Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.1 and Avaya Aura® Session Border Controller 6.0.3 with AT&T IP Flexible Reach SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Avaya Aura® Session Border Controller with the AT&T IP Flexible Reach service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 6.1 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. The Avaya Aura® Session Border Controller 6.0.3 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 SIP 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 5
2. General Test Approach and Test Results 5
  2.1. Interoperability Compliance Testing 5
  2.2. Test Results 6
    2.2.1. Known Limitations 6
  2.3. Support 7
3. Reference Configuration 7
  3.1. Illustrative Configuration Information 9
  3.2. Call Flows 11
    3.2.1. Inbound 11
    3.2.2. Outbound 12
    3.2.3. Call Forward Re-direction (Diversion Header) 13
    3.2.4. Coverage to Voicemail 14
4. Equipment and Software Validated 15
5. Configure Avaya Aura® Session Manager Release 6.1 16
  5.1. SIP Domain 18
  5.2. Locations 18
    5.2.1. Location for Avaya Aura® Communication Manager 18
    5.2.2. Location for the Avaya Aura® Session Border Controller 19
    5.2.3. Location for Modular Messaging 20
    5.2.4. Location for Other CPE Devices 21
  5.3. Configure Adaptations 22
    5.3.1. Adaptation for calls to AT&T 23
    5.3.2. Adaptation for calls to Avaya Aura® Communication Manager 24
    5.3.3. Adaptation for Avaya Modular Messaging 26
  5.4. SIP Entities 27
    5.4.1. Avaya Aura® Session Manager SIP Entity 28
    5.4.2. Avaya Aura® Communication Manager SIP Entity - Public 30
    5.4.3. Avaya Aura® Communication Manager SIP Entity – Local. 31
    5.4.4. Avaya Aura® Session Border Controller SIP Entity 32
    5.4.5. Avaya Modular Messaging SIP Entity 33
  5.5. Entity Links 34
    5.5.1. Entity Links to Avaya Aura® Communication Manager - Public 34
    5.5.2. Avaya Aura® Communication Manager Entity - Local 35
    5.5.3. Entity Link to AT&T IP Flexible Reach Service via Avaya Aura® SBC 36
    5.5.4. Entity Link to Avaya Modular Messaging 36
  5.6. Time Ranges 37
  5.7. Routing Policies 37
    5.7.1. Routing Policy for Routing to the AT&T Flexible Reach Service 38
    5.7.2. Routing Policy for Routing to Avaya Aura® Communication Manager from AT&T40
    5.7.3. Routing Policy for Routing to Avaya Aura® Communication Manager (local) 41
    5.7.4. Routing Policy for Routing to Modular Messaging 42
  5.8. Dial Patterns 43
    5.8.1. Matching Outbound Calls to the AT&T IP Flexible Reach Service 44
    5.8.2. Matching Inbound Calls to Avaya Aura® Communication Manager 46

5.8.3. Matching Outbound Calls to the Avaya Modular Messaging Pilot Number 47
5.9. Session Manager Administration 48
6. Avaya Aura® Communication Manager 5.2.1 50
6.1. System Parameters 50
6.2. Dial Plan 52
6.3. IP Node Names 53
6.4. IP Interface for IP Interface MainCLAN2 53
6.5. IP Network Regions 54
6.5.1. IP Network Region 1 – Local Region 55
6.5.2. IP Network Region 2 – AT&T Trunk Region 56
6.6. IP Codec Parameters 56
6.6.1. Codecs For IP Network Region 1 (local calls) 56
6.6.2. Codecs For IP Network Region 2 57
6.7. SIP Trunks 58
6.7.1. SIP Trunk for AT&T IP Flexible Reach calls 58
6.7.2. Local SIP Trunk (Modular Messaging) 60
6.8. Public Unknown Numbering 62
6.9. Private Numbering 63
6.10. Outbound Call Routing From Avaya Aura® Communication Manager 63
6.10.1. Route Pattern for Calls to AT&T 63
6.10.2. Route Pattern for Calls to Modular Messaging 64
6.10.3. ARS Dialing 65
6.10.4. AAR Dialing 65
6.11. Inbound Call Routing To Avaya Aura® Communication Manager 66
6.11.1. Calls from AT&T 66
6.11.2. Calls from Modular Messaging 66
6.12. Provisioning for Coverage to Modular Messaging 66
6.12.1. Hunt Group for Station Coverage to Modular Messaging 66
6.12.2. Coverage Path for Station Coverage to Modular Messaging 67
6.12.3. Station Coverage Path to Modular Messaging 67
6.12.4. Saving Translations 68
7. Avaya Modular Messaging 68
8. Configure Avaya Aura® Session Border Controller (SBC) 68
8.1. Logging into the Avaya Session Border Controller 68
8.2. Network Configuration 70
8.2.1. Verify IP Addressing 71
8.2.2. Transport Protocols 71
8.2.3. Setting the RTP Port Range on Eth2 73
8.2.4. Configuring the SIP-Gateways 74
8.2.5. Stripping SIP Headers (Optional) 76
8.2.6. Disable Third Party Call Control 77
8.2.7. SIP OPTIONS Messages for AT&T Network Status 77
8.3. Saving and Activating Configuration Changes 79
9. Verification Steps 80
9.1. General 80
9.2. Avaya Aura® Communication Manager 80

9.3. Avaya Aura® Session Manager 82
9.3.1. Call Routing Test 84
9.4. Protocol Traces 85
9.5. Avaya Aura® Session Border Controller Verification 86
9.5.1. Status Tab 86
9.5.2. Call Logs 87
10. Conclusion 90
11. References 91
12. Addendum 1 – Avaya Aura® Session Border Controller Redundancy to Multiple AT&T Border Elements 92

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Avaya Aura® Session Border Controller with the AT&T IP Flexible Reach service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 6.1 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 (note that SIP endpoint are not supported in an Aura® Communication Manager 5.2.1 Access Element configuration). An Avaya Aura® Session Border Controller 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. The AT&T IP Flexible Reach service utilizes AVPN[1] or MIS-PNT[2] transport services.

For more information on the, AT&T IP Flexible Reach service visit:
http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with System Manager, Session Manager, Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya Aura® Session Border Controller (SBC), 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.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 3.2** for examples) between Communication Manager, Session Manager, Avaya Aura® SBC, and the AT&T IP Flexible Reach service.

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

---

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

- SIP trunking of inbound and outbound calls.
  - Incoming calls from the PSTN were routed by the AT&T IP Flexible Reach service to Communication Manager. These incoming PSTN calls arrived via the SIP Trunk and were answered by Avaya IP (H.323) telephones and fax machine emulation software (Ventafax). Proper call disconnect was tested
  - Outgoing calls from Communication Manager to the PSTN were routed via the SIP Trunk to the AT&T IP Flexible Reach service. These outgoing PSTN calls were originated from Avaya IP (H.323) telephones, and fax machine emulation software (Ventafax). Proper call disconnect was tested.
  - Use of G.729B, G.729A and G.711Mu codecs were tested.
- Inbound and outbound T.38 Fax, using combinations of G3 and SG3 modes, were tested.
- Communication Manager station call coverage to Avaya Modular Messaging for message generation and retrieval.
- Passing of DTMF events (RFC2833/RFC4733) and their recognition by navigating automated menus (e.g. Avaya Modular Messaging message selection and retrieval).
- PBX features such as hold, resume, conference and transfer.
- Requests for privacy (i.e., caller anonymity) for outbound calls to the PSTN, and for inbound calls from the PSTN, were tested.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both the AT&T IP Flexible Reach service and the Avaya SBC were able to monitor health using SIP OPTIONS.
- Inbound calls to Communication Manager stations that were call forwarded back to PSTN destinations, through use of Diversion Header, were tested.
- Proper UDP port ranges for RTP media (16384-32767) were tested.

2.2. Test Results

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

- Inbound and outbound calls, and two-way talk path establishment, between PSTN and Communication Manager telephones 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 the AT&T IP Flexible Reach service/PSTN G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833/RFC4733 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 if unanswered, can be covered to Avaya Modular Messaging.
- Long duration calls.

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

2.2.1. Known Limitations

1. SIP stations are not supported by Communication Manager 5.2.1 in an Access Element configuration.
2. G.722 codec is not supported between Communication Manager and the AT&T IP Flexible Reach service.
3. G.711 faxing is not supported between Communication Manager and the AT&T IP Flexible Reach service. 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 in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Communication Manager.
4. The AT&T IP Flexible Reach service does not support SIP History-Info headers. However, the AT&T IP Flexible Reach service requires that SIP Diversion Header be sent for certain redirected calls (e.g. Call Forward). Communication Manager will insert the Diversion Header for these types of calls (see **Section 6.7.1)**. For all other calls, Session Manager was used in the reference configuration to strip off History-Info headers (see **Section 5.3.1**). Alternatively they may be disabled on the Communication Manager SIP trunk associated with calls to/from AT&T (see **Section 6.7.1**).
5. 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 the equipment/software vendor.

   While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the 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.

2.3. Support

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (800) 325-5555.

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

3. Reference Configuration

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

- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager provides the voice communication services for a particular enterprise site. In the reference configuration, Communication Manager 5.2.1 runs on an Avaya S8720 Server in a G650/Control LAN (C-LAN) configuration. This solution is extensible to other Avaya S8xxx Servers.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G650 Media Gateway is used. The G650 contains system boards such as the Control LAN (C-LAN) and Media Processor (MedPro). This solution is extensible to other Avaya Media Gateways.
- Avaya "desk" telephones are represented with Avaya 46x0, 96x0, and 96x1 Series IP Telephones running H.323, Avaya 6424 Series Digital Telephone, as well Avaya one-X® Communicator PC based softphone.
- The Avaya Aura® SBC provides SIP Session Border Controller functionality, including address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network[3]. UDP transport protocol is used between the Avaya Aura® SBC and the AT&T IP Flexible Reach service.
- An existing Avaya Modular Messaging system provides the corporate voice messaging capabilities in the reference configuration. The provisioning of Modular Messaging is beyond the scope of this document.
- Inbound and outbound calls were placed between PSTN and the Customer Premises Equipment (CPE) via the AT&T IP Flexible Reach service, through the Avaya Aura® SBC, Session Manager, and Communication Manager. Communication Manager originated/terminated the calls using appropriate phone or fax stations. The H.323 phones in the CPE registered to the Avaya Aura® Communication Manager C-LANs.

[3] The AT&T IP Flexible Reach service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya Aura® SBC in this sample configuration. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya Aura® SBC and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya Aura® SBC and Communication Manager.

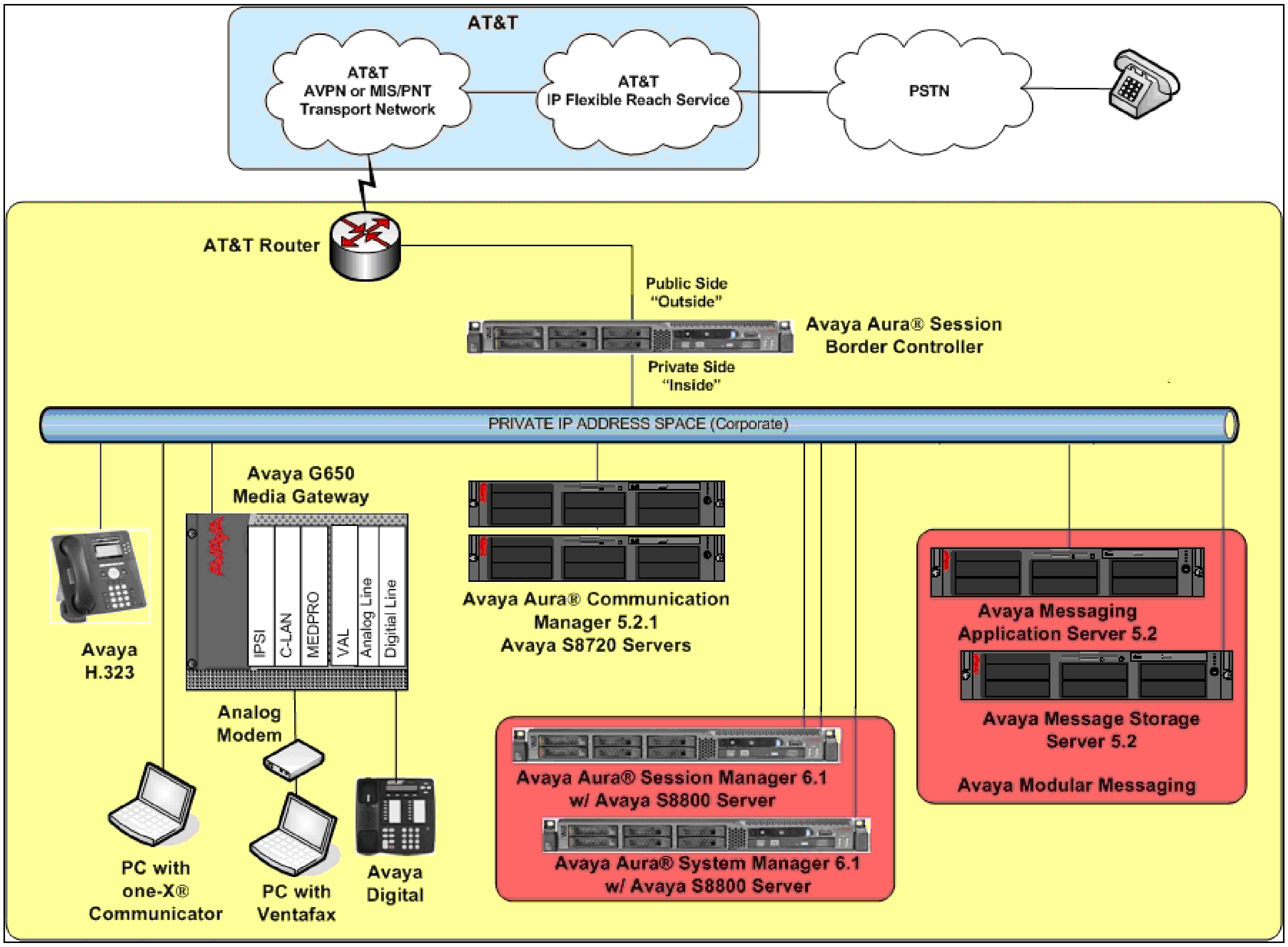


Figure 1: Reference configuration

3.1. Illustrative Configuration Information

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

Note - The AT&T IP Flexible Reach service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the AT&T Flexible Reach service) are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DNIS digits as part of the IP 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
Network IP Address	192.168.67.210
Avaya Aura® Communication Manager	
Control LAN (C-LAN) IP Address	192.168.67.14
Media Processor (MedPro) IP Address	192.168.67.15
Avaya Aura® Communication Manager extensions	26xxx
Avaya CPE local dial plan	2xxxx
Voice Messaging Pilot Extension	26000
Avaya Aura® Session Border Controller	
IP Address of "Outside" (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service)	192.168.64.130
IP Address of "Inside" (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.125
Avaya Modular Messaging	
Messaging Application Server (MAS) IP Address	192.168.67.141
Messaging Server (MSS) IP Address	192.168.67.140
Modular Messaging Dial Plan	1723112xxxx
AT&T IP Flexible Reach Service	
Border Element IP Address	135.25.29.74
AT&T Access router interface (to Avaya Aura® outside)	192.168.64.254

Table 1: Illustrative Values Used in these Application Notes

3.2. Call Flows

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

3.2.1. 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 Avaya Aura® SBC.
4. The Avaya Aura® 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.

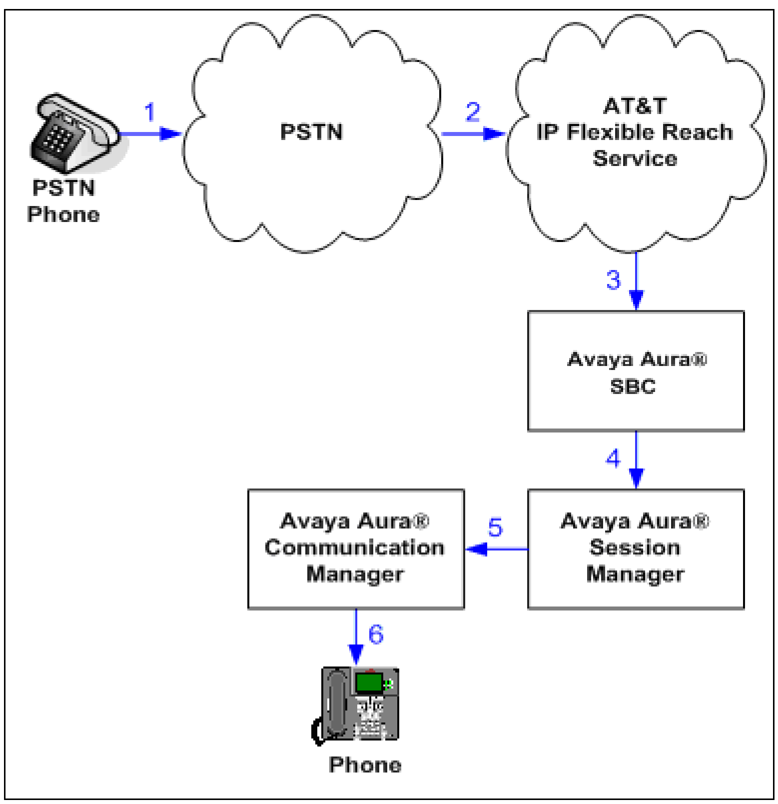


Figure 2: Inbound AT&T IP Flexible Reach Call

3.2.2. 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 Avaya Aura® SBC for delivery to AT&T IP Flexible Reach service.

1. 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 Avaya Aura® SBC.
4. The Avaya Aura® SBC performs SIP address translation 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.

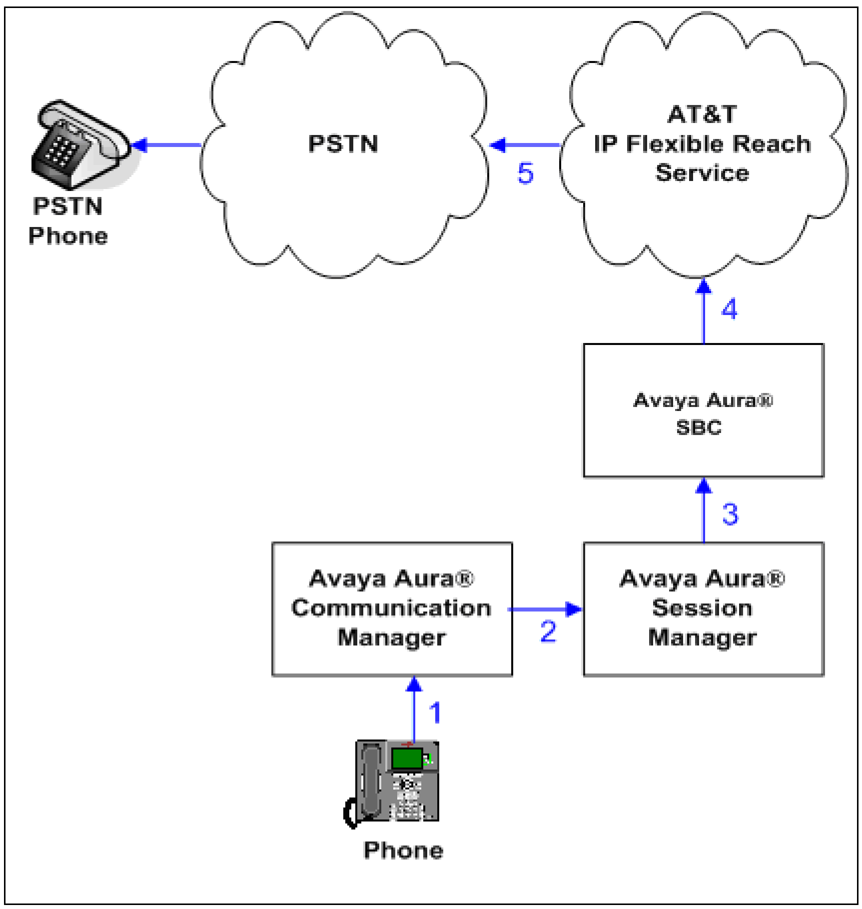


Figure 3: Outbound AT&T IP Flexible Reach Call

3.2.3. 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 3.2.1**.
2. Because the Communication Manager phone has set Call Forward to another number, it initiates a new call back out to Session Manager, the Avaya Aura® 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.

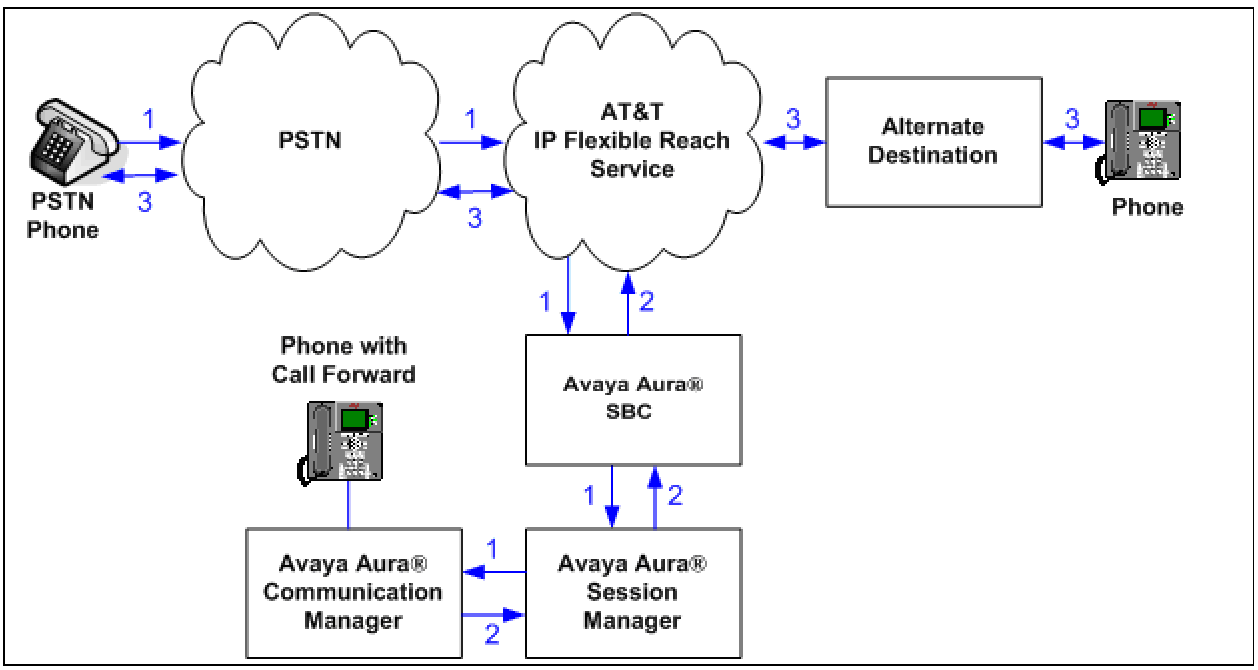


Figure 4: Re-directed (e.g. Call Forward) AT&T IP Flexible Reach Call

3.2.4. 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 3.2.1**.
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.

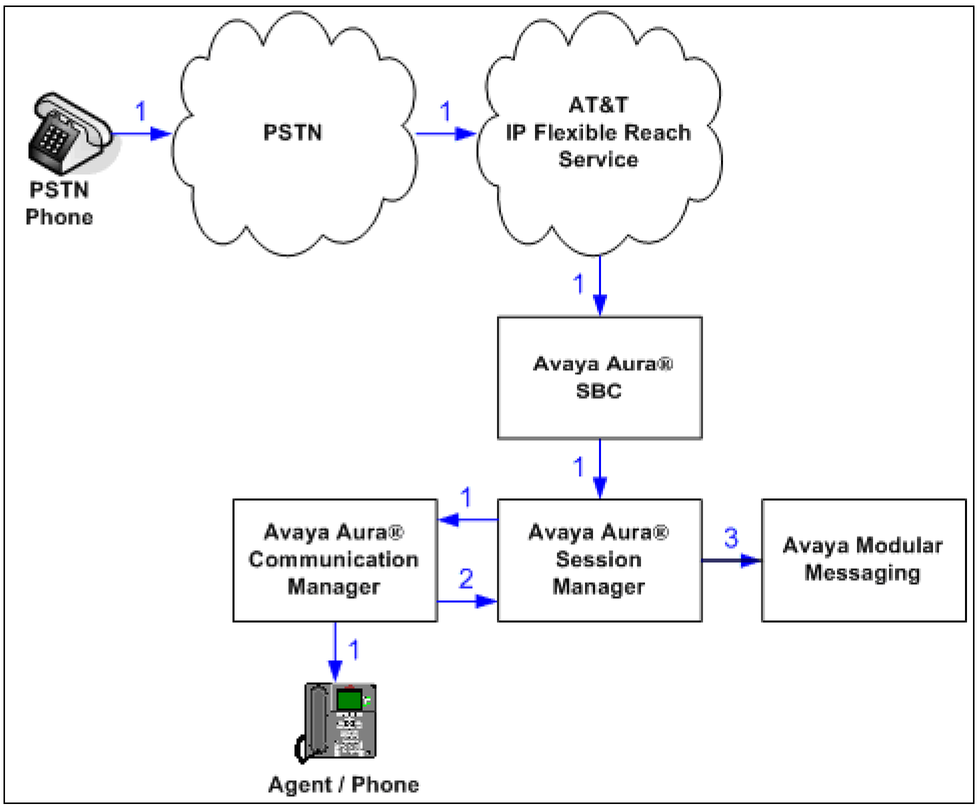


Figure 5: Coverage to Voicemail

[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.

4. 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 6.1 SP5 (6.1.0.0.7345-6.1.5.502) System Platform 6.0.3.3.3
Avaya S8800 Server	Avaya Aura® Session Manager 6.1 SP5 (6.1.5.0.615006)
Avaya S8720 Server	Avaya Aura® Communication Manager 5.2.1 SP10 (02.1.016.4-19191)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW15 FW054
TN799DP Control-LAN (C-LAN)	HW01 FW040
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW060
TN2501AP VAL-ANNOUNCEMENT	HW03 FW021
TN2224CP Digital Line	HW08 FW015
TN793B Analog Line	HW05 FW011
Avaya S8800 Server	Avaya Aura® Session Border Controller Template 6.0.3.0.2
Avaya 9630 IP Telephone	H.323 Version S3.102S
Avaya 9621 IP Telephone	H.323 version S6.010f
Avaya one-X® Agent	2.5.00467.09
Avaya 4610SW IP Telephone	H323 Version 2.9.1
Avaya 6211 Analog phone	-
Avaya Modular Messaging (MAS and MSS) on Avaya S3500 Servers	Release 5.2 – SP8
Fax device	Ventafax Home Version 6.1.59.144
AT&T IP Flexible Reach Service using AVPN/MIS-PNT transport service connection	VNI 22

Table 2: Equipment and Software Versions

5. Configure Avaya Aura® Session Manager Release 6.1

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

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

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Avaya Aura® SBC. In addition, provisioning for calls to Modular Messaging is described.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as "SIP Entities" and the connections/trunks between Session Manager and those components are represented as "Entity Links". Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely System Manager.

