225.0/24
      set gateway 192.168.62.1
     return
    return
   return
  return

  config cli
   set prompt AvayaSBC
  return
  config os
  return
 return
return
config services
 config event-log
  config file access
   set filter access info
  return
  config file system
   set filter general info
   set filter system info
  return
  config file errorlog
   set filter all error
  return
```

```
  config file db
   set filter db debug
   set filter dosDatabase info
  return
  config file management
   set filter management info
  return
  config file peer
   set filter sipSvr info
  return
  config file cac
   set filter sipCAC warning
  return
  config file dos
   set filter dos alert
   set filter dosSip alert
   set filter dosTransport alert
   set filter dosUrl alert
  return
  config file krnlsys
   set filter krnlsys debug
  return
  config file acct
   set filter acct debug
  return
 return
return
config master-services
 config accounting
 return
 config database
  set media enabled
 return
return
config vsp
 set admin enabled
 config default-session-config
  config media
   set anchor enabled
   set rtp-stats enabled
  return
  config sip-directive
   set directive allow
  return
  config log-alert
```

```
  set apply-to-methods-for-filtered-logs
 return
 config header-settings
  set blocked-header P-Site
 return

 config third-party-call-control
 return

return
config tls
 config certificate ws-cert
  set certificate-file /cxc/certs/ws.cert
 return
return
config session-config-pool
 config entry ToTelco
  config to-uri-specification
   set host next-hop
  return
  config from-uri-specification
   set host local-ip
  return
  config request-uri-specification
   set host next-hop
  return
  config p-asserted-identity-uri-specification
   set host local-ip
  return
 return
 config entry ToPBX
  config to-uri-specification
   set host next-hop-domain
  return
  config request-uri-specification
   set host next-hop-domain
  return

  config contact-uri-settings-in-leg
   set add-maddr disabled
   set use-incoming-contact enabled
  return
  config contact-uri-settings-out-leg
   set add-maddr disabled
   set use-incoming-contact enabled
```

```
  return
 return
 config entry Discard
  config sip-directive
  return
 return
return
config dial-plan
 config route Default
  set priority 500
  set location-match-preferred exclusive
  set session-config vsp\session-config-pool\entry Discard
 return
 config source-route FromTelco
  set peer server "vsp\enterprise\servers\sip-gateway PBX"
  set source-match server "vsp\enterprise\servers\sip-gateway Telco"
 return
 config source-route FromPBX
  set peer server "vsp\enterprise\servers\sip-gateway Telco"
  set source-match server "vsp\enterprise\servers\sip-gateway PBX"
 return
return
config enterprise
 config servers
  config sip-gateway PBX
   set domain avaya.com
   set outbound-session-config-pool-entry vsp\session-config-pool\entry ToPBX
   config server-pool
    config server PBX1
     set host 10.80.120.28
     set transport TCP
    return
   return
  return
  config sip-gateway Telco
   set outbound-session-config-pool-entry vsp\session-config-pool\entry ToTelco
   config server-pool
    config server Telco1
     set host 135.242.225.200
    return
   return
  return
 return
return
config dns
```

```
  config resolver
   config server 135.9.1.2
   return
  return
 return
 config settings
  set stack-socket-threads-max 2
 return
return
config external-services
return
config preferences
 config gui-preferences
 return
return
config access
 config permissions superuser
  set cli advanced
 return
 config permissions read-only
  set config view
  set actions disabled
 return
 config users
  config user admin
   set password 0x002bdd5d9fea2fefeb97b0115854a47db2c8b27a2fe0187e0274977f4b
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x004803cd9fae4ee1b2462598359d6c5e179008f9083caa7b30b9b19b43
   set permissions access\permissions read-only
  return
 return
return
config features
return
```

8. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura™ System Manager, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya Aura™ Session Border Controller, and Avaya Modular Messaging.
- A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise was connected via MIS/PNT transport.

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

- Inbound AT&T IP Toll Free service calls to Communication Manager telephones and VDNs/Vectors.
- Call and two-way talk path establishment between PSTN and Communication Manager phones via the AT&T Toll Free service..
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- T.38 fax calls between the AT&T IP Toll Free service/PSTN and Communication Manager G3/SG3 fax endpoints.
- DTMF tone transmission using RFC 2833 between the AT&T IP Toll Free service/PSTN and Communication Manager automated access systems.
- Inbound AT&T IP Toll Free service calls to Communication Manager that are directly routed to stations and, if unanswered, are covered to Avaya Modular Messaging.
