**Avaya Solution & Interoperability Test Lab**

# Applications Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.0 and Acme Packet Net-Net 6.2.0 with AT&T IP Flexible Reach 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 Acme Packet Net-Net 6.2 with the AT&T IP Flexible Reach service using **AVPN** or **MIS/PNT** transport service connections.

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 5.2.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Acme Packet Net-Net 3800 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

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 the Acme Packet Net-Net 3800 with the AT&T IP Flexible Reach service using **AVPN** or **MIS-PNT** transport service connections.

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 5.2.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. In the reference configuration, Avaya Aura® Communication Manager 5.2.1 is provisioned in an Access Element configuration. An Acme Packet Net-Net 3800 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

## 1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 2.2** for examples) between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Acme Packet Net-Net 3800, and the AT&T IP Flexible Reach service using **AVPN**[1] or **MIS/PNT**[2] transport.

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 menus.
- PBX features such as hold, resume, conference and transfer.
- Call redirection with Diversion Header.

## 1.2. Support

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

---

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

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. Although Avaya Aura® Session Manager release 6.0 supports the possibility of using SIP phones, SIP phones are not supported by Avaya Aura® Communication Manager 5.2.1 in an Access Element configuration.
2. G.711 faxing is not supported between Avaya Aura® Communication Manager and the AT&T IP Flexible Reach 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.
3. Emergency 911/E911 Services Limitations and Restrictions - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with its equipment/software vendor.

   While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when that E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.
4. Avaya Modular Messaging 5.2 currently uses a SIP telephone event type 127 DTMF signaling (RFC2833) for the Find-Me feature. This may cause connectivity issues with AT&T IP Flexible Reach service. As a result, the Find-Me feature is not supported until it is fixed in Modular Messaging.
   a. Note – A fix for this issue included in Modular Messaging R5.2 SP5 was tested and verified.
5. Avaya Aura® Communication Manager 6.0 currently uses a SIP RFC 2833 telephone event type 127 for the Extend-Call feature. This may cause connectivity issues with AT&T IP Flexible Reach service. As a result, the Extend-Call feature is not supported.
6. Avaya Network Call Redirection (NCR) must be disabled (default) on the Avaya Aura® Communication Manager SIP trunk to the AT&T Flexible Reach service. Otherwise, connectivity issues may result in call scenarios involving Hold being signaled with "sendonly" (Communication Manager signals Hold with "sendonly" only when NCR is enabled).

7. Avaya one-X® Communicator does not currently support G.729B codec, therefore Avaya Aura® Communication Manager renegotiates the call to G.729A to support Direct IP-to-IP media.

# 2. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** 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. Avaya Aura® 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.

- Avaya Aura® System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.

- Avaya Aura® Communication Manager Access Element provides the voice communications services for a particular enterprise site, including H.323 and Digital endpoints. In this reference configuration, Avaya Aura® Communication Manager runs on an Avaya S8720 Server. This solution is extensible to other Avaya S8xxx Servers.

- The Avaya Media Gateway provides the physical interfaces and resources for Avaya Aura® Communication Manager. In this 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, Avaya 6400 Series Digital Telephones, and Avaya one-X® Communicator, a PC based softphone configured to use H.323 protocol in the reference configuration.

- The Acme Packet Net-Net 3800[3] provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network.

- An existing Avaya Modular Messaging system (in Multi-Site mode in this reference configuration) provides the corporate voice messaging capabilities in the reference configuration. However the provisioning of Modular Messaging is beyond the scope of this document.

[3] Although an Acme Net-Net 3800 was used in the reference configuration, the 4250, 4500, and 9200 platforms are also supported.

- Outbound calls were originated from a phone or fax provisioned on Communication Manager. Signaling passed from Communication Manager to Session Manager and on to the Acme Packet Net-Net 3800, before being sent to the AT&T network for termination. Media was sent from the calling phone to the Communication Manager Media Processor initially on call setup, but when applicable, the media was redirected directly from the station ("shuffled") via the Acme Packet Net-Net 3800.

- Inbound calls were sent from AT&T, through the Acme Packet Net-Net 3800 to the Session Manager which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate phone or fax extension. The H.323 phones on the enterprise side registered directly to the Communication Manager Control LAN (C-LAN).

- Enterprise sites may have additional or alternate routes to PSTN using analog or digital TDM trunks. However these trunks were not available in the reference configuration.

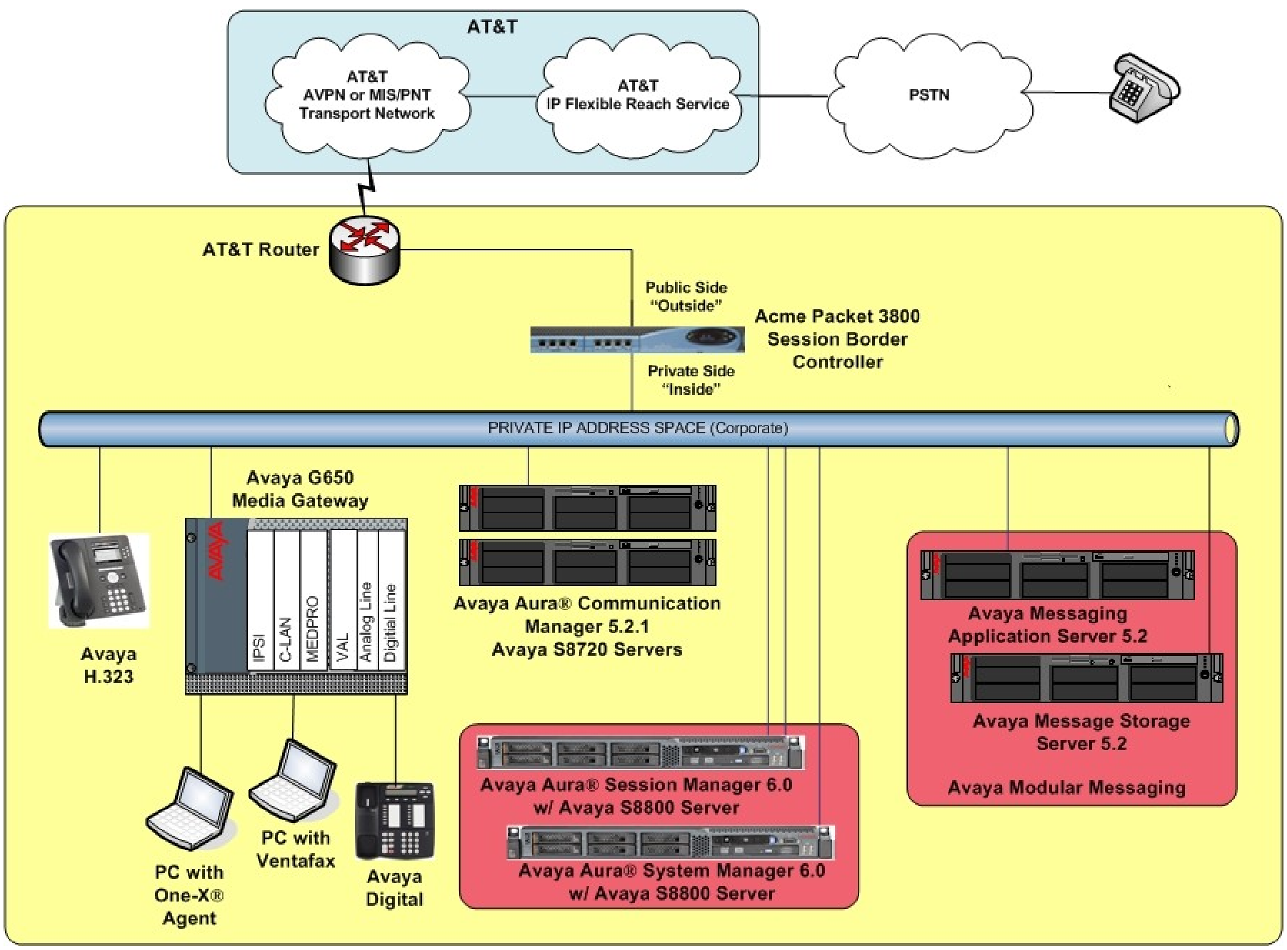



**Figure 1: Reference configuration**

## 2.1. Illustrative Configuration Information

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

**Note** - The AT&T IP Flexible Reach service border element IP address shown in this document is an example. AT&T Customer Care will provide the actual IP address as part of the AT&T IP Flexible Reach provisioning process.

| Component | Illustrative Value in these Application Notes |
|---|---|
| **Avaya Aura® System Manager** | |
| Management IP Address | 192.168.67.207 |
| **Avaya Aura® Session Manager** | |
| Management IP Address | 192.168.67.209 |
| SIP signaling IP Address | 192.168.67.210 |
| **Avaya Aura® Communication Manager** | |
| C-LAN IP Address | 192.168.67.14 |
| Avaya Aura® Communication Manager extensions | 26xxx |
| Avaya CPE local dial plan | 17231126xxx |
| Voice Messaging Pilot Extension | 26000 |
| **Avaya Modular Messaging** | |
| Messaging Application Server (MAS) IP Address | 192.168.67.141 |
| Messaging Server (MSS) IP Address | 192.168.67.140 |
| Pilot Number | 17231126000 |
| **Acme Packet SBC** | |
| IP Address of "Outside" (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service) | 192.168.64.130 (active) |
| IP Address of "Inside" (Private) Interface (connected to Avaya Aura® Session Manager) | 192.168.67.130 (active) |
| **AT&T IP Flexible Reach Service** | |
| Border Element IP Address | 135.25.29.74 |
| AT&T Access router interface (to Acme outside) | 192.168.64.254 |
| AT&T Access Router NAT address (Acme outside address) | 135.16.170.55 |

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

## 2.2. Call Flows

To understand how inbound AT&T IP Flexible Reach service calls are handled by Session Manager and Communication Manager, three basic call flows are described in this section, however for brevity not all possible call flows are described.

### 2.2.1. Inbound

The first call scenario illustrated in **Figure 2** is an inbound AT&T IP Flexible Reach 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 Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service routes the call to the Acme Packet SBC.
4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone, a fax or a vector.

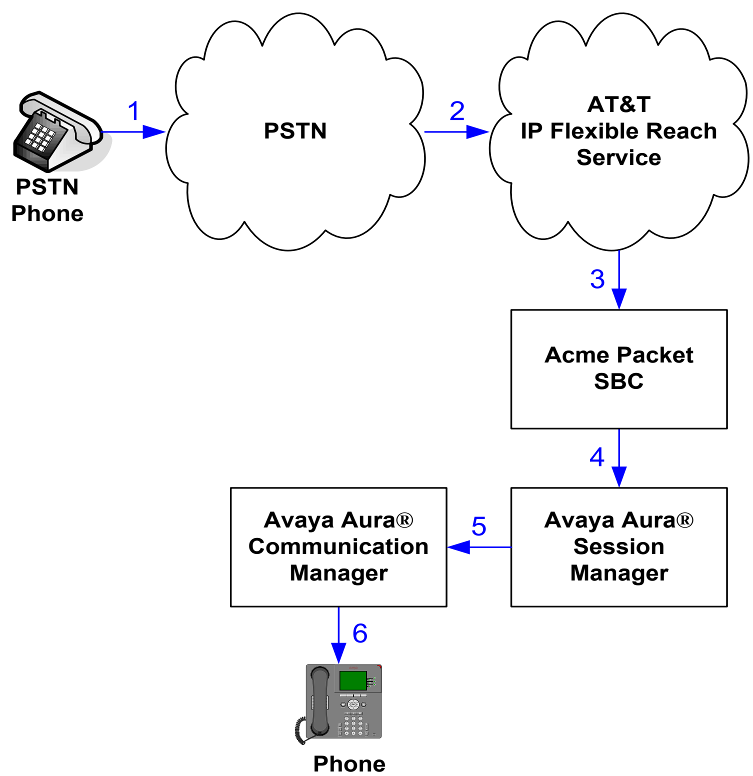



**Figure 2: Inbound AT&T IP Flexible Reach Call**

## 2.2.2. Outbound

The second call scenario illustrated in **Figure 3** is an outbound call initiated on Communication Manager, routed to Session Manager and is subsequently sent to the Acme SBC for delivery to AT&T IP Flexible Reach service.

1. An Communication Manager phone or fax originates a call to an AT&T IP Flexible Reach service number for delivery to PSTN.
2. Communication Manager routes the call to the Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to the Acme Packet SBC.
4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach service.
5. The AT&T IP Flexible Reach service delivers the call to PSTN.

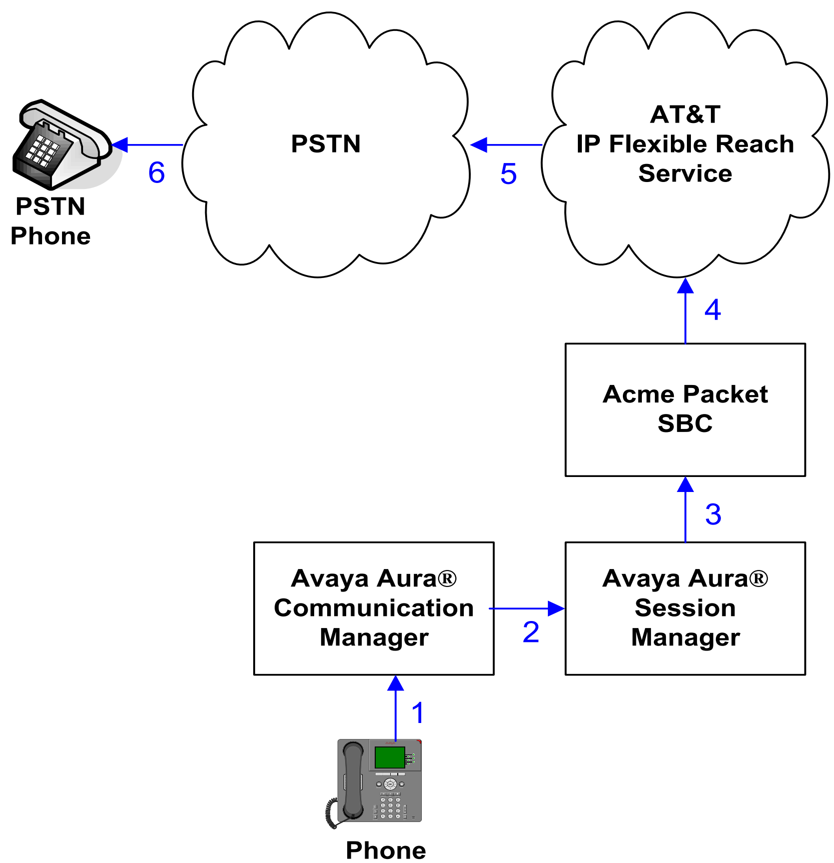



**Figure 3: Outbound AT&T IP Flexible Reach Call**

### 2.2.3. Call Forward Re-direction (Diversion Header)

The third call scenario illustrated in **Figure 4** is an inbound AT&T IP Flexible Reach service call that arrives on Session Manager and subsequently Communication Manager. Communication Manager routes the call to a destination station, however the station has set Call Forwarding to an alternate destination. Without answering the call, Communication Manager immediately redirects the call back to the AT&T IP Flexible Reach service for routing to the alternate destination.

1. Same as the first call scenario in **Section 2.2.1**.
2. Because the Communication Manager phone has set Call Forward to another AT&T IP Flexible Reach service number, Communication Manager initiates a new call back out to Session Manager, the Acme Packet SBC, and to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service places a call to the alternate destination and upon answer, Communication Manager connects the calling party to the target party.

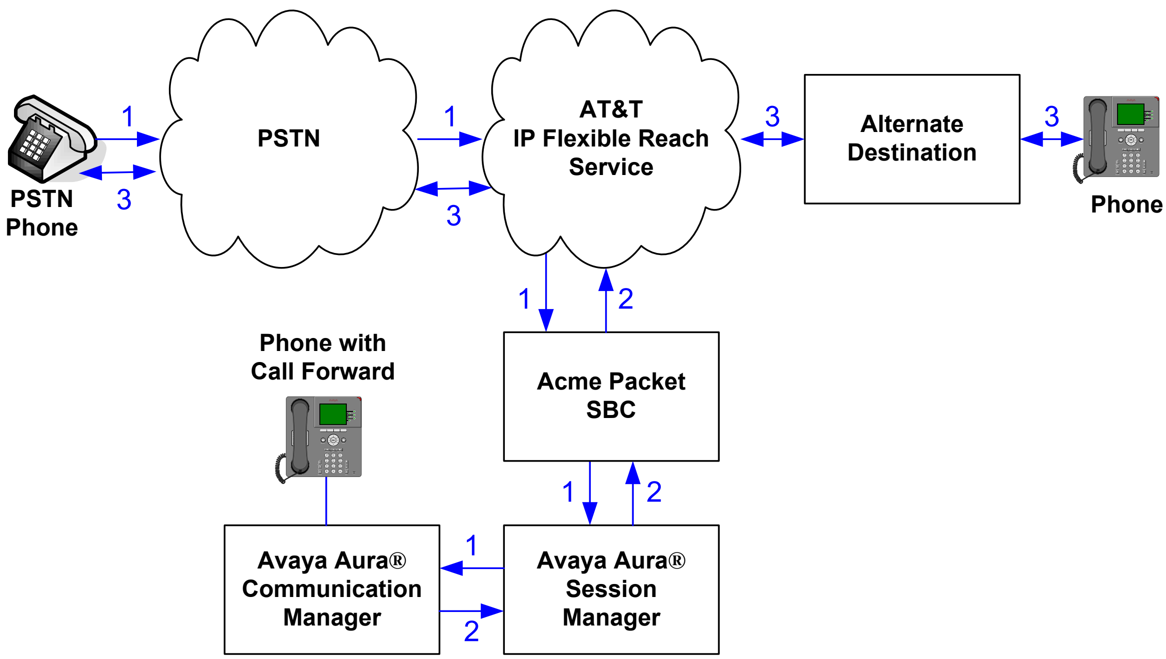



**Figure 4: Re-directed (e.g. Call Forward) AT&T IP Flexible Reach Call**

### 2.2.4. Coverage to Voicemail

The call scenario illustrated in **Figure 5** is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Modular Messaging system connected to Session Manager.

1. Same as the first call scenario in **Section 2.2.1**.
2. The called Communication Manager phone does not answer the call, and the call covers to the phone's voicemail. Communication Manager forwards[4] the call to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Avaya Modular Messaging. Avaya Modular Messaging answers the call and connects the caller to the called phone's voice mailbox. Note that the call[5] continues to go through Communication Manager.

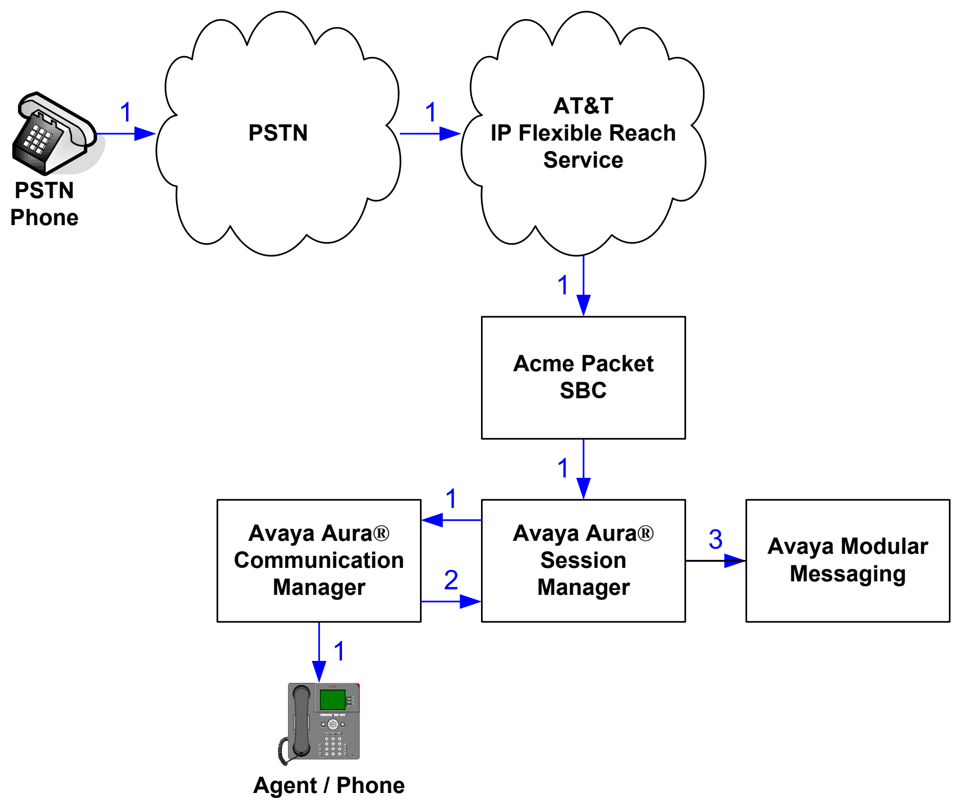



**Figure 5: Coverage to Voicemail**

---

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

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

# 3. Equipment and Software Validated

The following equipment and software was 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 S8720 Server | Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4) with patch 18433 |
| Avaya G650 Media Gateway | |
| TN2312BP IP Server Interface (IPSI) | HW15 FW051 |
| TN799DP Control-LAN (C-LAN) | HW01 FW038 |
| TN2302AP IP Media Processor (MedPro) | HW18 FW121 |
| TN2602AP IP Media Resource 320 (MedPro) | HW02 FW057 |
| TN2501AP VAL-ANNOUNCEMENT | HW03 FW021 |
| TN2224CP Digital Line | HW08 FW015 |
| TN793B Analog Line | HW05 FW010 |
| Avaya 9630 IP Telephone | Avaya one-X® Deskphone Edition H.323 Release 3.110b |
| Avaya one-X® Communicator | 5.2.0.14 |
| Avaya 6416D+ Digital Telephone | - |
| Avaya S3500 Server | Avaya Modular Messaging 5.2 (9.2.171.1009) |
| Fax device | Ventafax Home Version 6.3.102 |
| Acme Packet Net-Net 3800 | SCX6.2.0 MR3 Patch 1 (Build 642) |
| AT&T IP Flexible Reach Service using AVPN or MIS-PNT transport service connections. | 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 5.2.1 and Avaya Aura® Session Manager release 6.1. Avaya agrees to provide service and support for the integration of Avaya Aura® Communication Manager release 5.2.1 and Avaya Aura® Session Manager release 6.1 with the AT&T IP Flexible Reach service offer, in compliance with existing support agreements for Avaya Aura® Communication Manager release 5.2.1 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 6.0

These Application Notes assume that basic 6.0 Avaya Aura® 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 Avaya Aura® 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 Avaya Aura® 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. For example, an AT&T-specific Adaptation is used in these Application Notes to remove SIP History-Info headers from SIP messages sent to the AT&T IP Flexible Reach service network. 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[6] 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 Avaya Aura® System Manager Common Console (see **Figure 6**).

[6] The Routing Policy in effect at that time with highest ranking (e.g. 0 is ranked higher than 1) is attempted first. If that Routing Policy fails, then the Routing Policy with the next highest rankings is attempted, and so on.