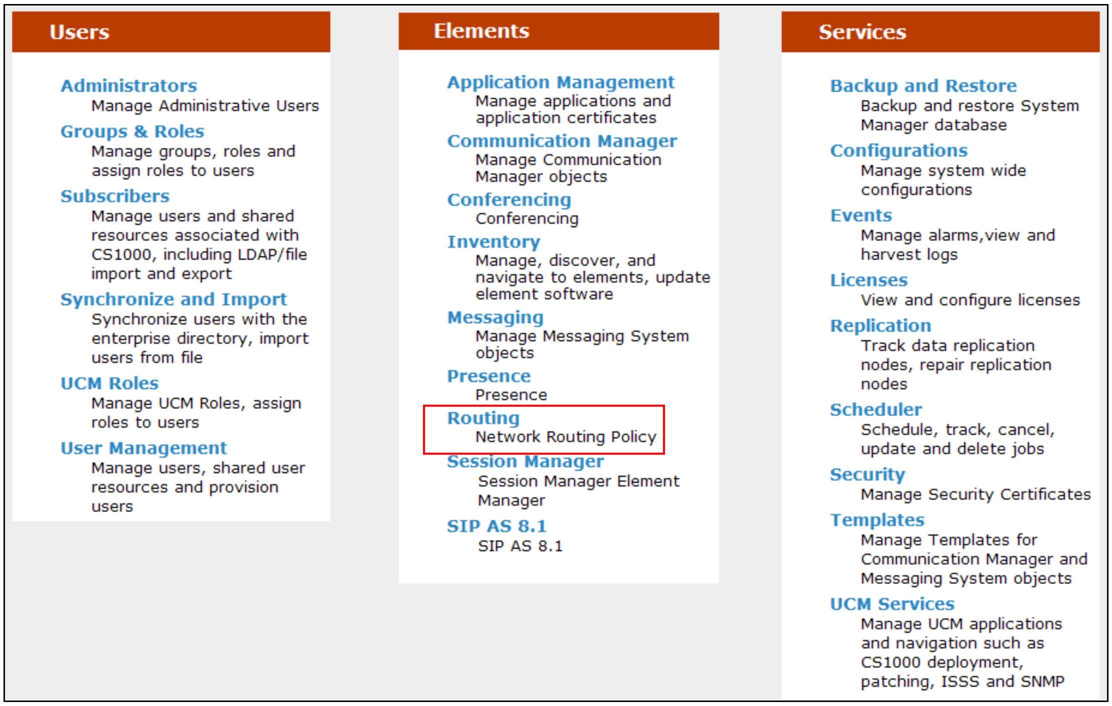
When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as "Adaptations", are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose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

The following administration activities will be described:

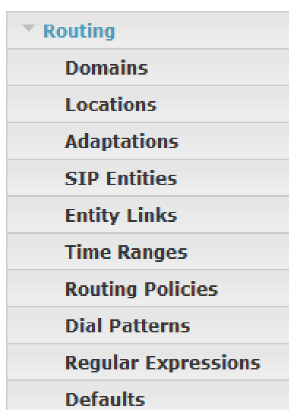
- Define SIP Domain
- Define Locations for Communication Manager, the Avaya Aura® SBC, and Modular Messaging.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Avaya Aura® SBC, and Modular Messaging.
- Define SIP Entities corresponding to Communication Manager, the Avaya Aura® SBC, and Modular Messaging.
- Define Entity Links describing the SIP trunk between Communication Manager and Session Manager, the SIP Trunk between Session Manager and the Avaya Aura® SBC, and the SIP trunk between Session manager and Modular Messaging.
- Define Routing Policies associated with the Communication, the Avaya Aura® SBC and Modular Messaging.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "**http://<ip-address>**", where **<ip-address>** is the IP address of System Manager and logging in with the appropriate credentials.

Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.



The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.

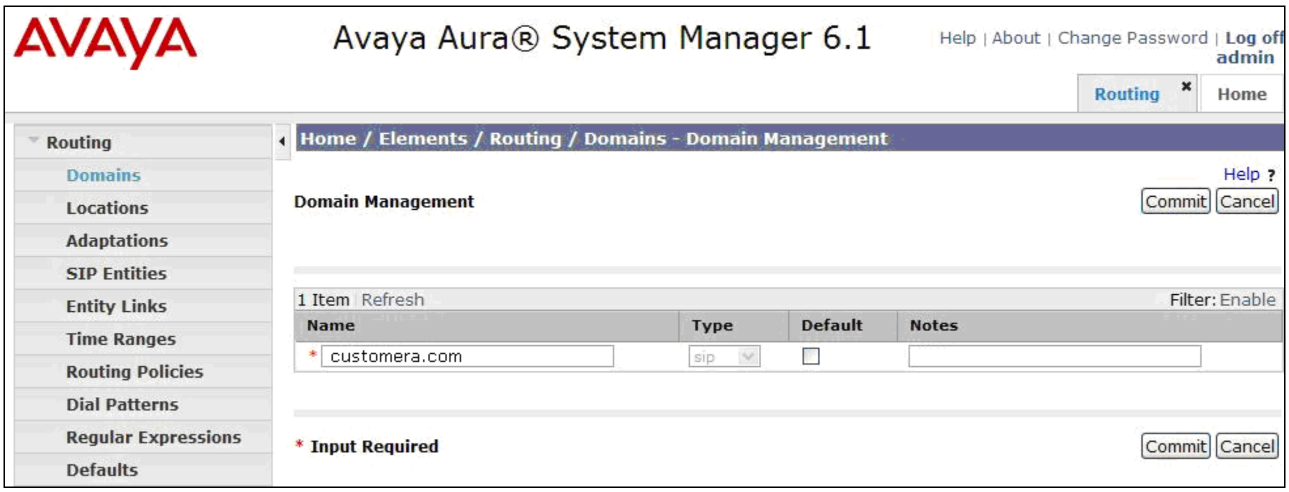


5.1. SIP Domain

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

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

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



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

Note - Multiple SIP Domains may be defined if required.

5.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g. 192.168.67.x for all devices on a particular subnet), or individual devices (e.g. 192.168.67.14 for a devices' IP address). In the reference configuration Communication Manager, Modular Messaging, and the Avaya Aura® SBC were each defined as individual Locations. A "wild card" location **main** was also defined to include other devices in the CPE.

5.2.1. Location for Avaya Aura® Communication Manager

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

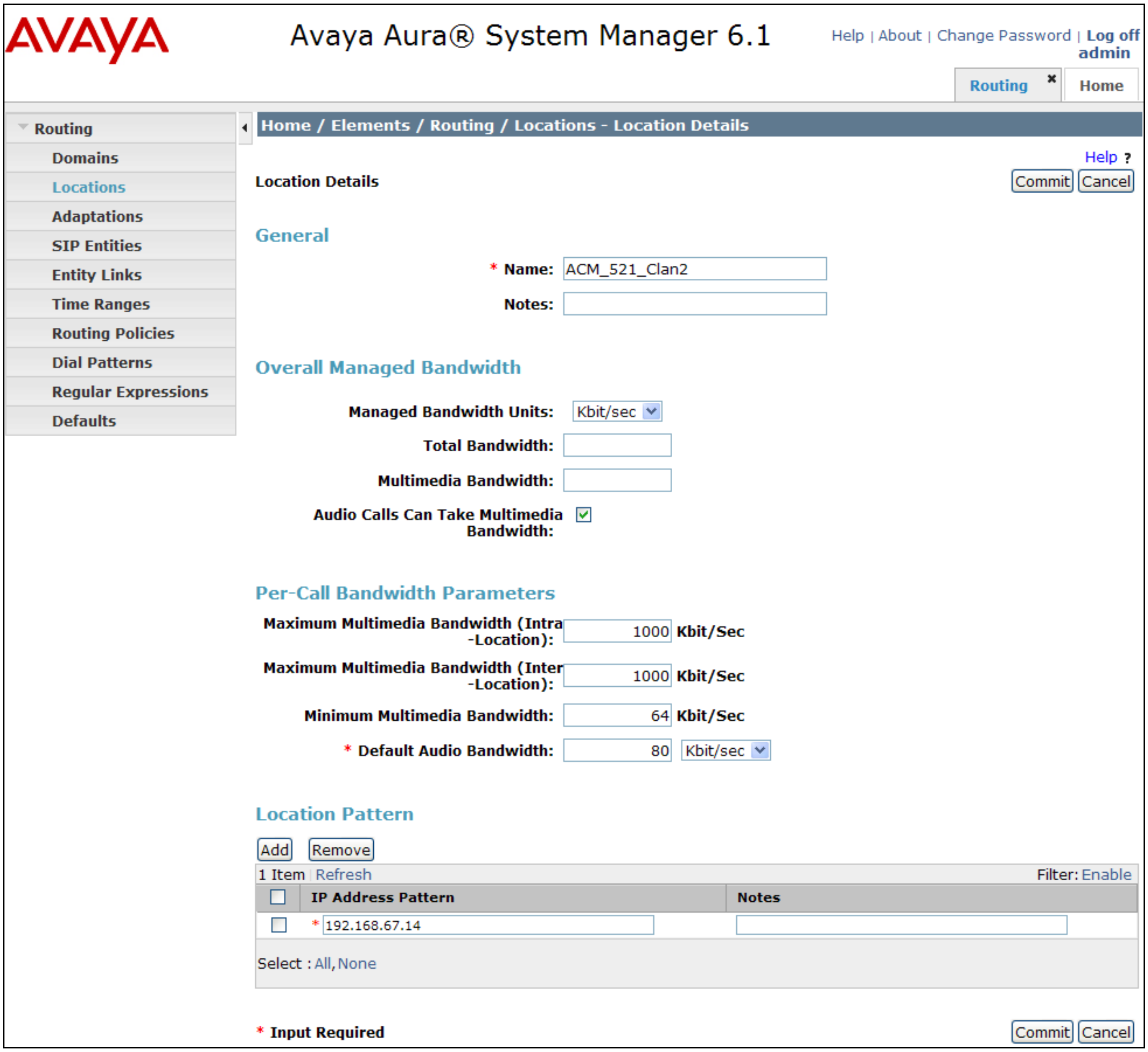
- **Name:** Enter a descriptive name for the location (e.g. **ACM_521_Clan2**).
- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern** - Enter the IP Address used to identify the Communication Manager location (e.g. **192.168.67.14** for the C-LAN described in **Section 6.4**).
- **Notes** - Add a brief description. [Optional]

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

The screen below shows the top portion of the screen for the Location defined for Communication Manager.



5.2.2. Location for the Avaya Aura® Session Border Controller

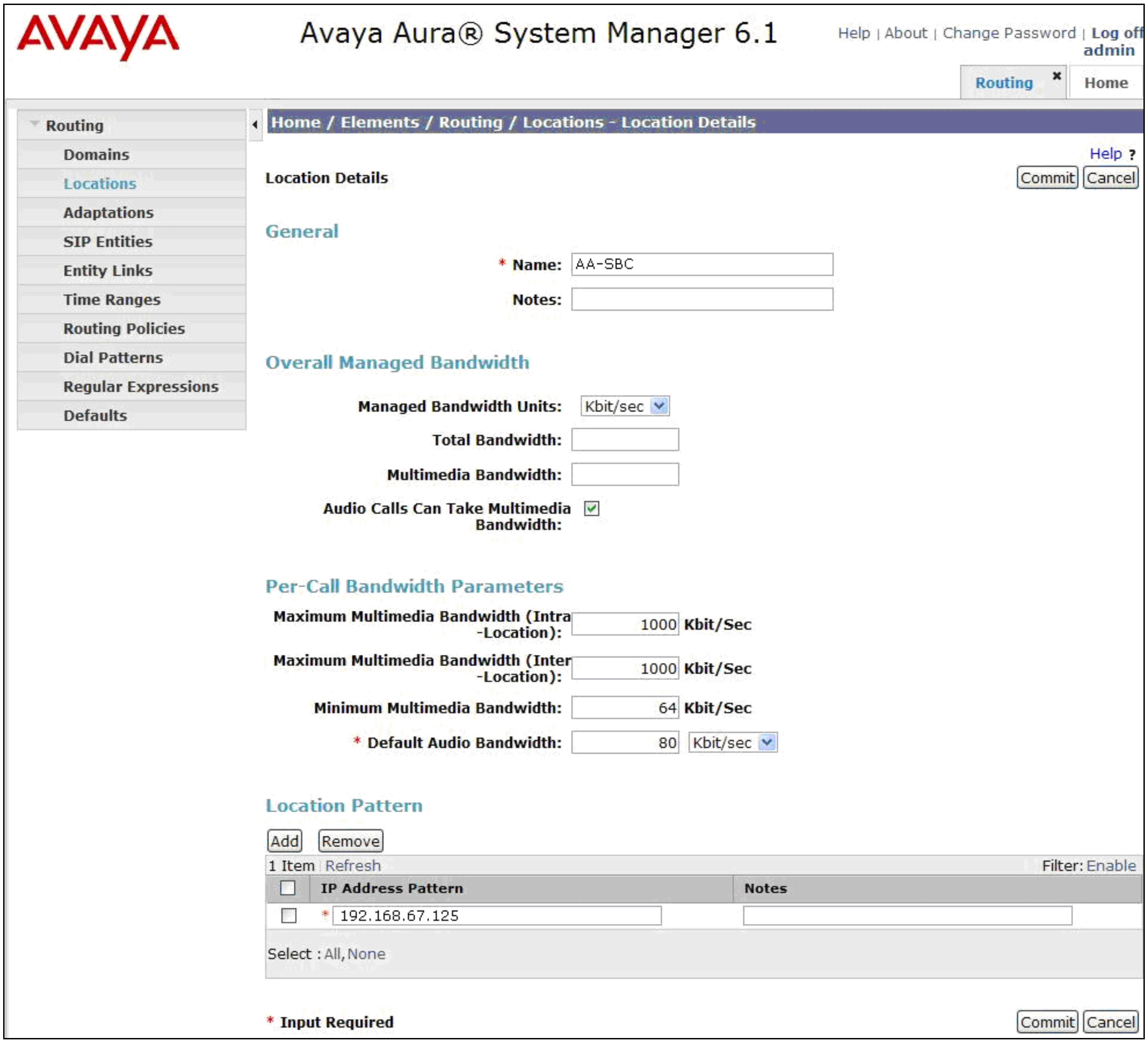
Step 1 - Select **Locations** from the left navigational menu and click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

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

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

- **IP Address Pattern** - Enter the IP Address or IP Address pattern used to identify the SBC location (e.g. **192.168.67.125** as defined in **Section 8.2.1**).
- **Notes** - Add a brief description. [Optional]

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



5.2.3. Location for Modular Messaging

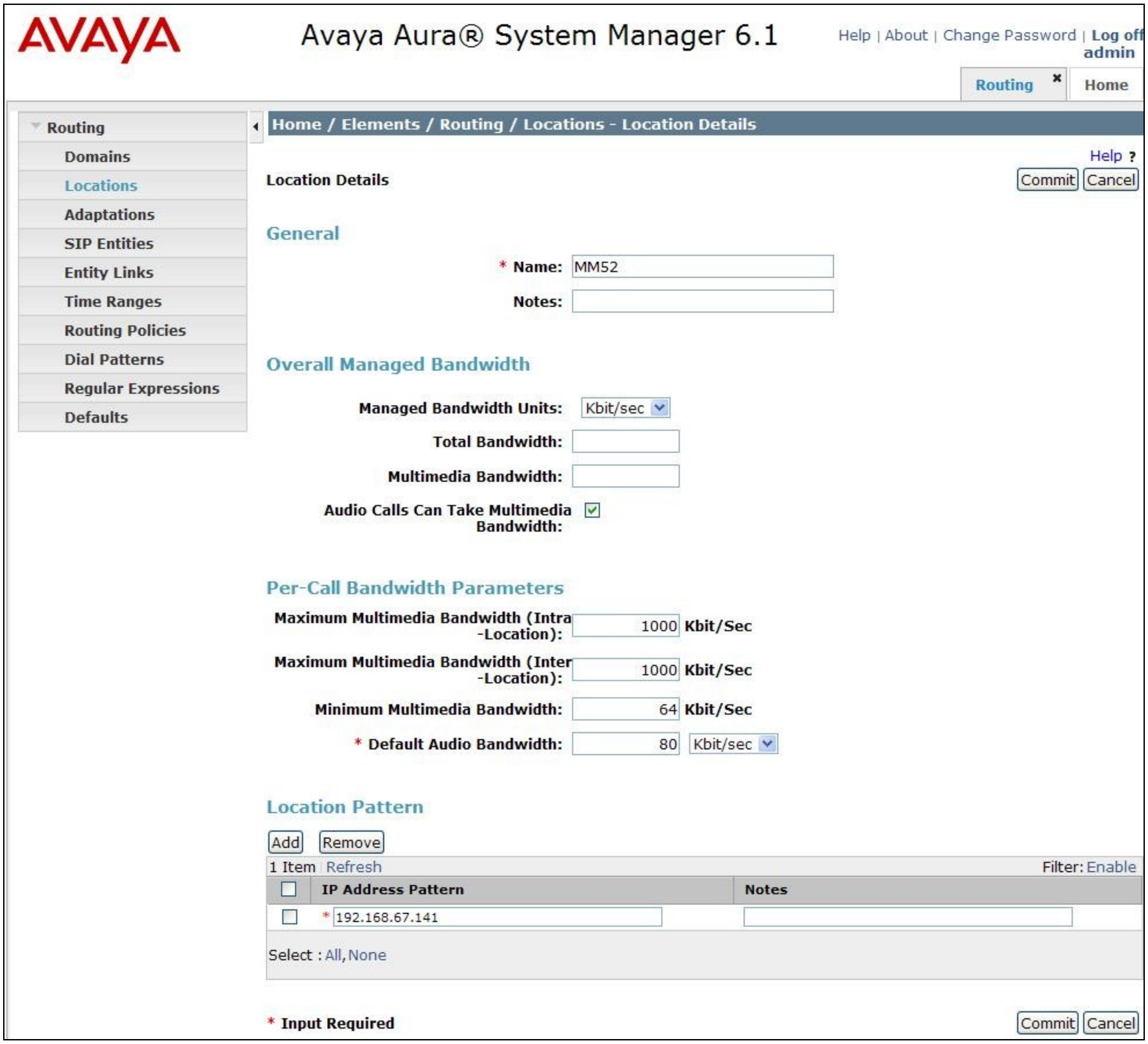
Step 1 - Select **Locations** from the left navigational menu and click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location (e.g. **MM52**).
- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern** - Enter the IP Address used to identify the Modular Messaging MAS location (e.g. **192.168.67.141**).
- **Notes** - Add a brief description. [Optional]

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



5.2.4. Location for Other CPE Devices

The location **main** is used as a "wild card" for any other devices in the CPE that may source traffic to Session Manager. In the Reference configuration Session Manager was assigned to this location (see **Section 5.4.1**) . Note that a specific location like those described in the previous sections could have been used as well.

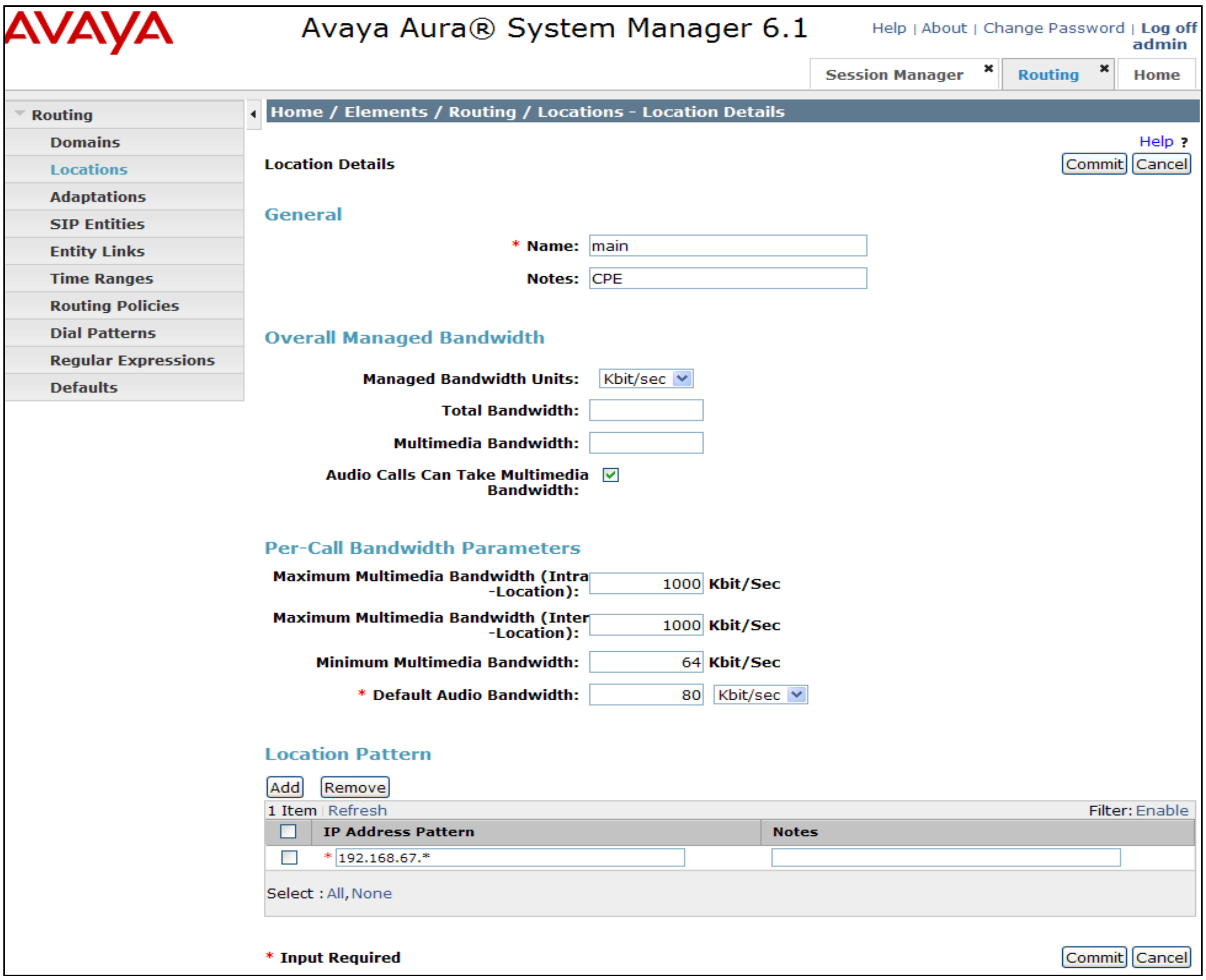
Step 1 - Select **Locations** from the left navigational menu and click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

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

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

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

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



5.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Modules to manipulate SIP headers in messages sent by AT&T to Communication Manager, Communication Manager to AT&T, and between Communication Manager and Modular Messaging.

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

- Calls to AT&T (**Section 5.3.1**) - Modification[6] 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) in the Request URI.
    - The "AttAdapter" module removes the History-Info SIP header on egress toward AT&T.
- Calls from AT&T (**Section 5.3.2**) - Modification of SIP messages sent to Communication Manager.
    - The IP address of Session Manager (192.168.67.210) is replaced with the CPE SIP domain (customera.com) in the Request URI.
    - The AT&T DNIS numbers in the Request URI are replaced with their associated Communication Manager extensions.
- Calls to/from Modular Messaging (**Section 5.3.3**) - Modification of SIP messages sent to and received from Avaya Modular Messaging.
    - From Modular Messaging
        - Modular Messaging 11 digit mailbox numbers are converted to the associated Communication Manager 5 digit extensions (NOTIFY for MWI).
        - Modular Messaging outbound "Find-Me" calls to PSTN have the Communication Manager ARS access code 9 added.
    - To Modular Messaging - Convert the Communication Manager extension defined for Modular Messaging access (26000) to the Modular Messaging pilot number (17231126000).

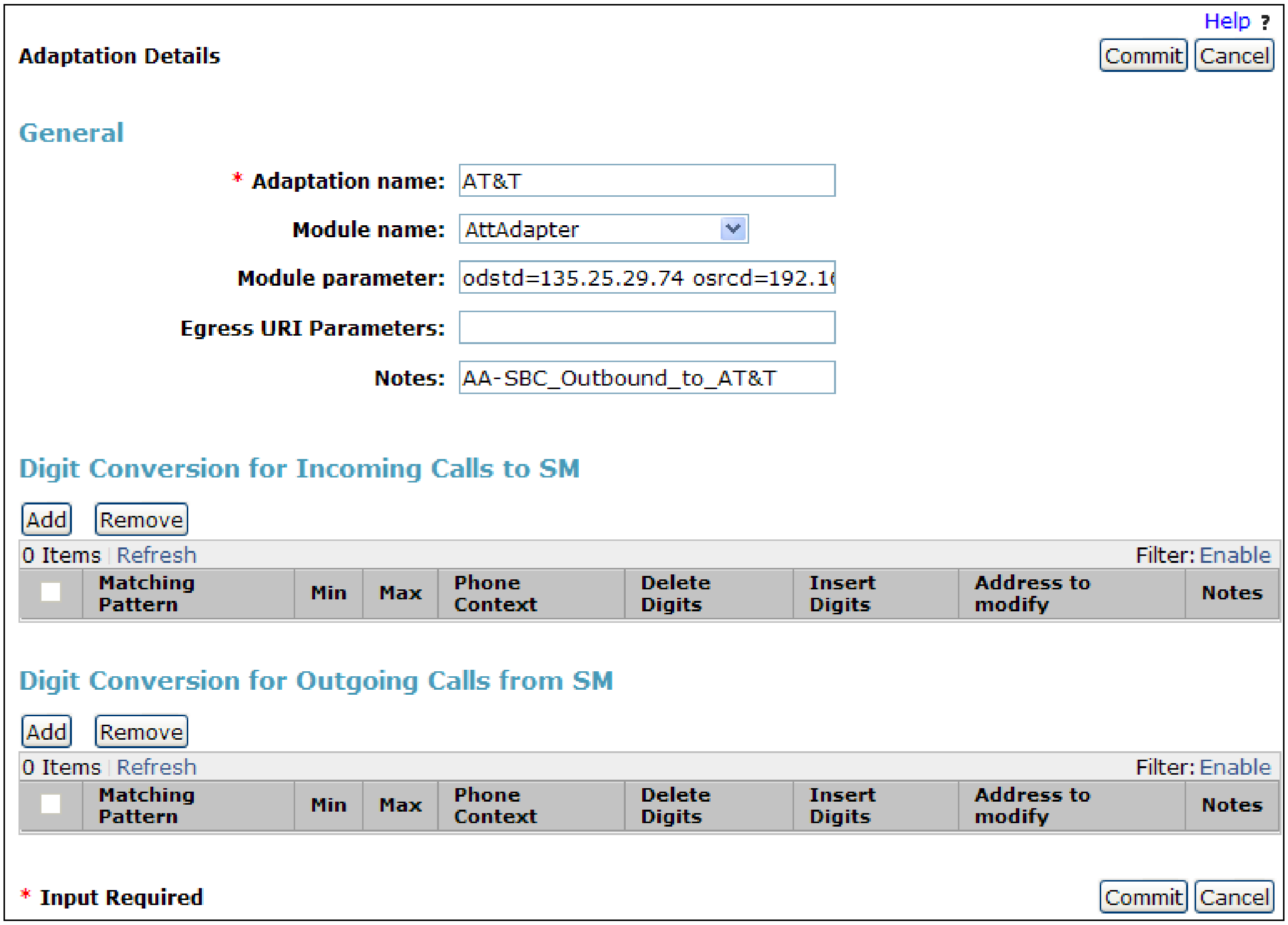
5.3.1. Adaptation for calls to AT&T

The Adaptation administered in this section is applied to SIP messages sent to the AT&T IP Flexible Reach service (by way of the Avaya Aura® 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 Avaya Aura® 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.