- Long duration calls.

The test objectives stated in **Section 8** with limitations as noted in **Section 1.3,** were verified.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

- Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly.
- Place an inbound call to an agent or phone, but do not answer the call. Verify that the call covers to Modular Messaging voicemail. Retrieve the message from Modular Messaging.

9.2. Avaya Aura™ Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See [3] for more information.

- From the Communcation Manager System Access Terminal (SAT) enter the command ***list trace tac xxx***, where **xxx** is a trunk access code defined for the SIP trunk to AT&T (e.g. 120).

```
list trace tac 120
                                LIST TRACE
time            data
16:50:47 TRACE STARTED 09/16/2010 CM Release String cold-00.0.345.0-18444
16:51:03 SIP<INVITE sip:6665310@avaya.com:5060 SIP/2.0
16:51:03     active trunk-group 20 member 1  cid 0xcc
16:51:03 SIP>SIP/2.0 180 Ringing
16:51:03     dial 6665310
16:51:03     ring vector 10    cid 0xcc
16:51:03     G729 ss:off ps:20
             rgn:20 [10.80.130.12]:20194
             rgn:20 [10.80.111.32]:25992
16:51:03     xoip options: fax:T38 modem:off tty:US  uid:0x5003b
             xoip ip: [10.80.111.32]:25992
16:51:05 SIP>SIP/2.0 200 OK
16:51:05     tone-receiver     01AXX06 cid 0xcc
16:51:05     active announcement    33002 cid 0xcc
16:51:05     hear annc board 01A14 ext 33002 cid 0xcc
16:51:05 SIP<ACK sip:10.80.111.31;transport=tcp SIP/2.0
16:51:11     active announcement    33003 cid 0xcc
16:51:11     hear annc board 01A14 ext 33003 cid 0xcc
16:51:14     idle announcement     cid 0xcc
16:51:14     G729A ss:off ps:20
             rgn:20 [10.80.130.21]:16384
             rgn:20 [10.80.111.32]:26004
             VOIP data from: [10.80.111.32]:25992
16:51:15     Jitter:1 1 0 0 0 0 0 0 0 0: Buff:12 WC:15 Avg:1
16:51:15     Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 WC:0 Avg:0
16:51:18 SIP>UPDATE sip:3035381760@10.80.130.12:5060;transport=t
16:51:18 SIP>cp SIP/2.0
16:51:18     active station    6665013 cid 0xcc
16:51:18 SIP<SIP/2.0 200 OK
16:51:18 SIP>INVITE sip:3035381760@10.80.130.12:5060;transport=t
16:51:18 SIP>cp SIP/2.0
16:51:18 SIP<SIP/2.0 100 Trying
16:51:18 SIP<SIP/2.0 200 OK
16:51:18 SIP>ACK sip:3035381760@10.80.130.12:5060;transport=tcp
16:51:18 SIP>SIP/2.0
16:51:18     G729A ss:off ps:20
             rgn:20 [10.80.130.12]:20194
             rgn:20 [10.80.130.21]:16384
16:51:18     G729 ss:off ps:20
             rgn:20 [10.80.130.21]:16384
             rgn:20 [10.80.130.12]:20194
16:51:20 SIP>BYE sip:3035381760@10.80.130.12:5060;transport=tcp
16:51:20 SIP>SIP/2.0
16:51:20     idle station    6665013 cid 0xcc
```

Figure 98: Communication Manager *list trace tac 120* – Outbound call.

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

9.3. Avaya Aura™ Session Manager

The following commands are issued from the System Manager console.

1. Verify the call routing administration on Session Manager.
   - In the left pane of the System Manager Common Console, under **Elements/Session Manager/System Tools**, click on "**Call Routing Test**". The **Call Routing Test** page shown figure below will open.
   - In the **Call Routing Test** page, enter the appropriate parameters of the test call. The figure below shows a routing test for an inbound call from PSTN to AT&T DNIS **000001057**. The call arrives from the Session Border Controller (note that the source address of the call, **10.80.130.12**, is the "Inside" IP address of the Session Border Controller) and the calling number **3035381760**.
   - Click on "**Execute Test**".