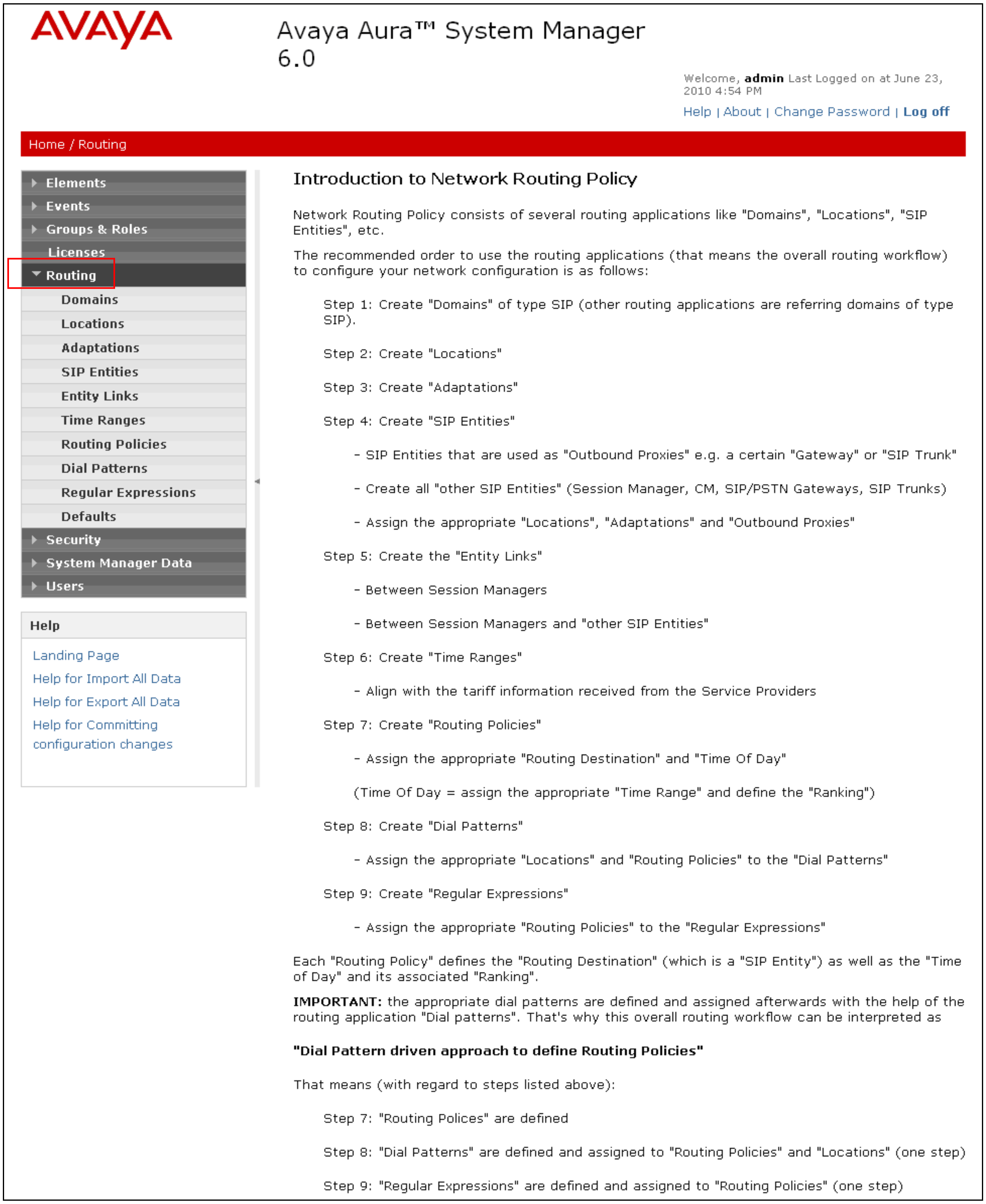



**Figure 6: Main Routing Page**

## 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),.
2. Continuing in the **Domain Management** page, enter a SIP domain (e.g. **customera.com**) for **Name**
3. Select **Type sip.**
4. (Optional) Add notes.
5. Click on "**Commit**".

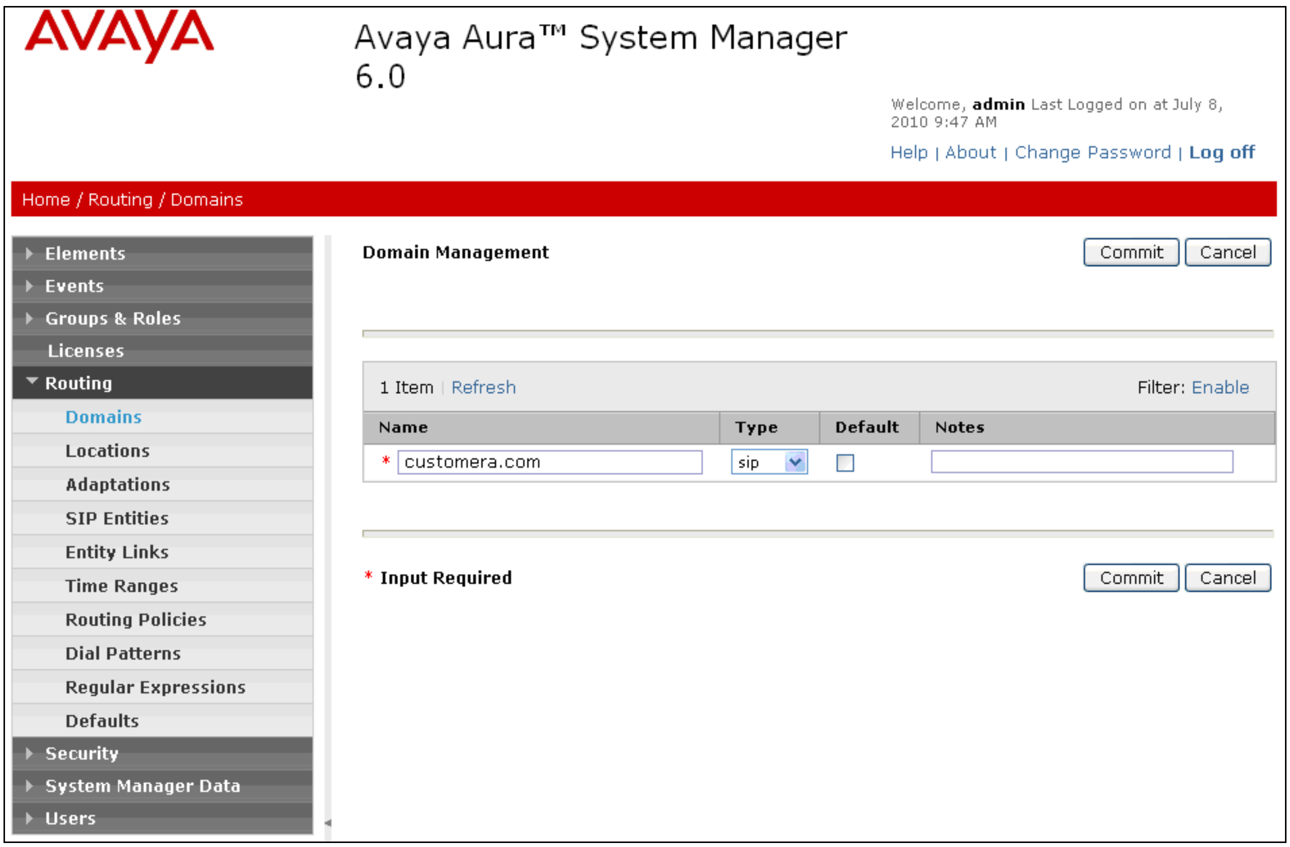



**Figure 7: Domain Management Page**

6. Repeat Steps 1 - 5 to add any additional SIP domains.

## 4.4. Locations

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

1. In the left pane under **Routing**, click on "**Locations**". In the **Location** page click on "**New**" (not shown),.
2. In the **Location Details** page, enter a descriptive **Name** (e.g. **main**).

3. [Optional] To limit the number of calls going to and from this Location, i.e., apply CAC, specify the **Managed Bandwidth** and **Average Bandwidth per Call**.
4. [Optional] To identify IP addresses associated with this Location, add **Location Pattern** entries accordingly. In the reference configuration all the Avaya CPE resided in the IP segment 192.168.67.*.
5. Click on "**Commit**".

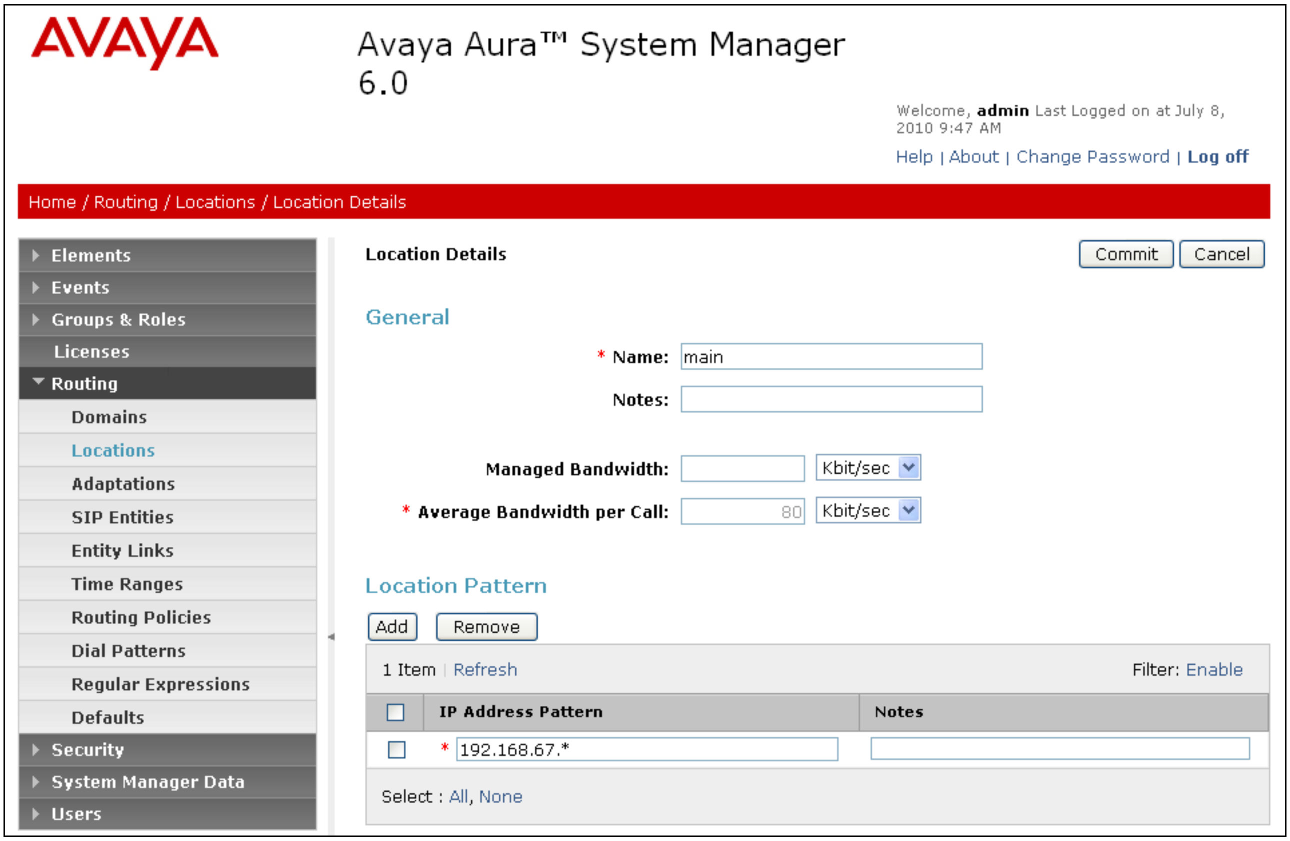



**Figure 8: Location Details Page**

6. Repeat Steps 1 - 5 to add any additional Locations.

## 4.5. Adaptations

In this section, Adaptations are administered for the following purposes:

- Calls to AT&T (**Section 4.5.1**) - Modification[7] of SIP messages sent to the AT&T IP Flexible Reach service.
    - The Avaya CPE domain (customera.com) is replaced with the IP address of the AT&T Border Element (e.g., 135.25.29.74, see **Section 7**) in the Request URI.
    - The "AttAdapter" module removes the History-Info SIP header on egress toward AT&T.

---

[7] Currently, the AT&T Adaptation automatically removes the History-Info header sent by default from Avaya Aura™ Communication Manager.

- Calls from AT&T (**Section 4.5.2**) - Modification of  SIP messages sent to Communication Manager.
  - The IP address of Session Manager (192.168.67.210) is replaced with the Avaya CPE SIP domain (customera.com) in the Request URI.
  - The AT&T DID called number digit strings in the Request URI are replaced with their associated Communication Manager extensions.
- Calls to/from Modular Messaging (**Sections 4.5.2 and 4.5.3**) - Modification of SIP messages sent to and received from Avaya Modular Messaging.
  - From Modular Messaging (**Section 4.5.2**) – Modular Messaging 11 digit mailbox numbers are converted to the associated Communication Manager 5 digit extensions (MWI).
  - To Modular Messaging (**Section 4.5.3**) - Convert the Communication Manager extension defined for Modular Messaging access (26000) to the  Modular Messaging pilot number (17231126000).

### 4.5.1. Adaptation for calls to AT&T

The Adaptation administered in this section is applied to SIP messages sent to the AT&T IP Flexible Reach service (by way of the Acme Packet SBC).

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, enter:
   a. A descriptive **Name (e.g. AT&T)**.
   b. Select "**AttAdapter**" from the **Module Name** drop down menu (if no module name is present, select "<click to add module>" and enter "**AttAdapter**".
   c. In the **Module parameter** field enter **odstd=135.25.29.74 osrcd=192.168.64.130,** where 135.25.29.74 is the IP address of the AT&T Border Element and 192.168.64.130 is the outside (public) address of the Acme SBC. This will replace the SIP Domain of Session manager (*customera.com*) with *135.25.29.74* in the *outbound* Request URI, and replace *customera.com* with *192.168.64.130* in the *outbound* PAI .
   d. Click on "**Commit**".

**Note** - No digit conversions are required for this Adaptation.

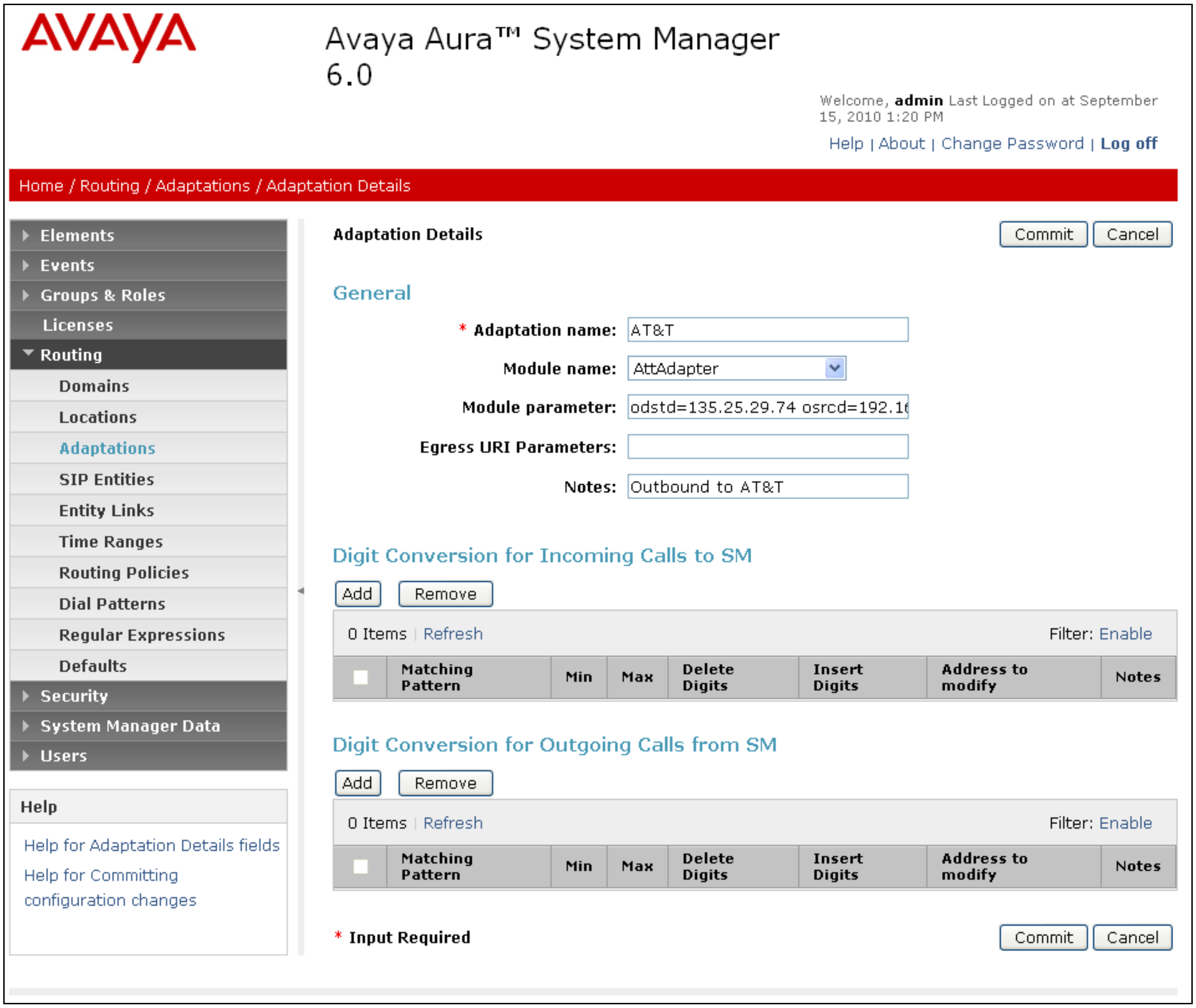



**Figure 9: Adaptation Details Page – Adaptation for AT&T**

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

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

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, enter:
    a. A descriptive **Name**, (e.g. To_ACM521).
    b. Select "**DigitConversionAdapter**" from the **Module Name** drop down menu (if no module name is present, select "<click to add module>" and enter **DigitConversionAdapter**).
    c. In the **Module parameter** field enter **odstd=customera.com osrcd=customera.com.** The odstd parameter will replace the IP address of

Session Manager (*192.168.67.210*) with *customera.com* in the *inbound* Request URI, and the osrcd parameter will replace the AT&T border element IP address (*135.25.29.74*) with *customera.com* in the *inbound* PAI.

d. In the **Digit Conversion for Outgoing Calls from SM** section, enter the *inbound* DID digits from AT&T that need to be replaced with their associated extensions before being sent to Communication Manager.
    i. Example 1:
        1. 7323204383 is an AT&T DID associated with Communication Manager extension 26103. Enter 7323204383 in the **Matching Pattern** column.
        2. Enter **10** in the **Min/Max** columns.
        3. Enter **10** in the **Delete Digits** column.
        4. Enter **26103** string in the **Insert Digits** column.
        5. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column.
        6. Enter any desired notes.
    ii. Example 2:
        1. 1723114xxxx is the format of the mailboxes sent by Avaya Modular messaging. These mailboxes must be converted to their associated Communication Manager extensions by deleting the first six digits.
        2. Enter **11** in the **Min/Max** columns.
        3. Enter **6** in the **Delete Digits** column.
        4. Leave the **Insert Digits** column blank.
        5. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column
        6. Enter any desired notes.

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

f. Click on "**Commit**".

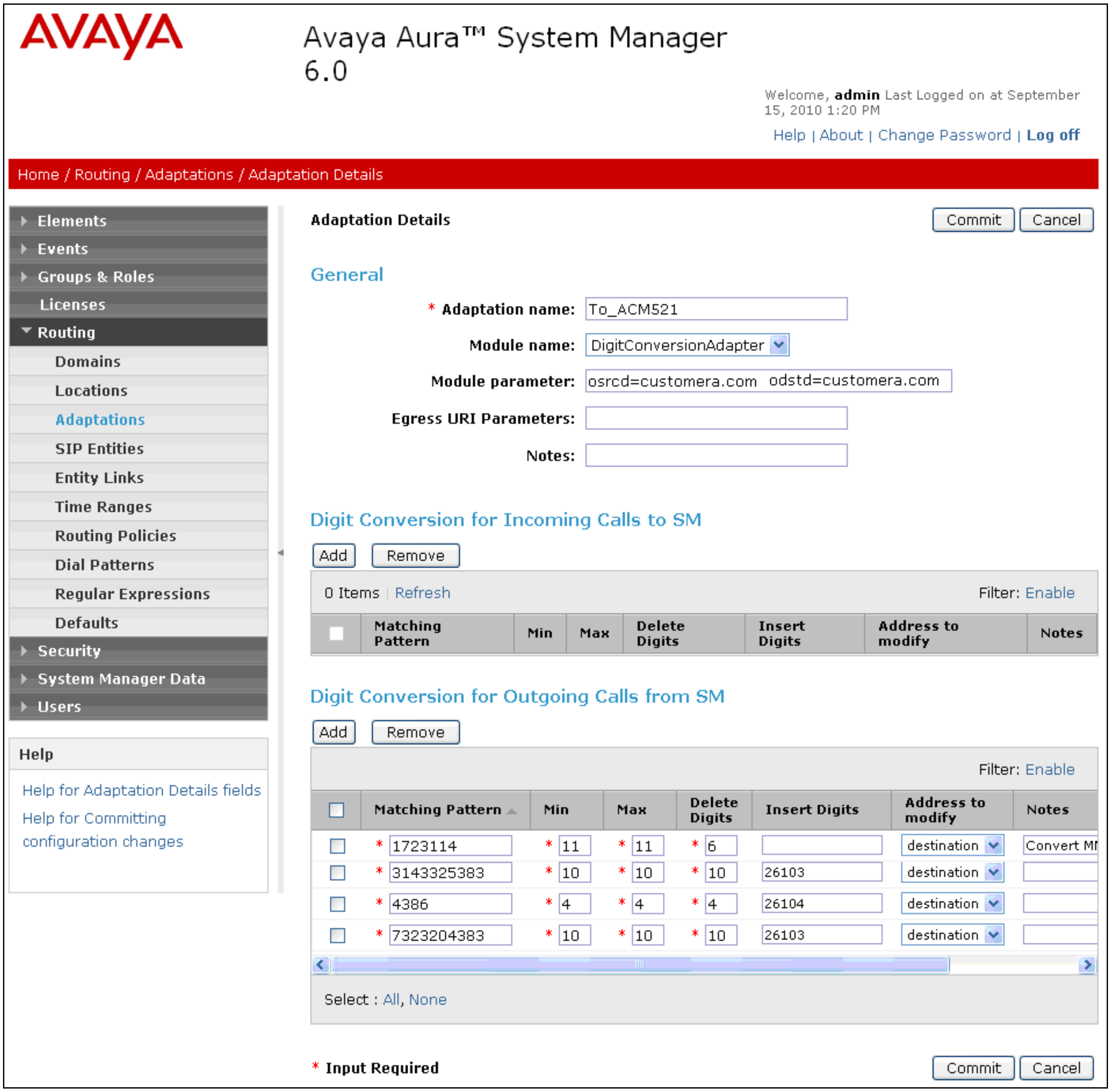



**Figure 10: Adaptation Details Page – Adaptation for Avaya Aura® Communication Manager 5.2.1**

### 4.5.3. Adaptation for Avaya Modular Messaging

The Adaptation administered in this section is used for digit conversion on SIP messages to and from Avaya Modular Messaging.

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, enter:
   a. A descriptive **Name**, (e.g. **MM_Digits**).

b. Select “**DigitConversionAdapter**” from the **Module Name** drop down menu (if no module name is present, select “<click to add module>” and enter **DigitConversionAdapter**).
c. No **Module parameter** is required.
d. Inbound calls to the Modular Messaging pilot number (message retrieval).
    a. In the **Digit Conversion for Outgoing Calls from SM** section, enter **26000** in the **Matching Pattern** column. This is the Modular Messaging pilot extension defined on Communication Manager.
    b. Enter **5** in the **Min/Max** columns.
    c. Enter **0** in the **Delete Digits** column.
    d. Enter **172311** in the **Insert Digits** column. This converts the pilot extension (26000) to the Modular Messaging pilot number (17231126000).
    e. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column.
    f. Enter any desired notes.
e. Click on “**Commit**”.