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



5.3.2. Adaptation for calls to Avaya Aura® Communication Manager

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

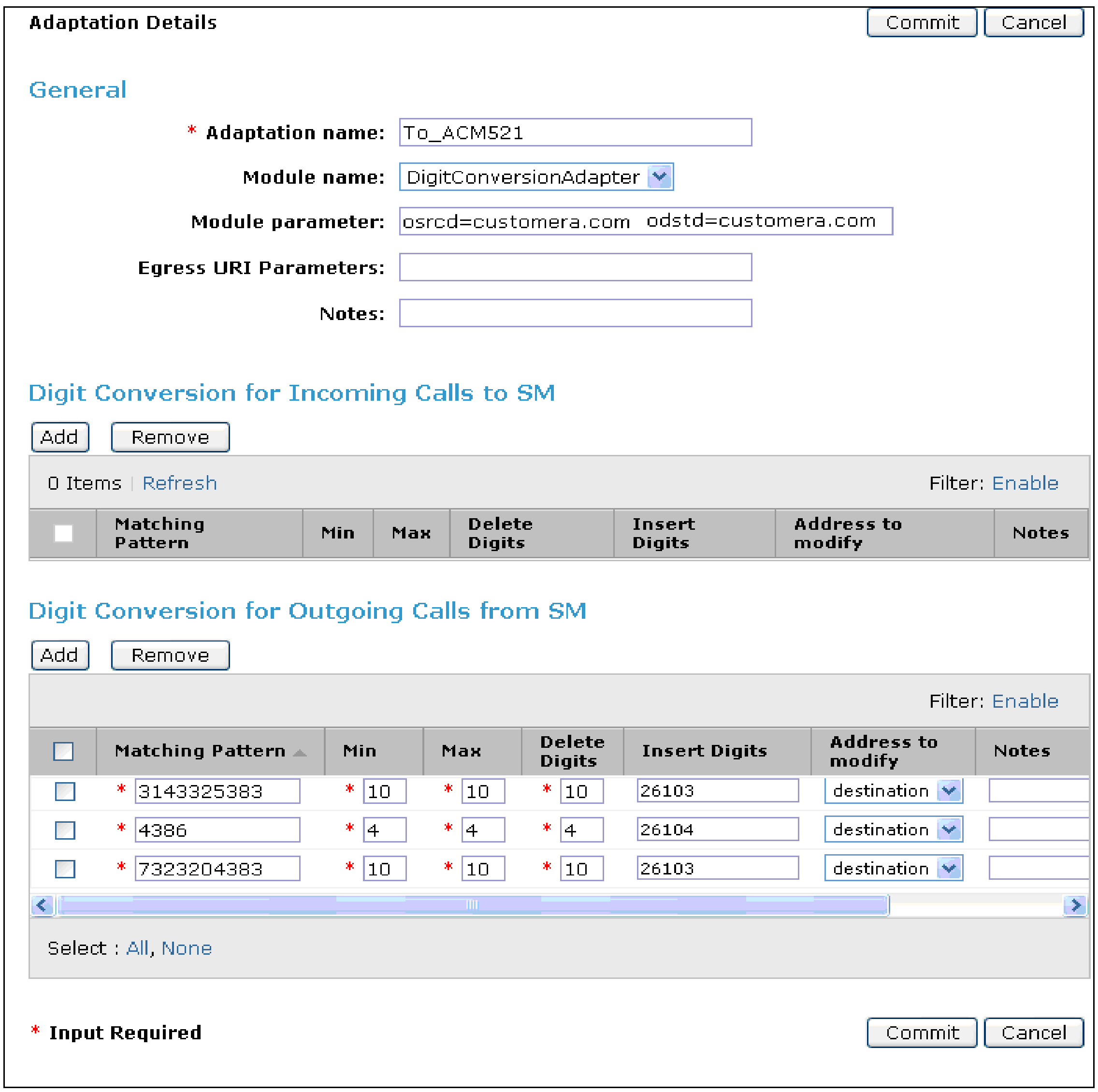
1. In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).
2. In the **Adaptation Details** page, enter:
    a. A descriptive **Name**, (e.g. **To_ACM521**).
    b. Select **DigitConversionAdapter** from the **Module Name** drop down menu (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* DNIS digits from AT&T that need to be replaced with their associated extensions before being sent to Communication Manager (Note – These are not the dialed digits, but the digits delivered by AT&T in the R-URI).
        i. Example 1:

1. 7323204383 are the AT&T DNIS digits 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. Other digit conversions examples shown below are AT&T digits 4386 to Communication Manager extension 26104, and 3143325383 to 26103

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

f. Click on **Commit**.



5.3.3. 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.

5.3.3.1 Inbound calls to the Modular Messaging pilot number (e.g. Message Retrieval)

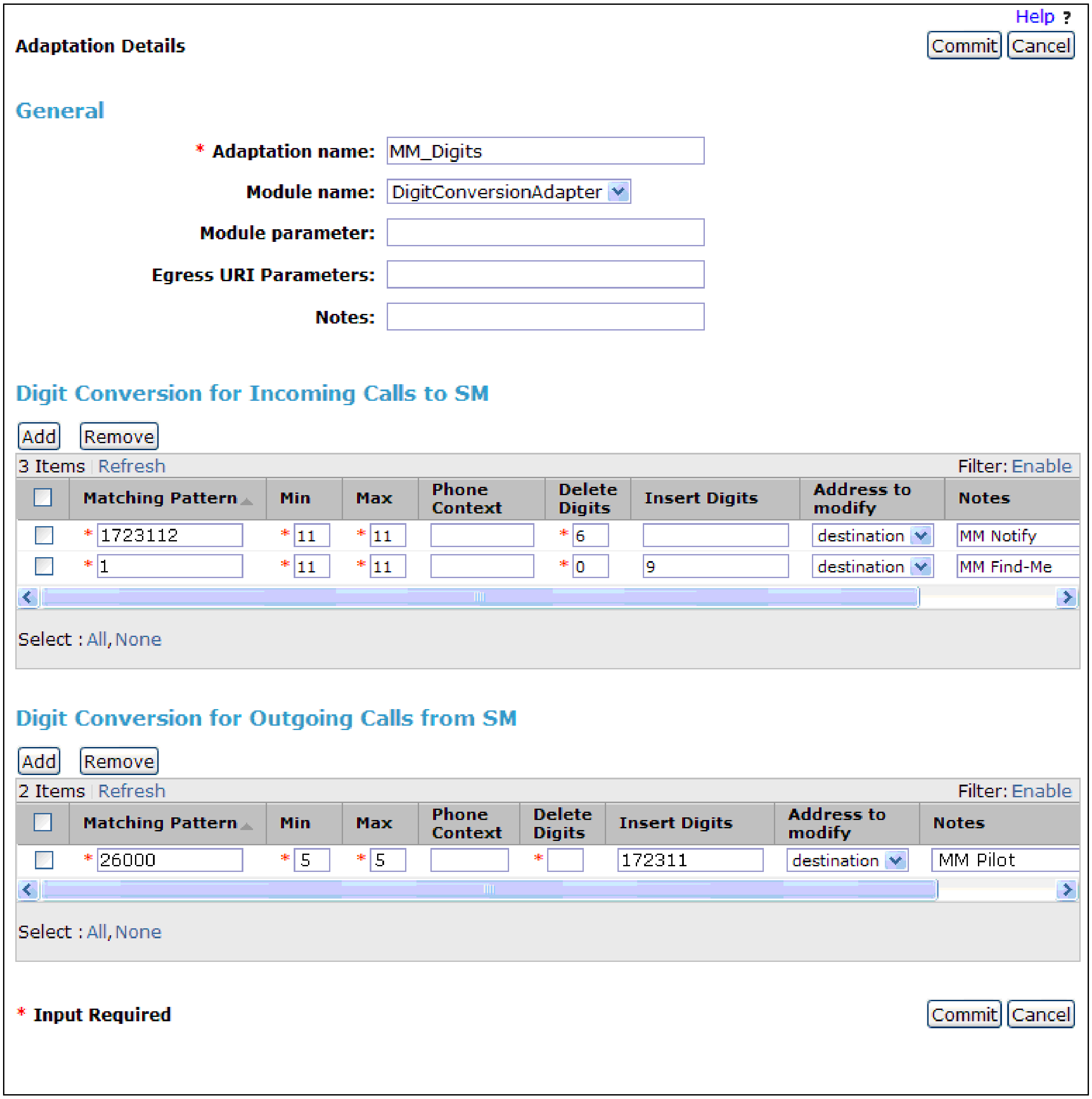
1. In the **Digit Conversion for Outgoing Calls from SM** section, enter **26000** in the **Matching Pattern** column. This is the Modular Messaging pilot extension defined on Communication Manager.
2. Enter **5** in the **Min/Max** columns.
3. Enter **0** in the **Delete Digits** column.
4. Enter **172311** in the **Insert Digits** column. This converts the pilot extension (26000) to the Modular Messaging pilot number (17231126000).
5. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column.
6. Enter any desired notes.

5.3.3.2 Outbound calls from Modular Messaging

1. Modular Messaging sending SIP NOTIFY to signal Message Waiting Indicator (MWI).
    a. In the **Digit Conversion for Incoming Calls to SM** section, enter **1723112** in the **Matching Pattern** column. This is the Modular Messaging mailbox format for Communication Manager extensions (e.g. **1723112**6102).
    b. Enter **11** in the **Min/Max** columns.
    c. Enter **6** in the **Delete Digits** column. This converts the Modular Messaging mailbox (e.g. 17231126102) to the Communication Manager extension (e.g. 26102).
    d. Enter **0** in the **Insert Digits** column.
    e. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column.
    f. Enter any desired notes.
2. Modular Messaging "Find-Me" calls out to PSTN.
    a. In the **Digit Conversion for Incoming Calls to SM** section, enter **1** in the **Matching Pattern** column.
    b. Enter **11** in the **Min/Max** columns. Items **a** and **b** will match any number with the format 1xxxyyyzzzz
    c. Enter **0** in the **Delete Digits** column.

d. Enter **9** in the **Insert Digits** column. This is the Automatic Route Selection (ARS) code defined in Communication Manager (see **Section 6.2**).
e. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column.
f. Enter any desired notes.

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



Help ?

Adaptation Details [Commit] [Cancel]

General

* Adaptation name: MM_Digits

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

[Add] [Remove]

3 Items | Refresh — Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
	* 1723112	* 11	* 11		* 6		destination	MM Notify
	* 1	* 11	* 11		* 0	9	destination	MM Find-Me

Select : All, None

Digit Conversion for Outgoing Calls from SM

[Add] [Remove]

2 Items | Refresh — Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
	* 26000	* 5	* 5		*	172311	destination	MM Pilot

Select : All, None

* Input Required [Commit] [Cancel]

5.4. SIP Entities

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

- Session Manager (**Section 5.4.1**).
- Communication Manager, Local and Public access. Two entities are defined to allow two different SIP trunks (public and private) to be defined on Communication Manager. This permits

different numbering plans to be administered on each so that the assigned AT&T IP Flexible Reach DID numbers are presented in the called number fields on the "public" trunk to AT&T, and local extensions are presented in the called number fields on the "local" trunk (e.g. coverage to Modular Messaging). See **Section 6.7** for the associated Communication Manager trunk provisioning.

  - Communication Manager for AT&T access (**Section 5.4.2**) – This entity, and its associated entity link (using port 5080), is for calls from AT&T to Communication Manager via the Avaya Aura® SBC. Note that port 5080 is only used between Communication Manager and Session Manager to differentiate from the "local" trunk.
  - Communication Manager for local access (**Section 5.4.3**) – This entity, and associated link (using port 5060), is for local connections (e.g. Modular Messaging).

- Avaya Aura® SBC (**Section 5.4.4**) - This entity, and its associated entity link (using port 5060), is for calls to/from the AT&T IP Flexible Reach service via the Avaya Aura® SBC.
- Avaya Modular Messaging (**Section 5.4.5**) – This entity, and its associated entity link (using port 5060), is for local calls from Modular Messaging to Communication Manager**.**

Note – In the reference configuration TCP 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 when possible.

5.4.1. Avaya Aura® Session Manager SIP Entity

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

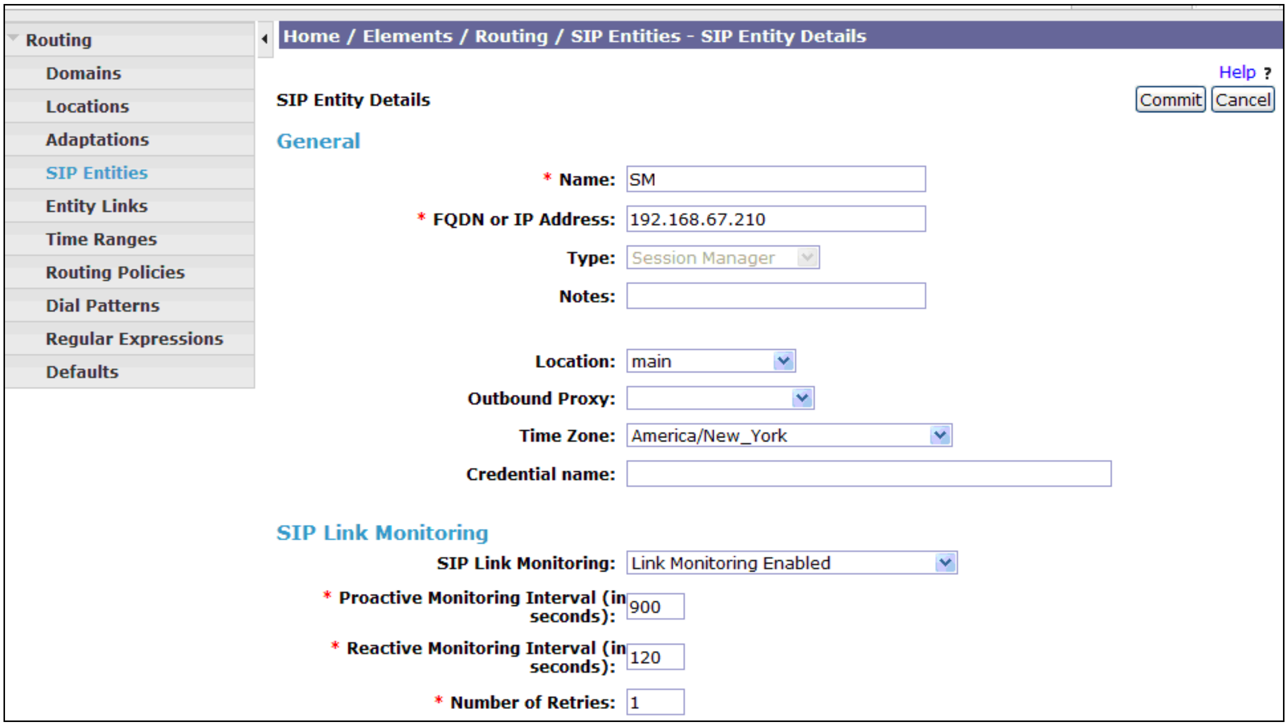
Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name for Session Manager (e.g. **SM**).
- **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 5.2.4**).
- **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.

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

- Select **Link Monitoring Enabled** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.

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.



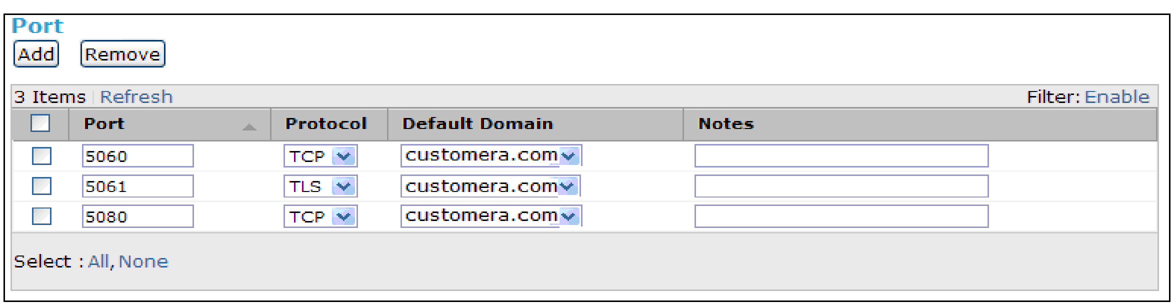
Step 4 - In the **Port** section of the **SIP Entity Details** page, click on **Add** and provision an entry as follows:

- **Port –** Enter **5080** (see note above).
- **Protocol –** Select **TCP** (see note above).
- **Default Domain** – (Optional) Select a SIP domain administered in **Section 5.1** in the **Default Domain** field (e.g. **customera.com**).

Step 5 - Repeat **Step 4** to provision another entry, except with **5060** for **Port** and **TCP** for **Protocol**. This is for local calls from the Avaya SIP phones (and Modular Messaging), to Communication Manager.

Step 6 – Repeat **Step 4** to provision another entry, except with **5061** for **Port** and **TLS** for **Protocol.** Although TLS was not used in the reference configuration (see the note at the beginning of this section), the addition of TLS is shown for completeness.

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



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

5.4.2. Avaya Aura® Communication Manager SIP Entity - Public

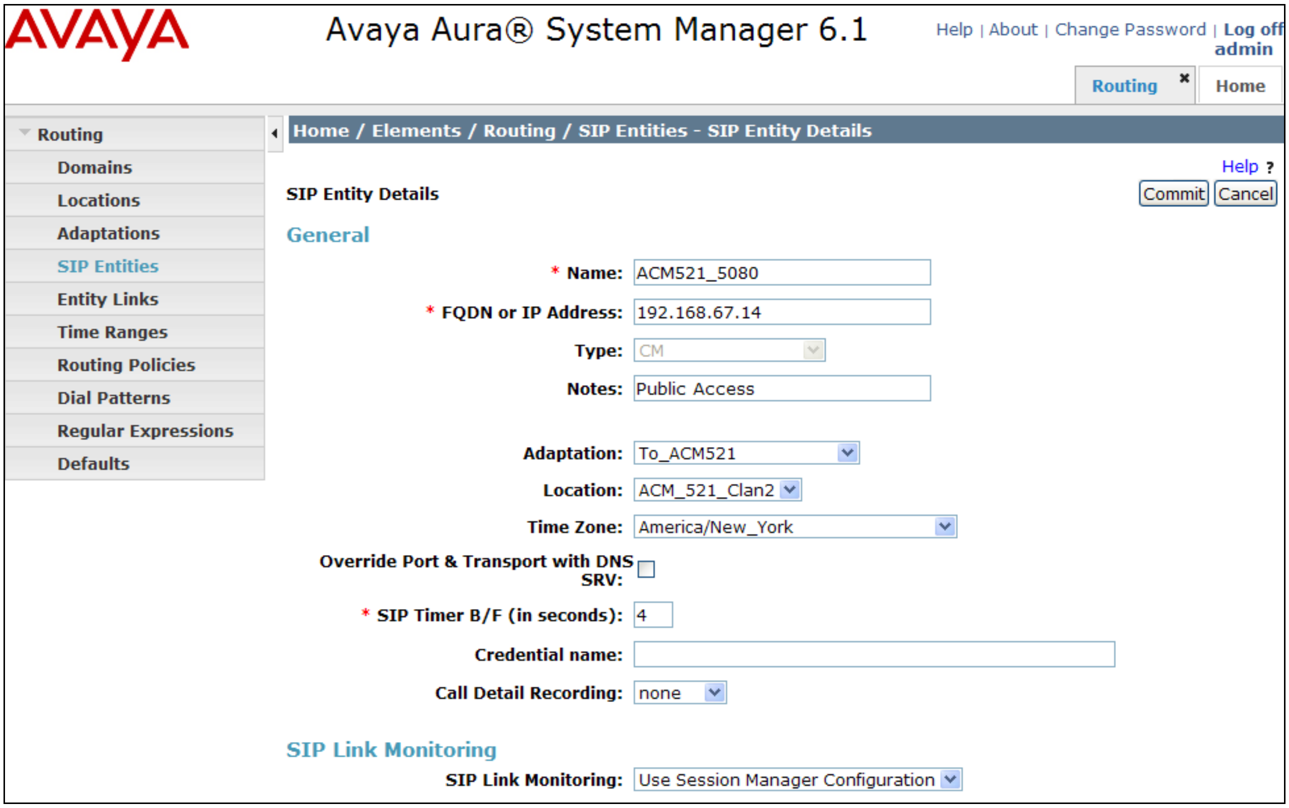
Step 1 - In the **SIP Entities** page, click on **New** (not shown).

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

- **Name –** Enter a descriptive name for the Communication Manager "public" trunk (e.g. **ACM521_5080**).
- **FQDN or IP Address –** Enter the IP address of the Communication Manager C-LAN described in **Section 6.3** (e.g. **192.168.67.14**).
- **Type –** Select **CM**.
- **Adaptation –** Select the Adaptation administered in **Section 5.3.2** (e.g. **To_ACM521**).
- **Location** – Select a Location administered in **Section 5.2.1** (e.g. **ACM_521_Clan2**).
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page select:
    - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
    - Use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

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

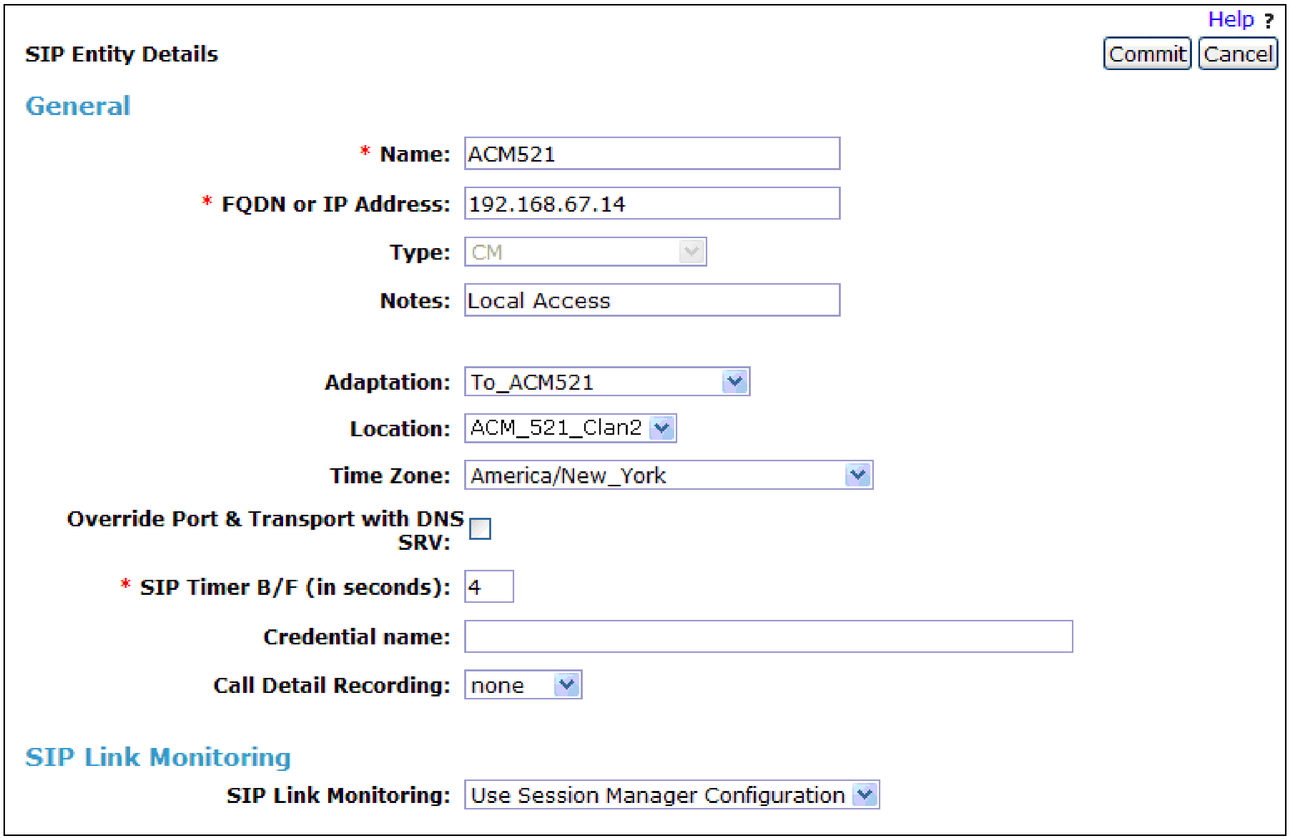


5.4.3. Avaya Aura® Communication Manager SIP Entity – Local.

Configuration for this entity is similar to the entity configured in **Section 5.4.2** with the following changes:

- **Name** – Enter a descriptive name for the Communication Manager "local" trunk (e.g. **ACM521**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager C-LAN provisioned in **Section 6.3** (e.g. **192.168.67.14**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.2** (e.g. **To_ACM521**).
- **Location** – Select a Location administered in **Section 5.2.1** (e.g. **ACM_521_Clan2**).

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

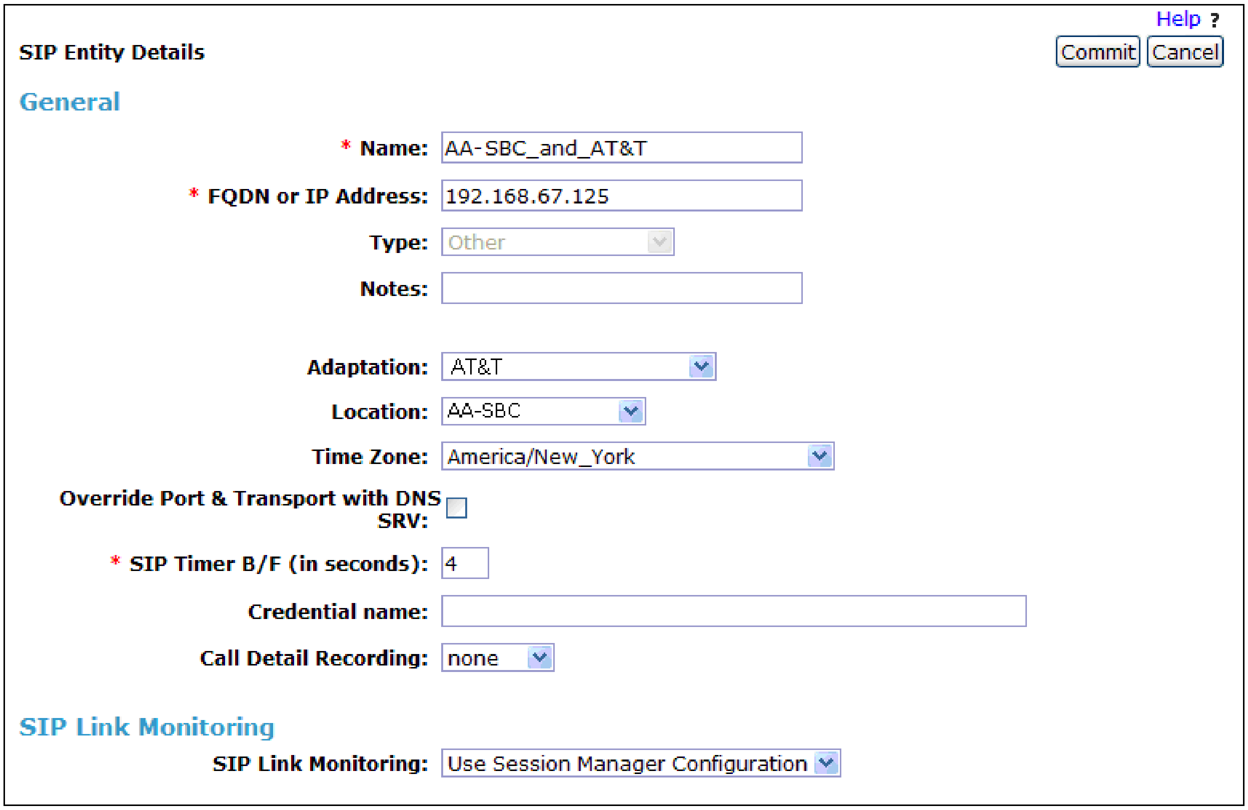


5.4.4. Avaya Aura® Session Border Controller SIP Entity

To configure the Avaya Aura® SBC entity, repeat the steps in **Section 5.4.2** with the following changes:

- **Name** – Enter a descriptive name (e.g. **AA-SBC_and_AT&T**).
- **FQDN or IP Address** – Enter the IP address of the "inside" interface of the Avaya Aura® SBC provisioned in **Section 8.2.1** (e.g. **192.168.67.125**).
- **Type** – Select **Other**.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.1** (e.g. **AT&T**).
- **Location** – Select a Location administered in **Section 5.2.2** (e.g. **AA-SBC**).