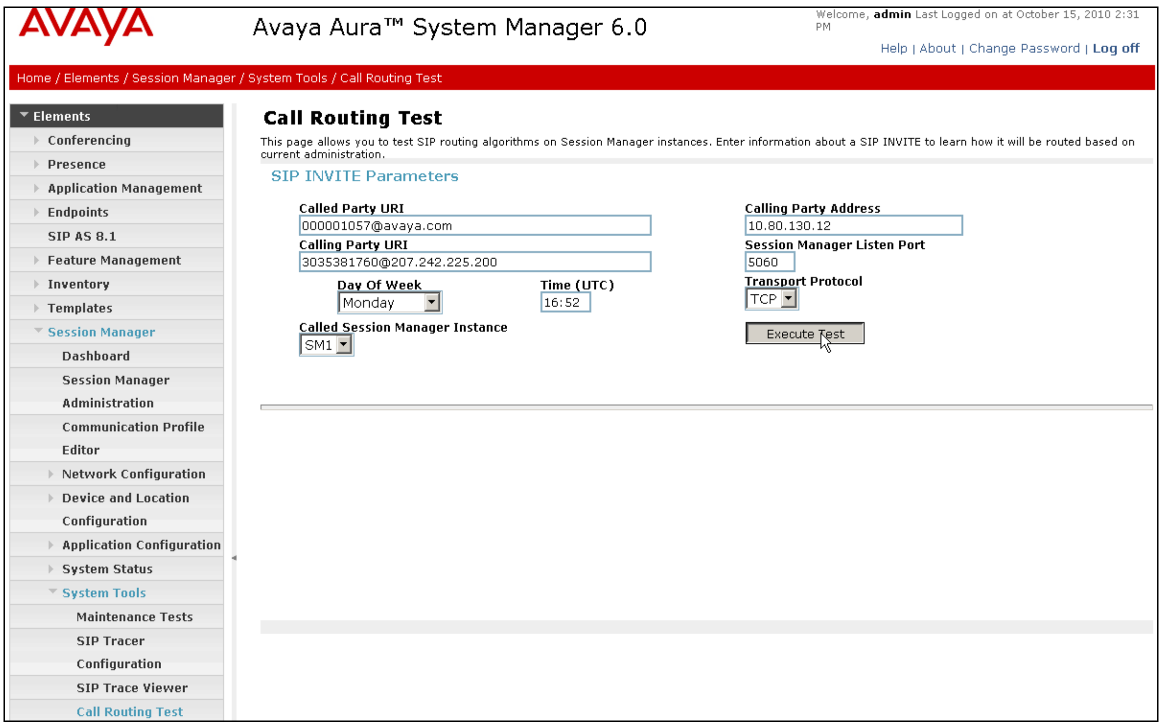

Figure 99: Session Manager Call Routing Test Page

- The results of the test are displayed as shown in figure below. The ultimate routing decision is displayed under the heading **Routing Decisions.** The example test shows that the PSTN call to **000001057** is sent by Session Manager to the Communication Manager extension **6665310**.Under that section the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated). Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 4**.