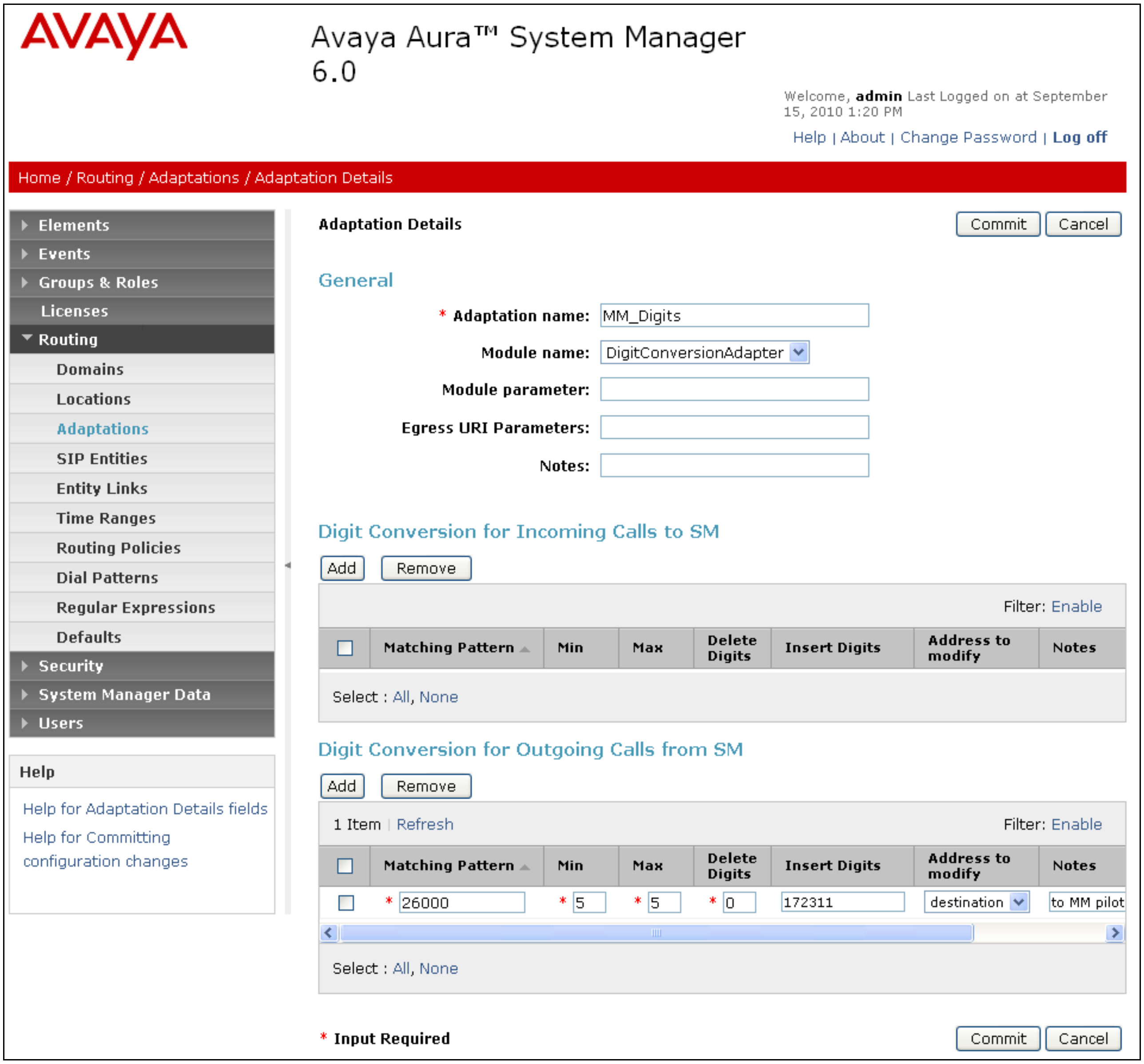



**Figure 11: Adaptation Details Page – Adaptation for Avaya Modular Messaging**

## 4.6. SIP Entities

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

- Avaya Aura® Session Manager – **Section 4.6.1**
- Avaya Aura® Communication Manager 5.2.1 (AT&T access) – This entity, and its associated entity link is for calls between Communication Manager and the Acme Packet SBC. – **Section 4.6.2**
- Acme Packet SBC – This entity, and its associated entity link is for calls between the Acme Packet SBC and AT&T. – **Section 4.6.3**

- Avaya Modular Messaging – This entity, and its associated entity link is for message coverage/retrieval calls from Communication Manager to Modular Messaging **- Section 4.6.4**

| |
|---|
| **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. |

### 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, provision the following:
   - **Name –** Enter a descriptive name for Session Manager (e.g. **SM60**).
   - **FQDN or IP Address –** Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation (e.g. **192.168.67.210**).
   - **Type –** Select "**Session Manager**".
   - **Location** – Select location "**Main**" (**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 (**Section 4.8**).
3. In the **SIP Monitoring** section of the **SIP Entity Details** page select:
   a. Select **Link Monitoring Enabled** for **SIP Link Monitoring**
   b. Use the default values for the remaining parameters.
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**.
   with the selected SIP **Default Domain** (e.g. **customera.com**)
5. Click on "**Commit**".

These entries enable Session Manager to accept SIP requests on the specified ports/protocols. In addition, Session Manager will associate SIP requests containing the IP address of Session Manager (192.168.67.210) in the host part of the Request-URI

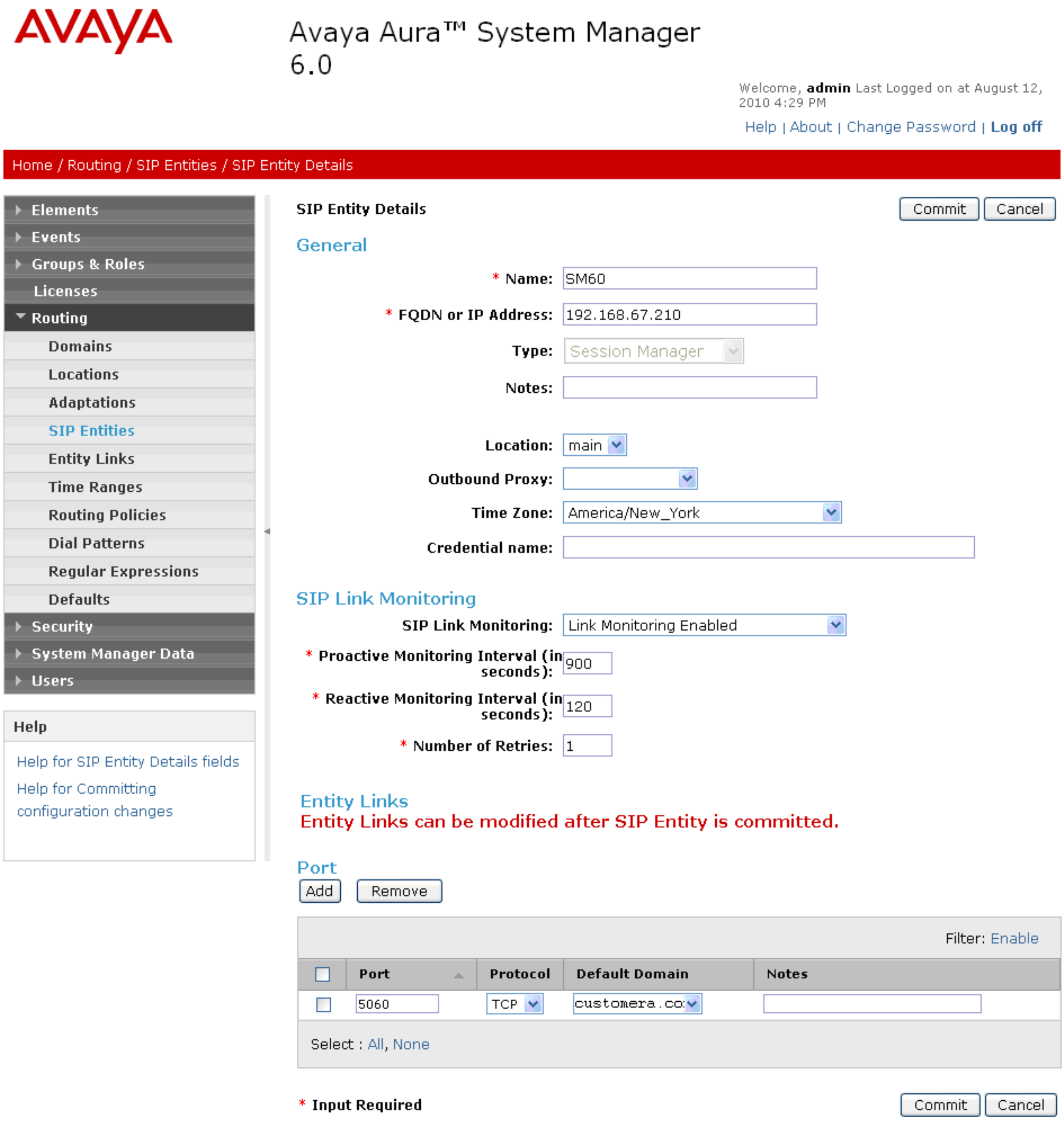



**Figure 12: SIP Entity Details Page – Avaya Aura® Session Manager SIP Entity**

### 4.6.2. Avaya Aura® Communication Manager SIP Entity

1. In the **SIP Entities** page, click on "**New**".
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name** – Enter a descriptive name for Communication Manager (e.g. **ACM521**).

- **FQDN or IP Address –** Enter the IP address of the Communication Manager Clan provisioned in **Section 5.3**.
- **Type –** Select "**CM**".
- **Adaptation –** Select the Adaptation administered in **Section 4.5.2**.
- **Location** – Select a Location administered in **Section 4.4**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page select:
    - Select **Link Monitoring Enabled** for **SIP Link Monitoring**
    - Use the default values for the remaining parameters.

3. Click on "**Commit**".

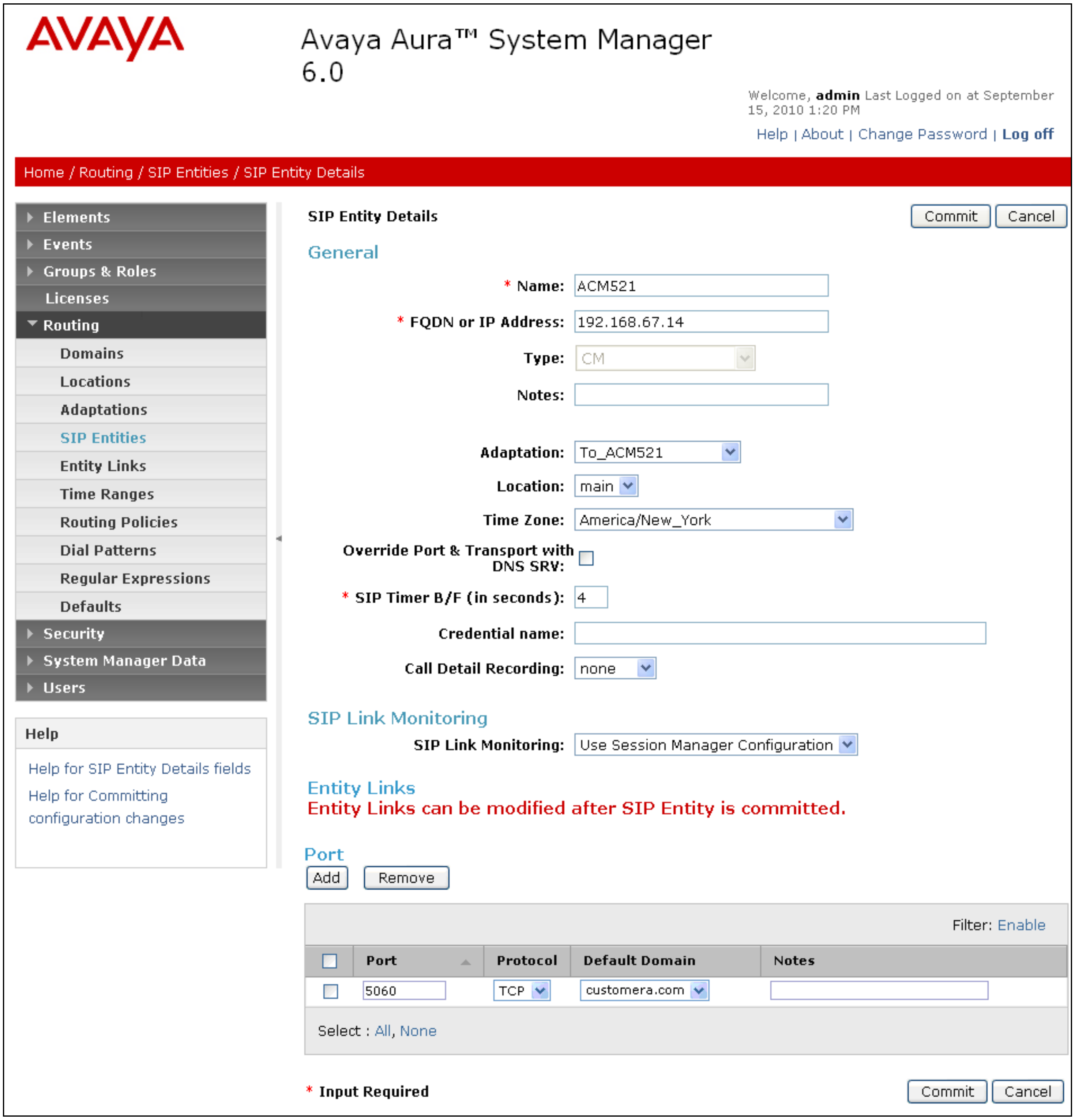



**Figure 13: SIP Entity Details Page – Avaya Aura® Communication Manager 5.2.1 SIP Entity**

## 4.6.3. Acme Packet SBC 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) Acme interface configured in **Section 7** and the **Type** field is set to "**Other**". See the figure below for the values used in the reference configuration.

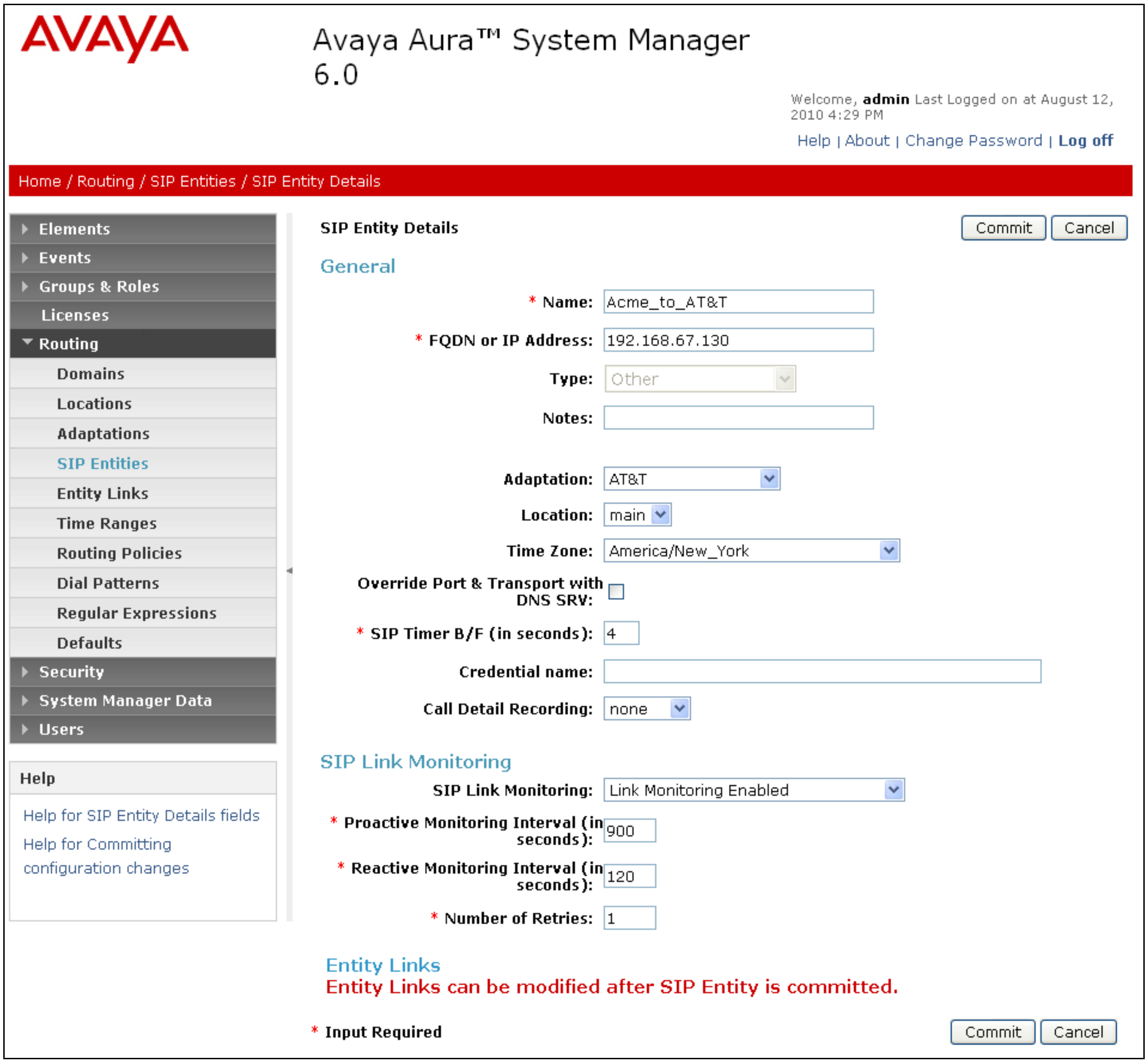



**Figure 14: SIP Entity Details Page – Acme Packet SBC SIP Entity**

### 4.6.4. 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 the reference configuration.

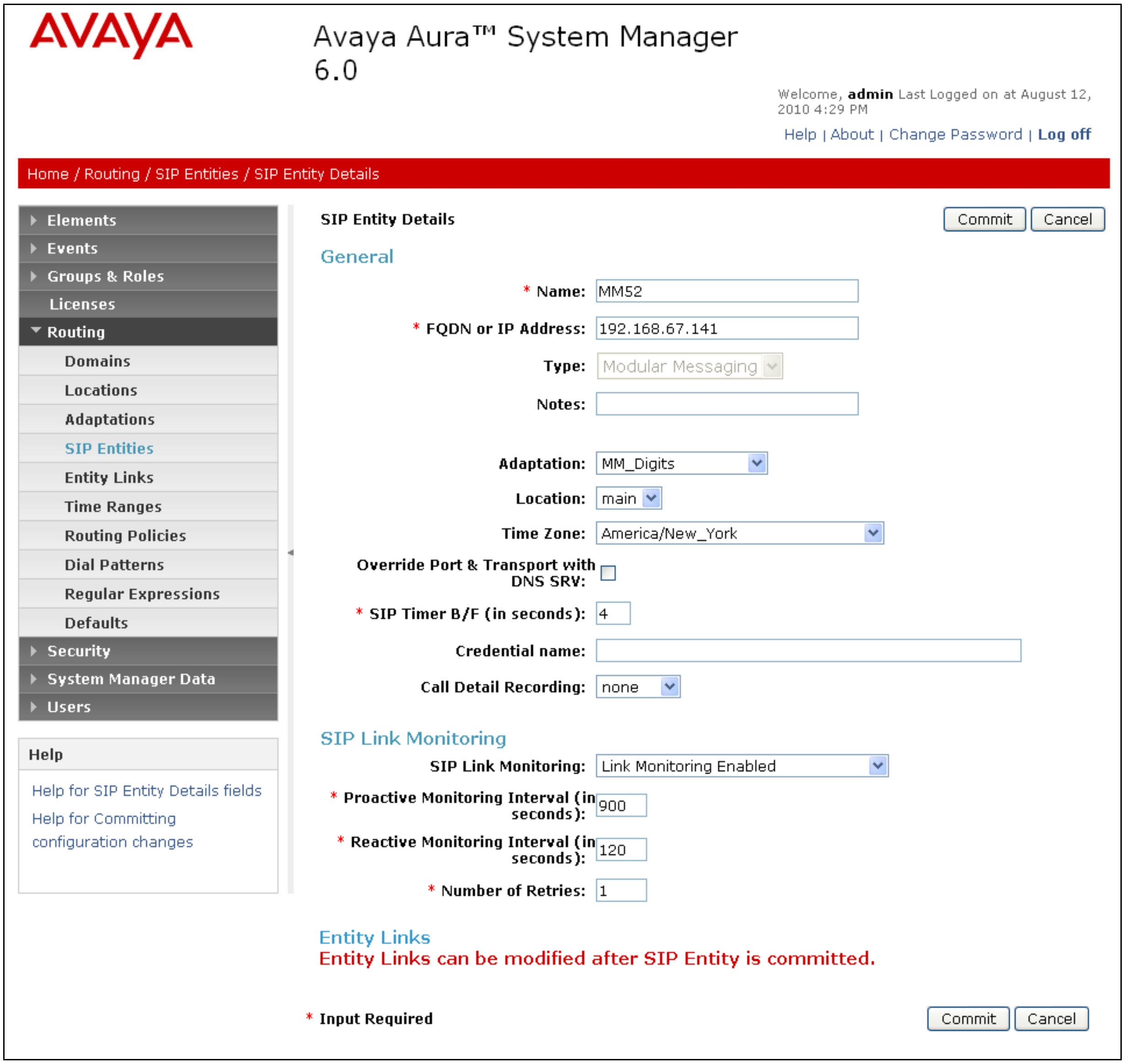



**Figure 15: SIP Entity Details Page – Avaya Modular Messaging SIP Entity**

## 4.7. Entity Links

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

- Avaya Aura® Communication Manager (4.7.1).
- Acme Packet SBC (4.7.2).
- Avaya Modular Messaging (4.7.3).

**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.

### 4.7.1. Entity Links to Avaya Aura® Communication Manager 5.2.1

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. **ACM521**).
   - **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 (e.g. **SM60**).
   - **SIP Entity 1 Port** – Enter "**5060**"
   - **SIP Entity 2** –Select the SIP Entity administered in **Section 4.6.2** for Communication Manager (e.g. **ACM521**).
   - **SIP Entity 2 Port** - Enter "**5060**".
   - **Trusted –** Check the checkbox.
   - **Protocol –** Select "**TCP**".
3. Click on "**Commit**".

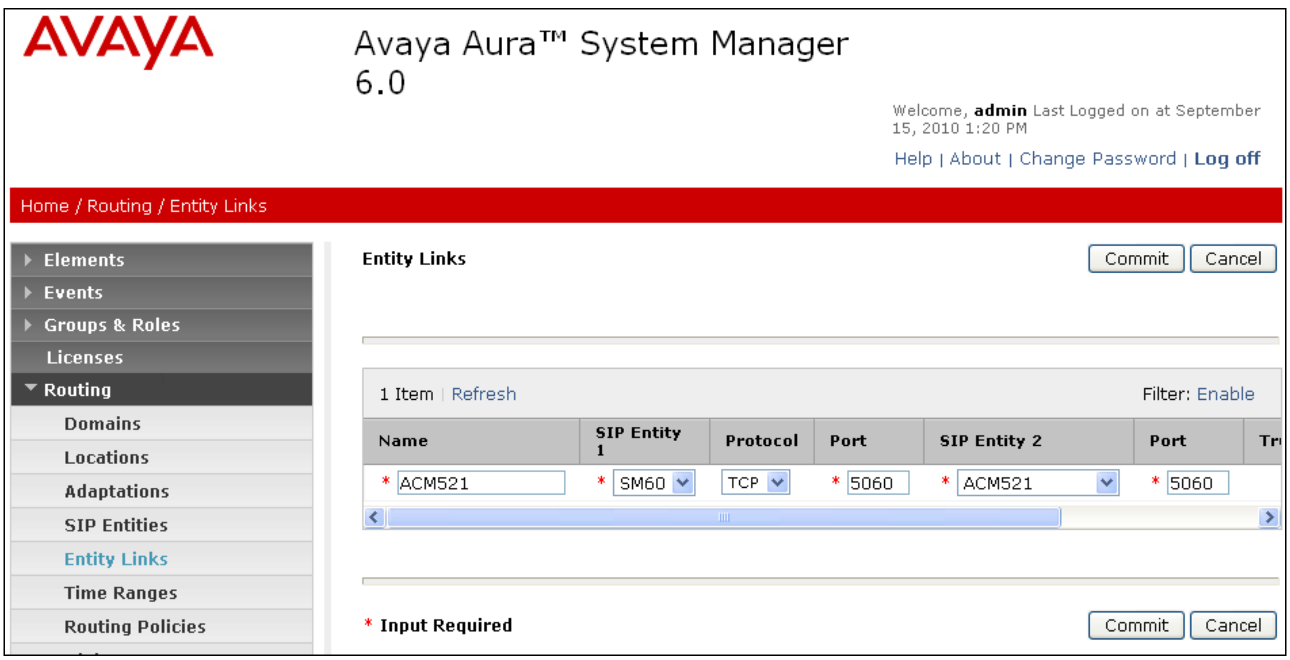



**Figure 16: Entity Links Page – Entity Link to Avaya Aura® Communication Manager 5.2.1**

## 4.7.2. Entity Link to AT&T IP Flexible Reach Service via Acme Packet SBC

To configure the entity link between Session Manager and Session Border Controller entity, 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** (e.g. **Acme_to_AT&T**). See the figure below for the values used in the reference configuration.