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

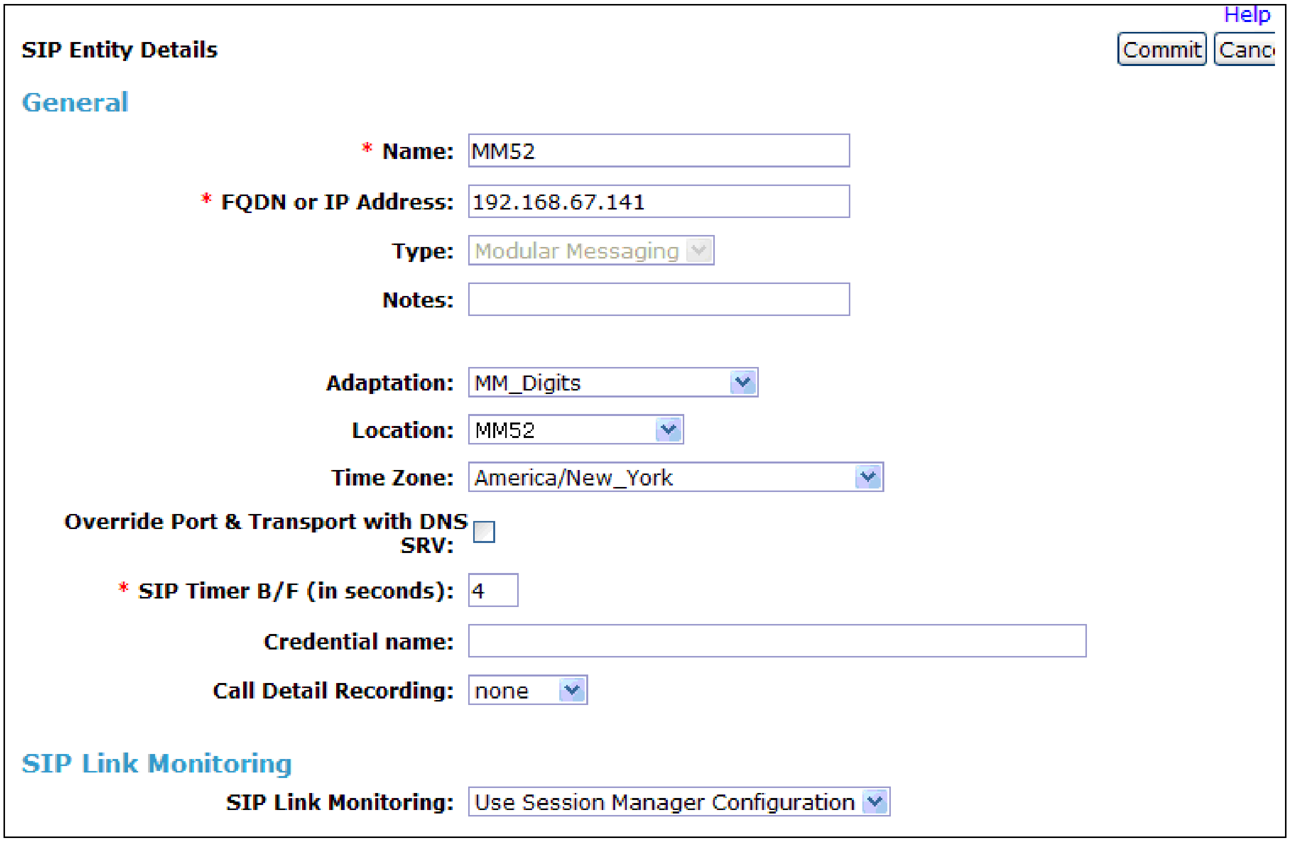


5.4.5. Avaya Modular Messaging SIP Entity

To configure the Modular Messaging SIP entity, repeat the Steps in **Section 5.4.2** with the following changes:

- **Name –** Enter a descriptive name (e.g. **MM52**).
- **FQDN or IP Address –** Enter the IP address of the Modular Messaging Application Server (MAS).
- **Type** – Select **Other**.
- **Adaptation –** Enter the Adaptaion defined in **Section 5.3.3** (e.g. **MM_Digits**).
- **Location** – Select the Location administered in **Section 5.2.3** (e.g. **MM52**).

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



5.5. Entity Links

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

- Communication Manager – Public (**Section 5.5.1**).
- Communication Manager - Local (**Section 5.5.2**).
- Avaya Aura® SBC (**Section 5.5.3**).
- Avaya Modular Messaging (**Section 5.5.4**).

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

Note – 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 when possible.

5.5.1. Entity Links to Avaya Aura® Communication Manager - Public

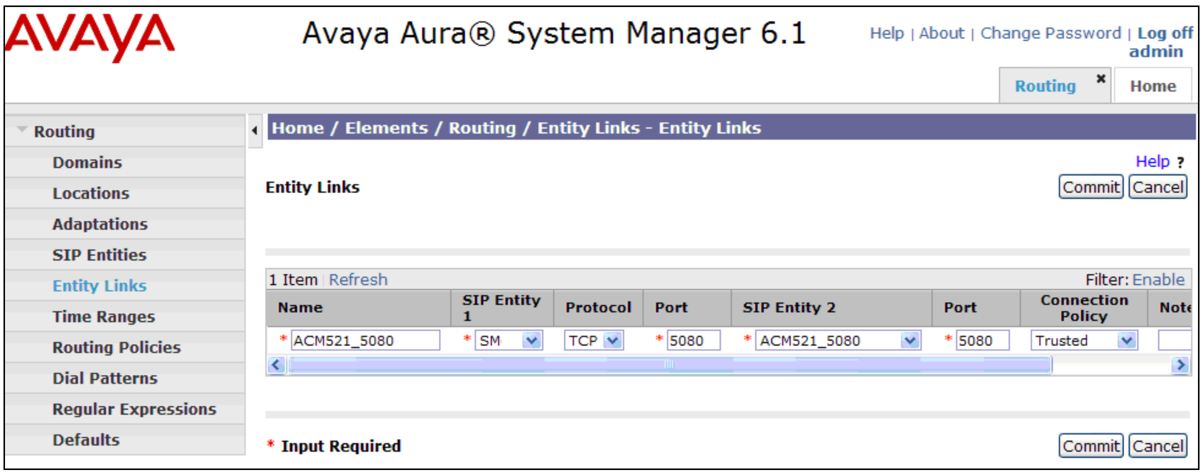
Step 1 - In the left pane under **Routing**, click on **Entity Links**. In the **Entity Links** page click on **New** (not shown).

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

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g. **ACM521_5080**).

- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g. **SM**). SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5080**
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager “public” entity (e.g. **ACM521_5080**).
- **SIP Entity 2 Port** - Enter **5080**.
- **Trusted** – Select **Trusted**.
- **Protocol** – Select **TCP**.

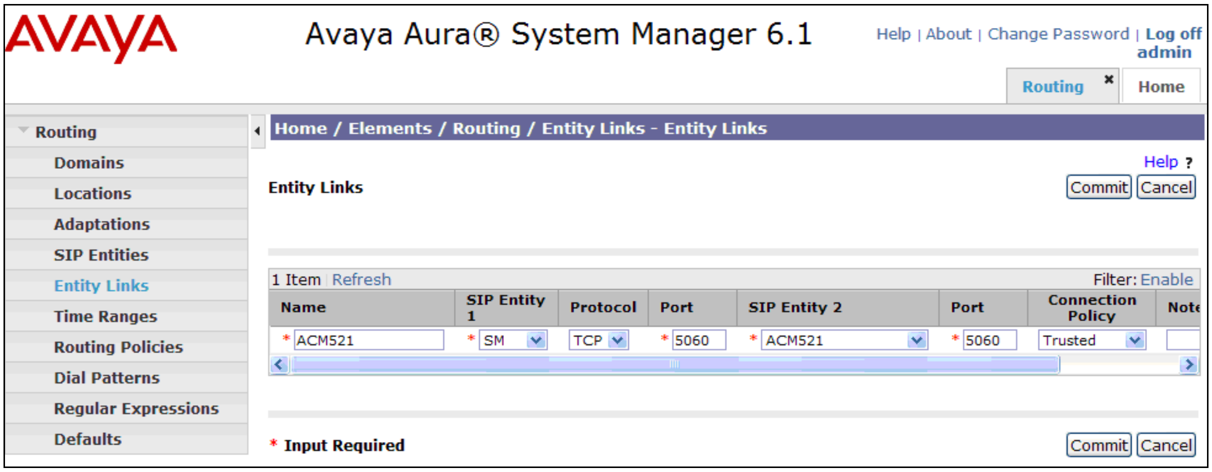
Step 3 - Click on **Commit**.



5.5.2. Avaya Aura® Communication Manager Entity - Local

To configure this entity link, repeat the steps in **Section 5.5.1** with the following differences:

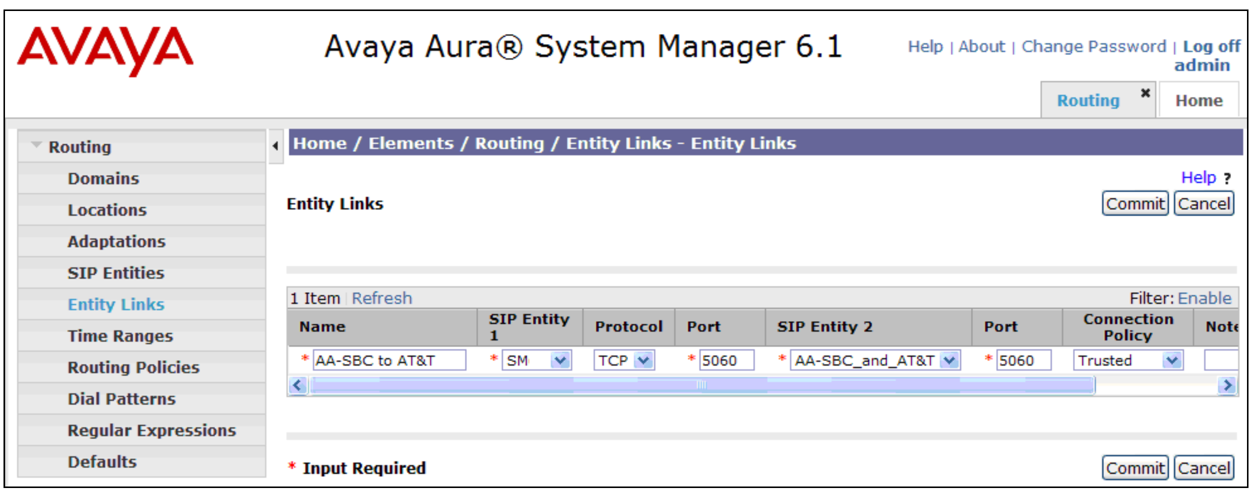
- **Name** – Enter a descriptive name for this link to Communication Manager (e.g. **ACM521**).
- **SIP Entity 1 Port** – Enter **5060**
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.3** for the Communication Manager “local” Entity (e.g. **ACM521**).
- **SIP Entity 2 Port** - Enter **5060**.
- **Protocol** – Select **TCP**.



5.5.3. Entity Link to AT&T IP Flexible Reach Service via Avaya Aura® SBC

Repeat **Section 5.5.1** steps with the following differences:

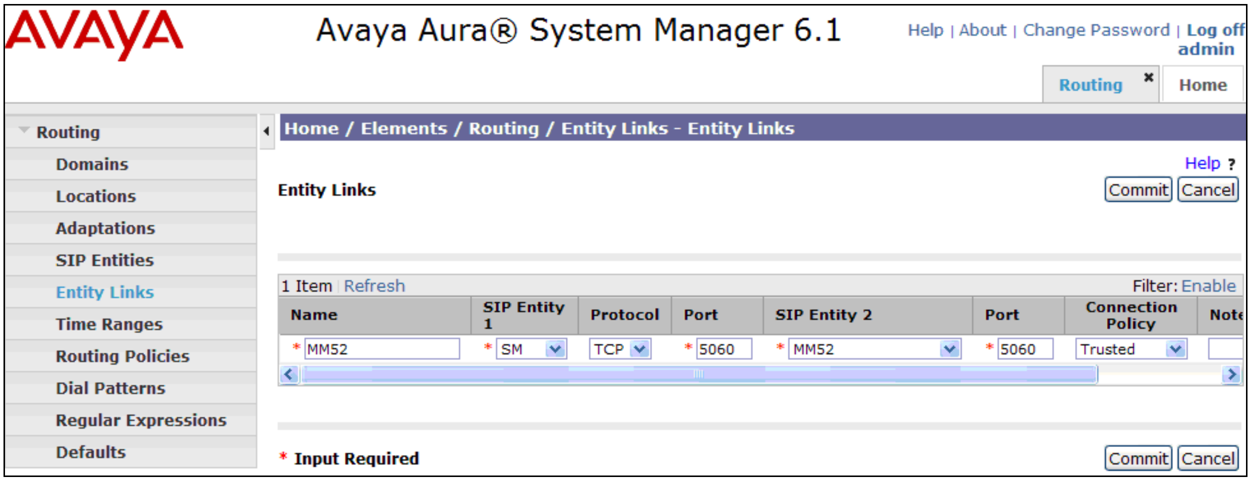
- **Name** – Enter a descriptive name for the link to the AT&T IP Flexible Reach service, by way of the Avaya Aura® SBC (e.g. **AA-SBC_to_AT&T**).
- **SIP Entity 1 Port** – Enter **5060**
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.4** for the Avaya Aura® SBC (e.g. **AA-SBC_and_AT&T**).
- **SIP Entity 2 Port** - Enter **5060**.
- **Protocol** – Select **TCP**.



5.5.4. Entity Link to Avaya Modular Messaging

Repeat **Section 5.5.1** steps with the following differences:

- **Name** – Enter a descriptive name for the link to Modular Messaging (e.g. **MM52**).
- **SIP Entity 1 Port** – Enter **5060**
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.5** for Avaya Modular Messaging (e.g. **MM52**).
- **SIP Entity 2 Port** - Enter **5060**.
- **Protocol** – Select **TCP**.



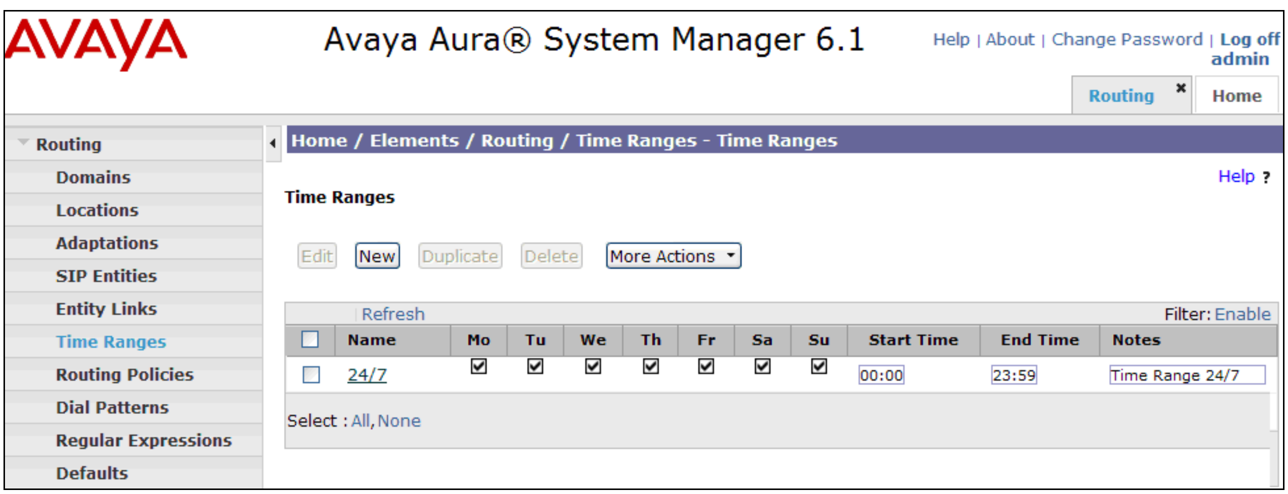
5.6. Time Ranges

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

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

Step 3 - Click on **Commit**.

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



5.7. Routing Policies

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

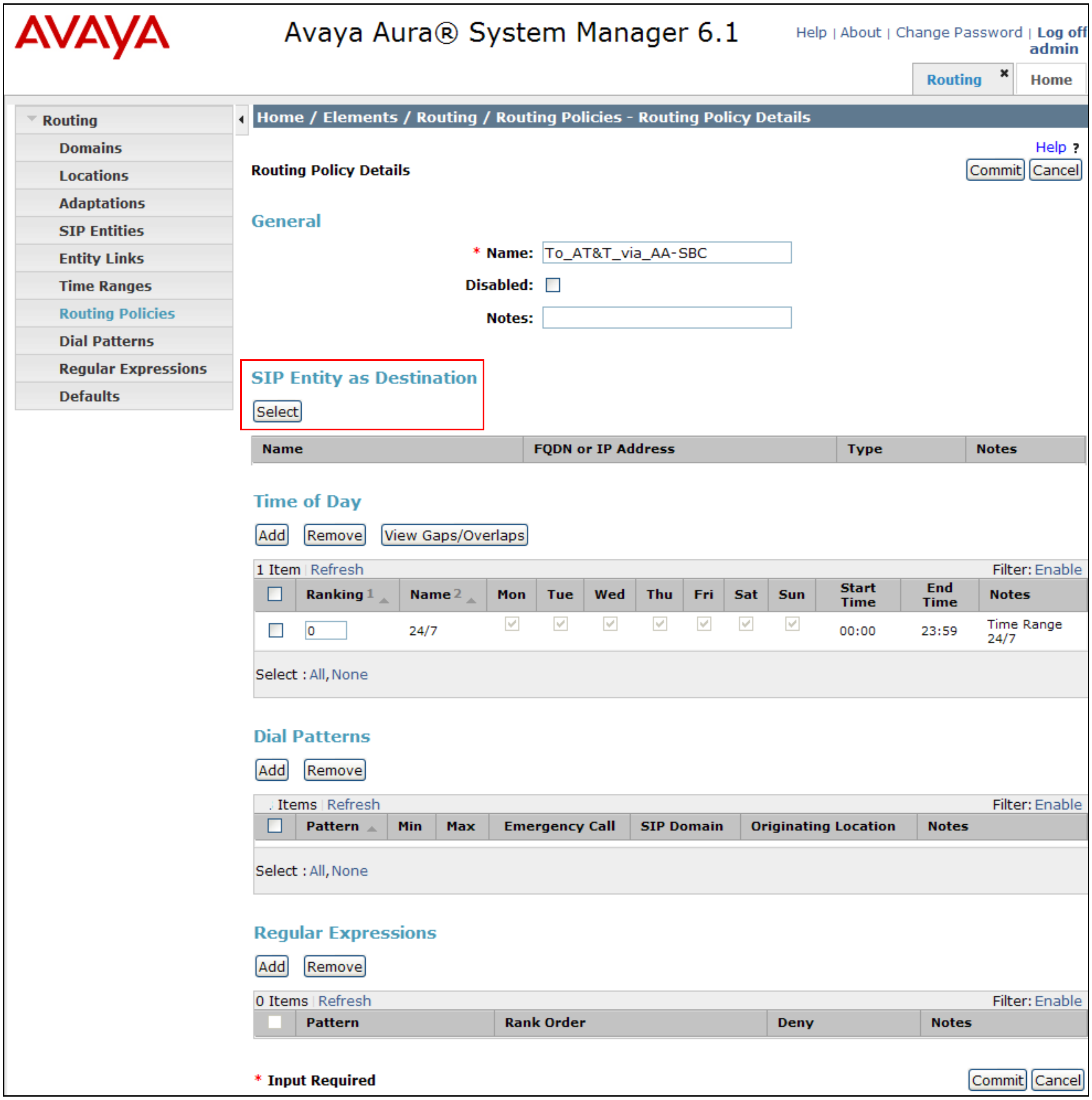
- To AT&T network via the Avaya Aura® SBC (**Section 5.7.1**).
- To Communication Manager 5.2.1 from AT&T (**Section 5.7.2**).
- To Communication Manager 5.2.1 from Modular Messaging (**Section 5.7.3**).
- To Modular Messaging (**Section 5.7.4**).

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

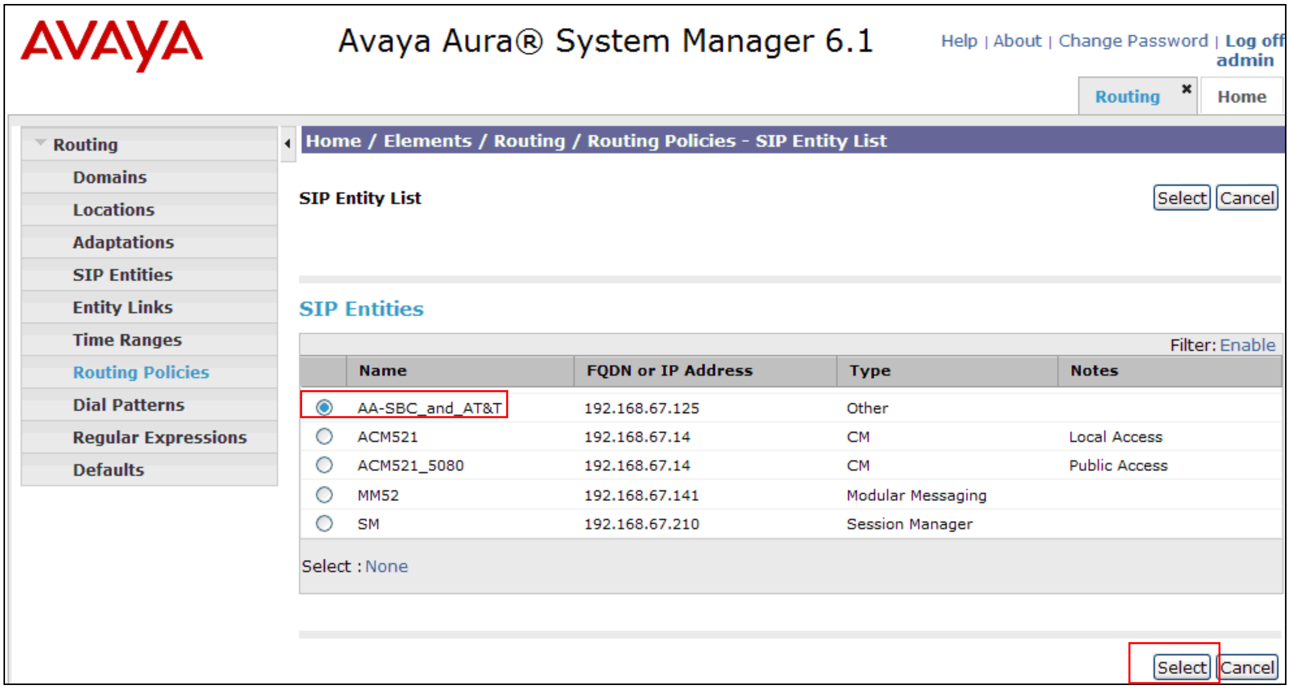
Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page enter a descriptive **Name** for routing calls to AT&T (**To_AT&T_via_AA-SBC**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select**.



Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.4** for the Avaya Aura® SBC (**AA-SBC_and_AT&T**), and click on **Select**.



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

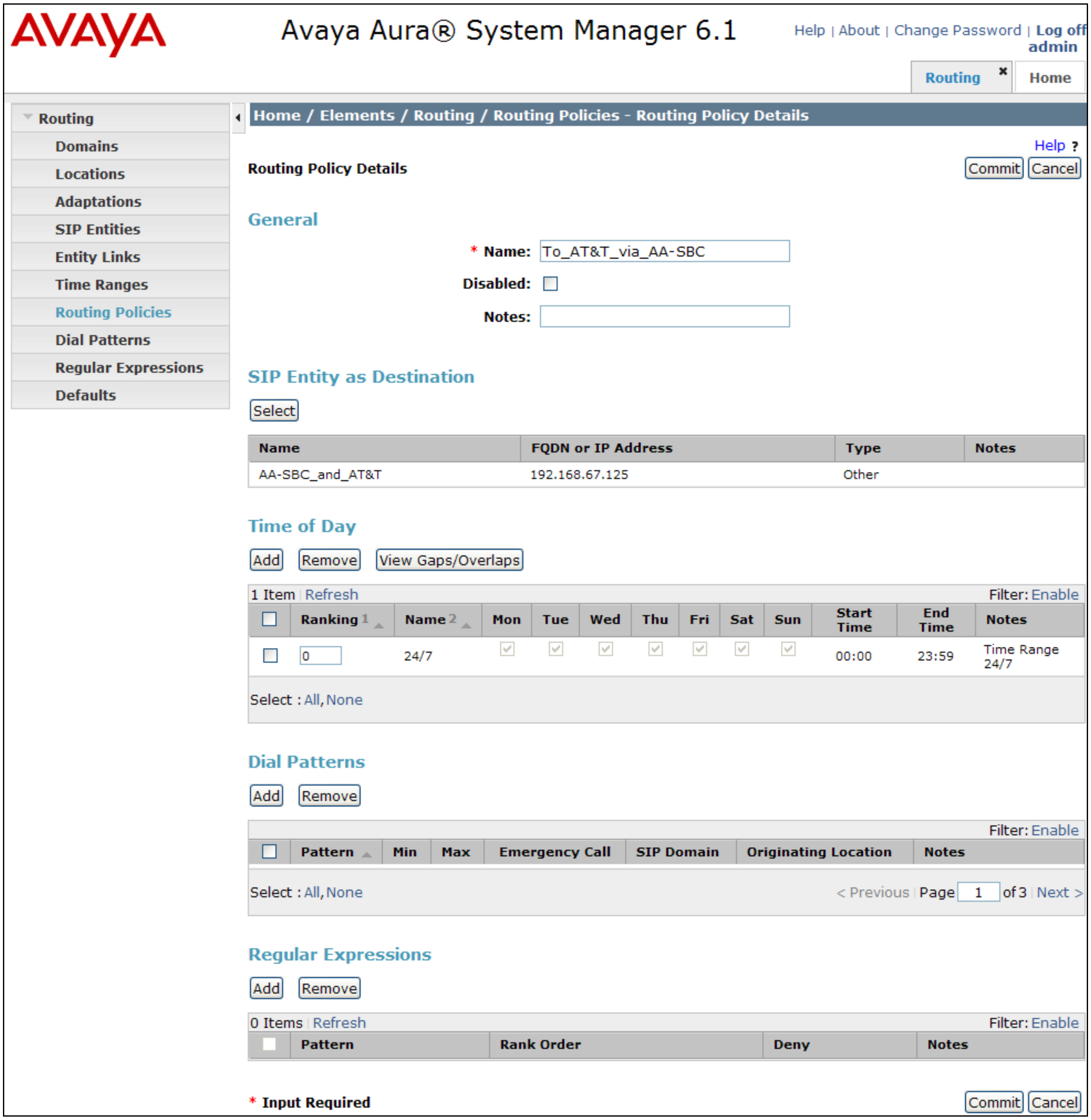
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on "**Select**".

Step 7 - Returning to the **Routing Policy Details** page, in the **Time of Day** section, enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on **Commit**.

Step 8 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section.

Step 9 - No **Regular Expressions** were used in the reference configuration.

Step 10 - Click on **Commit**.