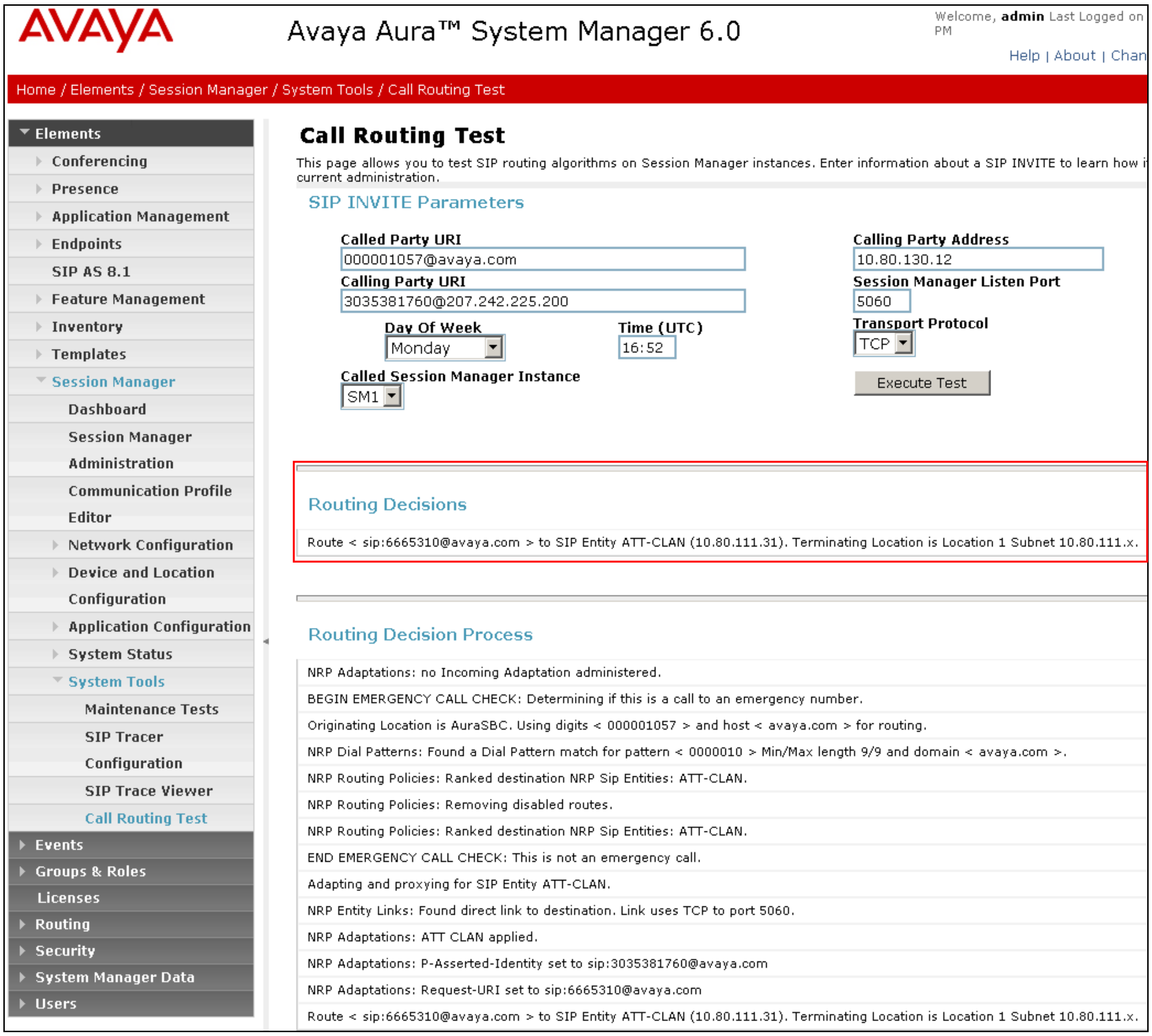

Figure 100: Call Routing Test Page -Completed

9.4. Protocol Traces

Using a SIP protocol analyzer (e.g. Wireshark), monitor the SIP traffic at the Session Border Controller "inside" interface connection to the AT&T IP Toll Free service.

1. The following are examples of inbound calls filtered for the SIP protocol.

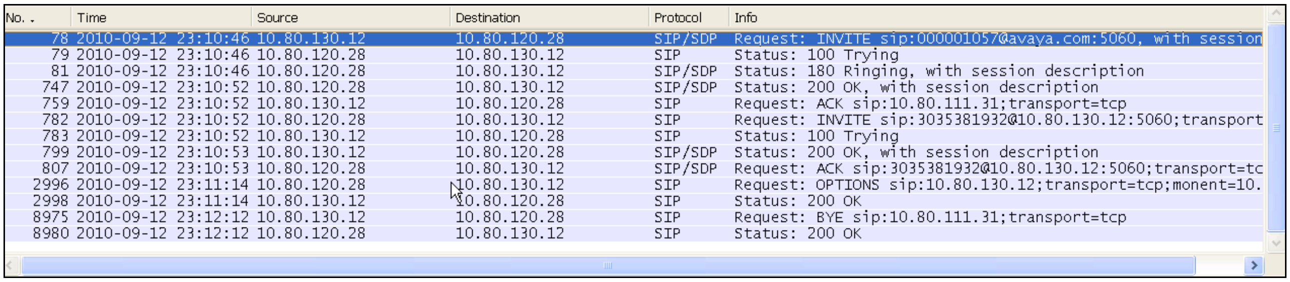

Figure 101: –SIP Protocol trace – Inbound call from AT&T

The following is an example of an inbound call filtered for RTP.