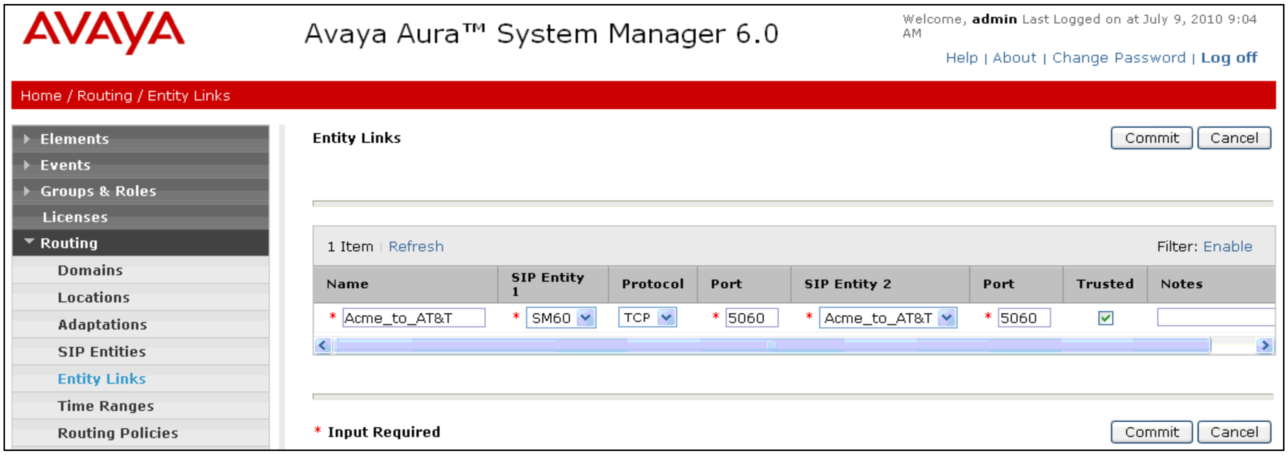



**Figure 17: Entity Links Page – Entity Link to AT&T IP Flexible Reach Service via Acme Packet SBC**

## 4.7.3. 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 4.6.4** (e.g., **MM52**). See the figure below for the values used in the reference configuration.

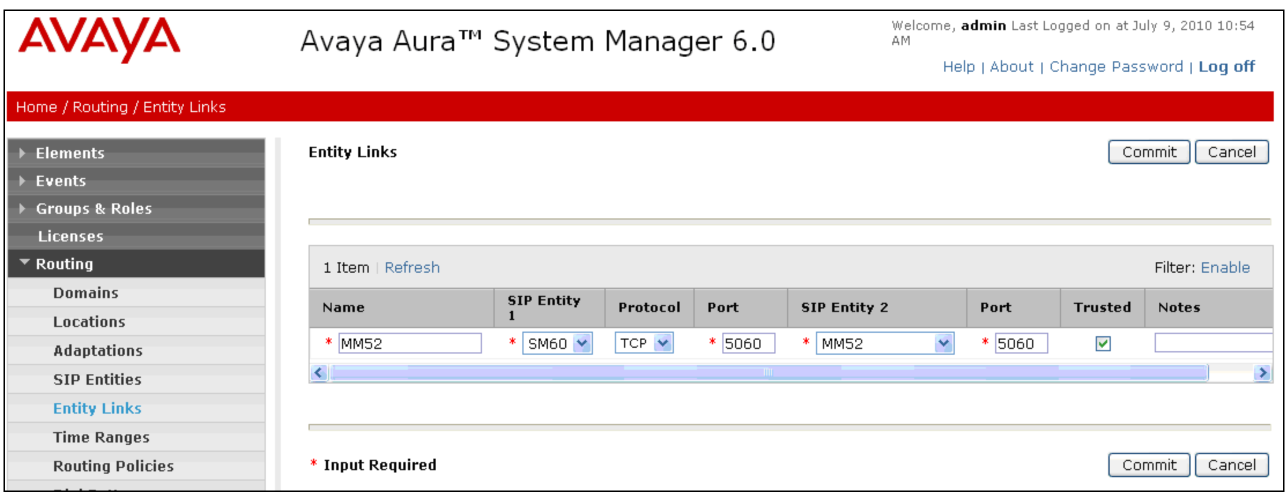



**Figure 18: Entity Links Page – Entity Link to Avaya Modular Messaging**

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

## 4.8. 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.

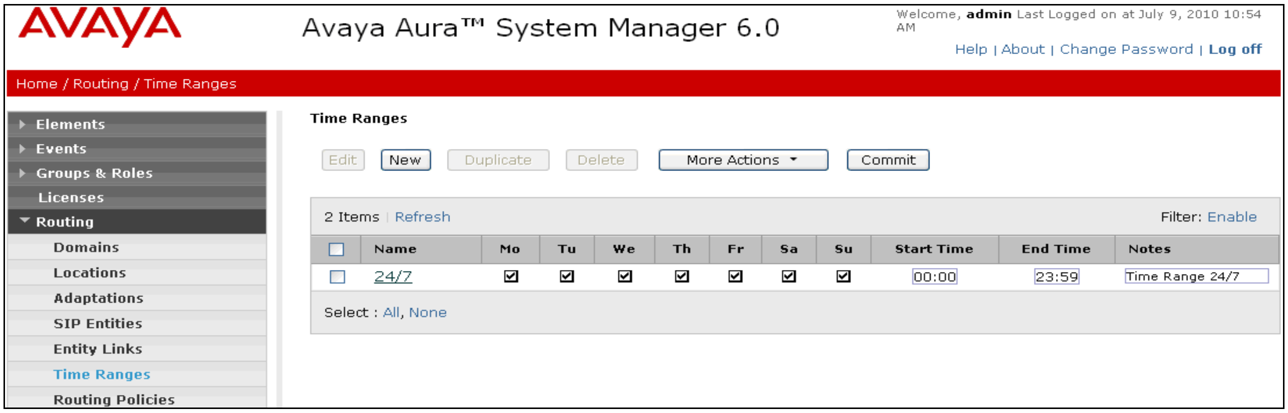



**Figure 19: Time Ranges Page**

## 4.9. Routing Policies

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

- To AT&T network via the Acme SBC (4.9.1).
- To Avaya Aura® Communication Manager 5.2.1 from AT&T (4.9.2).
- To Avaya Modular Messaging (4.9.3).

### 4.9.1. Routing Policy for Routing to the AT&T Flexible Reach Service

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 (see **Figure 20**), enter a descriptive **Name** for routing calls to AT&T (**To_AT&T**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on "**Select**".

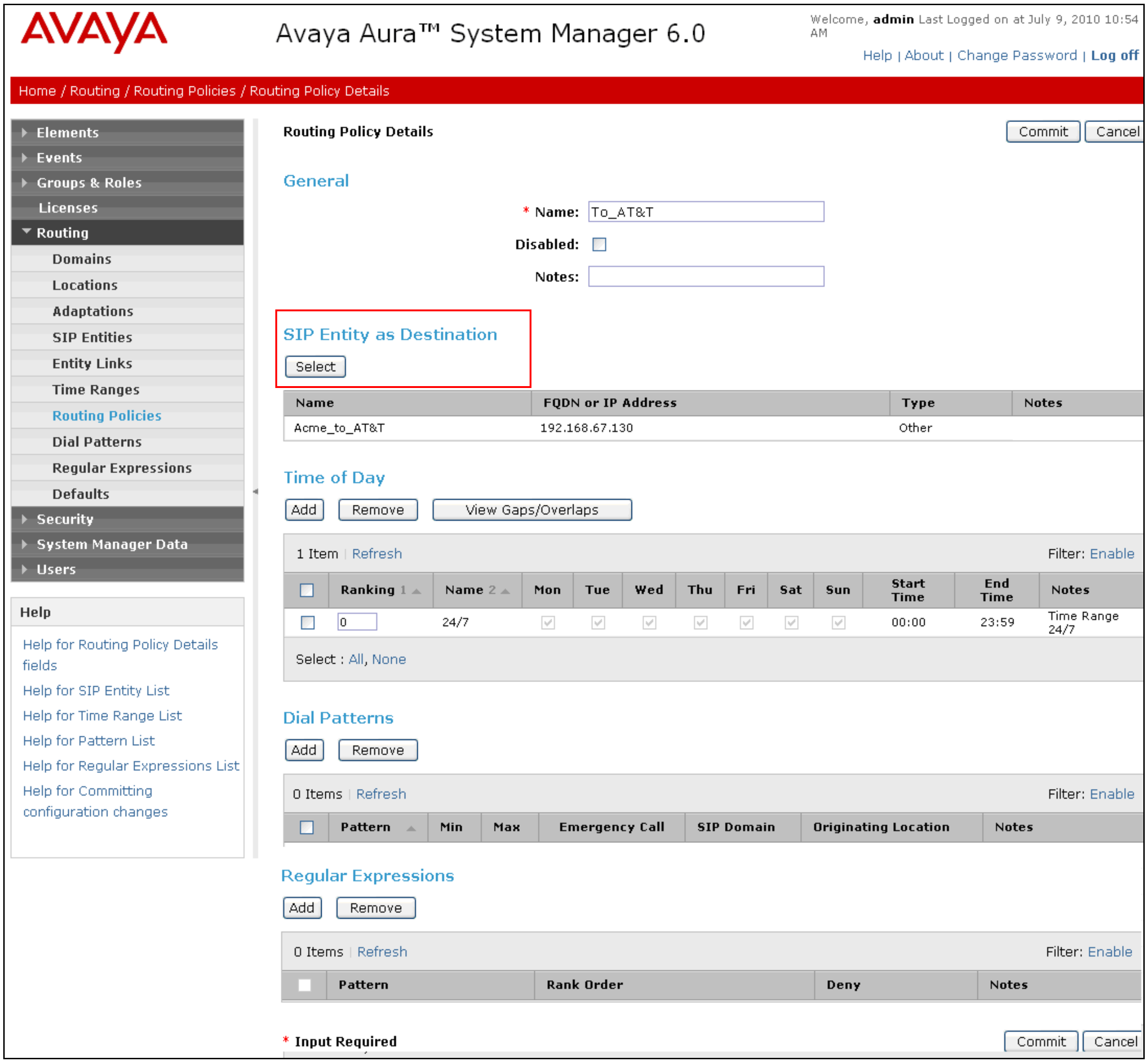



**Figure 20: Routing Policy Details Page – Outbound to AT&T**

4. In the **SIP Entity List** page (**Figure 21**), select the SIP Entity administered in **Section 4.6.3** for Acme (**Acme_to_AT&T**), and click on "**Select**".

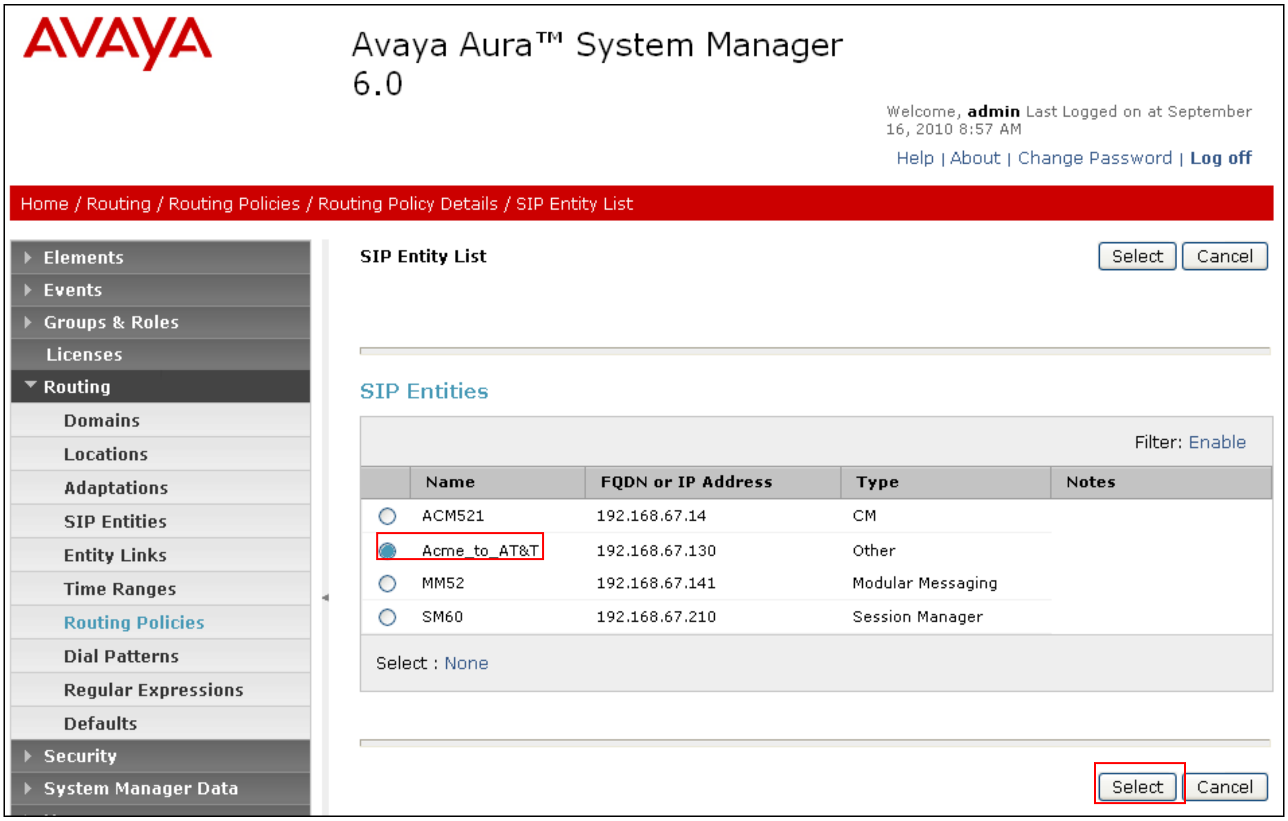



**Figure 21: SIP Entity List Page**

5. Returning to the Routing Policy Details page in the Time of Day section, click on "Add".
6. In the **Time Range List** page, check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 4.8**, and click on "**Select**".
7. Returning to the **Routing Policy Details** page (**Figure 20**), in the **Time of Day** section, enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on "**Commit**".
8. Note that once the **Dial Patterns** are defined (**Section 4.10**) they will appear in the **Dial Pattern** section.
9. No **Regular Expressions** were used in the reference configuration.
10. Click on **Commit**.

| |
|---|
| Note – Associated Dial Patterns will be displayed on this form after the Dial Pattern provisioning is completed in **Section 4.10**. |

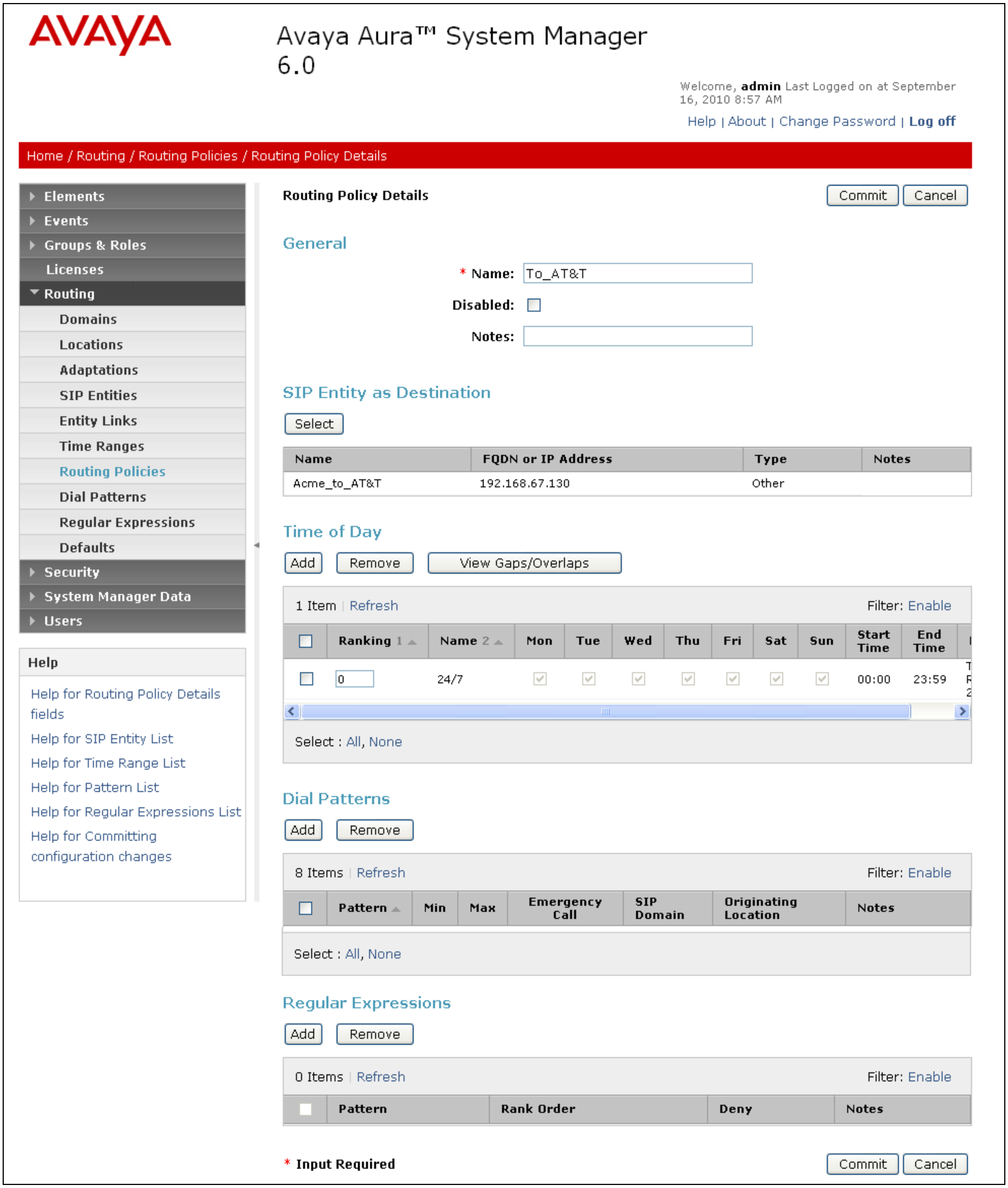



**Figure 22: Completed Routing Policy Details Page to AT&T**

### 4.9.2. Routing Policy for Routing to Avaya Aura® Communication Manager

Repeat **Section 4.9.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Communication Manager (**To_ACM_521**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.6.2** for Communication Manager (**ACM521**) and click on "**Select**".
- See **Section 4.10** for the associated Dial Patterns.

| |
|---|
| Note – Associated Dial Patterns will be displayed on this form after the Dial Pattern provisioning is completed in **Section 4.10**. |

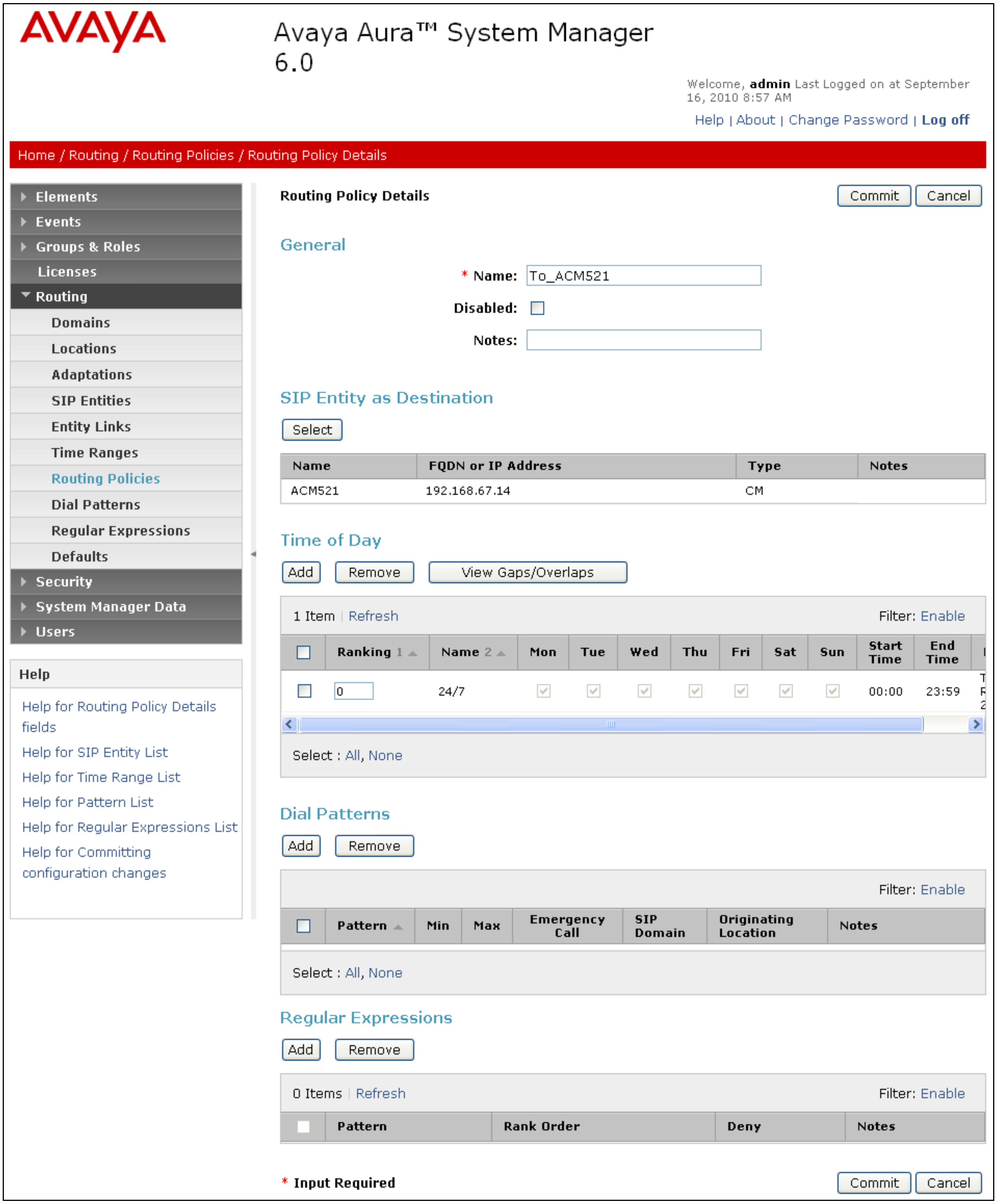



**Figure 23: Completed Routing Policy Details Page to Avaya Aura® Communication Manager 5.2.1**

### 4.9.3. Routing Policy for Routing to Avaya Modular Messaging

Repeat **Section 4.9.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Avaya Modular Messaging (**To_MM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.6.4** for Avaya Modular Messaging (**MM52**), and click on "**Select**".
- See **Section 4.10** for the associated Dial Patterns.

| |
|---|
| Note – Associated Dial Patterns will be displayed on this form after the Dial Pattern provisioning is completed in **Section 4.10**. |

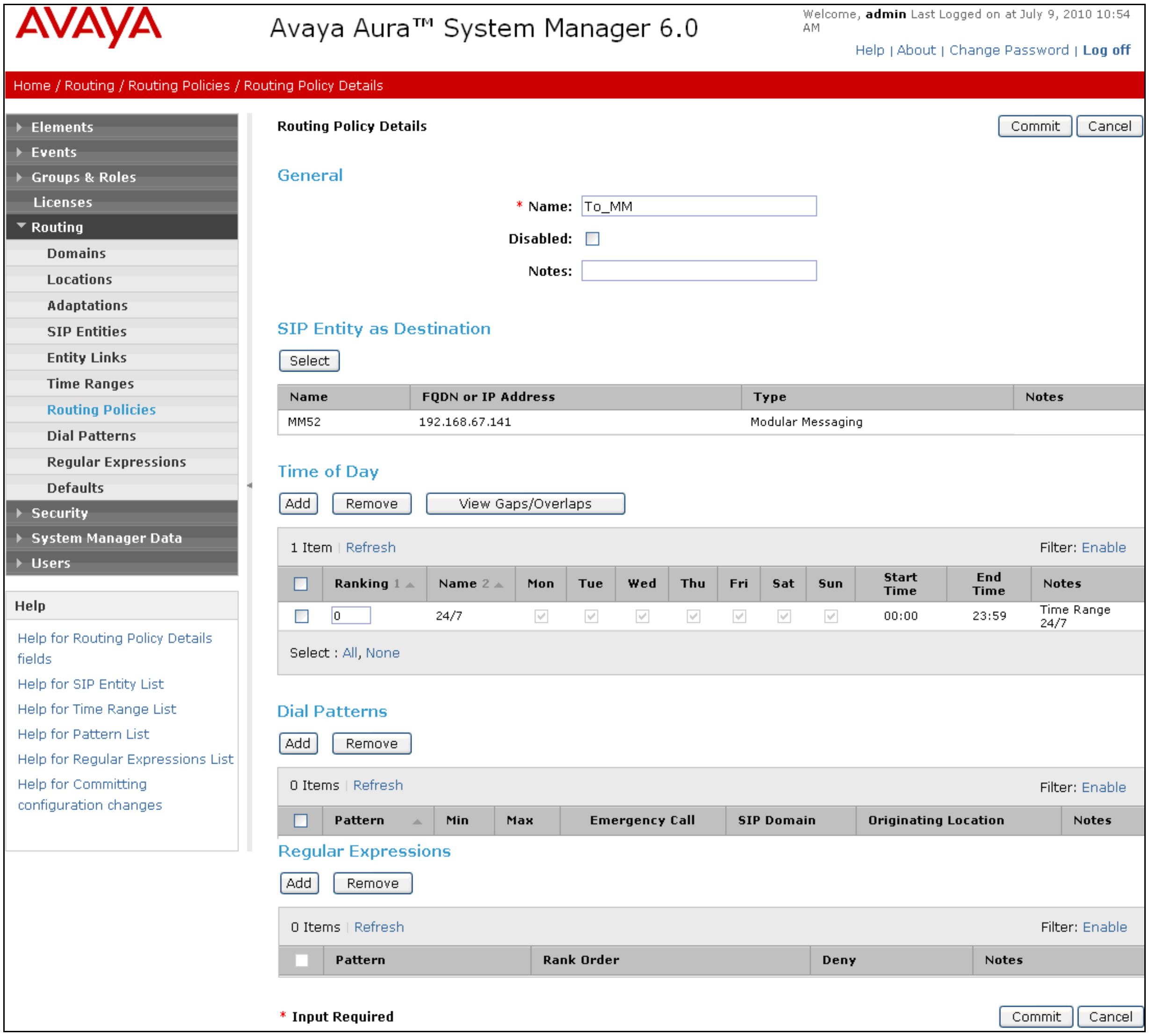



**Figure 24: Completed Routing Policy Details Page to Avaya Modular Messaging**

## 4.10. Dial Patterns

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

- Inbound/outbound PSTN calls via AT&T IP Flexible Reach service (4.10.1).
- Calls to/from 11-digit local dial plan numbers associated with extensions on Communication Manager or the Avaya Modular Messaging pilot number (4.10.2)
- Notifications from Avaya Modular Messaging (MWI) to Communications Manager 5 digit local extensions (4.10.3)

### 4.10.1. Matching Outbound Calls to the AT&T IP Flexible Reach Service

In this example, pattern 1732 is defined for outbound calls to PSTN numbers starting with 1732xxxxxxx.