5.7.2. Routing Policy for Routing to Avaya Aura® Communication Manager from AT&T

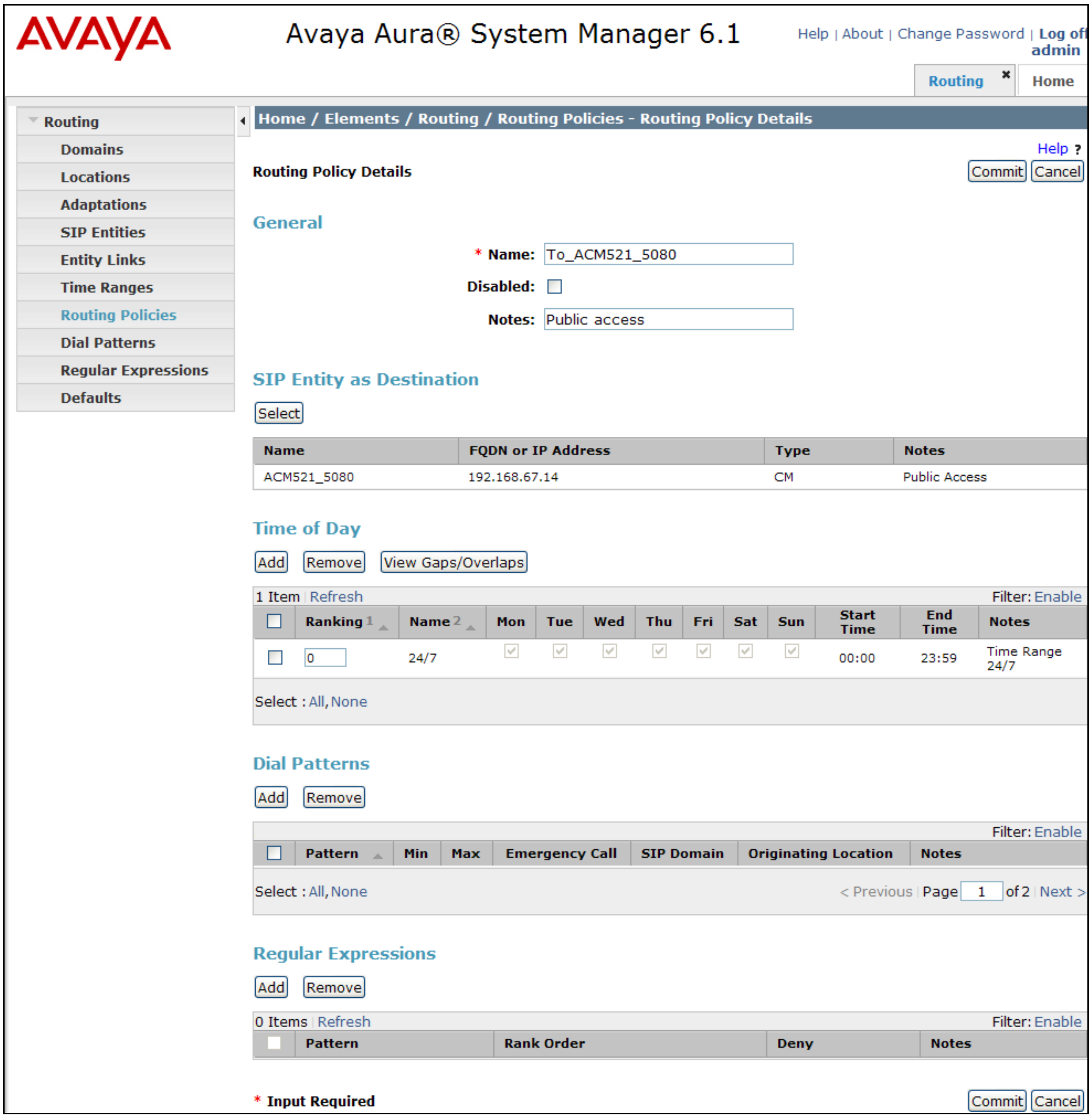
This Routing Policy will use the SIP Enity defined in **Section 5.4.2** (**ACM521_5080)**

Repeat **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Communication Manager (**To_ACM521_5080**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for Communication Manager (**ACM521_5080**) and click on **Select**.
- See **Section 5.8** for the associated Dial Patterns.

Note – Associated Dial Patterns will be displayed on this form after the Dial Pattern provisioning is completed in **Section 5.8**.



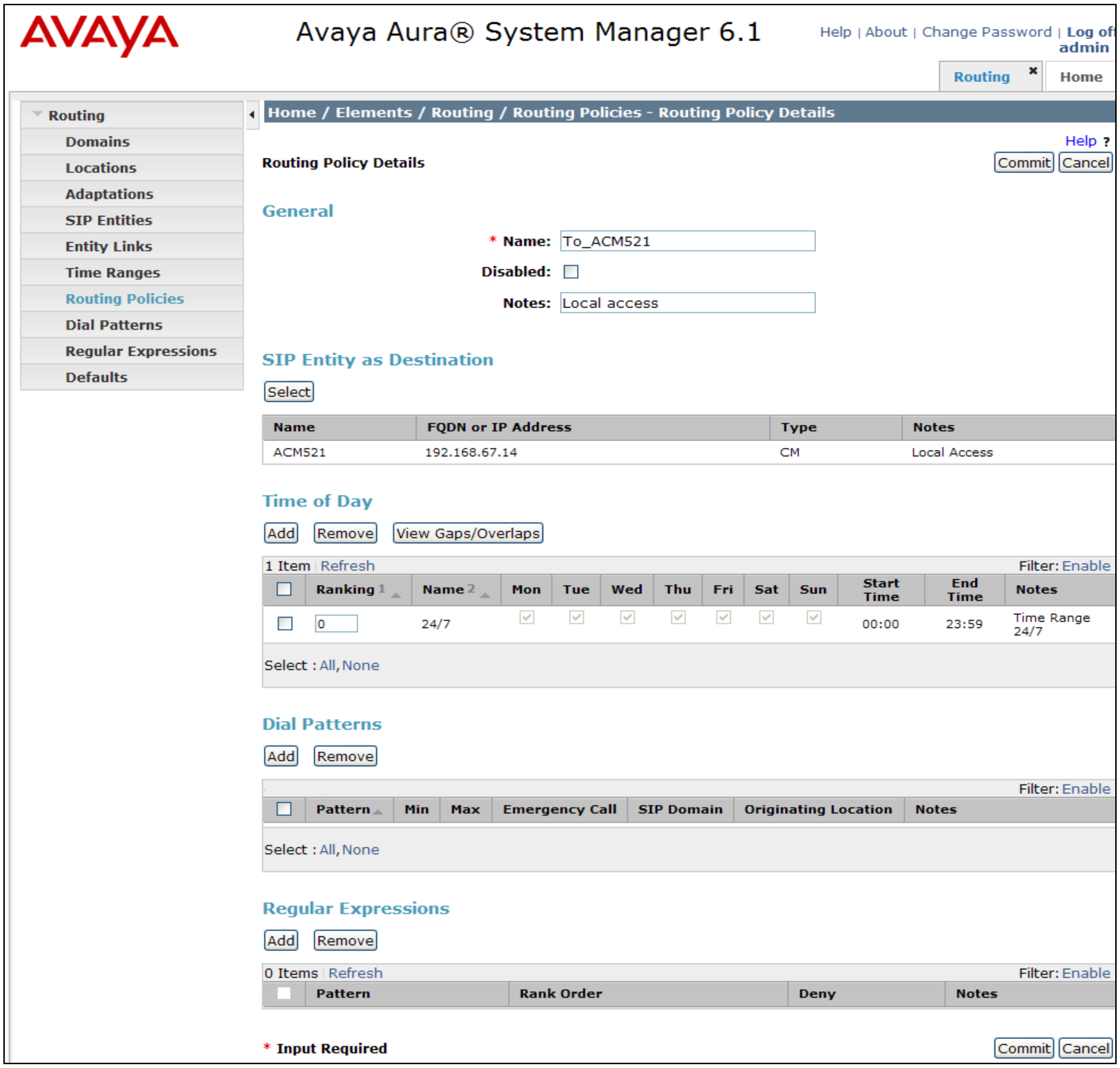
5.7.3. Routing Policy for Routing to Avaya Aura® Communication Manager (local)

Repeat **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Communication Manager (**To_ACM521**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for Communication Manager (**ACM521**) and click on **Select**.
- See **Section 5.8** for the associated Dial Patterns.

Note – Associated Dial Patterns will be displayed on this form after the Dial Pattern provisioning is completed in **Section 5.8**.

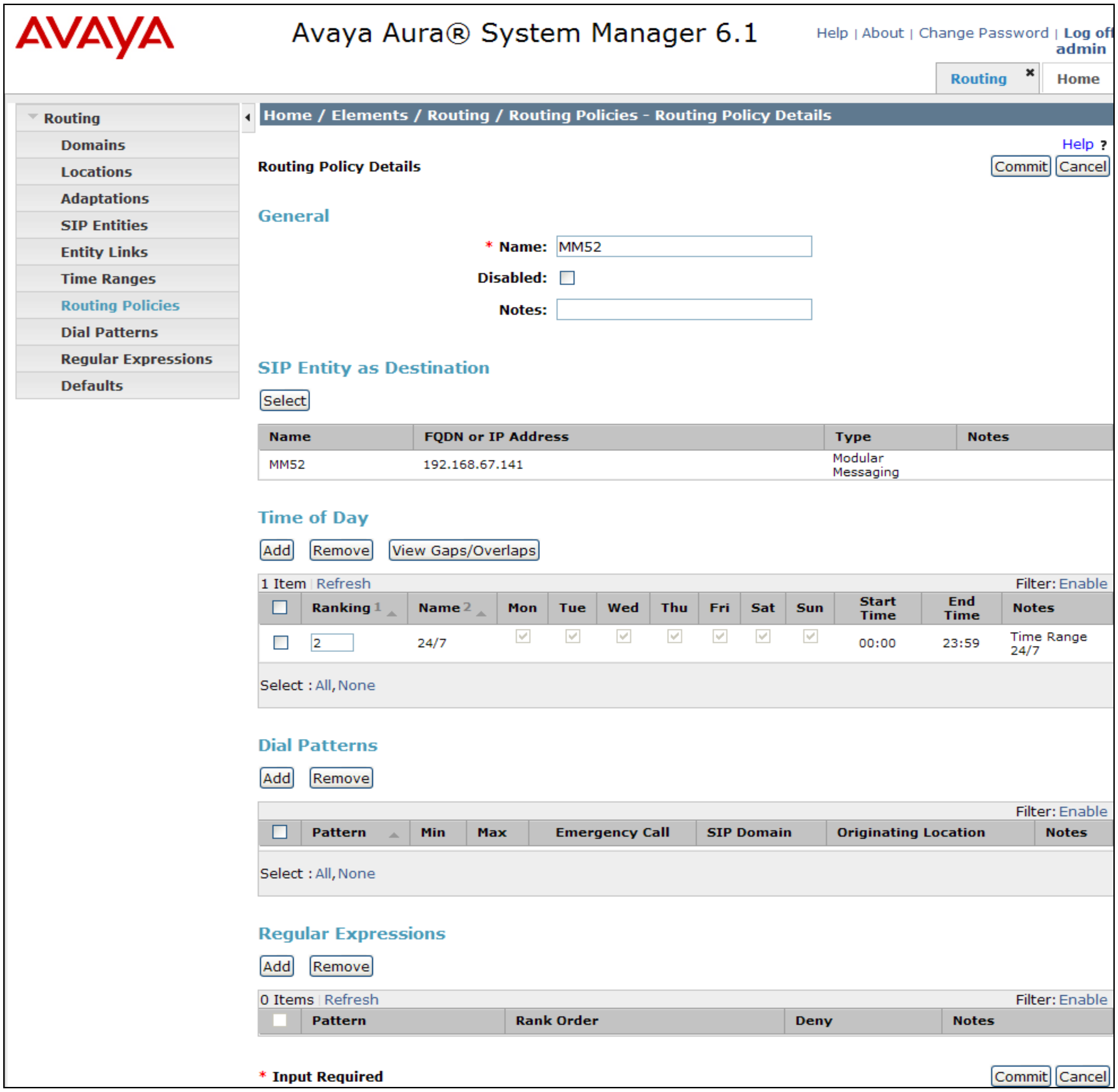


5.7.4. Routing Policy for Routing to Modular Messaging

Repeat **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Avaya Modular Messaging (**MM52**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.5** for Avaya Modular Messaging (**MM52**), and click on **Select**.
- See **Section 5.8** for the associated Dial Patterns.

Note – Associated Dial Patterns will be displayed on this form after the Dial Pattern provisioning is completed in **Section 5.8**.



5.8. Dial Patterns

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

- Outbound PSTN calls via AT&T IP Flexible Reach service (**Section 5.8.1**).
- Inbound PSTN calls via AT&T IP Flexible Reach service (**Section 5.8.2**).
- Calls to the Modular Messaging pilot number (**Section 5.8.3**).
- Notifications from Avaya Modular Messaging (MWI) to Communications Manager 5 digit local extensions (**Section 5.8.4**).

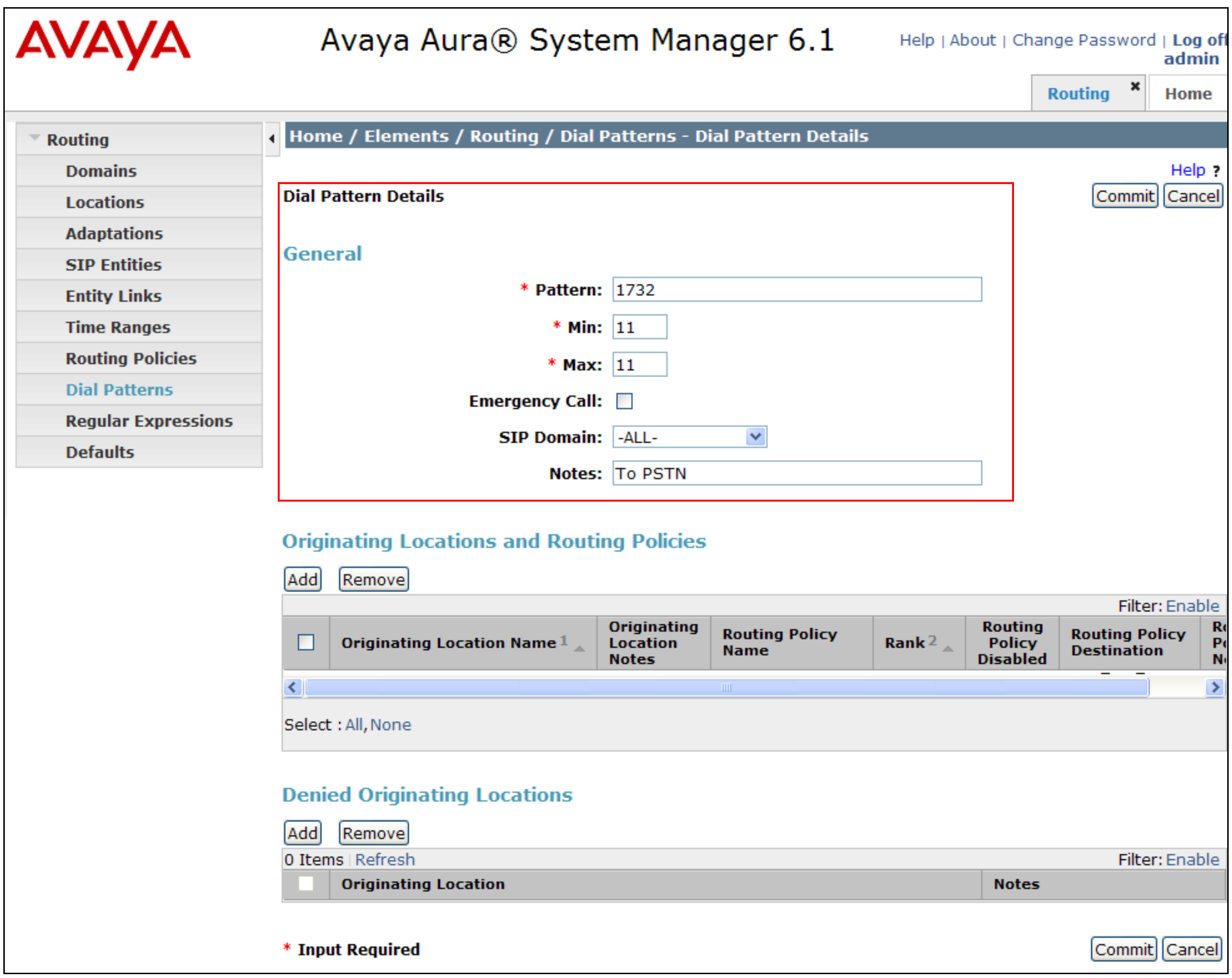
5.8.1. Matching Outbound Calls to the AT&T IP Flexible Reach Service

These Dial Patterns are associated with the Routing Policy **To_AT&T_via_AA-SBC** defined in **Section 5.7.1**. In this example, pattern 1732 is defined for outbound calls to PSTN numbers 11 digits in length (e.g. 1732xxxxxxx).

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

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

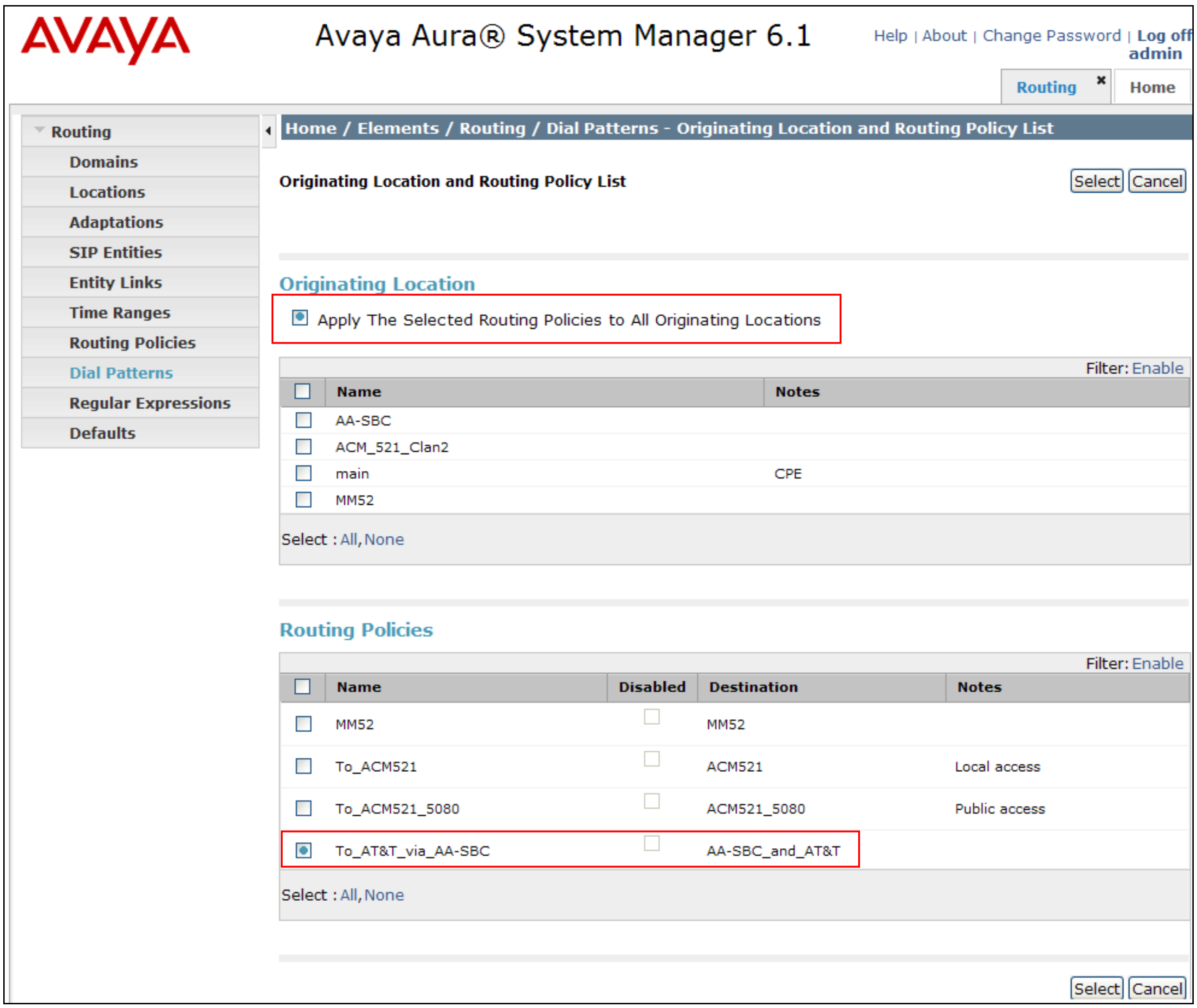
- **Pattern** – Enter matching patterns for outbound dialed digits, (e.g. **1732**).
- **Min** and **Max** – Enter **11**.
- **SIP Domain** – Select a SIP Domain defined in **Section 5.1** or "**-ALL-**", to select all of the administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if "**-ALL-**" is selected) can match this Dial Pattern.
  Note – As only one domain was administered for the reference configuration (customera.com), same result is achieved whether customera.com or All is specified.
- (Optional) Add any notes as desired.



Step 3 - In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.

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

Step 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_via_AA-SBC** administered for routing calls to the AT&T IP Flexible Reach service in **Section 5.7.1**.

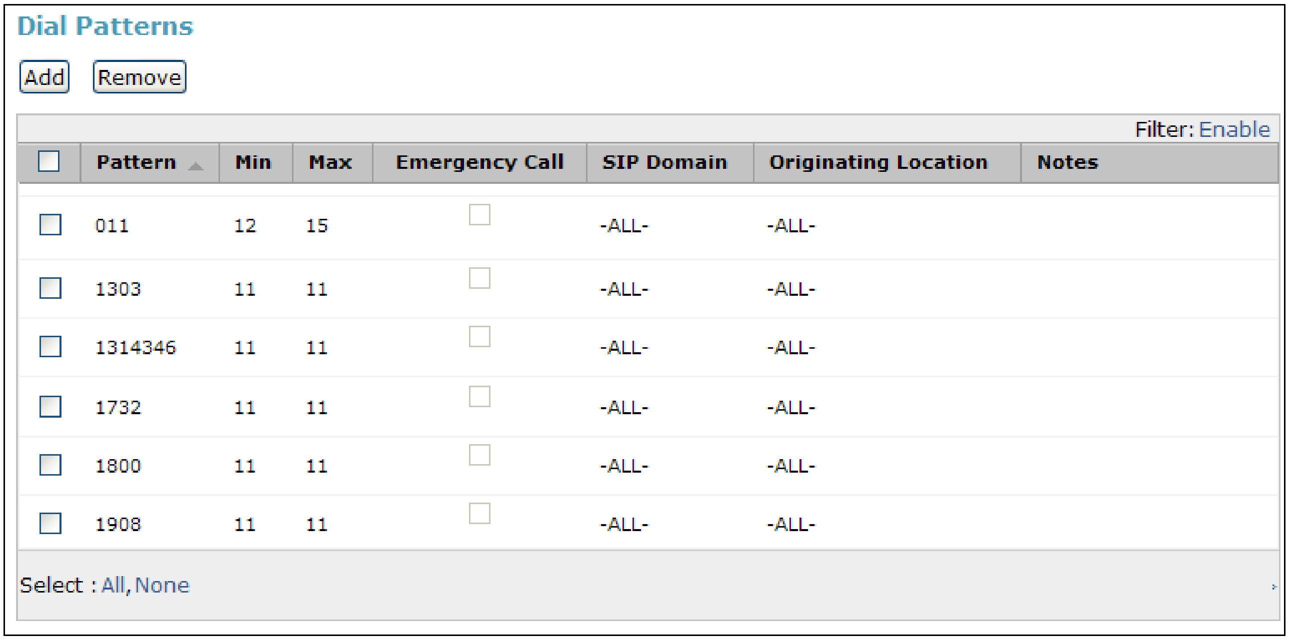


Step 6 - In the **Originating Location and Routing Policy List** page, click on **Select**.

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

Step 8 - Repeat **Steps 2** through 7 for each outbound matching dial patterns required. For example:

- Pattern 011 with 12 to 15 digits for international calls.
- 11 digit numbers matching the patterns 1303xxxxxxx, 1314346xxxx, 1732xxxxxxx, 1800xxxxxxx, 1908xxxxxxx .



Dial Patterns

Add Remove

Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
	011	12	15		-ALL-	-ALL-	
	1303	11	11		-ALL-	-ALL-	
	1314346	11	11		-ALL-	-ALL-	
	1732	11	11		-ALL-	-ALL-	
	1800	11	11		-ALL-	-ALL-	
	1908	11	11		-ALL-	-ALL-	

Select : All, None

5.8.2. Matching Inbound Calls to Avaya Aura® Communication Manager

Repeat the steps from **Section 5.8.1** with the following example entries for inbound calls to Communication Manager (4386, 732320xxxx, 172311xxxxx, 9xxxxxxxxxxx):

- Enter **4386** (inbound 4 digit DNIS from AT&T).
    1. Minimum and Maximum length of **4**.
    2. Routing Policy **To_ACM521_5080** defined in **Section 5.7.2**.
    3. Originating Location **AA-SBC** defined in **Section 5.2.2**.
- Enter **732320** (inbound 10 digit DNIS from AT&T).
    1. Minimum and Maximum length of **10**.
    2. Routing Policy **To_ACM521_5080** defined in **Section 5.7.2**.
    3. Originating Location **AA-SBC** defined in **Section 5.2.2**.
- Enter **172311** (Modular Messaging mailboxes to Communication Manager extensions for MWI).
    1. Minimum and Maximum length of **11**.
    2. Routing Policy **To_ACM521** defined in **Section 5.7.3**.
    3. Originating Location **MM52** defined in **Section 5.2.3**.
- Enter **9** (Modular Messaging “Find-Me” calls to PSTN via Communication Manager).
    1. Minimum and Maximum length of **12**
    2. Routing Policy **To_ACM521** defined in **Section 5.7.3**.
    3. Originating Location **MM52** defined in **Section 5.2.3**.

Note that the outbound dial patterns defined in **Section 5.8.1** are listed as well.

Dial Patterns

Add | Remove

Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	011	12	15	☐	-ALL-	-ALL-	
☐	1303	11	11	☐	-ALL-	-ALL-	
☐	1314346	11	11	☐	-ALL-	-ALL-	
☐	172311	11	11	☐	-ALL-	MM52	MM mailboxes (MWI)
☐	1732	11	11	☐	-ALL-	-ALL-	
☐	1800	11	11	☐	-ALL-	-ALL-	
☐	1908	11	11	☐	-ALL-	-ALL-	
☐	4386	4	4	☐	-ALL-	AA-SBC	
☐	732320	10	10	☐	-ALL-	AA-SBC	
☐	9	12	12	☐	-ALL-	MM52	MM and AA-M Find-Me to ACM

Select : All, None

5.8.3. Matching Outbound Calls to the Avaya Modular Messaging Pilot Number

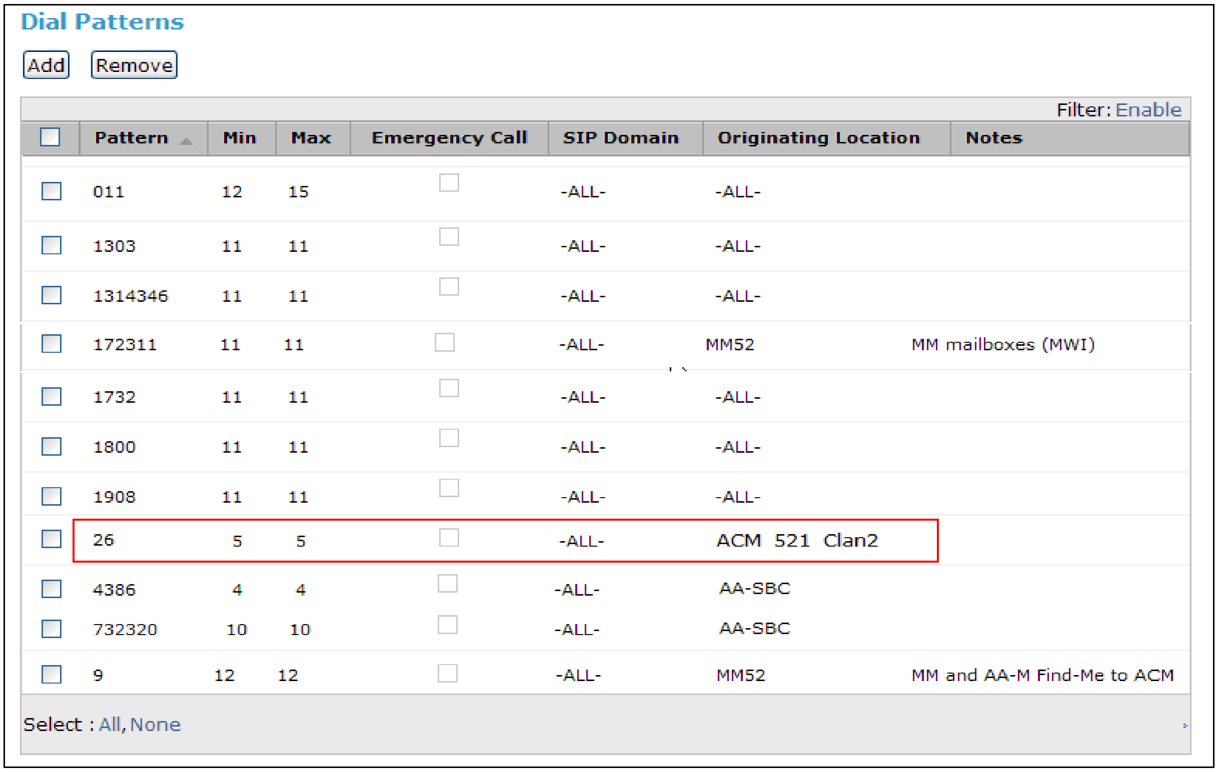
Repeat the steps from **Section 5.8.1** with the following entry for outbound calls to the Modular Messaging pilot number (17231126000) from Communication Manager. Communication Manager stations cover to Avaya Modular Messaging using a pilot extension (26000).