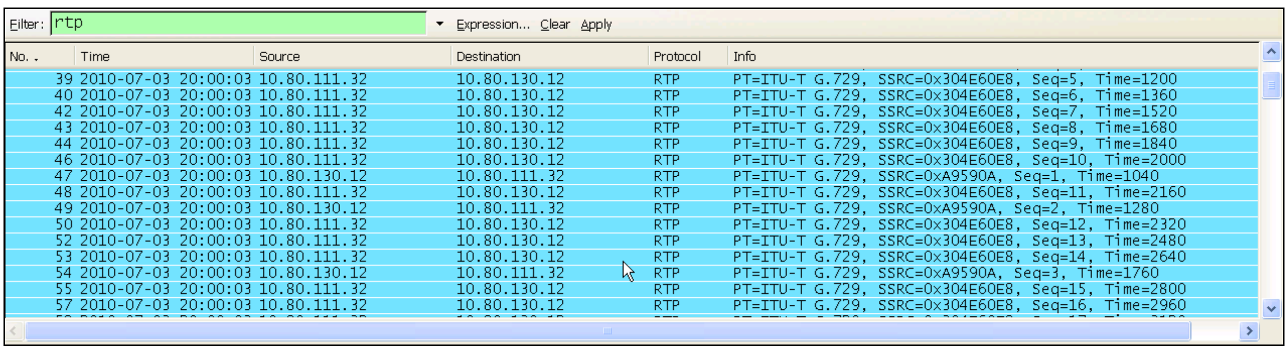

Figure 102: – RTP trace (showing codec used) – Inbound call to AT&T

9.5. Avaya Aura™ Session Border Controller

The Session Border Controller provisioning can be checked by entering the command **"show –v"**. Additionally, call logs can be verified by clicking on the **Call Logs** button (not shown) on the Session Border Controller GUI and then clicking on the **Session Diagram** for the call in question. A split screen showing the call diagram and the actual call flow will be displayed. For convenience, two separate screens are shown here.

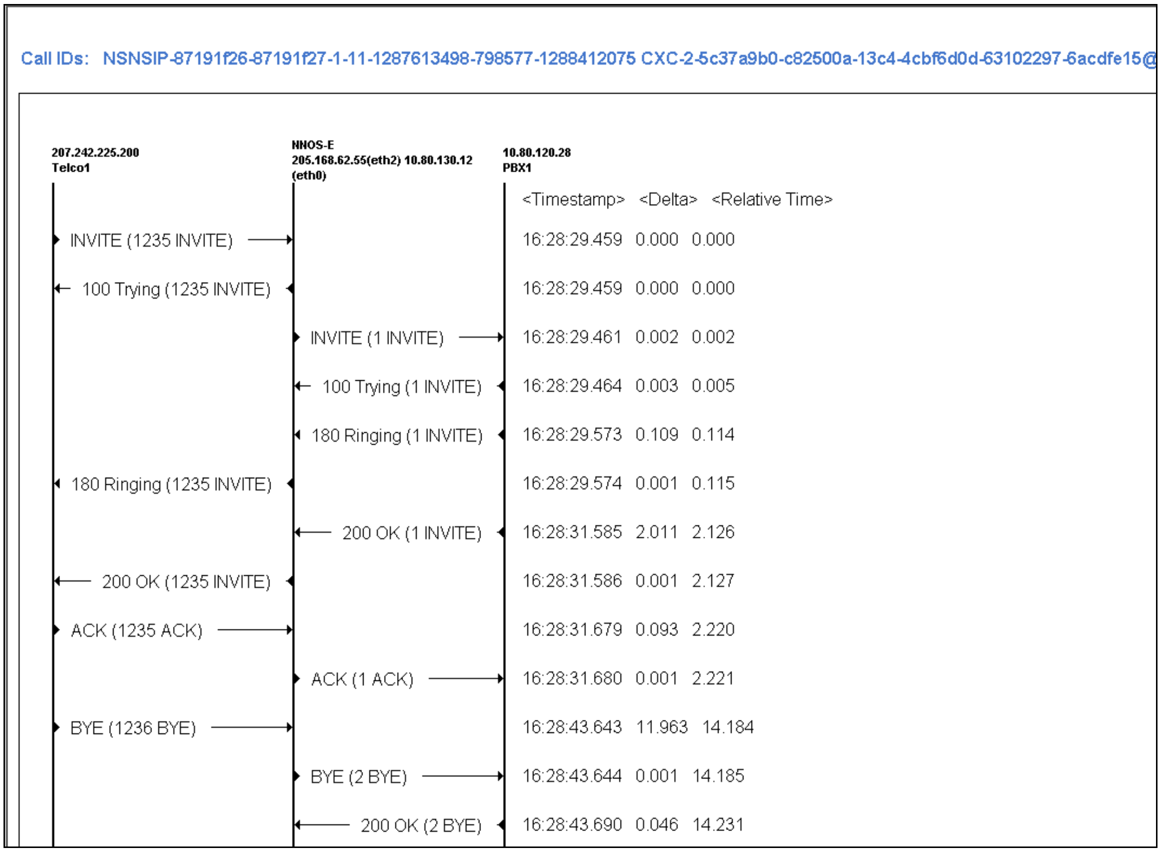

Figure 103: – Call Flow Diagram on Session Border Controller

Call Details: SIP Messages for Session0x04C2AE58ED630C1E

Time (ms)	Timestamp	Direction	Remote IP/Port	Local IP/Port	Message
0	16:28:29.459 2010-10-20	RX	207.242.225.200:5060	205.168.62.55(eth2):5060	**Message:** More INVITE sip:000001057@205.168.62.55:5060 SIP/2.0
0	16:28:29.459 2010-10-20	TX	207.242.225.200:5060	205.168.62.55(eth2):5060	**Message:** More SIP/2.0 100 Trying
2	16:28:29.461 2010-10-20	TX	10.80.120.28:5060	10.80.130.12(eth0):4278	**Message:** More INVITE sip:000001057@avaya.com:5060 SIP/2.0
5	16:28:29.464 2010-10-20	RX	10.80.120.28:5060	10.80.130.12(eth0):4278	**Message:** More SIP/2.0 100 Trying
114	16:28:29.573 2010-10-20	RX	10.80.120.28:5060	10.80.130.12(eth0):4278	**Message:** More SIP/2.0 180 Ringing
115	16:28:29.574 2010-10-20	TX	207.242.225.200:5060	205.168.62.55(eth2):5060	**Message:** More SIP/2.0 180 Ringing
2126	16:28:31.585 2010-10-20	RX	10.80.120.28:5060	10.80.130.12(eth0):4278	**Message:** More SIP/2.0 200 OK
2127	16:28:31.586 2010-10-20	TX	207.242.225.200:5060	205.168.62.55(eth2):5060	**Message:** More SIP/2.0 200 OK
2220	16:28:31.679 2010-10-20	RX	207.242.225.200:5060	205.168.62.55(eth2):5060	**Message:** More ACK sip:205.168.62.55:5060;transport=udp SIP/2.0
2221	16:28:31.680 2010-10-20	TX	10.80.120.28:5060	10.80.130.12(eth0):4278	**Message:** More ACK sip:10.80.111.31;transport=tcp SIP/2.0