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 (**Figure 25**), provision the following:
   - **Pattern** – Enter matching patterns for outbound dialed digits, **1732**
   - **Min** and **Max** – Enter **11**.
   - **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 all administered SIP Domains if "**-ALL-**" is selected) can match this Dial Pattern.
     **Note** – As only one domain was administered for the reference configuration ("Main"), the same result is achieved whether "Main" or "All" is specified.
   - (Optional) Add any notes as desired.

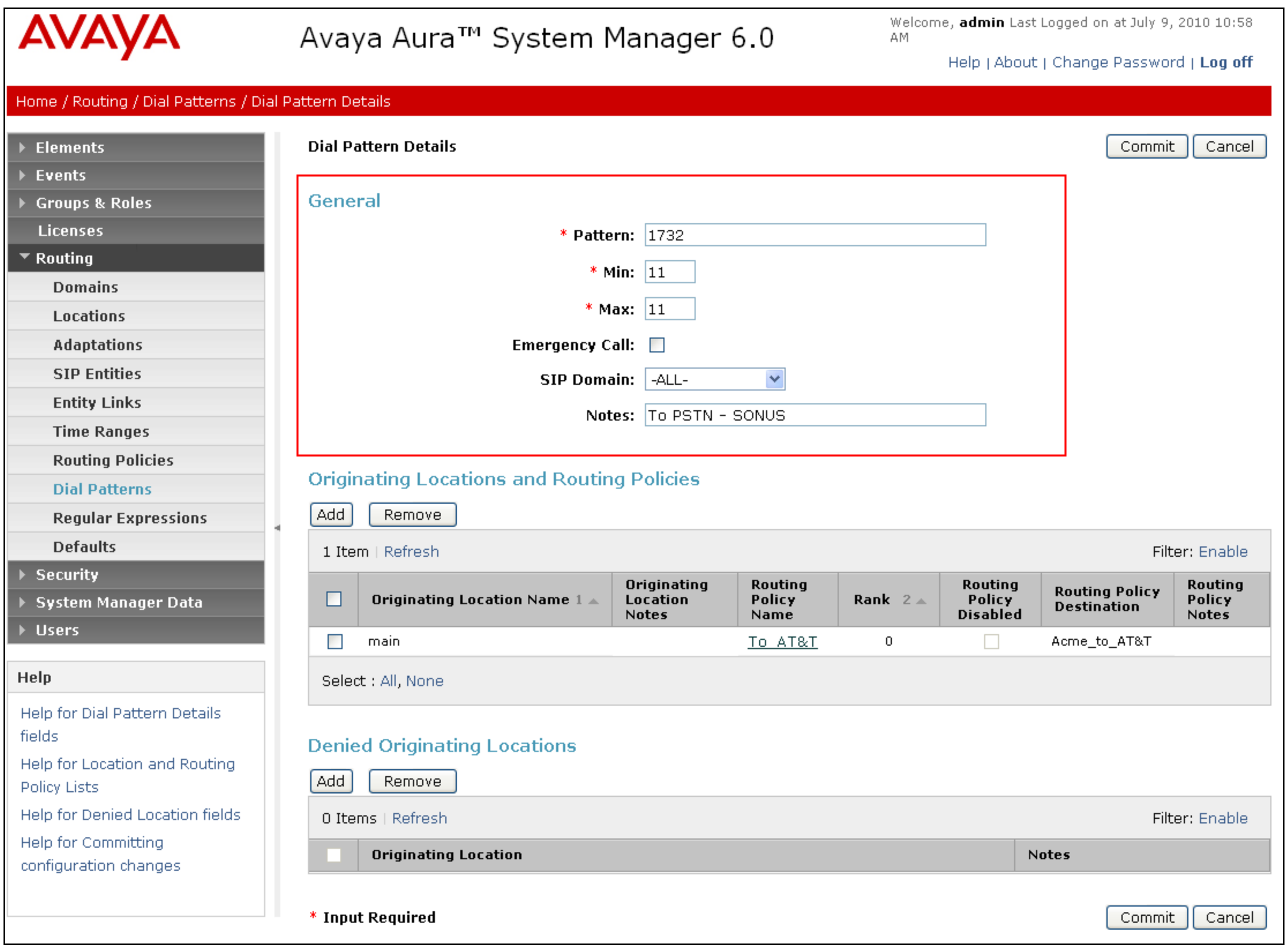



**Figure 25: Dial Pattern Details Page - Outbound 1732xxxxxxx Calls to AT&T IP Flexible Reach Service**

3. In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on "**Add**".
4. In the **Originating Location** section of the **Originating Location and Routing Policy List** page (**Figure 26**), check the checkbox corresponding to the Location **Main** (see **Section 4.4**). 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.
5. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **To_AT&T** administered for routing calls to the AT&T IP Flexible Reach service in **Section 4.9.1**.

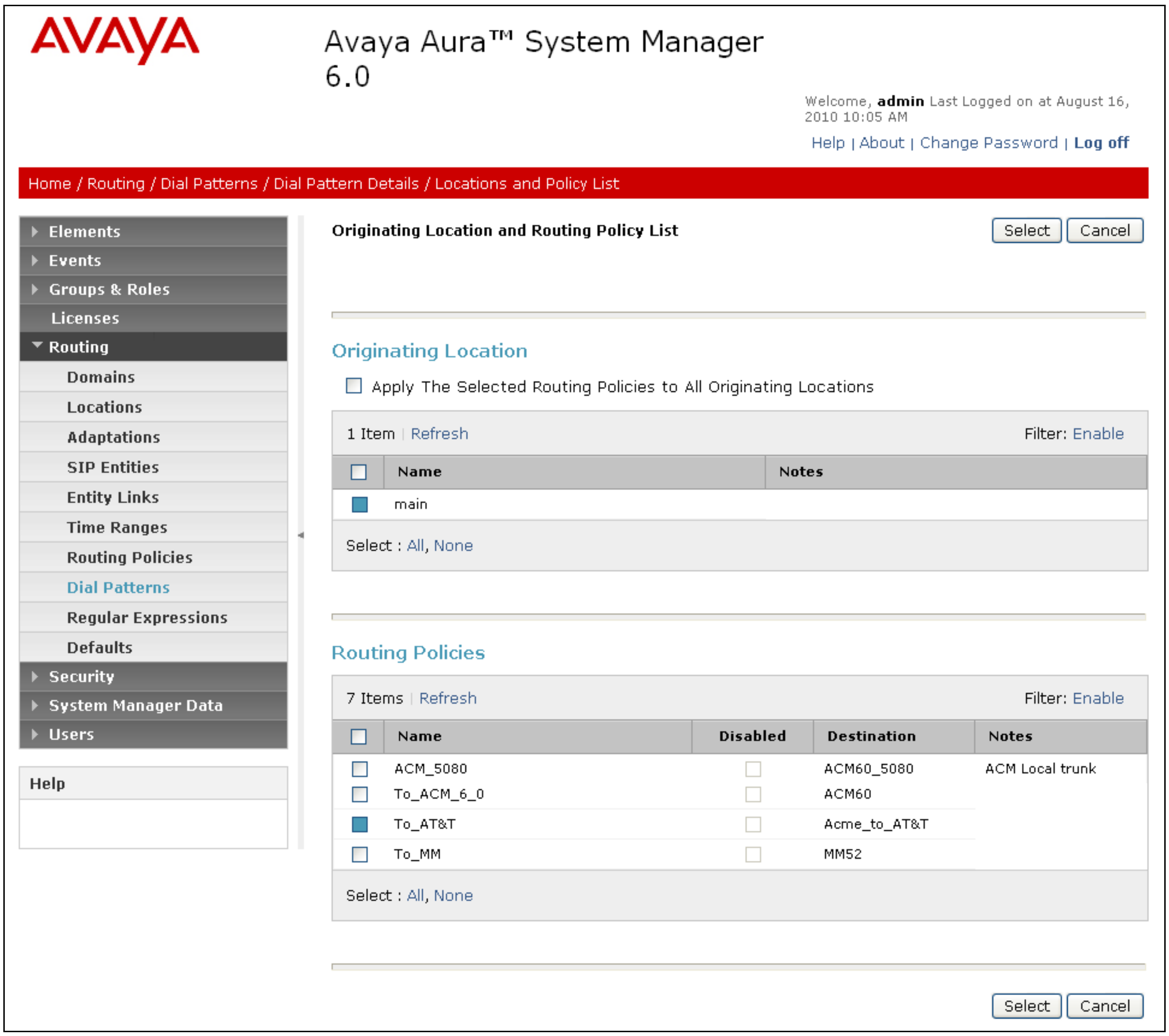



**Figure 26: Originating Location and Routing Policy List Page - Outbound AT&T IP Flexible Reach Service Calls**

6. In the **Originating Location and Routing Policy List** page, click on "**Select**".
7. Returning to the **Dial Pattern Details** page (**Figure 25**), click on "**Commit**".

8. Repeat steps 2 through 7 for each outbound matching dial pattern required. For example:1314346xxxx, 1800346xxxx, 1914222xxxx, and international 011 outbound calls.

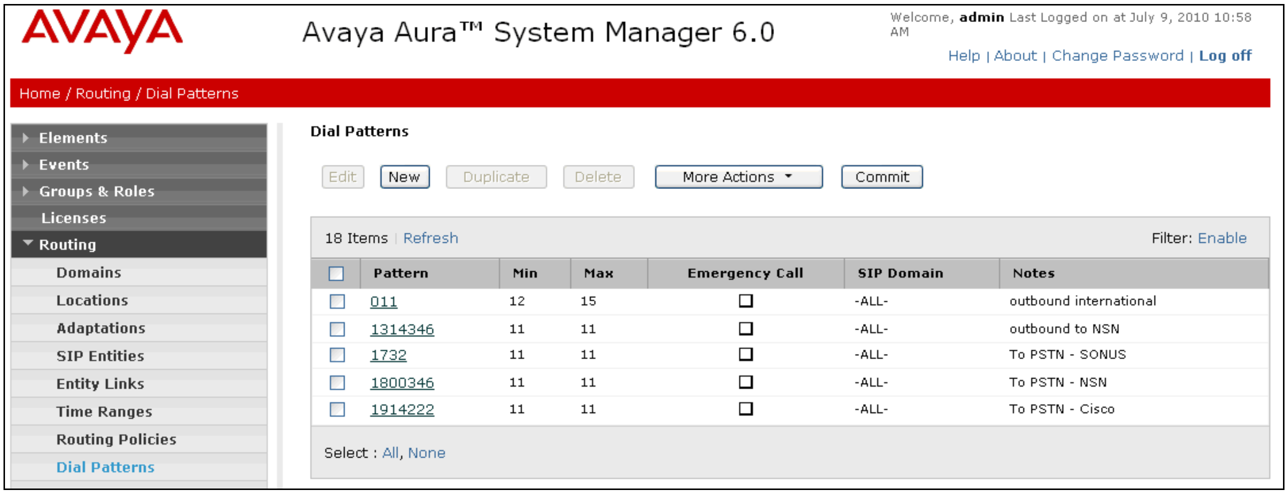



**Figure 27: Dial Pattern Details - Outbound Calls to the AT&T IP Flexible Reach Service**

### 4.10.2. Matching Inbound Calls to Avaya Aura® Communication Manager 5.2.1

Repeat the steps from **Section 4.10.1** with the following entries for inbound calls to Communication Manager 5.2.1:

- 314332xxxx, 4386, and 732320xxxx (inbound calls from AT&T)
- 723114xxxx (Modular Messaging mailboxes to Communication Manager extensions for MWI).

1. In the **General** section of the **Dial Pattern Details** page, provision the following:
   - **Pattern** – In the reference configuration, AT&T sends 10 digit called numbers with the format 732320xxxx. Enter **732320**. Note - The adaptation define for Communication Manager in **Section 4.5.2** will convert the various 732320xxxx numbers into their corresponding extensions.
   - **Min** and **Max –** Enter **10**.
   - **SIP Domain –ALL**
2. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Main**.
3. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **To_ACM_521.**
4. Repeat steps 1 through 3 for the remaining inbound matching dial patterns.
5. Returning to the **Dial Pattern Details** page (**Figure 28**), click on "**Commit**". Note that the outbound dial patterns defined in **Section 4.10.1** are listed as well.

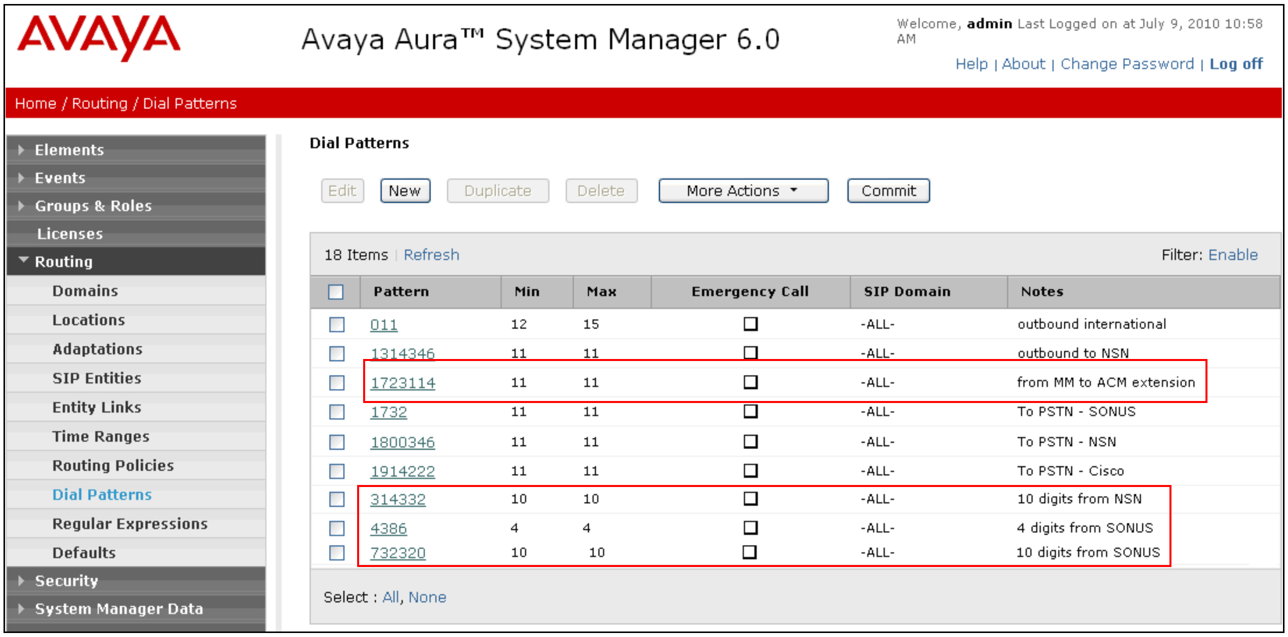



**Figure 28: Dial Pattern Details - Inbound (and Outbound) AT&T IP Flexible Reach Service Calls**

### 4.10.3. Matching Outbound Calls to the Avaya Modular Messaging Pilot Number

Repeat the steps from **Section 4.10.1** with the following entries for outbound calls to the Modular Messaging pilot number from Communication Manager. Communication Manager stations cover to Avaya Modular Messaging using a pilot extension (26000 in the reference configuration). Additionally stations may dial this extension to retrieve messages or modify mailbox settings. Note – Extension 26000 is converted to the Modular Messaging mailbox format 17321126000 in the adaptation defined in **Section 4.5.3**.

1. In the **General** section of the **Dial Pattern Details** page, provision the following:
   - **Pattern** – Enter the Avaya Modular Messaging pilot extension (e.g. **26000**)
   - **Min** and **Max** – Enter **5**.
   - **SIP Domain** – **ALL**
2. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to **Main**.
3. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **To_MM**.
4. In the **Originating Location and Routing Policy List** page, click on "**Select**".
5. Returning to the **Dial Pattern Details** page (**Figure 29**), click on "**Commit**". Note that the outbound dial patterns defined in **Section 4.10.1** and **4.10.2** are listed as well.

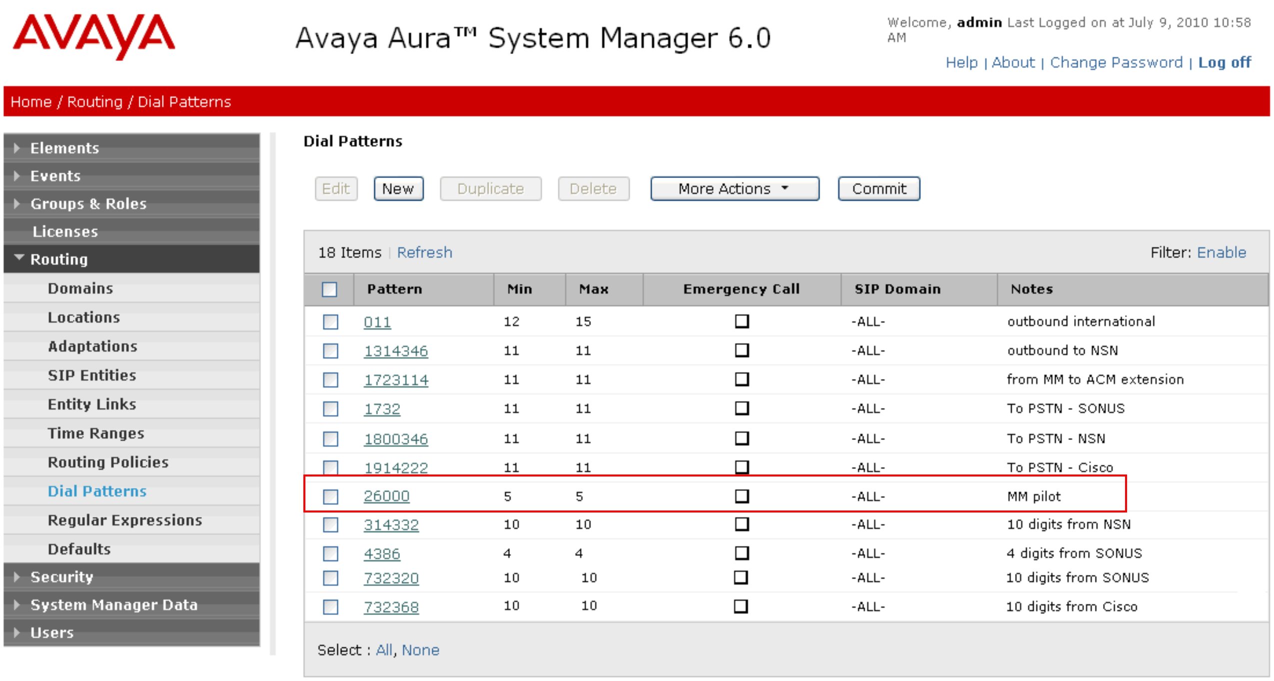



**Figure 29: Dial Pattern Details – Modular Messaging Pilot number (with Inbound and Outbound) Calls**

## 4.11. Session Manager Administration

Note – The Session Manager provisioning is typically performed during the Session Manager installation process. The Session Manager provisioning is shown here for illustrative purposes.

1. In the left pane under **Session Manager**, click on **Elements → Session Manager Administration**. In the **Session Manager Administration** page click on "**New**" (not shown).
2. In the **General** section of the **Add Session Manager** page, provision the following:
   - **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 e.g. **192.168.67.209**, (*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, e.g. **255.255.255.0 and 192.168.67.1**
4. In the **Monitoring** section, verify that the **Enable Monitoring** box is checked.
5. Use the default values for the remaining fields.
6. Click on "**Commit**".

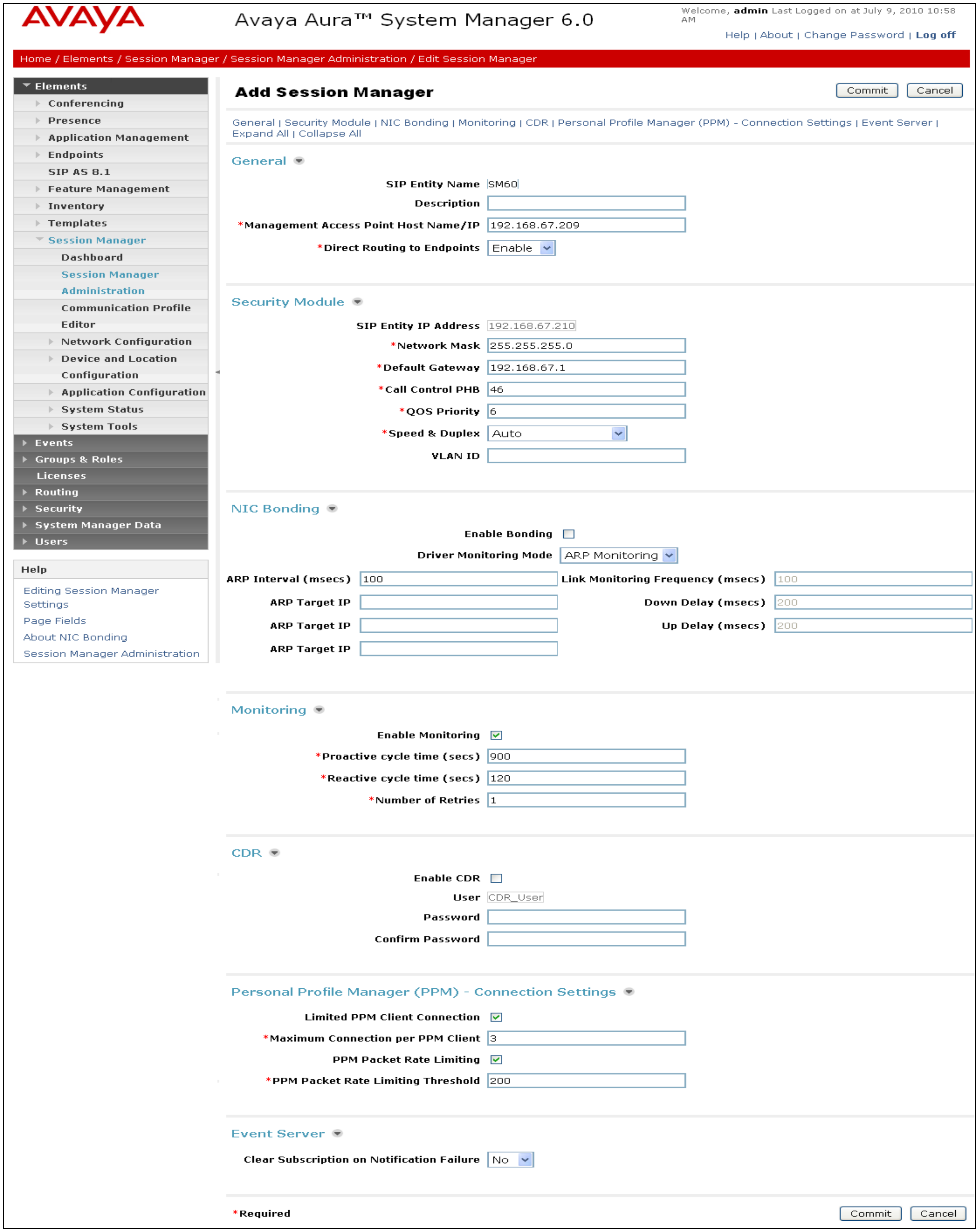



**Figure 30: Add Session Manager Page**

# 5. Avaya Aura® Communication Manager 5.2.1

In the reference configuration Communication Manager 5.2.1 is provisioned in an Access Element configuration, supporting H.323 and Digital endpoints (SIP endpoints are not supported in this configuration). This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration, including stations, C-LAN, Media Processor, and announcement boards, etc., 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 these application notes. Other parameter values may or may not match based on 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 (e.g. 5000).

```
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: 5000  250
  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 31: System-Parameters Customer-Options Form – Page 2**

2. On Page 4 of the **system-parameters customer-options** form:
   a. Verify that the **IP Trunks** field in the following screenshot is set to "**y**".

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

   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? 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 32: System-Parameters Customer-Options Form – Page 4**

## 5.2. Dial Plan

Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings administered in **Figure 33**:

- 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.
- 5-digit extensions with a **Call Type** of "**ext**" beginning with the digits "**26**" – 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**") beginning with the digit "**8**" – access code for outbound AAR dialing
- 1-digit facilities access code (indicated with a **Call Type** of "**fac**") beginning with the digit "**9**" – access code for outbound ARS dialing.