Additionally stations may dial extension 26000 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 5.3.3**.

- Enter **26** (coverage or dialed string from Communication Manager).
  1. Minimum and maximum length of **5**.
  2. Routing Policy **MM52** defined in **Section 5.7.4**.
  3. Originating Location **ACM_521_Clan2** defined in **Section 5.2.1**.

Note that the outbound dial patterns defined in **Section 5.8.1** are listed as well.



Dial Patterns

Add Remove

Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	011	12	15	☐	-ALL-	-ALL-	
☐	1303	11	11	☐	-ALL-	-ALL-	
☐	1314346	11	11	☐	-ALL-	-ALL-	
☐	172311	11	11	☐	-ALL-	MM52	MM mailboxes (MWI)
☐	1732	11	11	☐	-ALL-	-ALL-	
☐	1800	11	11	☐	-ALL-	-ALL-	
☐	1908	11	11	☐	-ALL-	-ALL-	
☐	26	5	5	☐	-ALL-	ACM 521 Clan2	
☐	4386	4	4	☐	-ALL-	AA-SBC	
☐	732320	10	10	☐	-ALL-	AA-SBC	
☐	9	12	12	☐	-ALL-	MM52	MM and AA-M Find-Me to ACM

Select : All, None

5.9. 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.

Step 1 - In the left pane under **Session Manager**, click on **Elements → Session Manager → Session Manager Administration**. In the **Session Manager Administration** page click on **New** (not shown).

Step 2 - In the **General** section of the **Add Session Manager** page, provision the following:

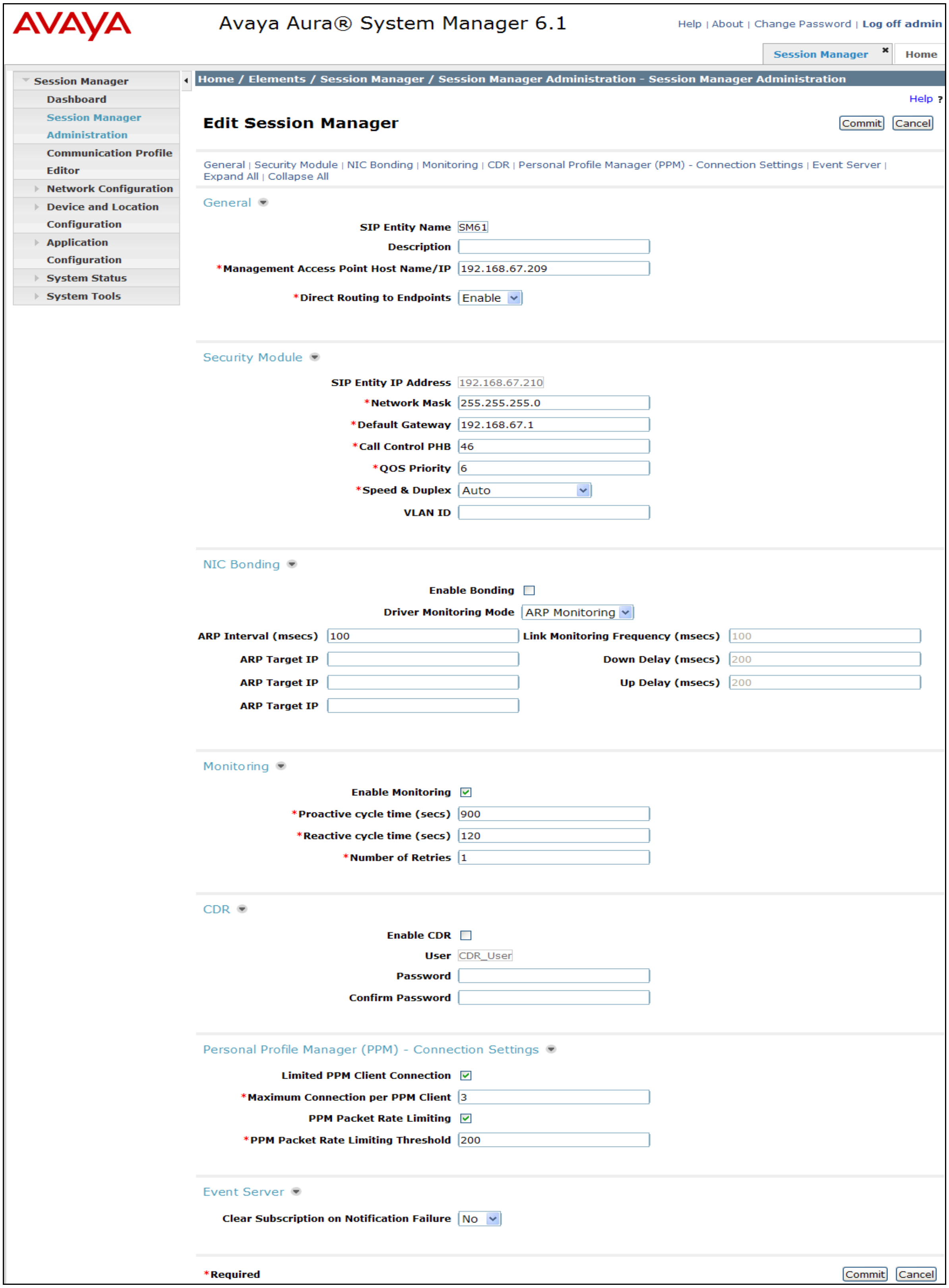
- **SIP Entity Name** – Select the SIP Entity administered for Session Manager in **Section 5.4.1**.
- **Management Access Point Host Name/IP** – Enter the IP address of the management interface on Session Manager as defined during installation e.g. **192.168.67.209**, (*not* the network interface).

Step 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**

Step 4 - In the **Monitoring** section, verify that the **Enable Monitoring** box is checked.

Step 5 - Use the default values for the remaining fields.

Step 6 - Click on **Commit**.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration
Help ?
Edit Session Manager
Commit
Cancel
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All
General
SIP Entity Name SM61
Description
*Management Access Point Host Name/IP 192.168.67.209
*Direct Routing to Endpoints Enable
Security Module
SIP Entity IP Address 192.168.67.210
*Network Mask 255.255.255.0
*Default Gateway 192.168.67.1
*Call Control PHB 46
*QOS Priority 6
*Speed & Duplex Auto
VLAN ID
NIC Bonding
Enable Bonding
Driver Monitoring Mode ARP Monitoring
ARP Interval (msecs) 100
Link Monitoring Frequency (msecs) 100
ARP Target IP
Down Delay (msecs) 200
ARP Target IP
Up Delay (msecs) 200
ARP Target IP
Monitoring
Enable Monitoring
*Proactive cycle time (secs) 900
*Reactive cycle time (secs) 120
*Number of Retries 1
CDR
Enable CDR
User CDR_User
Password
Confirm Password
Personal Profile Manager (PPM) - Connection Settings
Limited PPM Client Connection
*Maximum Connection per PPM Client 3
PPM Packet Rate Limiting
*PPM Packet Rate Limiting Threshold 200
Event Server
Clear Subscription on Notification Failure No
*Required
Commit
Cancel

6. 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 **[5]** and **[6]** for further details if necessary.

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

6.1. System Parameters

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

Step 1 - Enter the **display system-parameters customer-options** command. On **Page 2** of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks (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  94
  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.)
```

Step 2 - On **Page 3** of the **System-Parameters Customer-Options** form, verify that the **ARS** feature is enabled.

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

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

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

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

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

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

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

           IP Attendant Consoles? n
        (NOTE: You must logoff & login to effect the permission changes.)
```

Step 4 - On **Page 5** of the **System-Parameters Customer-Options** form, verify that the **Private Networking** is set to **y**.

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

6.2. Dial Plan

The dial plan defines how digit string will be used locally by Communication manager. Note that the values shown below are examples used in the referenece configuration.

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

- 3-digit dial access codes (indicated with a **Call Type** of **dac**) beginning with the digit **1** (e.g. 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 **2xxxxx** (e.g. Local extensions for Communication Manager stations, agents, and Vector Directory Numbers, VDNs, in this reference configuration conform to this format).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g. **8** access code for outbound AAR dialing). Note – AAR is typically used for local trunk calls. In the reference configuration AAR is used for call coverage to Modular Messaging (see **Section 6.10.3**).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g. **9** access code for outbound ARS dialing). Note – ARS is typically used for public trunk calls. In the reference configuration ARS is used for calls to PSTN via the AT&T IP Flexible Reach service (see **Section 6.10.2**).

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

6.3. IP Node Names

Node names define IP addresses to various Avaya components in the Customer Premisis Equipment (CPE) location. These node names will be used to define the SIP trunks in **Section 6.7**.

Step 1 - Enter the **change node-names ip** command, and add a node name and the IP address for the Avaya Aura® SBC "private" interface (e.g. **AA-SBC** & **192.168.67.125**)

Step 2 – Repeat **Step 1** to add a node name for Modular Messaging (e.g. **MM** & **192.168.67.141**).

Step 3 - Repeat **Step 1** to add a node name for Control LAN (C-LAN) signaling boards used in the reference configuration. These entries were defined during Communication Manager installation (e.g. **MainCLAN2** & **192.168.67.14**).

Step 4 – Repeat **Step 1** to add a node name for Session Manager (e.g. **SM** & **192.168.67.210**).

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
AA-SBC                  192.168.67.125
Gateway001              192.168.67.1
MM                      192.168.67.141
MainCLAN1               192.168.67.13
MainCLAN2               192.168.67.14
MainMP1                 192.168.67.15
MainMP2                 192.168.67.16
SM                      192.168.67.210
VAL                     192.168.67.17
default                 0.0.0.0
```

6.4. IP Interface for IP Interface MainCLAN2

In the reference configuration, the C-LAN board **MainCLAN2** was used for the SIP Trunks.

Step 1 – Enter the **list ip-inteface all** command. Note the slot value associated with the C-LAN to be used to define the SIP Trunks (e.g. **01A03** for **MainCLAN2**).

```
list ip-interface all
                                IP INTERFACES
                                                                Net
ON Type   Slot  Code/Sfx      Node Name/       Mask  Gateway Node     Rgn  VLAN
                              IP-Address
-- ------ ----- --------      ---------------  ----  ---------------  ---  ----
 y C-LAN  01A02 TN799  D      MainCLAN1        /24   Gateway001       1    n
                              192.168.67.13
 y C-LAN  01A03 TN799  D      MainCLAN2        /24   Gateway001       1    n
                              192.168.67.14
 y MEDPRO 01A04 TN2602        MainMP1A04       /24   Gateway001       1    n
                              192.168.67.15
 y MEDPRO 01A05 TN2602        MainMP1A05       /24   Gateway001       1    n
                              192.168.67.16
```

Step 2 - The **display ip-interface 01a03** command can be used to verify the **MainCLAN2** parameters. The following screen shows the parameters used in the reference configuration.

- On **Page 1** of the form verify that **Enable Interface?, Allow H.323 Endpoints?,** and **Allow H248 Gateways?** Fields are set to "**y**".
- Verify/assign a **Network Region** (e.g. **1**).
- Use default values for the remaining parameters.

```
display ip-interface 01a03                                  Page   1 of   3
                                  IP INTERFACES

                  Type: C-LAN
                  Slot: 01A03      Target socket load and Warning level: 400
           Code/Suffix: TN799  D         Receive Buffer TCP Window Size: 8320
      Enable Interface? y                         Allow H.323 Endpoints? y
                  VLAN: n                          Allow H.248 Gateways? y
        Network Region: 1                           Gatekeeper Priority: 5


                                 IPV4 PARAMETERS

             Node Name: MainCLAN2
           Subnet Mask: /24
     Gateway Node Name: Gateway001

         Ethernet Link: 2
         Network uses 1's for Broadcast Addresses? y
```

Step 3 – On **Page 2** of the form, check if the interface is set to auto-negotiate **Auto? y** (default), or set to a specific rate (e.g **10Mbps, 100Mbps, Half, Full**) as required.

```
display ip-interface 01a03                                     Page   2 of   3
                                  IP INTERFACES

                                 ETHERNET OPTIONS
                  Slot: 01A03
                  Auto? y
                                 IPV6 PARAMETERS
             Node Name:
           Subnet Mask: /64
     Gateway Node Name:
      Enable Interface? n

         Ethernet Link:
```

6.5. IP Network Regions

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

6.5.1. IP Network Region 1 – Local Region

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

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

- Enter a descriptive name (e.g. **Local**).
- Enter **customera.com** in the **Authoritative Domain** field.
- 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 media 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 media resources when possible between regions.
- **UDP Port Min**: - Set to **16384 (AT&T requirement).**
- **UDP Port Max**: - Set to **32767 (AT&T requirement).**

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       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
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **2** in the **dst rgn** column, enter **2** (this means Region 1 is permitted to talk to region 2 and they will use codec set 2 to do so). The **WAN** and **Units** columns will self populate with **y** and **NoLimit**. Note that the region 2 form will automatically be populated with the equivalent value.
- Let all other values default for this form.

```
change ip-network-region 1                                      Page   4 of  20
 Source Region: 1     Inter Network Region Connection Management     I       M
```

```
                                                                G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions         CAC  R  L    e
 1    1                                                               all
 2    2     y    NoLimit                                            n       t
```

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

In the reference configuration AT&T SIP trunk calls are assigned to ip-network-region 2.

Step 1 - Repeat the steps in **Section 5.5.1** with the following changes:

- **Page 1**
  - Enter a descriptive name (e.g. **AT&T**)
  - Enter **2** for the **Codec Set** parameter.

```
change ip-network-region 2                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: customera.com
    Name: AT&T
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
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Step 2 – On **Page 4** of the form:

- Verify that codec **2** is listed for **dst rgn 1** and **2** (as was populated in **Section 6.5.1, Step 2**).

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

6.6. IP Codec Parameters

6.6.1. Codecs For IP Network Region 1 (local calls)

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

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

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

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

```
change ip-codec-set 1                                           Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits
                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

6.6.2. Codecs For IP Network Region 2

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

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

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

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

```
change ip-codec-set 2                                          Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? n
                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         off                  0
```

```
   Clear-channel   n                 0
```

6.7. SIP Trunks

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

- AT&T access – SIP Trunk 22
- Local for Modular Messaging access – SIP Trunk 21

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

Note – In the reference configuration TCP (port 5060) is used as the transport protocol between Communication Manager and the Avaya Aura® SBC. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as transport protocol in customer environments whenever possible.

6.7.1. SIP Trunk for AT&T IP Flexible Reach calls

This section describes the steps for administering the SIP trunk used for AT&T IP Flexible Reach calls.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **22**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp**. Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Avaya Aura® SBC and the AT&T IP Flexible Reach service is UDP.
- Verify the **IMS Enabled?** Is set to **N**.
- **Near-end Node Name** – Set to the node name of **MainCLAN2** noted in **Section 6.3** and **6.4**
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g. **SM**).
- **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 **2**, as defined in **Section 6.5.2**.
- **Far-end Domain** – Enter **customera.com**. This is the CPE domain used in the reference configuration and defined in Session Manager (**see Section 5.1**).
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible (known as “shuffling”).
- **Enable Layer 3 Test** – Set to **y**. This initiates Communication Manager to send OPTIONS “pings” to the Avaya Aura® SBC to provide link status.

```
add signaling-group 22                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 22             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

 Near-end Node Name: MainCLAN2             Far-end Node Name: SM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2
Far-end Domain: customera.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **22**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g. **ATT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **122**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 0** (e.g. **22**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g. **10**).

```
add trunk-group 22                                              Page   1 of  21
                               TRUNK GROUP

Group Number: 22                   Group Type: sip           CDR Reports: y
  Group Name: ATT                         COR: 1        TN: 1        TAC: 122
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                                       Signaling Group: 22
                                                     Number of Members: 10
```

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

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

```
add trunk-group 22                                              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
 Disconnect Supervision - In? y  Out? y
```

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

- Set N**umbering Format:** to **public**

```
add trunk-group 22                                              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
```

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

- Verify that **Network Call Redirection?** is set to **n** (default).
- Set **Send Diversion Header?** field to **y**.
- Set **Telephone Event Payload Type** field to the RTP payload type required by the AT&T IP Flexible Reach service (e.g. **100**).
- Use default for all other values.

```
add trunk-group 22                                              Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                Network Call Redirection? n
                   Send Diversion Header? y
                 Support Request History? y
             Telephone Event Payload Type: 100
```

NOTE – As noted in **Section 2.2.1**, the AT&T IP Flexible Reach service does not support History-Info headers. In the reference configuration, Session Manager was used to remove these headers from frames sent to AT&T (see **Section 5.3.1**). Alternatively, the "**Support Request History?**" paramater may be set to **n** (**y** is the default value).

6.7.2. Local SIP Trunk (Modular Messaging)

This section describes the steps for administering the local SIP trunk for calls to Avaya Modular Messaging.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **21**), and follow the procedures shown in **Section 5.7.1 Step 1** except:

- **Far-end Node Name** – Set to the node name of Modular Messaging as administered in **Section 6.3** (e.g. **MM**).
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.5.1**.

```
add signaling-group 21                                          Page   1 of   1
                                SIGNALING GROUP
 Group Number: 21             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

 Near-end Node Name: MainCLAN2           Far-end Node Name: MM
 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? 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
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **21**). Follow the procedures shown in **Section 6.7.1 Steps 2-5** except:

On **Page 1** of the **trunk-group** form, provision the following:

- **Group Name** – Enter a descriptive name (e.g. **Local**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **121**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g. **21**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g. **10**).

```
add trunk-group 21                                              Page   1 of  21
                                TRUNK GROUP
Group Number: 21                   Group Type: sip           CDR Reports: y
  Group Name: Direct_to_MM                COR: 1        TN: 1        TAC: 121
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                                       Signaling Group: 21
                                                     Number of Members: 10
```

Step 3 - On **Page 2** of the **Trunk Group** form, enter the same information as in **Section 6.7.1**.

```
add trunk-group 21                                              Page   2 of  21
  Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                                Redirect On OPTIM Failure: 5000
```

```
           SCCAN? n                                Digital Loss Group: 18
                    Preferred Minimum Session Refresh Interval(sec): 900
Disconnect Supervision - In? y  Out? y
```

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

- Set N**umbering Format:** to **private**

```
add trunk-group 21                                          Page   3 of  21

TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                  Maintenance Tests? y
                     Numbering Format: private
                                              UUI Treatment: service-provider
                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n
```

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

- Verify that **Network Call Redirection?** is set to **n** (default).
- Verify that **Send Diversion Header?** field is set to **n** (default).
- Verify that **Support Request History?** field is set to **y** (default).
- Set **Telephone Event Payload Type** field to the RTP payload type required by the AT&T IP Flexible Reach service (e.g. **100**).

```
add trunk-group 21                                          Page   4 of  21

                              PROTOCOL VARIATIONS

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

6.8. Public Unknown Numbering

In the public unknown numbering form, Communication Manager local extensions are converted to AT&T Flexible Reach numbers (previously assigned by AT&T) and directed to the "public" trunk defined in **Section 6.7.1**.

Step 1 - Using the **change public-unknown-numbering 0** command, enter.

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. **5**).
- **Ext Code –** Enter a Communication Manager extension (e.g. **26101**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g. **22**).
- **CPN Prefix** – Enter an assigned AT&T P Flexible Reach number (e.g. **7325554050**) that corresponds to the Communication Manager extension.
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g. **10**).

Step 2 – Repeat **Step 1** for all corresponding AT&T IP Flexible Reach number/Communication Manager extensions.

```
change public-unknown-numbering 0                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                            Total
Ext Ext             Trk       CPN            CPN
Len Code            Grp(s)    Prefix         Len
 5  26101           22         7325554050     10      Total Administered: 3
 5  26102           22         7325554051     10         Maximum Entries: 9999
 5  26103           22         7325554052     10
```

6.9. Private Numbering

The private-numbering form is used for calls to Modular Messaging (call coverage/retrieval) via the "local" trunk defined in **Section 6.7.2**.

Step 1 - Using the **change private-numbering 0** command, enter the Modular Messaging pilot number (e.g. 26000).

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. **5**).
- **Ext Code –** Enter the Communication Manager extension (e.g. **26000**).assigned to the Modular Messaging coverage hunt group defined in **Section 6.12**.
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g. **21**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g. **5**).

```
change private-numbering 0                                       Page   1 of   2
                           NUMBERING - PRIVATE FORMAT
Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  26000            21                           5     Total Administered: 1
                                                           Maximum Entries: 540
```

6.10. Outbound Call Routing From Avaya Aura® Communication Manager

Route patterns are used to direct calls to the appropriate SIP trunk using either the Automatic Route Selection (ARS) or Automatic Alternate Routing (AAR) dialing tables.

6.10.1. Route Pattern for Calls to AT&T

This form defines the "public" SIP trunk, based on the route-pattern selected by the ARS table in **Section 6.10.3** (e.g. calls to the AT&T IP Flexible Reach service).

Step 1 – Enter the **change route-pattern x** command where **x** is an available route-pattern (e.g. **22**) and enter the following:

- In the Pattern Name field, enter a descriptive name (e.g. **To_ATT**).
- In the **Grp No** column enter **22** for SIP trunk 22 ("public" trunk).
- In the **FRL** column enter **0** (zero).

```
change route-pattern 22                                           Page   1 of   3
                          Pattern Number: 22  Pattern Name: To_ATT
                                     SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                 DCS/ IXC
    No          Mrk Lmt List Del  Digits                                   QSIG
                                 Dgts                                      Intw
 1: 22   0                                                                  n   user
 2:                                                                         n   user
 3:                                                                         n   user
 4:                                                                         n   user
      BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                  Dgts Format
                                                          Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
```

6.10.2. Route Pattern for Calls to Modular Messaging

This form defines the "local" SIP trunk, based on the route-pattern selected by the AAR table in **Section 6.10.4** (e.g. calls to the Modular messaging pilot number 26000).

Step 1 – Enter the **change route-pattern x** command where **x** is an available route-pattern (e.g. **21**) and enter the following:

- In the Pattern Name field, enter a descriptive name (e.g. **To_MM**).
- In the **Grp No** column enter **21** for SIP trunk 21 ("local" trunk).
- In the **FRL** column enter **0** (zero).
- In the **1:** row near the bottom of the form, enter **unk-unk** under the **Numbering Format** column.

```
change route-pattern 1                                            Page   1 of   3
                Pattern Number: 11  Pattern Name: To_MM
                                     SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                 DCS/ IXC
    No          Mrk Lmt List Del  Digits                                   QSIG
                                 Dgts                                      Intw
 1: 21   0                                                                  n   user
 2:                                                                         n   user
 3:                                                                         n   user
 4:                                                                         n   user
 5:                                                                         n   user
 6:                                                                         n   user

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

```
 4: y y y y y n  n            rest                                        none
 5: y y y y y n  n            rest                                        none
 6: y y y y y n  n            rest                                        none
```

6.10.3. ARS Dialing

Automatic Route Selection (ARS) is used to direct calls to AT&T via the route pattern defined in **Section 6.10.1**.

Step 1 – Enter the change **ars analysis x** command where "x' is a digit string dialed to AT&T . In the following example calls to PSTN using an 11 digit number and beginning with 1732 are defined.

- **Dialed String** enter **1732**
- **Min** & **Max** enter **11**
- **Route Pattern** enter **22**
- **Call Type** enter **ars**

Step 2 – Repeat **Step 1** for any additional dialed strings to AT&T. When completed, the command "**list ars analysis**" may be used to display the entire ars routing table.

Note that the system comes with some dial strings predefined, most specifying a route pattern of "deny" by default. In the example below, the 11 digit string 173 is denied by default. That means calls to the dialed number 173**3**xxxxxxx will be blocked, but calls to 1732xxxxxxx will be routed.

```
change ars analysis 1732                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

         Dialed            Total      Route     Call   Node  ANI
         String           Min  Max   Pattern    Type   Num   Reqd
    173                   11   11     deny      fnpa         n
    1732                  11   11     22        fnpa         n
```

6.10.4. AAR Dialing

Automatic Alternate Routing (AAR) is used to direct local trunk calls, such as coverage calls for the Modular Messaging pilot number (**26000**) to the route pattern defined in **Section 5.10.1.2**.

Step 1 – Enter the change **aar analysis 2** command and for the Modular Messaging coverage hunt group extension enter the following:

- **Dialed String** enter **26000**
- **Min** & **Max** enter **5**
- **Route Pattern** enter **21**
- **Call Type** enter **aar**

```
change aar analysis 2                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1
         Dialed            Total      Route     Call   Node  ANI
         String           Min  Max   Pattern    Type   Num   Reqd
     26000                 5    5      21        aar           n
```

6.11. Inbound Call Routing To Avaya Aura® Communication Manager

6.11.1. Calls from AT&T

The AT&T IP Flexible Reach service will assign DNIS digits that will be inserted in the Request URI of inbound calls. These DNIS digit strings are converted to Communication Manager extensions in Session Manager (see **Section 5.3.2**) before delivery to Communication Manager.

6.11.2. Calls from Modular Messaging

Modular Messaging supports an outbound calling feature called "Find Me". This feature has Modular Messaging call a remote number (previously defined by the user) to notify the user that someone is trying to reach them when the call goes to coverage. In order for Communication Manager to route this call over the "public" trunk to AT&T, the ARS access code defined in **Section 6.2** (e.g. **9**) must be added to the dialed string sent by Modular Messaging. This is performed by Session Manager (see **Section 5.3.3**) before delivery to Communication Manager.

6.12. Provisioning for Coverage to Modular Messaging

To provide coverage to Modular Messaging for Communication Manager extensions, a hunt group is defined using the Modular Messaging pilot number (e.g. **26000**).

6.12.1. Hunt Group for Station Coverage to Modular Messaging

Step 1 – Enter the command **add hunt-group x**, where x is an available hunt group (e.g. **1**).

- **Group Name** – Enter a descriptive name (e.g. **MM**).
- **Group Extension** – Enter an available extension (e.g. **26000**). Note that the hunt group extension need *not* be the same as the Modular Messaging pilot number.
- **ISDN/SIP Caller Display** – Enter **mbr-name**.
- Let all other fields default.

```
add hunt-group 1                                               Page   1 of  60
                                  HUNT GROUP
            Group Number: 1                                 ACD? n
              Group Name: 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
```

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

- **Message Center –** Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Modular Messaging pilot number (e.g. **26000**).
- **Voice Mail Handle** - Enter the Modular Messaging pilot number (e.g. **26000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 6.2** (e.g. **8**).

```
change hunt-group 1                                              Page   2 of  60
                                 HUNT GROUP
                      Message Center: sip-adjunct          Routing Digits
     Voice Mail Number        Voice Mail Handle     (e.g., AAR/ARS Access Code)
          26000                     26000                       8
```

6.12.2. Coverage Path for Station Coverage to Modular Messaging

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

Step 1 – Enter the command **add coverage path x**, where x is an available coverage path (e.g. **1**).

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

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

6.12.3. Station Coverage Path to Modular Messaging

The coverage path defined in the previous section, is then defined to the stations or agents.

Step 1 – Enter the command **cha station xxxxx**, where xxxxx is a previously defined station or agent extension (e.g. station **26102**).

- **Coverage path** – Specify the coverage path defined in **Section 6.12.2** (e.g. **1**). Note that the coverage path field will appear at different positions on the form depending on whether agent or station extensions are being provisioned.