14184	16:28:43.643 2010-10-20	RX	207.242.225.200:5060	205.168.62.55(eth2):5060	**Message:** More BYE sip:205.168.62.55:5060;transport=udp SIP/2.0
14185	16:28:43.644 2010-10-20	TX	10.80.120.28:5060	10.80.130.12(eth0):4278	**Message:** More BYE sip:10.80.111.31;transport=tcp SIP/2.0

Figure 104: – Call Flow Diagram on Session Border Controller

10. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and the Avaya Aura™ Session Border Controller can be configured to interoperate successfully with the AT&T IP Toll Free service. This solution provides users of Avaya Aura™ Communication Manager the ability to support inbound toll free calls over an AT&T IP Toll Free SIP trunk service connection via MIS/PNT transport. These Application Notes further demonstrated that the Avaya Aura™ Session Manager Adaptation Module could be utilized to do digit manipulation for inbound calls.

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

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

11. References

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

[1] *Installing and Configuring Avaya Aura™ Session Manager,* Doc ID 03-603473, Release 6, June 2010.
[2] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Release 6.0, June 2010
[3] *Installing and Configuring Avaya Aura™ Communication Manager*, Doc ID 03-603558, Release 6.0 June, 2010
[4] *Avaya Aura™ Communication Manager Feature Description and Implementation,* Release 6.0, 555-245-205, Issue 8.0, June 2010
[5] *Administering Avaya Aura™ Call Center Features*, Release 6.0, June 2010
[6] *Programming Call Vectors in Avaya Aura™ Call Center*, 6.0, June 2010
[7] *Modular Messaging Multi-Site Guide Release 5.1*, June 2009
[8] *Modular Messaging for Microsoft Exchange Release 5.1 Installation and Upgrades*, June 2009
[9] *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.1 Installation and Upgrades*, June 2009
[10] *Modular Messaging for IBM Lotus Domino 5.1 Installation and Upgrades*, June 2009

AT&T IP Toll Free Service Descriptions:
[11] *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.