```
change dialplan analysis                                      Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location:  all         Percent Full:    2
       Dialed    Total  Call    Dialed    Total  Call     Dialed    Total  Call
       String    Length Type    String    Length Type     String    Length Type
     1             3    dac
     26            5    ext
     8             1    fac
     9             1    fac
```

**Figure 33: Dialplan Analysis 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 (region 1) and all internal calls use a single IP codec set. This section describes the steps for administering an additional IP network region to represent the AT&T IP Flexible Reach service, and another IP codec set for inbound or outbound AT&T IP Flexible Reach calls.

### 5.3.1. IP Codec Parameters

1. Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used only for internal calls. On Page 1 of the **ip-codec-set** form, ensure that "**G.711MU**", "**G.729B**", and "**G.729A**" are included in the codec list as shown in **Figure 34**.
2. Use the default values for page 2 of this form.

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

                          IP Codec Set

    Codec Set: 1

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

**Figure 34: IP-Codec-Set Form for Internal Calls – Page 1**

3. Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g. **2**). This IP codec set will be used for inbound and outbound AT&T IP Flexible Reach calls.
    a. On Page 1 of the **ip-codec-set** form, provision the codecs in the order shown in **Figure 35**.
    b. For G729B and G729A, set the **Frames Per Pkt** to **3** (the **Packet Size** column will automatically change to **30**). Let the G711MU codec default to 20.

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

                          IP Codec Set
    Codec Set: 2

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

**Figure 35: IP-Codec-Set 2 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 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         off                     0
    Clear-channel   n                       0
```

**Figure 36: IP-Codec-Set 2 Form for External Calls – Page 2**

## 5.3.2. IP Network Regions

### 5.3.2.1 IP Network Region 1 – Local Region

In the reference configuration local Communication Manager elements (e.g. C-LANs) as well as other local Avaya devices (e.g. Modular Messaging) are assigned to ip-network-region 1.

1. Enter a descriptive name (e.g. **Local**).
2. Enter the **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g. **region 1**). This IP network region will be used to represent the AT&T IP Flexible Reach service.
   - Enter **1** for the **Codec Set** parameter.
   - **Intra IP-IP Audio Connections** – Set to "**yes**", indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible within the same region.
   - **Inter IP-IP Audio Connections** – Set to "**yes**", indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible between regions.
   - **UDP Port Min**: - Set to **16384**
   - **UDP Port Max**: - Set to **32767**

```
change ip-network-region 1                                    Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: customera.com
    Name: Local
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                      IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS                    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
```

**Figure 37: IP-Network-Region Form for the Avaya Aura® Communication Manager elements – Page 1**

On page 3 of the form, you can verify that region 1 is using codec 1 as specified on page 1 (this field is automatically populated).

```
change ip-network-region 1                                     Page   3 of  19

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

**Figure 38: IP-Network-Region Form for the Avaya Aura® Communication Manager elements – Page 3**

On Page 6 of the **ip-network-region** form, set region 51 (see the next section) to communicate to region 1 using codec 2 as follows:

- **codec set** – Set to codec set **2**.
- **direct WAN** – Set to "**y**".
- **WAN-BW-limits** – Set to the maximum number of calls or bandwidth allowed between the two IP network regions.

```
change ip-network-region 1                                     Page   6 of  19

 Source Region:  1    Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 48
 49
 50
 51    2     y    NoLimit                                               n
```

**Figure 39: IP-Network-Region Form for the Avaya Aura® Communication Manager elements – Page 6**

### 5.3.2.2 IP Network Region 51 – SIP Trunking Region

In the reference configuration SIP trunk calls to and from AT&T are assigned to ip-network-region 51.

1. Enter the **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g. **region 51**). This IP network region will be used to access the AT&T IP Flexible Reach service.
   - Enter **2** for the **Codec Set** parameter.
   - **Intra IP-IP Audio Connections** – Set to "**yes**", indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible within the same region.
   - **Inter IP-IP Audio Connections** – Set to "**yes**", indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible between regions.
   - **UDP Port Min**: - Set to **16384**
   - **UDP Port Max**: - Set to **32767**

```
change ip-network-region 51                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 51
Location:        Authoritative Domain: customera.com
    Name: AT&T IPFR
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 40: IP-Network-Region Form for the AT&T IP Flexible Reach Service – Page 1**

On Page 3 of the **ip-network-region** form, set region 1 to communicate to region 51 using codec 2 as follows:

- **codec set** – Set to the codec to **2**.
- **direct WAN** – Set to "**y**".
- **WAN-BW-limits** – Set to the maximum number of calls or bandwidth allowed between the two IP network regions.

```
change ip-network-region 51                                     Page   3 of  19

 Source Region: 51    Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    2     y    NoLimit                                             n
 2
 3
```

**Figure 41: IP-Network-Region Form for the AT&T IP Flexible Reach Service– Page 3**

On page 6 of the form, you can verify that region 51 is using codec 2 as specified on page 1 (this field is automatically populated).

```
change ip-network-region 51                                 Page   6 of  19

 Source Region: 51    Inter Network Region Connection Management     I      M
                                                                     G  A   e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G   a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L   s
 48
 49
 50
 51    2
```

**Figure 42: IP-Network-Region Form for the AT&T IP Flexible Reach Service – Page 6**

### 5.3.3. IP Node Names Parameters

Node names define IP addresses to various Avaya components in the CPE.

1. Enter the **change node-names ip** command, and add a node name and the IP address for Session Manager (**SM60**). Also note the node name and IP address of a C-LAN board (**MainCLAN1a03**) that is assigned to IP network region 1 as described in **Section 5.3**. The C-LAN board will be used in **Section 5.4** for administering a SIP trunks to Session Manager.

```
change node-names ip                                        Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
Gateway001          192.168.67.1
MainCLAN1A03        192.168.67.14
MainMP1A04          192.168.67.15
SM60                192.168.67.210
MainVAL1A06         192.168.67.17
default             0.0.0.0
procr               0.0.0.0
```

**Figure 43: Change Node-Names IP Form**

## 5.4. SIP Trunks

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

- Inbound – SIP Trunk 52
- Outbound – SIP Trunk 51
- Modular Messaging – SIP Trunk 50

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

### 5.4.1. Inbound SIP Trunk

This section describes the steps for administering the inbound SIP trunk from Session Manager. This trunk corresponds to the Main_Site_CLAN_1 SIP Entity defined in **Section 4.6.2**. Communication Manager looks at the contents of the PAI for admission control to the Signaling Groups.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **52**), and provision the following:
   - **Group Type** – Set to "**sip**".
   - **Transport Method** – Set to "**tcp**". **Note** – In the reference configuration TCP was used to simplify protocol tracing, however TLS/port 5061 is the Avaya best practices recommendation. The transport protocol used between Session Manager and the Acme Packet SBC is TCP, and the transport protocol used between the Acme Packet SBC and the AT&T IP Flexible Reach service is UDP.
   - **Near-end Node Name** – Set to the node name of the C-LAN board noted in **Section 5.3.3**.
   - **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.3.3**.
   - **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 **51**, as defined in **Section 5.3.2** to represent the AT&T IP Flexible Reach service.
   - **Far-end Domain** – Leave blank. **Note** – leaving this field blank allows inbound calls from any source IP address or FQDN.
   - **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 MedPro resources when possible.
   - **Enable Layer 3 Test** – Set to "y" to have Communication Manager send SIP OPTIONS "pings" to Session Manager for link status.

```
add signaling-group 52
                                SIGNALING GROUP
 Group Number: 52             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
   Near-end Node Name: MainCLAN1A02          Far-end Node Name: MainSM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 51
Far-end Domain:
                                             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                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

**Figure 44: Signaling-Group 52 Form for Inbound AT&T Calls**

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **52**). On Page 1 of the **trunk-group** form, provision the following:
   - **Group Type** – Set to "**sip**".
   - **Group Name** – Enter a descriptive name (e.g. **ASM-Inbound**).

- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **152**).
- **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 52                                                     Page   1 of  21
                                TRUNK GROUP

Group Number: 52                   Group Type: sip           CDR Reports: y
  Group Name: ASM - Inbound             COR: 1        TN: 1        TAC: 152
   Direction: incoming        Outgoing Display? n
 Dial Access? n                                     Night Service:
                                     Auth Code? n
Service Type: public-ntwrk
                                                           Signaling Group: 52
                                                         Number of Members: 20
```

**Figure 45: Trunk-Group 52 Form for Inbound AT&T Calls – Page 1**

### 5.4.2. Outbound SIP Trunk

This section describes the steps for administering the outbound SIP trunk to Session Manager. This trunk corresponds to the Acme SIP Entity defined in **Section 4.6.3.**

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **51**), and provision the following:
    - **Group Type** – Set to "**sip**".
    - **Transport Method** – Set to "**tcp**". **Note** – In the reference configuration TCP was used to simplify protocol tracing, however TLS/port 5061 is the Avaya best practices recommendation. The transport protocol used between Session Manager and the Acme Packet SBC is TCP, and the transport protocol used between the Acme Packet SBC and the AT&T IP Flexible Reach service is UDP.
    - **Near-end Node Name** – Set to the node name of the C-LAN board noted in **Section 5.3.3**.
    - **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 3.3.3**.
    - **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 **51**, as defined in **Section 5.3.2 Step 1** to represent the AT&T IP Flexible Reach service.
    - **Far-end Domain** – Set to the local SIP domain – **customera.com**. This is the same SIP domain specified for Session Manager in **Section 4.3**.
    - **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 MedPro resources when possible.

- **Enable Layer 3 Test** – Set to “y” to have Communication Manager send SIP OPTIONS “pings” to Session Manager for link status.

```
add signaling-group 51
                                SIGNALING GROUP
 Group Number: 51              Group Type: sip
                         Transport Method: tcp
  IMS Enabled? n
   Near-end Node Name: MainCLAN1A02          Far-end Node Name: MainSM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 51
Far-end Domain:customera.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

**Figure 46: Signaling-Group 51 Form for Outbound Calls to AT&T**

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group.
   a. On Page 1 of the **trunk-group** form, provision the following:
      - **Group Type** – Set to “**sip**”.
      - **Group Name** – Enter a descriptive name (e.g. **ASM - Outbound**).
      - **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **151**).
      - **Direction** – Set to “**outgoing”**
      - **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 51                                            Page   1 of  21
                                TRUNK GROUP
Group Number: 51                   Group Type: sip            CDR Reports: y
  Group Name: ASM - Outbound             COR: 1        TN: 1        TAC: 151
   Direction: outgoing       Outgoing Display? n
 Dial Access? n                                    Night Service:
                                    Auth Code? n
Service Type: public-ntwrk
                                                      Signaling Group: 51
                                                    Number of Members: 20
```

**Figure 47: Trunk-Group 51 Form for Outbound Calls to AT&T – Page 1**

   b. On Page 2 of the **Trunk Group** form:
      - Set the **Preferred Minimum Session Refresh Interval(sec):** to **900.** This entry will actually cause a value of 1800 to be generated in the SIP header.

```
add trunk-group 51                                              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
```
**Figure 48: Outbound Voice Trunk Group 51 – Page 2**

c. On Page 3 of the **Trunk Group** form:
   - Set N**umbering Format:** to **public**

```
add trunk-group 51                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y
                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
 Show ANSWERED BY on Display? y
```
**Figure 49: Outbound Voice Trunk Group 51 – Page 3**

d. On Page 4 of the **Trunk Group** form:
   - Set "**Send Diversion Header"** to **Y**
   - Set "**Telephone Event Payload Type**" to the RTP payload type required by the AT&T IP Flexible Reach service. Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Flexible Reach service to determine this value.
   - Let all other values default.

**Note** – The AT&T IP Flexible Reach service does not support History Info headers however Communication Manager enables History Info Headers by default (*Support Request History? y*). Although these headers could be disabled my changing this setting to "N", in the reference configuration this default value is used and Session Manager is configured to remove any History Info Headers sent by Communication Manager.

```
add trunk-group 51                                          Page   4 of  21
                               PROTOCOL VARIATIONS
                       Mark Users as Phone? n
             Prepend '+' to Calling Number? n
      Send Transferring Party Information? n

                      Send Diversion Header? y
                     Support Request History? y
             Telephone Event Payload Type: 100
```
**Figure 50: Outbound Voice Trunk Group 51 – Page 4**

### 5.4.3. Modular Messaging SIP Trunk

This section describes the steps for administering the outbound SIP trunk to Avaya Modular Messaging. This trunk corresponds to the Modular Messaging SIP Entity defined in **Section 4.6.4.**

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **50**), and provision the following:
    - **Group Type** – Set to "**sip**".
    - **Transport Method** – Set to "**tcp**".
    - **Near-end Node Name** – Set to the node name of the C-LAN board noted in **Section 5.3.3**.
    - **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.3.3**.
    - **Near-end Listen Port** and **Far-end Listen Port** – set to "**5060**"
    - **Far-end Network Region** – Set to the IP network region to **1**, as defined in **Section 5.3.2**.
    - **Far-end Domain** – Set to the local SIP domain – customera.com. **Note** – This is the same SIP domain specified for Session Manager in **Section 4.3**.
    - **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 "**n**".

```
add signaling-group 50
                                SIGNALING GROUP
 Group Number: 50             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
   Near-end Node Name: MainCLAN1A02          Far-end Node Name: MainSM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
Far-end Domain: customera.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                       Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

**Figure 51: Signaling-Group 50 Form for Modular Messaging Calls**

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **50**). On Page 1 of the **trunk-group** form, provision the following:
    - **Group Type** – Set to "**sip**".
    - **Group Name** – Enter a descriptive name (e.g. **Modular_Messaging**).
    - **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **150**).
    - **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 (e.g. **20**).

```
add trunk-group 50                                              Page   1 of  21
                                TRUNK GROUP
Group Number: 50                   Group Type: sip          CDR Reports: y
  Group Name: ASM - Outbound             COR: 1        TN: 1        TAC: 150
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
                                    Auth Code? n
Service Type: tie
                                                        Signaling Group: 50
                                                      Number of Members: 20
```

**Figure 52: Trunk-Group 50 Form for Modular Messaging Calls – Page 1**

## 5.5. Public Unknown Numbering

For AT&T IP Flexible Reach service call admission control purposes, calling number origination SIP header contents (e.g. From and PAI) need to be converted to public numbers (previously identified to AT&T), instead of Communication Manager local extensions. In addition, Avaya Modular Messaging also uses these headers for mail-box processing. These functions may be accomplished using the Communication Manager *change public-unknown-numbering* command.

1. Enter the **change public-unknown-numbering 0** command to specify that the numbers assigned by the AT&T IP Flexible Reach service are returned to the PSTN. In the **public-unknown-numbering** form, for each local extension range assigned to Avaya Aura® Communication Manager (phones, agents, skills, hunt groups, or VDNs), provision an entry as follows:
   - **Ext Len** – Enter the total number of digits in the local extension range.
   - **Ext Code –** Enter enough leading digits to identify the local extension range.
   - **Trk Grp(s)** – Enter the number of the outbound trunk group (e.g. **51**).
   - **CPN Prefix** – Leave blank.
   - **CPN Len** – Enter the total number of digits in the local extension range.

   For example, in **Figure 53**, any extension beginning with 26 and 5 digits long will remain unchanged for trunk 50 (e.g. 26000 Modular Messaging pilot extension processing). However when 5 digit extension 26101 calls out to Session Manager, the originating number will be converted to 17323204383 .

```
change public-unknown-numbering 0                                 Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN            CPN      Total Administered: 3
Len Code          Grp(s)    Prefix         Len      Maximum Entries: 9999
 5  26            50                        5
 5  26101         51        17323204383    11
 5  26103         51        17323204384    11
```

**Figure 53: Public-Unknown-Numbering Form**

## 5.6. Optional Features

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

- Hunt Group 1 – Modular Messaging coverage for Communication Manager extensions.
- VDN 26298/Vector 8 – Auto-attendant.
- VDN 26299/Vector 5 – Meet-me Conference

**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.

### 5.6.1. Hunt Group for Station Coverage to Modular Messaging

Hunt group 1 is used in the reference configuration to verify the Send-All-Calls functionality. The hunt group (e.g. **1**) is defined with the 5 digit Modular Messaging pilot number (e.g. **26000** in **Figure 54**). The hunt group is associated with a coverage path (e.g.**H1** in **Figure 62**) and the coverage path is assigned to a station (e.g. **26102** in **Figure 63**).

```
display hunt-group 1                                          Page   1 of  60
                                  HUNT GROUP
            Group Number: 1                                    ACD? n
              Group Name: MM                                 Queue? n
         Group Extension: 26000                             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 54: Hunt Group 1Form – 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)
     26000                     26000                      8
```

**Figure 55: Hunt Group 1 Form – Page 2**

```
display coverage path 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: 3
                All?             n              n
 DND/SAC/Goto Cover?             y              y
   Holiday Coverage?             n              n
COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1            Rng: 2  Point2:
  Point3:                       Point4:
  Point5:                       Point6:
```

**Figure 56: Coverage Path 1 Form**

```
display station 26102                                       Page   1 of   5
                                     STATION

Extension: 26102                         Lock Messages? n             BCC: 0
     Type: 9620                          Security Code: 123456         TN: 1
     Port: S00000                      Coverage Path 1: 1             COR: 1
     Name: H323-9630                   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: 26102
            Speakerphone: 2-way             Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n
                                             Customizable Labels? y
```

**Figure 57: Station 26102 Form**

## 5.6.2. Auto Attendant

A basic auto-attendant functionality is defined in the reference configuration for DTMF testing. The auto-attendant is defined by a VDN (e.g. **26298**) and a Vector (e.g. **8**). As with other inbound calls from the AT&T IP Flexible Reach service, calls may be directed to the auto-attendant VDN extension via the adaptation described in **Section 4.5.2**.

```
display vdn 26298                                               Page   1 of   2
                            VECTOR DIRECTORY NUMBER

                             Extension: 26298
                                 Name*: auto attend
                           Destination: Vector Number        8

                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

**Figure 58: Auto Attendant VDN**

```
display vector 8                                                Page   1 of   6
                                  CALL VECTOR

    Number: 8                Name: auto attend
                                             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    4   secs hearing ringback
02 collect      5    digits after announcement 26504
03 route-to     digits with coverage n
04 wait-time    5   secs hearing silence
05 stop
06
07
```

**Figure 59: Auto Attendant Vector**

### 5.6.3. Meet-me Conference

A basic meet-me conference functionality is defined in the reference configuration for DTMF testing. The meet-me conference functionality is defined by a VDN (e.g. **26299**) and a Vector (e.g. **5**). As with other inbound calls from the AT&T IP Flexible Reach service, calls may be directed to the meet-me conference VDN extension via the adaptation described in **Section 4.5.2**.

```
display vdn 26299                                               Page   1 of   2
                            VECTOR DIRECTORY NUMBER

                             Extension: 26299
                                  Name: meet-me vdn 1
                           Destination: Vector Number        5

                  Meet-me Conferencing? y
                                   COR: 1
                                    TN: 1
```

**Figure 60: Meet-me Conference VDN – Page 1**

```
display vdn 26299                                               Page   2 of   2
                            VECTOR DIRECTORY NUMBER

                  MEET-ME CONFERENCE PARAMETERS:

                    Conference Access Code: 123456
                     Conference Controller: 26201
                           Conference Type: 6-party
```

**Figure 61: Meet-me Conference VDN – Page 2**

```
display vector 5                                                Page   1 of   6
                                  CALL VECTOR
    Number: 5                Name: meet-me vec
                                             Meet-me Conf? y           Lock? y
     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    5   secs hearing ringback
02 collect      6    digits after announcement 26501
03 goto step    5             if digits           =      meet-me-access
04 goto step    2             if unconditionally
05 announcement 26503
06 route-to     meetme
07 stop
08
```

**Figure 62: Meet-me Conference Vector**

# 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. Configure Acme Packet SBC

These Application Notes assume that basic Acme Packet SBC administration has already been performed. In the reference configuration two Acme Packet Net-Net 3800s[8] are implemented in a High Availability (HA) configuration. The Acme Packet SBC configuration used in the reference configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Consult with Acme Packet Support **[11]** for further details and explanations on the configuration below.

**Note** - The AT&T IP Flexible Reach 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 Flexible Reach provisioning process.