```
change station 26102                                          Page   1 of   5
                                     STATION
Extension: 26102                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code: 123456           TN: 1
     Port: S00000                      Coverage Path 1: 1               COR: 1
     Name: Keith Richards              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                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n
```

6.12.4. Saving Translations

To save all Communication Manager provisoning changes, enter the command **save translations.**

7. 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]** and **[8]** for further details.

8. Configure Avaya Aura® Session Border Controller (SBC)

This section illustrates an example configuration of the Avaya Aura® SBC. In the sample configuration, the Avaya Aura® SBC resides on its own S8800 Server as an application template running on System Platform operating system. The application template defines basic functionality for the SBC such as IP addressing, SIP domains, etc. The installation of the System Platform and application template is assumed to have been previously completed (see the Avaya Aura® SBC references **[9]** and **[10])** for additional information on the Avaya Aura® SBC installation.

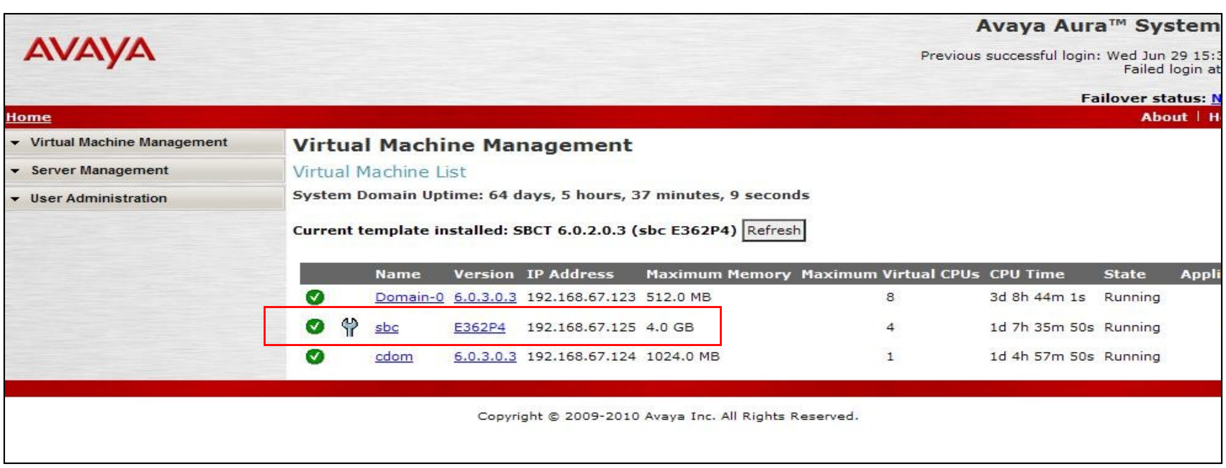
Note - The AT&T IP Flexible Reach service border element IP addresses shown in this document are examples. AT&T Customer Care will provide the actual IP addresses as part of the IP Flexible Reach provisioning process.

8.1. Logging into the Avaya Session Border Controller

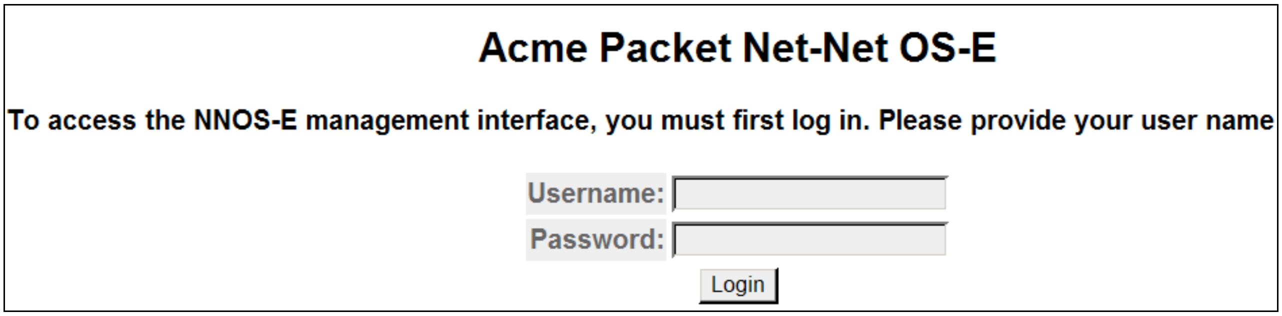
Log in to the System Platform console domain by entering https://<ip-addr>/webconsole as shown in the example screen below. In the reference configuration, the console domain uses the IP Address 192.168.67.124. Enter an appropriate **User Id** and press the **Continue** button.

On the subsequent screen, enter the appropriate **Password** and click the **Log On** button.

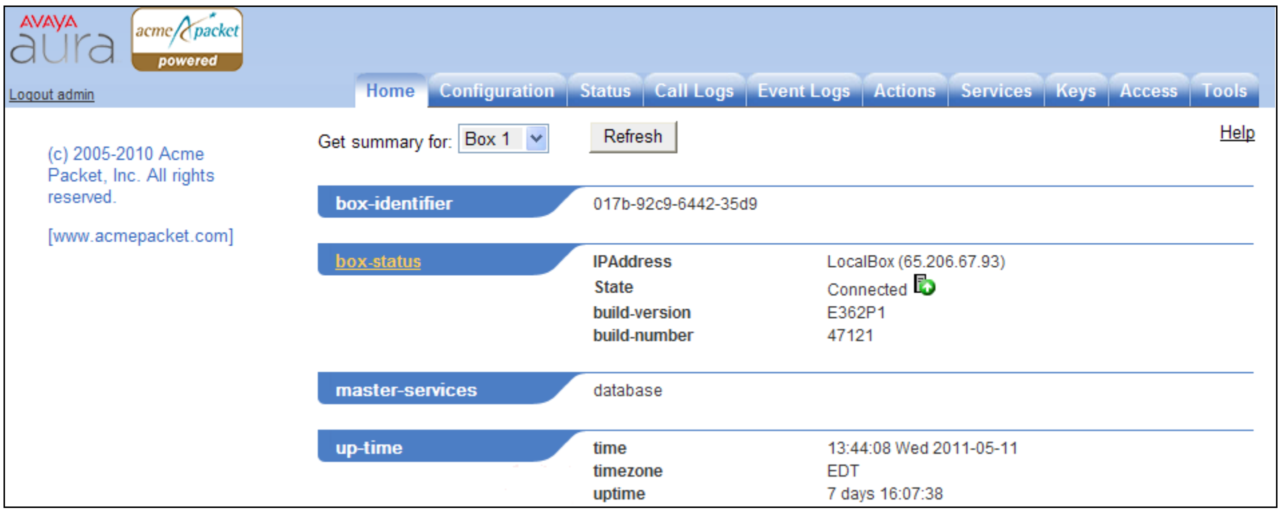
The **Virtual Machine List** will show the SBC Template. Click on the to access the Avaya SBC GUI interface.



Enter appropriate **Username** and **Password** and click **Login**.



The following shows an abridged **Home** screen after logging in. Note the tabs at the top.



8.2. Network Configuration

As described previously much of the network information is defined during installation of the SBC application template. However there may be occasions where these parameters need to be modified. Therefore these values are described below.

In the reference configuration, the Avaya S8800 Server has four physical network interfaces, labeled 1 through 4. The port labeled **1** (virtual **eth0**) is used for the management and private (inside) network interface of the SBC (toward the customer equipment). The port labeled **4** (virtual **eth2**) is used for the public (outside) network interface of the SBC (toward AT&T). These can be verified by checking the **interface eth0** and **interface eth2** settings (see **Section 8.2.1**).

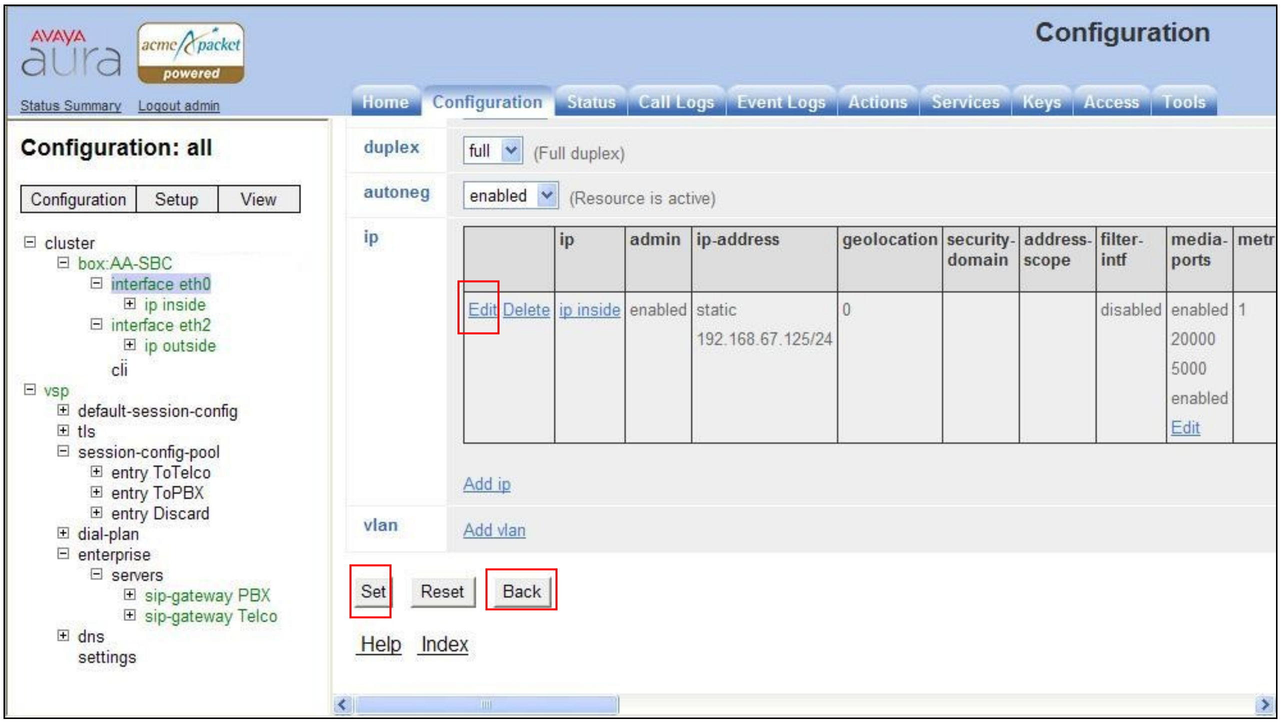
The AT&T AVPN transport service requires that RTP media traffic use UDP port range 16384-32767. This range is defined as part of **interface eth2** (see **Section 8.2.3**).

SIP-Gateways are defined for corresponding to the private and public interfaces. In the reference configuration the private interface is defined as "PBX" and the public interface is defined as **Telco1** (see **Section 8.2.4**).

8.2.1. Verify IP Addressing

Step 1 - From the **Configuration** tab, select **cluster → box <name defined during install>** (e.g. **AA-SBC**). The **interface eth0** and **interface eth2** will be displayed. Click on **ip inside** (eth0) or **ip outside** (eth2) to display the interface configuration. Note that AT&T may require the eth2 IP address as part of the IP Flexible Reach service provisioning.

Step 2 - The configuration may be modified by clicking the **Edit** button. If changes are made, click on the **Set** button. To cancel changes or to go to a previous screen, click on **Back**.



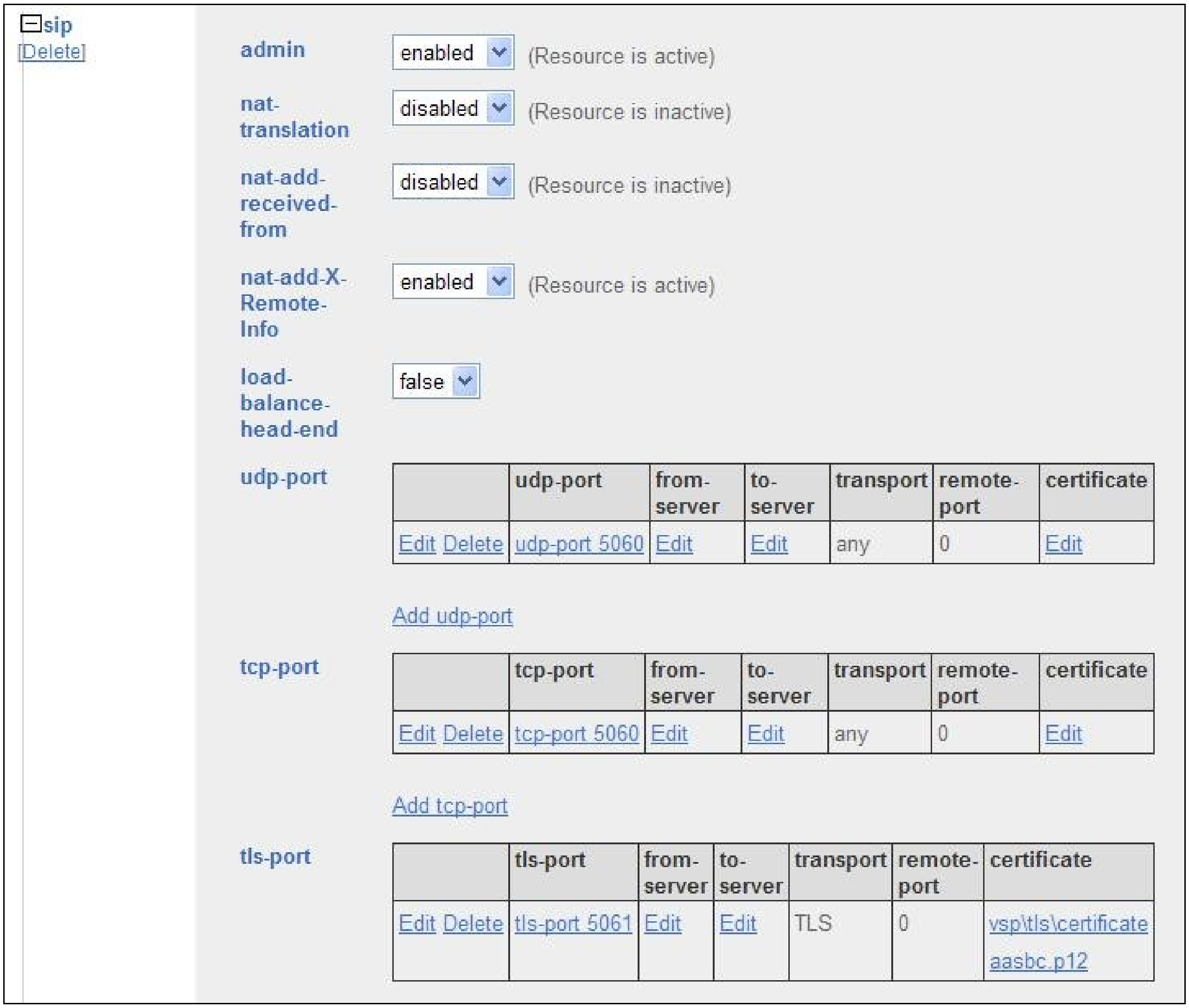
8.2.2. Transport Protocols

8.2.2.1 Private Interface – Eth0

The private interface, eth0, was provisioned to support UDP, TCP, and TLS transport protocols. However, TCP (port 5060) was used in the reference configuration for the connection to Session Manager (see **Section 5.4.4** and **5.5.3**). This can be displayed by the following:

Step 1 – Navigate to **cluster → box <name defined during install> → interface eth0 → ip inside.**

Step 2 – Scroll down to, and click on the **SIP** heading. The UDP, TCP, and TLS supported protocols are displayed.



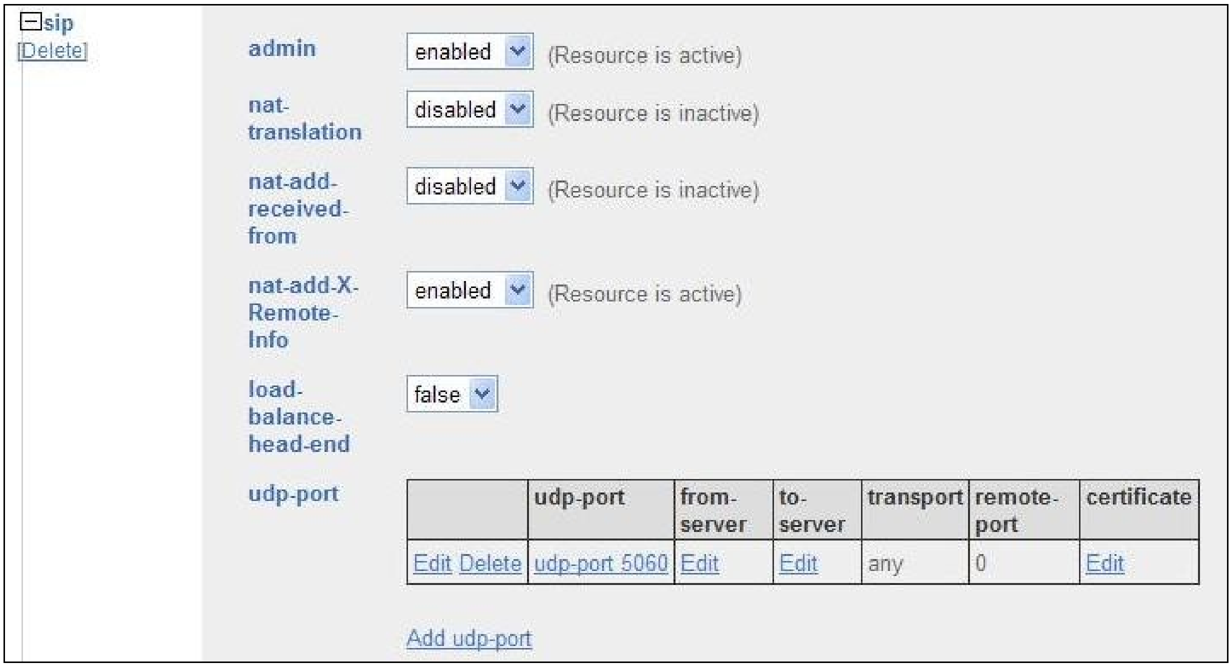
Step 3 - The configuration may be modified by clicking the **Edit** buttons. If changes are made, click on the **Set** button (not shown). To cancel changes or to go to a previous screen, click on **Back** (not shown).

8.2.2.2 Public Interface – Eth2

The AT&T IP Flexible Reach service requires UDP transport protocol between the Avaya SBC and the AT&T IP Flexible Reach service border element. Therefore, the public interface, eth2, was provisioned to support UDP transport protocol only. This can be displayed by the following:

Step 1 – Navigate to **cluster → box <name defined during install> → interface eth2 → ip outside.**

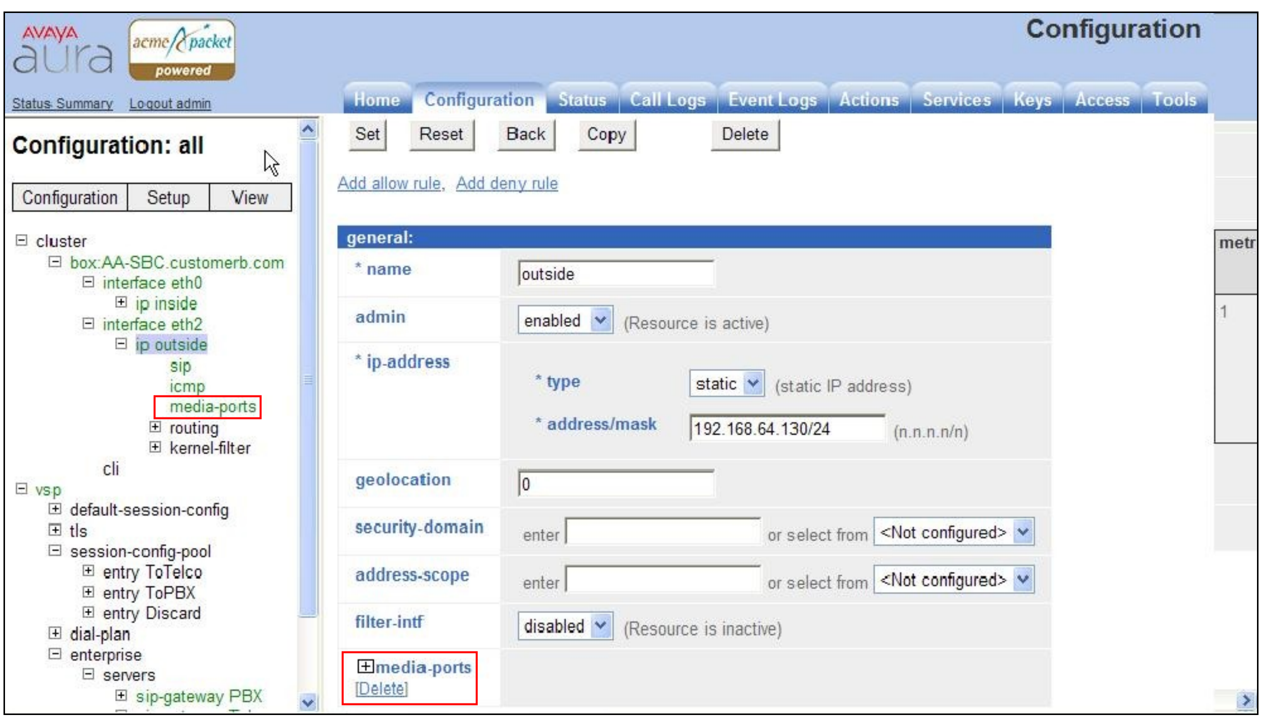
Step 2 – Scroll down to, and click on the **SIP** heading. The UDP (port 5060) transport protocol is displayed.



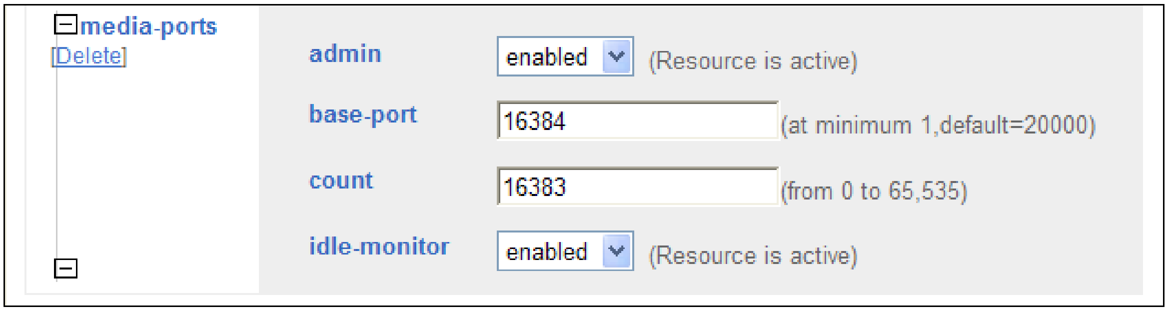
Step 3 - The configuration may be modified by clicking the **Edit** buttons. If changes are made, click on the **Set** button (not shown). To cancel changes or to go to a previous screen, click on **Back** (not shown).

8.2.3. Setting the RTP Port Range on Eth2

Step 1 - Go to **cluster → box <name defined during install> → interface eth2 → ip outside** to display the eth2 configuration toward AT&T. Select **media-ports**.



Step 2 - The media port section will be displayed. Enter **16384** in the **base-port** field and **16383** in the **count** field.



Step 3 - Click on the **Set** button (not shown) to save.

Step 4 - Proceed to save and activate the configuration as described in **Section 8.3**.

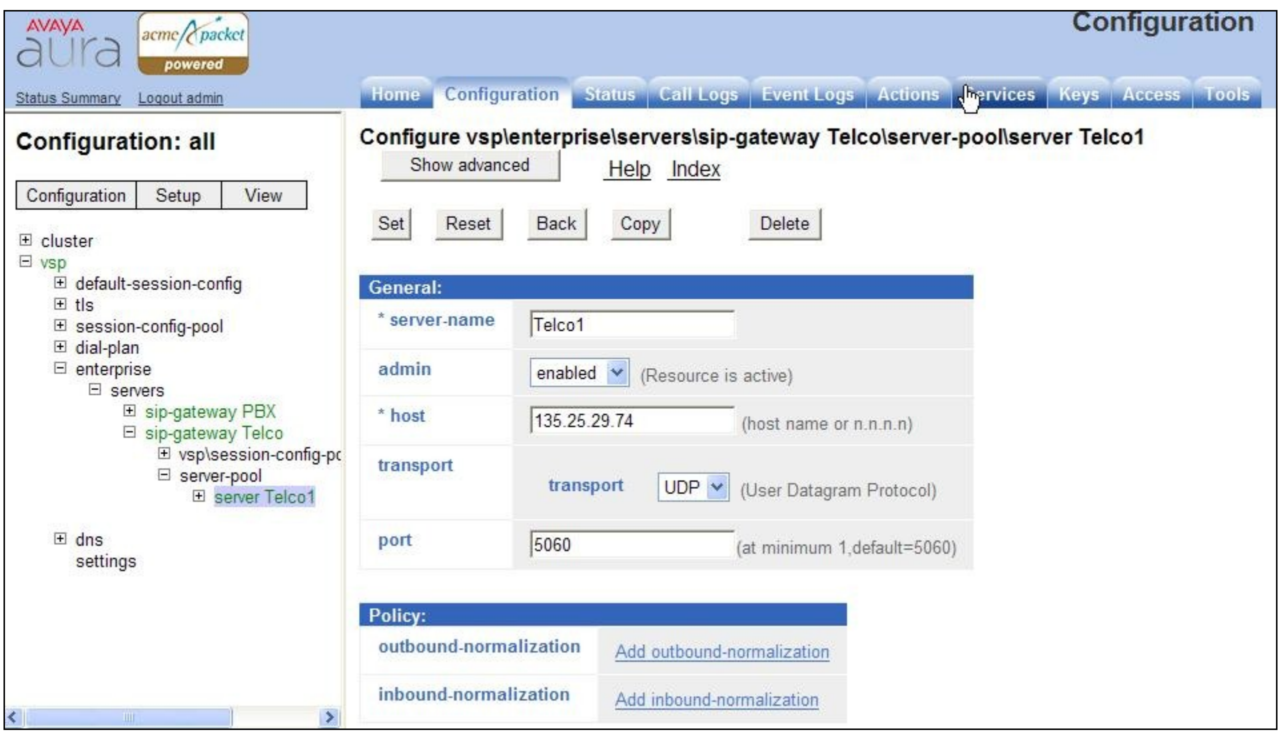
8.2.4. Configuring the SIP-Gateways

In the reference configuration, a sip-gateway was defined to AT&T (the IP Flexible Reach border element) and to the customer site (Session Manager). The AT&T gateway was defined as **Telco1** and customer gateway was defined as **PBX**.

8.2.4.1 Telco1

Step 1 - Go to **vsp → enterprise → servers** and any previously defined sip-gateways will be displayed. In the reference configuration sip-gateways **PBX** and **Telco1** were defined.

Step 2 - Click on **sip-gateway Telco → servers → server-pool → server Telco1** and the Telco1 sip-gateway configuration will be displayed.



Step 3 - Verify the following:

- **admin** state is **enabled**.
- **host** address is the IP address of the AT&T IP Flexible Reach border element (e.g. **135.25.29.74**).
- **transport** protocol is **UDP**.
- **port** is **5060**.

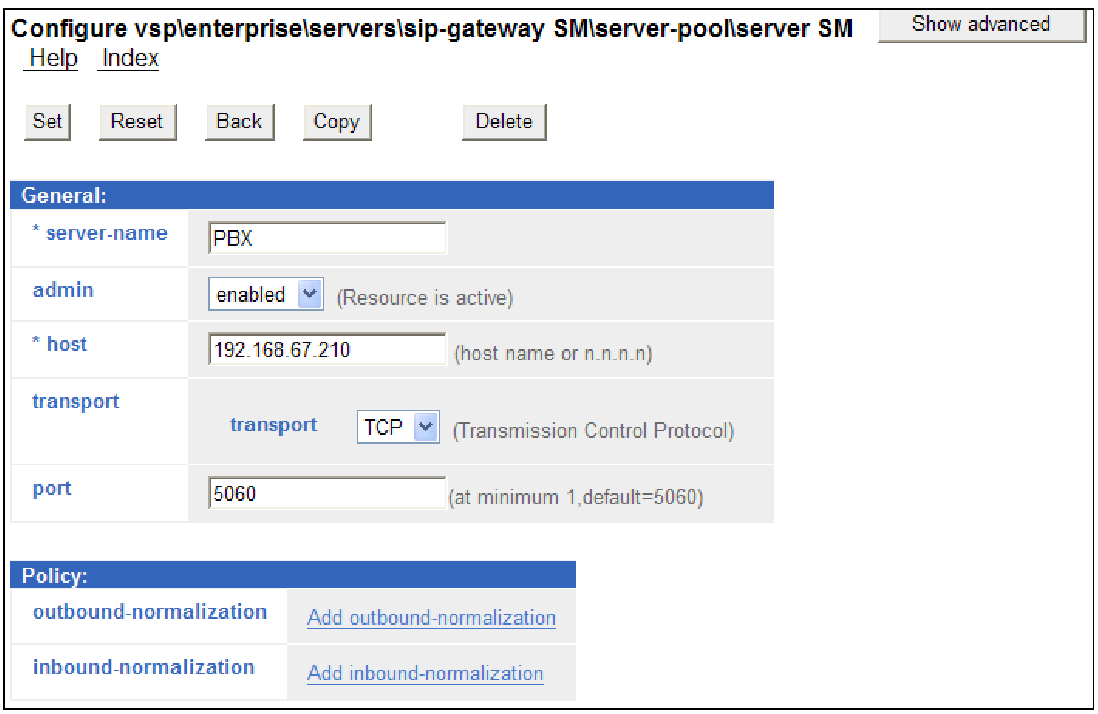
Step 4 - Click on the **Set** button to save any changes or **Back** if no changes are required.

Step 5 - Proceed to save and activate the configuration as described in **Section 8.3**.

8.2.4.2 PBX

Repeat the steps in **Section 8.2.4.1** and verify the following:

- **admin** state is **enabled**.
- **host** address is the IP address of Session Manager (e.g. **192.168.67.210**).
- **transport** protocol is **TCP**. Note that TCP was used in the reference configuration to facilitate protocol trace verification and troubleshooting. TLS may be used as well.
- **port** is **5060**.

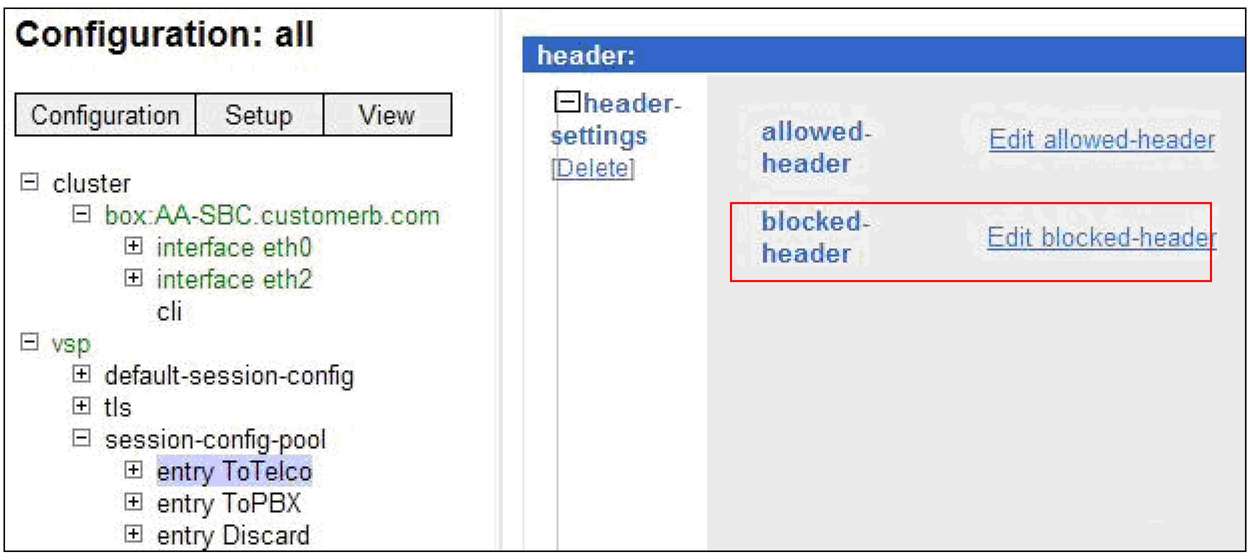


8.2.5. Stripping SIP Headers (Optional)

The Avaya SBC can be used to strip SIP headers that are not required or supported by AT&T. For headers that have relevance only within the enterprise, it may be desirable to prevent the header from being sent to the public SIP Service Provider. For example, Session Manager Release 6.1 may insert the **P-Location** headers. The following procedures may be used to strip such headers that AT&T does not process.

Undesired headers may be removed via the session-config-pool. For example, during installation, two session-config-pools were created, **To-Telco** and **To-PBX**. First the headers are removed session-config-pool **To-Telco**. This will remove the specified headers for calls sent by the customer location to AT&T.

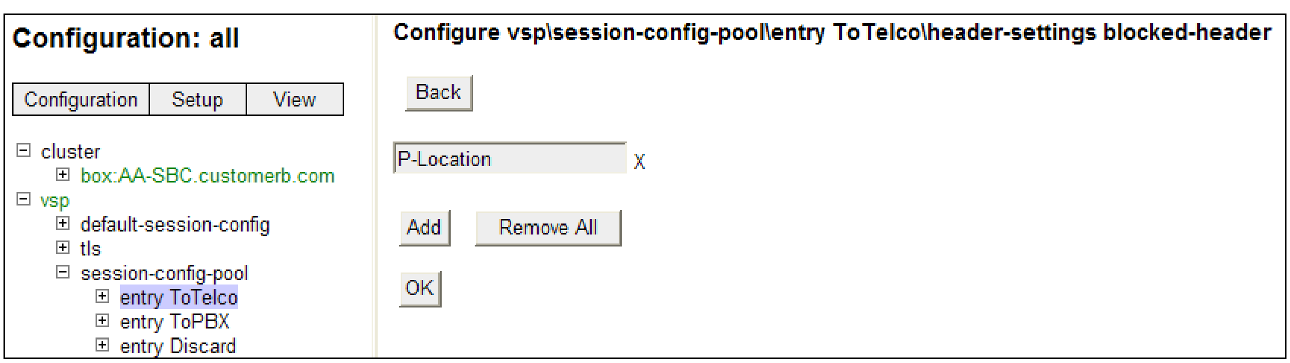
Step 1 - Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. In the resultant screen, click **Edit blocked-header.**



Step 2 – Enter **P-Location** into the selection box.

Step 3 – If additional headers need to be blocked, click on the **Add** button.

Step 4 – When all headers are entered, click on **OK**.

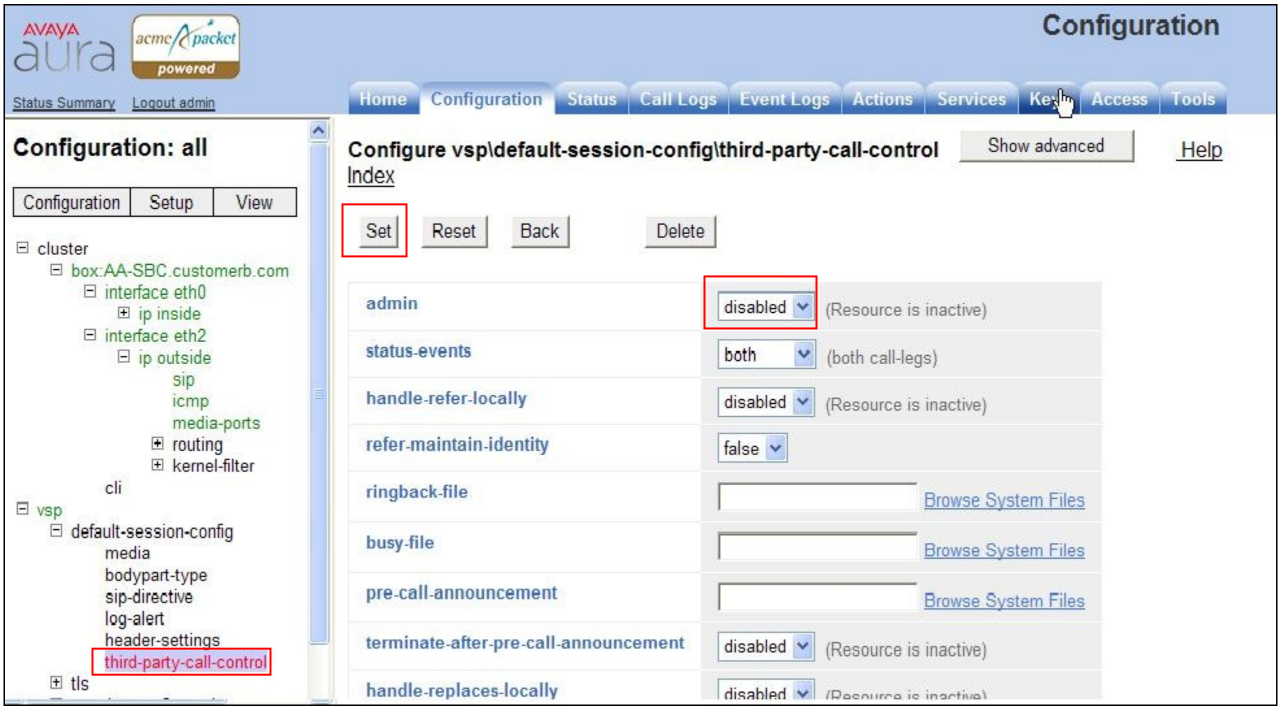


Step 5 - Proceed to save and activate the configuration as described in **Section 8.3**.

8.2.6. Disable Third Party Call Control

Step 1 - Navigate to **vsp → default-session-config → third-party-call-control**. To disable third-party-call-control, select **disabled** from the **admin** drop-down. Note - After disabling, the third-party-call-control link becomes red as shown below.

Step 2 - click **Set** as shown below.



Step 3 - Proceed to save and activate the configuration as described in **Section 8.3**.

8.2.7. SIP OPTIONS Messages for AT&T Network Status

In the reference configuration the Avaya SBC sent SIP OPTIONS messages to the AT&T IP Flexible Reach border element to verify the state of the network connection. The AT&T response to the OPTIONS is "405 Method Not Allowed". Although this appears to be an error, in fact the arrival of the message assures the Avaya SBC that the network connection is up.

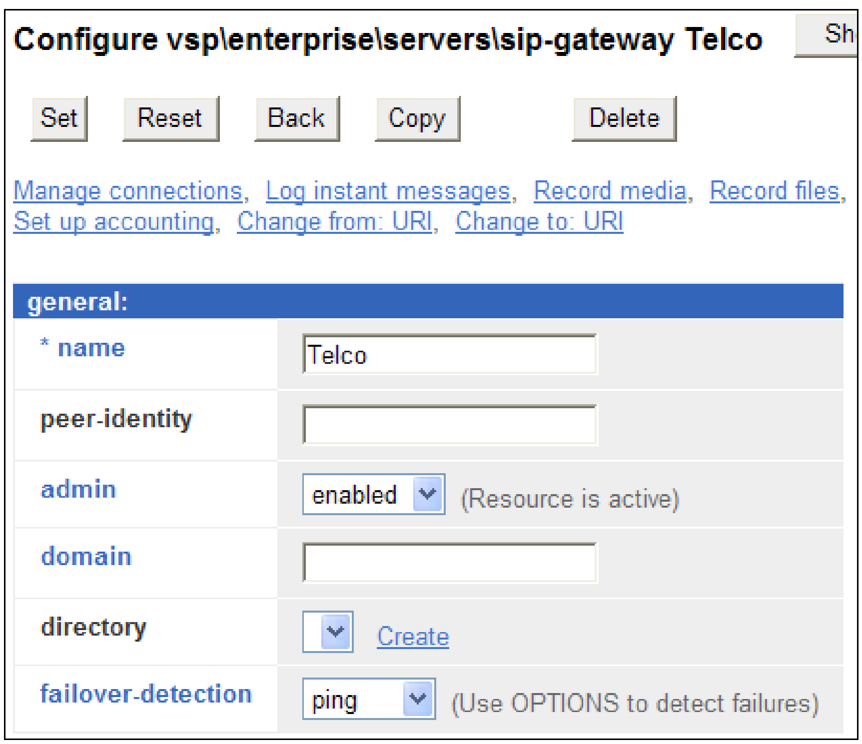
Step 1 - Navigate to **cluster → box:AvayaSBC → interface eth2 → ip outside**. Scroll down to, and click on, the **icmp** option.

Step 2 - Set the **admin** option to **enabled**.

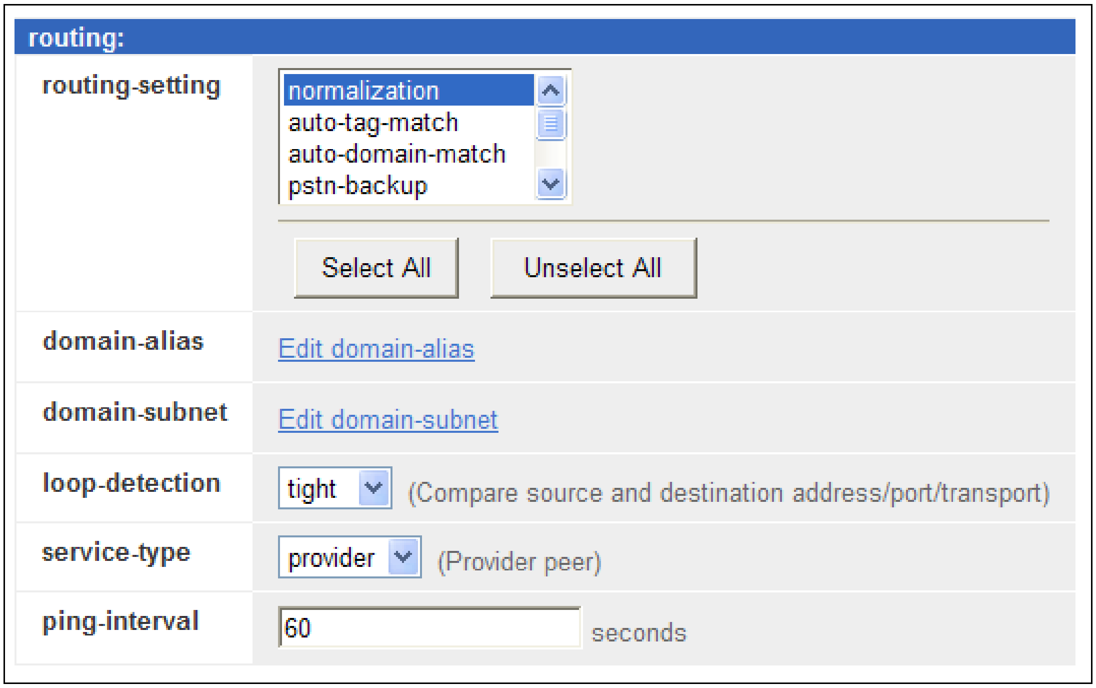
Step 3 - Scroll to the bottom of the screen and click **Set**.

Step 4 - Navigate to **vsp → enterprise → servers → sip-gateway Telco**. Click on the **Show Advanced** button at the top of the page (not shown) to display all the configurable parameters.

Step 5 – In the **general:** section of the form, set the **failover-detection** option to **ping** from the drop down menu.



Step 6 – Scroll down to the **routing**: section and set the **ping-interval** as desired (e.g. **60**).

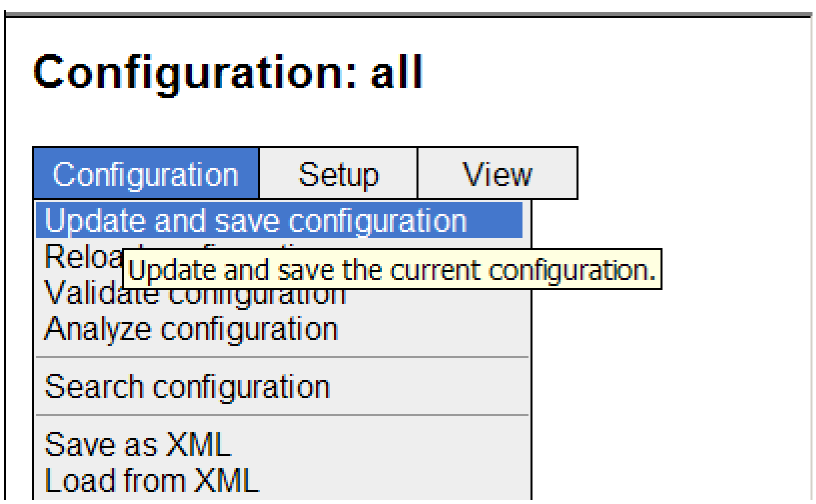


Step 7 - Scroll to the bottom of the screen and click **Set**.

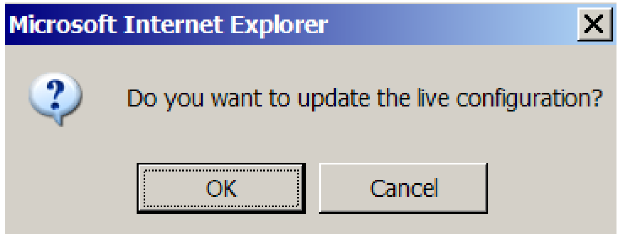
Step 8 - Proceed to save and activate the configuration as described in **Section 8.3**.

8.3. Saving and Activating Configuration Changes

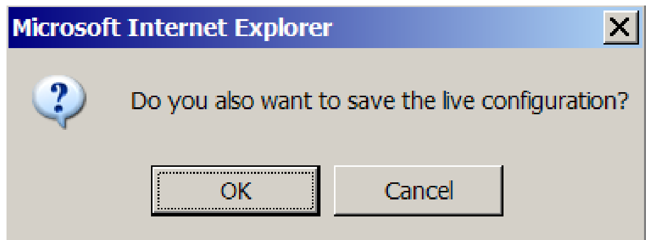
Step 1 - To save and activate configuration changes, select **Configuration → Update and save configuration** from the upper left hand side of the user interface, as shown below.



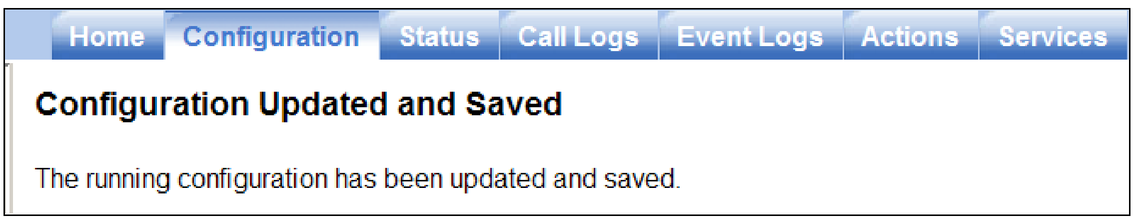
Step 2 - Click **OK** to update the live configuration.



Step 3 - Click **OK** to save the live configuration.



A screen that includes the following should appear.



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

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

1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where xxx is a trunk access code defined for the SIP trunk to AT&T (e.g. **122**). Note that Session Manager has previously converted the AT&T IP Flexible Reach DNIS to the Communication Manager extension 26103, before sending the INVITE to Communication Manager.

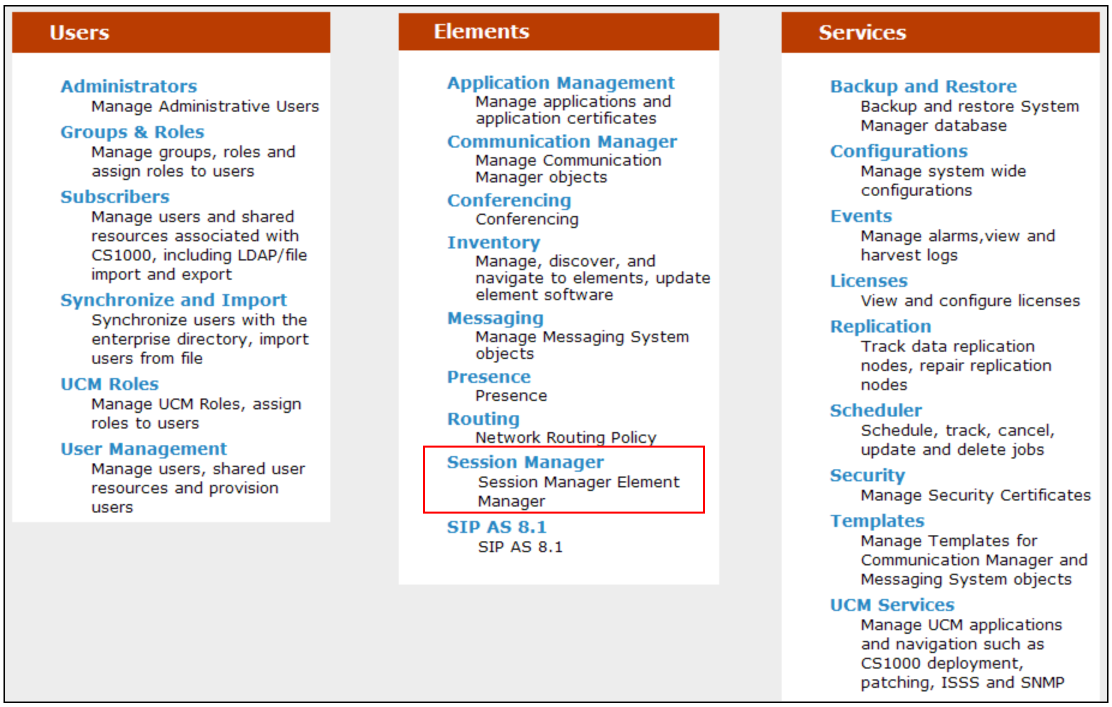
list trace tac 122