**ANNOTATION**: The local policies below govern the routing of SIP messages from elements on the network on which the Avaya elements, e.g., Session Manager, Communication Manager, etc., reside to the AT&T IP Flexible Reach service. The Session Agent Groups (SAG) defined here, and further down, provisioned under the session-groups "SP-PROXY" and "ENTERPRISE".

```
local-policy
      from-address
                               *
      to-address
                               *
      source-realm
                               INSIDE
      description
      activate-time            N/A
      deactivate-time          N/A
      state                    enabled
      policy-priority          none
      last-modified-by         admin@console
      last-modified-date       2009-11-05 17:50:26

      policy-attribute
            next-hop                 SAG:SP_PROXY
            realm                    OUTSIDE
            action                   none
            terminate-recursion      disabled
            carrier
            start-time               0000
            end-time                 2400
            days-of-week             U-S
            cost                     0
            app-protocol             SIP
```

[8]Although an Acme Net-Net 3800 was used in the reference configuration, theses configurations also apply to the 4250, 4500, and 9200 platforms.

```
          state                            enabled
          methods
          media-profiles
```

**ANNOTATION:** The local policy below governs the routing of SIP messages from the AT&T IP Flexible Reach service to Session Manager.

```
local-policy
      from-address
                                      *
      to-address
                                      *
      source-realm
                                      OUTSIDE
      description
      activate-time                   N/A
      deactivate-time                 N/A
      state                           enabled
      policy-priority                 none
      last-modified-by                admin@console
      last-modified-date              2009-11-04 00:56:55
      policy-attribute
            next-hop                        SAG:ENTERPRISE
            realm                           INSIDE
            action                          none
            terminate-recursion             disabled
            carrier
            start-time                      0000
            end-time                        2400
            days-of-week                    U-S
            cost                            0
            app-protocol                    SIP
            state                           enabled
            methods
            media-profiles


media-manager
      state                           enabled
      latching                        enabled
      flow-time-limit                 86400
      initial-guard-timer             300
      subsq-guard-timer               300
      tcp-flow-time-limit             86400
      tcp-initial-guard-timer         300
      tcp-subsq-guard-timer           300
      tcp-number-of-ports-per-flow    2
      hnt-rtcp                        disabled
      algd-log-level                  NOTICE
      mbcd-log-level                  NOTICE
      red-flow-port                   1985
      red-mgcp-port                   1986
      red-max-trans                   10000
      red-sync-start-time             5000
```

```
      red-sync-comp-time             1000
      media-policing                 enabled
      max-signaling-bandwidth        775880
      max-untrusted-signaling        80
      min-untrusted-signaling        20
      app-signaling-bandwidth        0
      tolerance-window               30
      rtcp-rate-limit                0
      min-media-allocation           2000
      min-trusted-allocation         4000
      deny-allocation                64000
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      dnsalg-server-failover         disabled
      last-modified-by               admin@console
      last-modified-date             2009-11-04 00:34:23


network-interface
      name                           wancom1
      sub-port-id                    0
      description
      hostname
      ip-address
      pri-utility-addr               169.254.1.1
      sec-utility-addr               169.254.1.2
      netmask                        255.255.255.252
      gateway
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list
      ftp-address
        icmp-address
      snmp-address
      telnet-address
      last-modified-by               admin@console
      last-modified-date             2009-11-04 00:33:51

network-interface
```

```
name                          wancom2
sub-port-id                   0
description
hostname
ip-address
pri-utility-addr              169.254.2.1
sec-utility-addr              169.254.2.2
netmask                       255.255.255.252
gateway
sec-gateway
gw-heartbeat
      state                         disabled
      heartbeat                     0
      retry-count                   0
      retry-timeout                 1
      health-score                  0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout                   11
  hip-ip-list
ftp-address
  icmp-address
snmp-address
telnet-address
last-modified-by              admin@console
last-modified-date            2009-11-04 00:33:51
```

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

```
network-interface
      name                          s0p0
      sub-port-id                   0
      description
      hostname
      ip-address                    192.168.64.130
      pri-utility-addr              192.168.64.131
      sec-utility-addr              192.168.64.132
      netmask                       255.255.255.0
      gateway                       192.168.64.1
      sec-gateway
      gw-heartbeat
            state                         disabled
            heartbeat                     0
            retry-count                   0
            retry-timeout                 1
            health-score                  0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
```

```
        dns-timeout                   11
          hip-ip-list                   192.168.64.130
        ftp-address
          icmp-address                  192.168.64.130
        snmp-address
        telnet-address
        last-modified-by              admin@console
        last-modified-date            2009-11-06 13:33:09
```

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

```
network-interface
        name                          s0p1
        sub-port-id                   0
        description
        hostname
        ip-address                    192.168.67.130
        pri-utility-addr              192.168.67.131
        sec-utility-addr              192.168.67.132
        netmask                       255.255.255.0
        gateway                       192.168.67.1
        sec-gateway
        gw-heartbeat
              state                         disabled
              heartbeat                     0
              retry-count                   0
              retry-timeout                 1
              health-score                  0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                   11
          hip-ip-list                   192.168.67.130
        ftp-address                   192.168.67.130
          icmp-address                  192.168.67.130
        snmp-address
        telnet-address
        last-modified-by              admin@console
        last-modified-date            2009-11-04 01:40:53


ntp-config
        server                        135.8.139.1
        last-modified-by              admin@console
        last-modified-date            2009-11-04 00:27:53


phy-interface
        name                          s0p1
        operation-type                Media
        port                          1
```

```
        slot                              0
        virtual-mac                       00:08:25:a0:f3:69
        admin-state                       enabled
        auto-negotiation                  enabled
        duplex-mode                       FULL
        speed                             100
        last-modified-by                  admin@console
        last-modified-date                2009-11-04 00:24:39

phy-interface
        name                              s0p0
        operation-type                    Media
        port                              0
        slot                              0
        virtual-mac                       00:08:25:a0:f3:68
        admin-state                       enabled
        auto-negotiation                  enabled
        duplex-mode                       FULL
        speed                             100
        last-modified-by                  admin@console
        last-modified-date                2009-11-04 00:29:41

phy-interface
        name                              s1p0
        operation-type                    Media
        port                              0
        slot                              1
        virtual-mac                       00:08:25:a0:f3:6e
        admin-state                       disabled
        auto-negotiation                  enabled
        duplex-mode                       FULL
        speed                             100
        last-modified-by                  admin@console
        last-modified-date                2009-11-04 00:33:23

phy-interface
        name                              s1p1
        operation-type                    Media
        port                              1
        slot                              1
        virtual-mac                       00:08:25:a0:f3:6f
        admin-state                       disabled
        auto-negotiation                  enabled
        duplex-mode                       FULL
        speed                             100
        last-modified-by                  admin@console
        last-modified-date                2009-11-04 00:33:23

phy-interface
        name                              wancom1
        operation-type                    Control
```

```
        port                          1
        slot                          0
        virtual-mac
        wancom-health-score           8
        last-modified-by              admin@console
        last-modified-date            2009-11-04 00:33:51


phy-interface
        name                          wancom2
        operation-type                Control
        port                          2
        slot                          0
        virtual-mac
        wancom-health-score           9
        last-modified-by              admin@console
        last-modified-date            2009-11-04 00:33:51
```

**ANNOTATION**: The realm configuration "OUTSIDE" below represents the external network on which the AT&T IP Flexible Reach service resides, and applies the SIP manipulation NAT_IP.

```
realm-config
        identifier                    OUTSIDE
        description
        addr-prefix                   0.0.0.0
        network-interfaces
                                      s0p0:0
        mm-in-realm                   enabled
        mm-in-network                 enabled
        mm-same-ip                    enabled
        mm-in-system                  enabled
        bw-cac-non-mm                 disabled
        msm-release                   disabled
        generate-UDP-checksum         disabled
        max-bandwidth                 0
        fallback-bandwidth            0
        max-priority-bandwidth        0
        max-latency                   0
        max-jitter                    0
        max-packet-loss               0
        observ-window-size            0
        parent-realm
        dns-realm
        media-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid            NAT_IP
        manipulation-string
        class-profile
        average-rate-limit            0
        access-control-trust-level    medium
```

```
invalid-signal-threshold       4
maximum-signal-threshold       3000
untrusted-signal-threshold     10
nat-trust-threshold            0
deny-period                    60
ext-policy-svr
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            disabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
last-modified-by               admin@console
last-modified-date             2009-11-04 00:41:24
```

**ANNOTATION**: The realm configuration "INSIDE" below represents the internal network on which the Avaya elements reside.

```
realm-config
      identifier                     INSIDE
      description
      addr-prefix                    0.0.0.0
      network-interfaces
                                     s0p1:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
```

```
msm-release                    disabled
generate-UDP-checksum          disabled
max-bandwidth                  0
fallback-bandwidth             0
max-priority-bandwidth         0
max-latency                    0
max-jitter                     0
max-packet-loss                0
observ-window-size             0
parent-realm
dns-realm
media-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
class-profile
average-rate-limit             0
access-control-trust-level     high
invalid-signal-threshold       0
maximum-signal-threshold       0
untrusted-signal-threshold     0
nat-trust-threshold            0
deny-period                    30
ext-policy-svr
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            disabled
codec-policy
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
```

```
      qos-constraint
      last-modified-by               admin@console
      last-modified-date             2009-11-04 00:49:58


redundancy-config
      state                          enabled
      log-level                      INFO
      health-threshold               75
      emergency-threshold            50
      port                           9090
      advertisement-time             500
      percent-drift                  210
      initial-time                   1250
      becoming-standby-time          180000
      becoming-active-time           100
      cfg-port                       1987
      cfg-max-trans                  10000
      cfg-sync-start-time            5000
      cfg-sync-comp-time             1000
      gateway-heartbeat-interval     0
      gateway-heartbeat-retry        0
      gateway-heartbeat-timeout      1
      gateway-heartbeat-health       0
      media-if-peercheck-time        0
      peer
            name                           acmesbc-pri
            state                          enabled
            type                           Primary
            destination
                  address                        169.254.1.1:9090
                  network-interface              wancom1:0
            destination
                  address                        169.254.2.1:9090
                  network-interface              wancom2:0
      peer
            name                           acmesbc-sec
            state                          enabled
            type                           Secondary
            destination
                  address                        169.254.1.2:9090
                  network-interface              wancom1:0
            destination
                  address                        169.254.2.2:9090
                  network-interface              wancom2:0
      last-modified-by               admin@console
      last-modified-date             2009-11-04 00:34:07
```

**ANNOTATION**: The **session agent** below represents the AT&T IP Flexible Reach service border element. The Acme will attempt to send calls to the border element based on successful responses to the OPTIONS "ping-method". The AT&T IP Flexible Reach service border element is also specified in the **session-group** section below. Note – See Addendum 1 for an example of redundant session-agents.

```
session-agent
      hostname                       135.25.29.74
      ip-address                     135.25.29.74
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       OUTSIDE
      egress-realm-id
      description                    AT&T_BE
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=20
      ping-interval                  60
      ping-send-mode                 keep-alive
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                       disabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                    disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
```

```
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
last-modified-by               admin@console
last-modified-date             2009-12-01 14:51:04
```

| |
|---|
| **ANNOTATION**: The session agent below represents the Session Manager used in the reference configuration. |

```
session-agent
      hostname                       192.168.67.210
      ip-address                     192.168.67.210
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               staticTCP
      realm-id                       INSIDE
      egress-realm-id
      description                    Session Manager_6_0
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
```

```
redirect-action
loose-routing                   enabled
send-media-session              enabled
response-map
ping-method                     OPTIONS;hops=0
ping-interval                   60
ping-send-mode                  keep-alive
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                        disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                     disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate       0
early-media-allow
invalidate-registrations        disabled
rfc2833-mode                    none
rfc2833-payload                 0
codec-policy
enforcement-profile
refer-call-transfer             disabled
reuse-connections               TCP
tcp-keepalive                   none
tcp-reconn-interval             0
max-register-burst-rate         0
register-burst-window           0
last-modified-by                admin@console
last-modified-date              2009-11-04 00:54:44
```

**ANNOTATION**: The **session group** below specifies the AT&T IP Flexible Reach service border element (see **session-agent 135.25.29.74** above).

Note - Multiple session-agents may be specified in a session-group. The *strategy* parameter may be used to select how these multiple session-agents are used (e.g. *Hunt* and *RoundRobin*).

```
session-group
      group-name                SP_PROXY
      description
      state                     enabled
      app-protocol              SIP
      strategy                  RoundRobin
      dest
```

```
                                       135.25.29.74
      trunk-group
      sag-recursion                    disabled
      stop-sag-recurse                 401,407
      last-modified-by                 admin@console
      last-modified-date               2009-12-04 20:10:41
```

> **ANNOTATION**: The session group below represents Session Manager. This session-group is specified in the local-policy source-realm "OUTSIDE". Please note that multiple destinations can be added if more than one Session Manager exists.

```
session-group
      group-name                       ENTERPRISE
      description
      state                            enabled
      app-protocol                     SIP
      strategy                         Hunt
      dest
                                       192.168.67.210
      trunk-group
      sag-recursion                    disabled
      stop-sag-recurse                 401,407
      last-modified-by                 admin@console
      last-modified-date               2009-11-05 17:52:47
```

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

```
sip-config
      state                            enabled
      operation-mode                   dialog
      dialog-transparency              enabled
      home-realm-id                    INSIDE
      egress-realm-id                  INSIDE
      nat-mode                         None
      registrar-domain
      registrar-host
      registrar-port                   0
      register-service-route           always
      init-timer                       500
      max-timer                        4000
      trans-expire                     32
      invite-expire                    180
      inactive-dynamic-conn            32
      enforcement-profile
      pac-method
      pac-interval                     10
      pac-strategy                     PropDist
      pac-load-weight                  1
```

```
      pac-session-weight            1
      pac-route-weight              1
      pac-callid-lifetime           600
      pac-user-lifetime             3600
      red-sip-port                  1988
      red-max-trans                 10000
      red-sync-start-time           5000
      red-sync-comp-time            1000
      add-reason-header             disabled
      sip-message-len               4096
      enum-sag-match                disabled
      extra-method-stats            enabled
      registration-cache-limit      0
      register-use-to-for-lp        disabled
      options                       max-udp-length=0
                                      set-inv-exp-at-100-resp
      add-ucid-header               disabled
      last-modified-by              admin@console
      last-modified-date            2009-11-04 00:34:23


sip-feature
      name                          Replaces
      realm
      support-mode-inbound          Pass
      require-mode-inbound          Pass
      proxy-require-mode-inbound    Pass
      support-mode-outbound         Pass
      require-mode-outbound         Pass
      proxy-require-mode-outbound   Pass
      last-modified-by              admin@console
      last-modified-date            2010-03-11 15:51:36
```

**ANNOTATION**: The SIP interface below is used to communicate with the AT&T IP Flexible Reach service.

```
sip-interface
      state                         enabled
      realm-id                      OUTSIDE
      description
      sip-port
            address                       192.168.64.130
            port                          5060
            transport-protocol            UDP
            tls-profile
            allow-anonymous               agents-only
            ims-aka-profile
      carriers
      trans-expire                  0
      invite-expire                 0
      max-redirect-contacts         0
      proxy-mode
      redirect-action
      contact-mode                  none
```

```
nat-traversal                  none
nat-interval                   30
tcp-nat-interval               90
registration-caching           disabled
min-reg-expire                 300
registration-interval          3600
route-to-registrar             disabled
secured-network                disabled
teluri-scheme                  disabled
uri-fqdn-domain
trust-mode                     all
max-nat-interval               3600
nat-int-increment              10
nat-test-increment             30
sip-dynamic-hnt                disabled
stop-recurse                   401,407
port-map-start                 0
port-map-end                   0
in-manipulationid
out-manipulationid
manipulation-string
sip-ims-feature                disabled
operator-identifier
anonymous-priority             none
max-incoming-conns             0
per-src-ip-max-incoming-conns  0
inactive-conn-timeout          0
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
refer-call-transfer            disabled
route-unauthorized-calls
tcp-keepalive                  none
add-sdp-invite                 disabled
add-sdp-profiles
last-modified-by               admin@console
last-modified-date             2009-11-04 00:49:24
```

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

```
sip-interface
      state                           enabled
      realm-id                        INSIDE
      description
      sip-port
            address                         192.168.67.130
            port                            5060
            transport-protocol              TCP
            tls-profile
            allow-anonymous                 agents-only
            ims-aka-profile
      carriers
      trans-expire                    0
      invite-expire                   0
      max-redirect-contacts           0
      proxy-mode
      redirect-action
      contact-mode                    none
      nat-traversal                   none
      nat-interval                    30
      tcp-nat-interval                90
      registration-caching            disabled
      min-reg-expire                  300
      registration-interval           3600
      route-to-registrar              disabled
      secured-network                 disabled
      teluri-scheme                   disabled
      uri-fqdn-domain
      trust-mode                      all
      max-nat-interval                3600
      nat-int-increment               10
      nat-test-increment              30
      sip-dynamic-hnt                 disabled
      stop-recurse                    401,407
      port-map-start                  0
      port-map-end                    0
      in-manipulationid
      out-manipulationid
      manipulation-string
      sip-ims-feature                 disabled
      operator-identifier
      anonymous-priority              none
      max-incoming-conns              0
      per-src-ip-max-incoming-conns   0
      inactive-conn-timeout           0
      untrusted-conn-timeout          0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode            pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                  none
```

```
      implicit-service-route         disabled
      rfc2833-payload                101
      rfc2833-mode                   transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                disabled
      enforcement-profile
      refer-call-transfer            disabled
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      last-modified-by               admin@console
      last-modified-date             2009-11-04 00:50:10
```

**ANNOTATION**: The **NAT_IP** SIP manipulation below performs address translation and topology hiding for SIP messages between the AT&T IP Flexible Reach services and the Avaya elements. The NAT function is comprised of the header rules **manipFrom** and **manipTo**.
In the header-rule **manipFrom**, the **match-val-type** value **any** allows the either the IP address or SIP Domain of Session Manager to be specified in the far-end domain field of the Communication Manager signaling group 51 (see **Section 5.4**). In either case, the Acme will convert this value to the "outside" IP address of the Acme (**$Local_IP**).
In the header-rule **manipTo**, the **match-val-type** value **any** allows either the IP address or SIP Domain of Session Manager to be specified in the far-end domain field of the Communication Manager signaling group 51 (see **Section 5.4**). In either case the Acme will convert this value to the IP address of the AT&T IP Flexible Reach border element (**$Remote_IP**).

```
sip-manipulation
      name                           NAT_IP
      description
      header-rule
            name                           manipFrom
            header-name                    From
            action                         manipulate
            comparison-type                case-sensitive
            match-value
            msg-type                       request
            new-value
            methods
            element-rule
                  name                           FROM
                  parameter-name
                  type                           uri-host
                  action                         replace
                  match-val-type                 any
                  comparison-type                case-sensitive
                  match-value
                  new-value                      $LOCAL_IP
```

```
header-rule
      name                              manipTo
      header-name                       To
      action                            manipulate
      comparison-type                   case-sensitive
      match-value
      msg-type                          request
      new-value
      methods
      element-rule
            name                              TO
            parameter-name
            type                              uri-host
            action                            replace
            match-val-type                   any
            comparison-type                   case-sensitive
            match-value
            new-value                         $REMOTE_IP
```

**ANNOTATION**: - In order to provide the Acme outside address in the Diversion headers, the following header-rule was added to the existing NAT_IP sip-manipulation.

```
header-rule
      name                              manipDiversion
      header-name                       Diversion
      action                            manipulate
      comparison-type                   case-sensitive
      msg-type                          any
      methods                           INVITE
      match-value
      new-value
      element-rule
            name                              Diversion
            parameter-name
            type                              uri-host
            action                            replace
            match-val-type                    any
            comparison-type                   case-sensitive
            match-value
            new-value                         $LOCAL_IP
      last-modified-by              admin@console
      last-modified-date            2010-09-15 12:44:02
```

**ANNOTATION**: *OPTIONAL* - In addition to manipulating the From and To headers, the NAT_IP SIP manipulation also is used to delete a P-Site header inserted by Session Manager. Session Manager Release 6.0 inserts a P-Site header which contains the IP-Address of System Manager as a parameter. Since there is no value in sending this header to AT&T in the sample configuration, the header is stripped by the Acme Packet SBC. Calls can still be completed successfully if the configuration in this section is not performed and the P-Site header is sent to AT&T. This information is included to allow the reader to delete the P-Site header if desired so that the private IP address of System Manager is not revealed on the public side of the SBC.

```
header-rule
        name                            deletePSITE
        header-name                     P-Site
        action                          delete
        comparison-type                 pattern-rule
        match-value
        msg-type                        request
        new-value
        methods
    last-modified-by                admin@console
    last-modified-date              2010-06-09 19:58:37
```

**ANNOTATION**: The steering pools below define the IP Addresses and RTP port ranges on the respective realms. The "OUTSIDE" realm IP Address will be used as the CPE media traffic IP Address to communicate with AT&T. **The "OUTSIDE" realm RTP port range is an AT&T IP Flexible Reach service requirement.** Likewise, the IP Address and RTP port range defined for the "INSIDE" realm steering pool will be used to communicate with the Avaya elements. Please note that the "INSIDE" realm port range does not have to be within the range specified below.

```
steering-pool
    ip-address                      192.168.64.130
    start-port                      16384
    end-port                        32767
    realm-id                        OUTSIDE
    network-interface
    last-modified-by                admin@console
    last-modified-date              2009-11-04 00:49:36

steering-pool
    ip-address                      192.168.67.130
    start-port                      16384
    end-port                        32767
    realm-id                        INSIDE
    network-interface
    last-modified-by                admin@console
    last-modified-date              2009-11-04 00:50:20


system-config
    hostname                        acmesbc
    description
    location
    mib-system-contact
    mib-system-name
    mib-system-location
    snmp-enabled                    enabled
    enable-snmp-auth-traps          disabled
    enable-snmp-syslog-notify       disabled
    enable-snmp-monitor-traps       disabled
```

```
enable-env-monitor-traps        disabled
snmp-syslog-his-table-length    1
snmp-syslog-level               WARNING
system-log-level                WARNING
process-log-level               NOTICE
process-log-ip-address          0.0.0.0
process-log-port                0
collect
      sample-interval                 5
      push-interval                   15
      boot-state                      disabled
      start-time                      now
      end-time                        never
      red-collect-state               disabled
      red-max-trans                   1000
      red-sync-start-time             5000
      red-sync-comp-time              1000
      push-success-trap-state         disabled
call-trace                      disabled
internal-trace                  disabled
log-filter                      all
default-gateway                 135.8.139.1
restart                         enabled
exceptions
telnet-timeout                  0
console-timeout                 0
remote-control                  enabled
cli-audit-trail                 enabled
link-redundancy-state           disabled
source-routing                  enabled
cli-more                        disabled
terminal-height                 24
debug-timeout                   0
trap-event-lifetime             0
last-modified-by                admin@console
last-modified-date              2009-11-04 00:27:17
```

# 8. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura® System Manager 6.0, Avaya Aura® Session Manager 6.0, Avaya Aura® Communication Manager 5.2.1, Avaya phones, fax machines (Ventafax application), Acme Packet Net-Net 3800, and Avaya Modular Messaging.
- A laboratory version of the AT&T IP Flexible Reach service, to which the simulated enterprise was connected via **AVPN** or **MIS/PNT** transport.

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

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

1. 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.
2. 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 5.2.1

The following examples are only a few of the monitoring commands available on Communication Manager. See **[3] and [4]** for more information.

1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where **xx** is a trunk access code defined for the SIP trunk to AT&T (e.g. 151)

```
list trace tac 151                                                Page   1

                                LIST TRACE

time            data

11:41:07 SIP>INVITE sip:15556712438@customera.com SIP/2.0
11:41:07     dial 915556712438 route:PREFIX|FNPA|ARS
11:41:07     route-pattern  51 preference 1  cid 0x9a
11:41:07     seize trunk-group 51 member 2  cid 0x9a
11:41:07     Setup digits 17326712438
11:41:07     Calling Number & Name 15553204384 H323-9650
11:41:07 SIP<SIP/2.0 100 Trying
11:41:07     Proceed trunk-group 51 member 2  cid 0x9a
11:41:09 SIP<SIP/2.0 180 Ringing
11:41:09     Alert trunk-group 51 member 2  cid 0x9a
11:41:09     G729 ss:off ps:30
             rgn:51 [192.168.67.130]:16934
             rgn:1 [192.168.67.15]:26644
11:41:09     xoip options: fax:T38 modem:off tty:US  uid:0x500ae
             xoip ip: [192.168.67.15]:26644
11:41:11 SIP<SIP/2.0 200 OK
11:41:11 SIP>ACK sip:15556712438@192.168.67.130:5060;transport=t
11:41:11 SIP>cp SIP/2.0
11:41:11     active trunk-group 51 member 2  cid 0x9a
11:41:14 SIP>BYE sip:15556712438@192.168.67.130:5060;transport=t
11:41:14 SIP>cp SIP/2.0
11:41:14     idle station    26103 cid 0x9a
```

**Figure 63: Communication Manager *list trace tac 151* – Outbound call.**

2. 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 6.0

The following commands are issued from the System Manager console.

1. Verify the call routing administration on Session Manager.
    a. In the left pane of the Avaya Aura® System Manager Common Console, under **Elements/Session Manager/System Tools**, click on "**Call Routing Test**". The **Call Routing Test** page shown in **Figure 64** will open.
    b. In the **Call Routing Test** page, enter the appropriate parameters of the test call. **Figure 64** shows a routing test for an inbound call from PSTN to AT&T DID

**7323204383** at the IP address of Session Manager (**192.168.67.210**). The call arrives from the Acme Packet SBC and the calling number +1**7323681000**.

c. Click on "**Execute Test**".

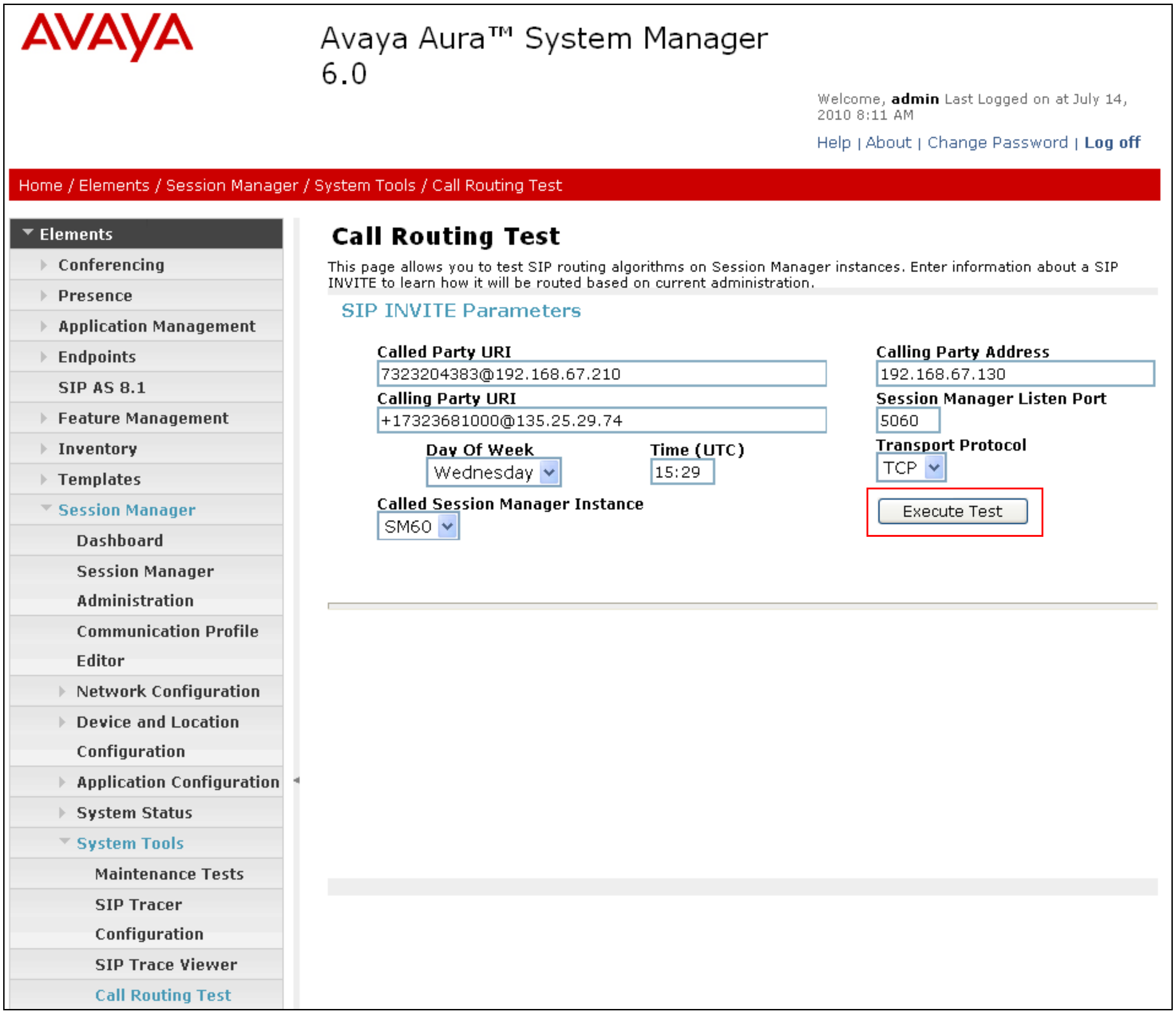



**Figure 64: Session Manager Call Routing Test Page**

d. The results of the test are displayed as shown in **Figure 65.** The ultimate routing decision is displayed under the heading **Routing Decisions.** The example test shows that the PSTN call to **7323204383** is sent by Session Manager to the Communication Manager extension **26103**.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**.

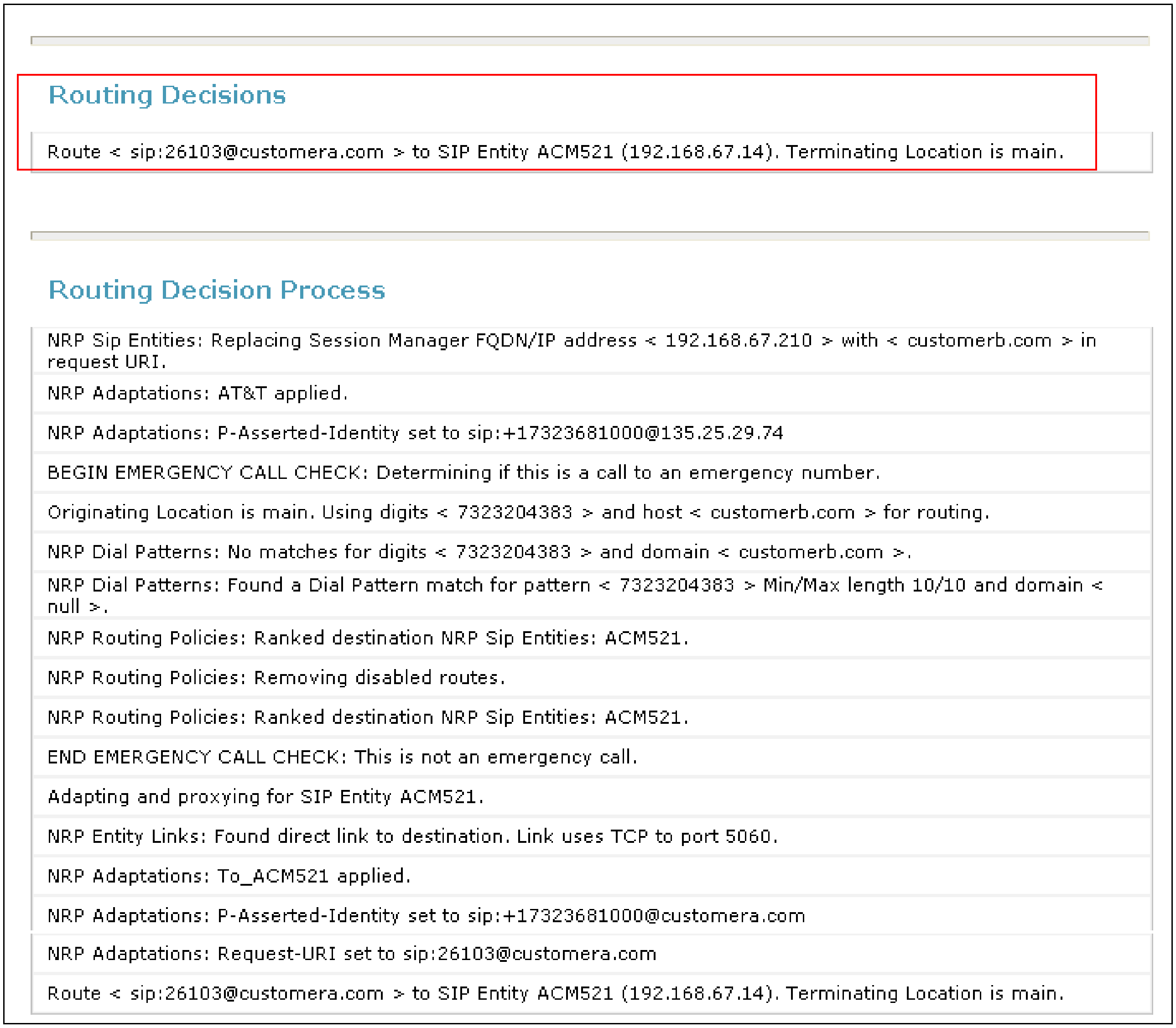
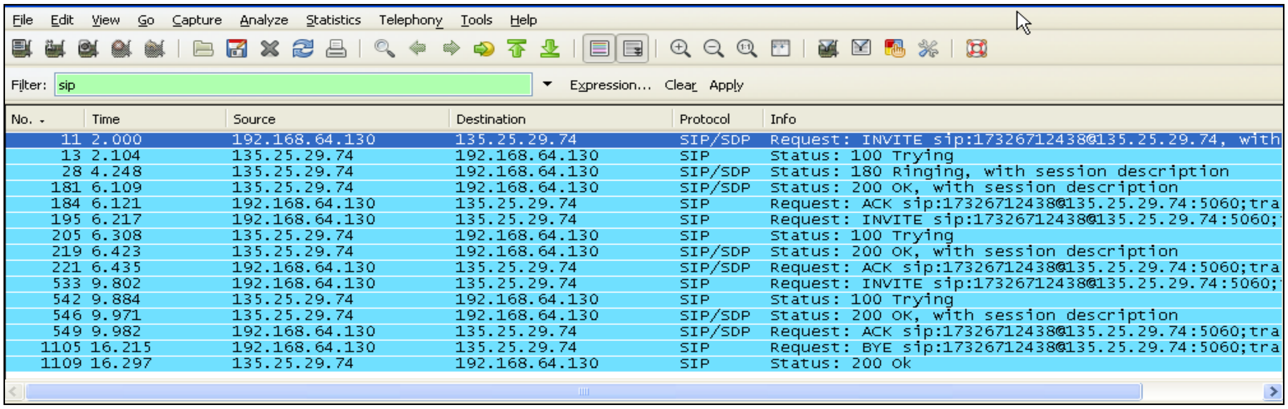



**Figure 65: Call Routing Test Page -Completed**

## 9.4. Protocol Traces

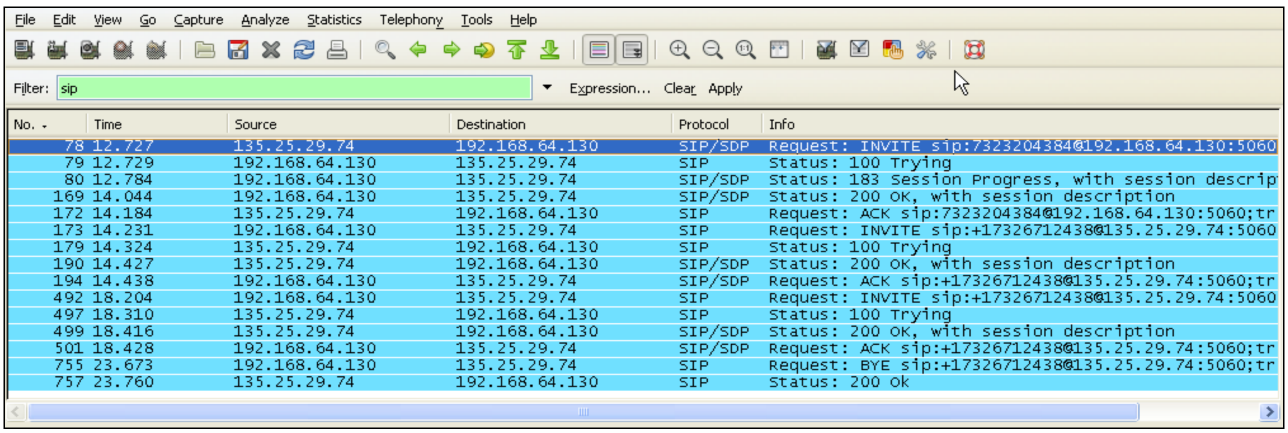
Using a SIP protocol analyzer (e.g. Wireshark), monitor the SIP traffic at the Acme Packet SBC public "outside" interface connection to the AT&T IP Flexible Reach service.

1. The following are examples of outbound and inbound calls filtering on the SIP protocol.




| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 11 | 2.000 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Request: INVITE sip:17326712438@135.25.29.74, with |
| 13 | 2.104 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 100 Trying |
| 28 | 4.248 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Status: 180 Ringing, with session description |
| 181 | 6.109 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Status: 200 OK, with session description |
| 184 | 6.121 | 192.168.64.130 | 135.25.29.74 | SIP | Request: ACK sip:17326712438@135.25.29.74:5060;tra |
| 195 | 6.217 | 192.168.64.130 | 135.25.29.74 | SIP | Request: INVITE sip:17326712438@135.25.29.74:5060; |
| 205 | 6.308 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 100 Trying |
| 219 | 6.423 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Status: 200 OK, with session description |
| 221 | 6.435 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Request: ACK sip:17326712438@135.25.29.74:5060;tra |
| 533 | 9.802 | 192.168.64.130 | 135.25.29.74 | SIP | Request: INVITE sip:17326712438@135.25.29.74:5060; |
| 542 | 9.884 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 100 Trying |
| 546 | 9.971 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Status: 200 OK, with session description |
| 549 | 9.982 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Request: ACK sip:17326712438@135.25.29.74:5060;tra |
| 1105 | 16.215 | 192.168.64.130 | 135.25.29.74 | SIP | Request: BYE sip:17326712438@135.25.29.74:5060;tra |
| 1109 | 16.297 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 200 Ok |

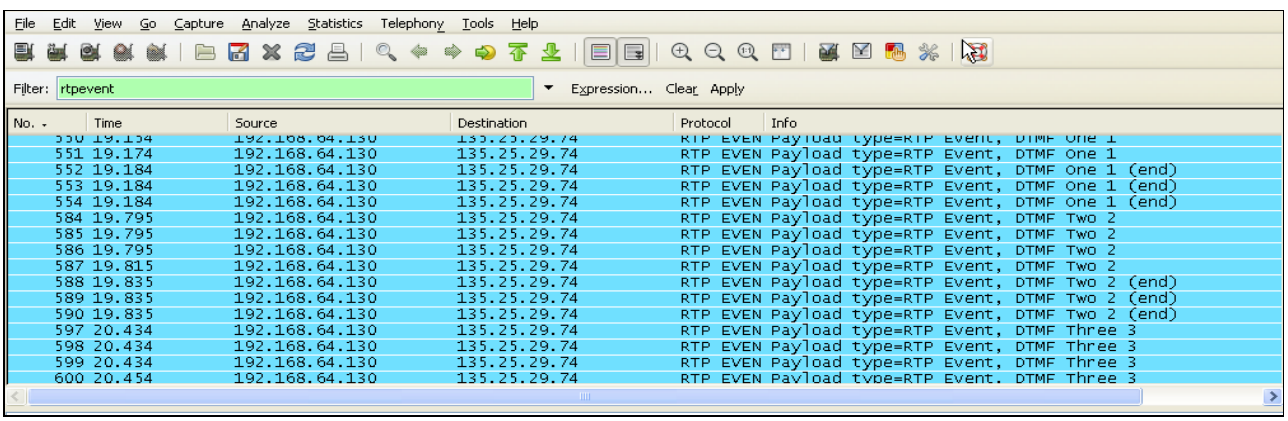
**Figure 66: –SIP Protocol trace – Outbound call to AT&T**




| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 78 | 12.727 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Request: INVITE sip:7323204384@192.168.64.130:5060 |
| 79 | 12.729 | 192.168.64.130 | 135.25.29.74 | SIP | Status: 100 Trying |
| 80 | 12.784 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Status: 183 Session Progress, with session descrip |
| 169 | 14.044 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Status: 200 OK, with session description |
| 172 | 14.184 | 135.25.29.74 | 192.168.64.130 | SIP | Request: ACK sip:7323204384@192.168.64.130:5060;tr |
| 173 | 14.231 | 192.168.64.130 | 135.25.29.74 | SIP | Request: INVITE sip:+17326712438@135.25.29.74:5060 |
| 179 | 14.324 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 100 Trying |
| 190 | 14.427 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Status: 200 OK, with session description |
| 194 | 14.438 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Request: ACK sip:+17326712438@135.25.29.74:5060;tr |
| 492 | 18.204 | 192.168.64.130 | 135.25.29.74 | SIP | Request: INVITE sip:+17326712438@135.25.29.74:5060 |
| 497 | 18.310 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 100 Trying |
| 499 | 18.416 | 135.25.29.74 | 192.168.64.130 | SIP/SDP | Status: 200 OK, with session description |
| 501 | 18.428 | 192.168.64.130 | 135.25.29.74 | SIP/SDP | Request: ACK sip:+17326712438@135.25.29.74:5060;tr |
| 755 | 23.673 | 192.168.64.130 | 135.25.29.74 | SIP | Request: BYE sip:+17326712438@135.25.29.74:5060;tr |
| 757 | 23.760 | 135.25.29.74 | 192.168.64.130 | SIP | Status: 200 Ok |

**Figure 67: –SIP Protocol trace – Inbound call from AT&T**

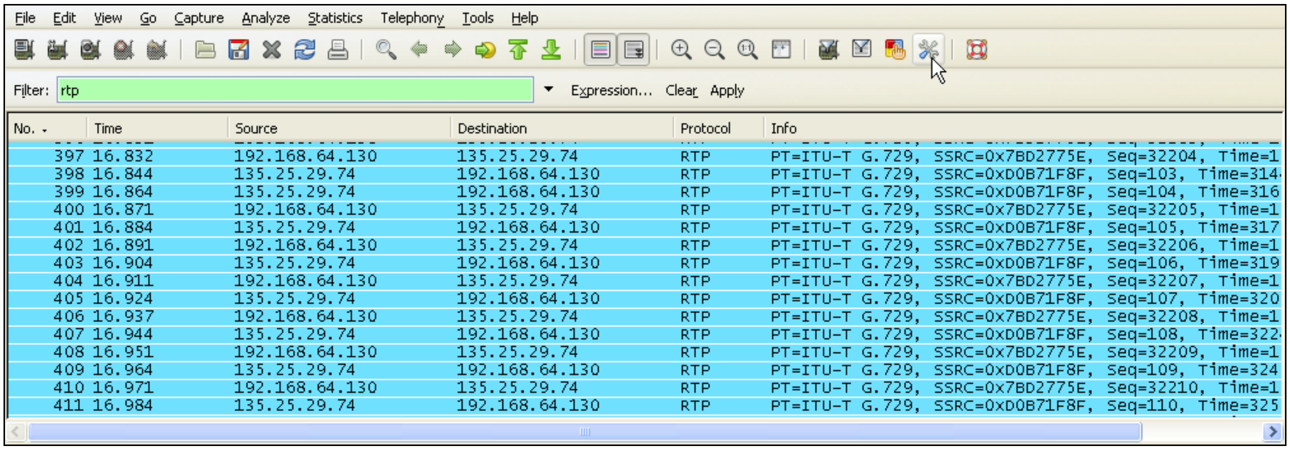
2. The following is an example of an outbound call filtering on DTMF.




| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 550 | 19.154 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF One 1 |
| 551 | 19.174 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF One 1 |
| 552 | 19.184 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF One 1 (end) |
| 553 | 19.184 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF One 1 (end) |
| 554 | 19.184 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF One 1 (end) |
| 584 | 19.795 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 |
| 585 | 19.795 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 |
| 586 | 19.795 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 |
| 587 | 19.815 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 |
| 588 | 19.835 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 (end) |
| 589 | 19.835 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 (end) |
| 590 | 19.835 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Two 2 (end) |
| 597 | 20.434 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Three 3 |
| 598 | 20.434 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Three 3 |
| 599 | 20.434 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Three 3 |
| 600 | 20.454 | 192.168.64.130 | 135.25.29.74 | RTP EVEN | Payload type=RTP Event, DTMF Three 3 |

**Figure 68: – RTPEvent (DTMF) trace – Outbound call to AT&T**

3. The following is an example of an outbound call filtering on RTP.



| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 397 | 16.832 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32204, Time=1 |
| 398 | 16.844 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=103, Time=314 |
| 399 | 16.864 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=104, Time=316 |
| 400 | 16.871 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32205, Time=1 |
| 401 | 16.884 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=105, Time=317 |
| 402 | 16.891 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32206, Time=1 |
| 403 | 16.904 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=106, Time=319 |
| 404 | 16.911 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32207, Time=1 |
| 405 | 16.924 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=107, Time=320 |
| 406 | 16.937 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32208, Time=1 |
| 407 | 16.944 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=108, Time=322 |
| 408 | 16.951 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32209, Time=1 |
| 409 | 16.964 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=109, Time=324 |
| 410 | 16.971 | 192.168.64.130 | 135.25.29.74 | RTP | PT=ITU-T G.729, SSRC=0x7BD2775E, Seq=32210, Time=1 |
| 411 | 16.984 | 135.25.29.74 | 192.168.64.130 | RTP | PT=ITU-T G.729, SSRC=0xD0B71F8F, Seq=110, Time=325 |

**Figure 69: – RTP trace (showing codec used) – Outbound call to AT&T**

## 9.5. Acme Packet SBC

The Acme Packet SBC provisioning can be checked by entering the command **verify-config**. Acme maintenance manuals may be found at **[11].**

# 10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager 6.0, Avaya Aura® Communication Manager 5.2.1, and the Acme Packet Net-Net 3800 can be configured to interoperate successfully with the AT&T IP Flexible Reach service. This solution provides users of Avaya Aura® Communication Manager the ability to support inbound and outbound calls over an AT&T IP Flexible Reach SIP trunk service connection via **AVPN** or **MIS/PNT** transport. These Application Notes further demonstrated that the Avaya Aura® Session Manager AT&T Adaptation Module could be utilized to remove History-Info header information on egress SIP messages to the AT&T IP Flexible Reach service as well as provide required digit manipulation for inbound and outbound calls. Additionally the ability of Avaya Aura® Communication Manager to provide SIP Diversion Header to the AT&T IP Flexible Reach service for certain out bound call scenarios (see **Section 2.2.3**) was demonstrated.

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. Addendum 1 - Acme Packet Net-Net Redundancy to Multiple AT&T Border Elements

AT&T may provide multiple network border elements for redundancy purposes. The Acme Packet Net-Net SBC can be provisioned to support this redundant configuration.

Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, and building on the configuration shown in **Section 7**, the Acme Packet Net-Net SBC is provisioned as follows.

**ANNOTATION**: The **session agents** below represent the AT&T IP Flexible Reach service border elements. The Acme will attempt to send calls to the Primary or Secondary border elements based on successful responses to the OPTIONS "ping-method". Both AT&T IP Flexible Reach service border elements are also specified in the **session-group** section below.

```
session-agent
      hostname                        135.25.29.74
      ip-address                      135.25.29.74
      port                            5060
      state                           enabled
      app-protocol                    SIP
      app-type
      transport-method                UDP
      realm-id                        OUTSIDE
      egress-realm-id
      description                     AT&T_BE_Primary
      carriers
      allow-next-hop-lp               enabled
      constraints                     disabled
      max-sessions                    0
      max-inbound-sessions            0
      max-outbound-sessions           0
      max-burst-rate                  0
      max-inbound-burst-rate          0
      max-outbound-burst-rate         0
      max-sustain-rate                0
      max-inbound-sustain-rate        0
      max-outbound-sustain-rate       0
      min-seizures                    5
      min-asr                         0
      time-to-resume                  0
      ttr-no-response                 0
      in-service-period               0
      burst-rate-window               0
      sustain-rate-window             0
      req-uri-carrier-mode            None
      proxy-mode
      redirect-action
      loose-routing                   enabled
      send-media-session              enabled
      response-map
      ping-method                     OPTIONS;hops=20
      ping-interval                   60
```

```
      ping-send-mode                  keep-alive
      ping-in-service-response-codes
      out-service-response-codes
      media-profiles
      in-translationid
      out-translationid
      trust-me                        disabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                     disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
      p-asserted-id
      trunk-group
      max-register-sustain-rate       0
      early-media-allow
      invalidate-registrations        disabled
      rfc2833-mode                    none
      rfc2833-payload                 0
      codec-policy
      enforcement-profile
      refer-call-transfer             disabled
      reuse-connections               NONE
      tcp-keepalive                   none
      tcp-reconn-interval             0
      max-register-burst-rate         0
      register-burst-window           0


session-agent
      hostname                        135.25.29.75
      ip-address                      135.25.29.75
      port                            5060
      state                           enabled
      app-protocol                    SIP
      app-type
      transport-method                UDP
      realm-id                        OUTSIDE
      egress-realm-id
      description                     AT&T_BE_Secondary
      carriers
      allow-next-hop-lp               enabled
      constraints                     disabled
      max-sessions                    0
      max-inbound-sessions            0
      max-outbound-sessions           0
      max-burst-rate                  0
      max-inbound-burst-rate          0
      max-outbound-burst-rate         0
      max-sustain-rate                0
      max-inbound-sustain-rate        0
```

```
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method                    OPTIONS;hops=20
ping-interval                  60
ping-send-mode                 keep-alive
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
```

**ANNOTATION**: The **session group** below specifies the AT&T IP Flexible Reach service border elements (see **session-agents** above). Also a **strategy** of "RoundRobin" is defined. This means the Acme will alternatively select between the two session-agents. An alternative is to use a strategy of "Hunt" (the secondary BE will only be used if access to the Primary fails). This session-group is also specified in the local-policy source-realm "INSIDE".

```
session-group
      group-name                    SP_PROXY
      description
      state                         enabled
      app-protocol                  SIP
      strategy                      RoundRobin
      dest
                                         135.25.29.74
                                         135.25.29.75
      trunk-group
      sag-recursion                 enabled
      stop-sag-recurse              401,407
```

**ANNOTATION**: - The following header-rule is added to the "**NAT_IP**" sip-manipulation shown in **Section 7**. This header-rule inserts the IP address of the AT&T BE being used for the call (determined by the session-group above) into the SIP Request-URI header.

```
header-rule
                name                           manipRURI
                header-name                    request-uri
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       request
                methods                        INVITE
                match-value
                new-value
                element-rule
                        name                           modRURI
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $REMOTE_IP
```

# 12. 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.
[2] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Release 6.0, June 2010
[3] *Administering Avaya Aura® Communication Manager*, Issue 5.0, Release 5.2, May 2009, Document Number 03-300509
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 7, Release 5.2, May 2009, Document Number 555-245-205
[5] *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent Selection (EAS) Reference*, Release 5.2, April 2009, Document Number 07-600780
[6] *Avaya Aura® Call Center 5.2 Automatic Call Distribution Reference*, Release 5.2, April 2009, Document Number 07-602568
[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

Acme Packet Support (login required):
[11] http://www.acmepacket.com/support.htm
AT&T IP Flexible Reach Service Descriptions:
[12] *AT&T IP Flexible Reach*
http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/