```
                              LIST TRACE

time          data

14:31:44 SIP<INVITE sip:26103@customera.com:5060  SIP/2.0
14:31:44     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:44     2-6f328733@135.25.29.74
14:31:44     active trunk-group 10 member 1    cid 0xb4
14:31:44 SIP>SIP/2.0 180 Ringing
14:31:44     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:44     2-6f328733@135.25.29.74
14:31:44     dial 26103
14:31:44     ring station      26103 cid 0xb4
14:31:44     G711MU ss:off ps:20
             rgn:1 [192.168.67.81]:31202
             rgn:1 [192.168.67.16]:16588
14:31:44     G729 ss:off ps:30
             rgn:2 [192.168.67.125]:28536
             rgn:1 [192.168.67.16]:16580
14:31:44     xoip options: fax:T38 modem:off tty:US  uid:0x5000a
             xoip ip: [192.168.67.16]:16580
14:31:45 SIP>SIP/2.0 200 OK
14:31:45     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45     2-6f328733@135.25.29.74
14:31:45     active station      26103 cid 0xb4
14:31:45 SIP<ACK sip:7323204302@192.168.67.14:5080;transport=tcp  SI
14:31:45 SIP<P/2.0
14:31:45     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45     2-6f328733@135.25.29.74
14:31:45 SIP>INVITE sip:7326712438@135.25.29.74:5060;maddr=192.168.6
14:31:45 SIP>7.125;transport=tcp SIP/2.0
14:31:45     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45     2-6f328733@135.25.29.74
14:31:45 SIP<SIP/2.0 100 Trying
14:31:45     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45     2-6f328733@135.25.29.74
14:31:45 SIP<SIP/2.0 200 OK
14:31:45     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45     2-6f328733@135.25.29.74
14:31:45 SIP>ACK sip:7326712438@135.25.29.74:5060;maddr=192.168.67.1
14:31:45 SIP>25;transport=tcp SIP/2.0
14:31:45     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45     2-6f328733@135.25.29.74
14:31:45     G729A ss:off ps:30
             rgn:2 [192.168.67.125]:28536
             rgn:1 [192.168.67.81]:31202
14:31:45     G729 ss:off ps:30
             rgn:1 [192.168.67.81]:31202
             rgn:2 [192.168.67.125]:28536
14:31:48 SIP>BYE sip:7326712438@135.25.29.74:5060;maddr=192.168.67.1
14:31:48 SIP>25;transport=tcp SIP/2.0
14:31:48     Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:48     2-6f328733@135.25.29.74
14:31:48     idle station      26103 cid 0xb4
```

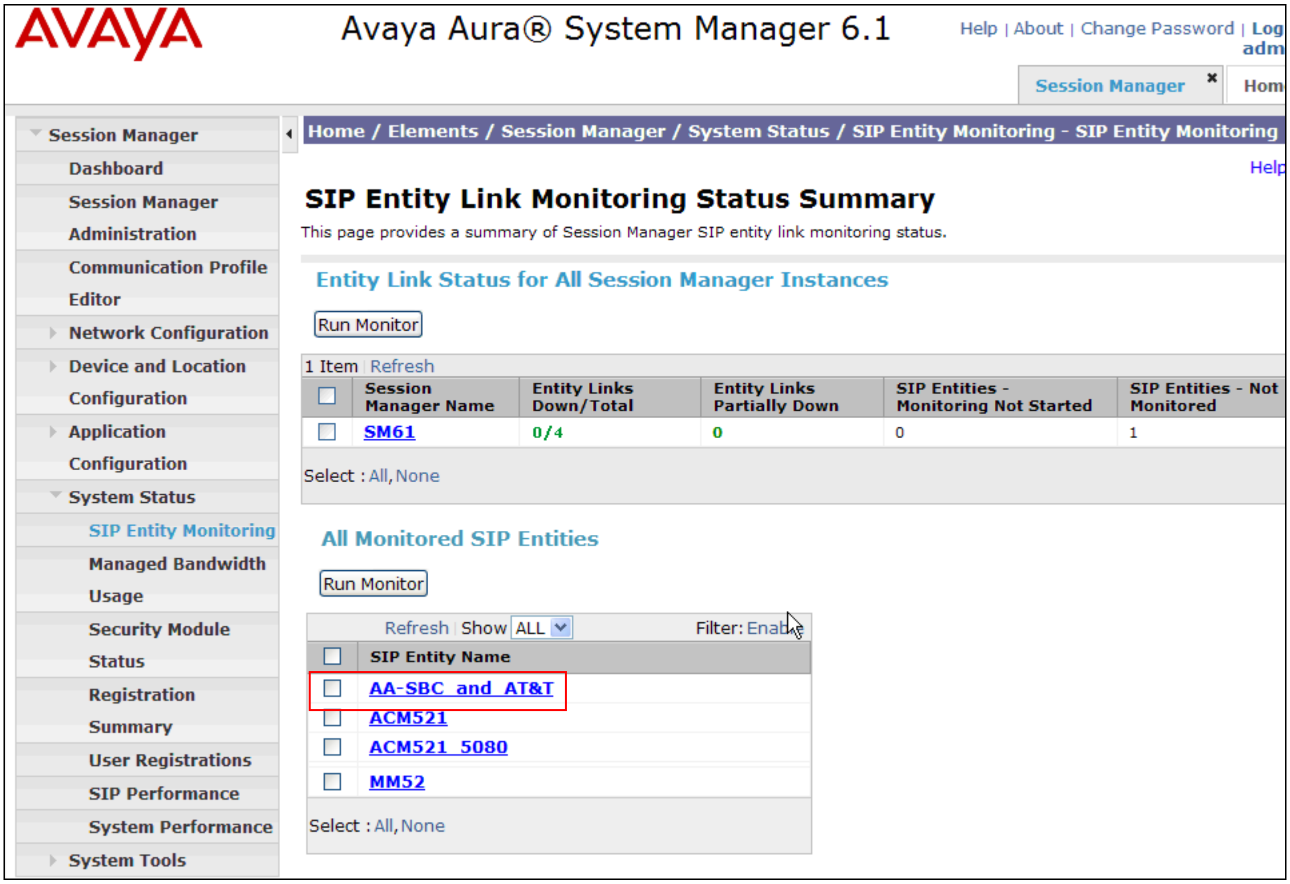
2. Similar Communication Manager commands are, ***list trace station***, ***list trace vdn***, and ***list trace vector***. Other useful commands are ***status trunk*** and ***status station***.

9.3. Avaya Aura® Session Manager

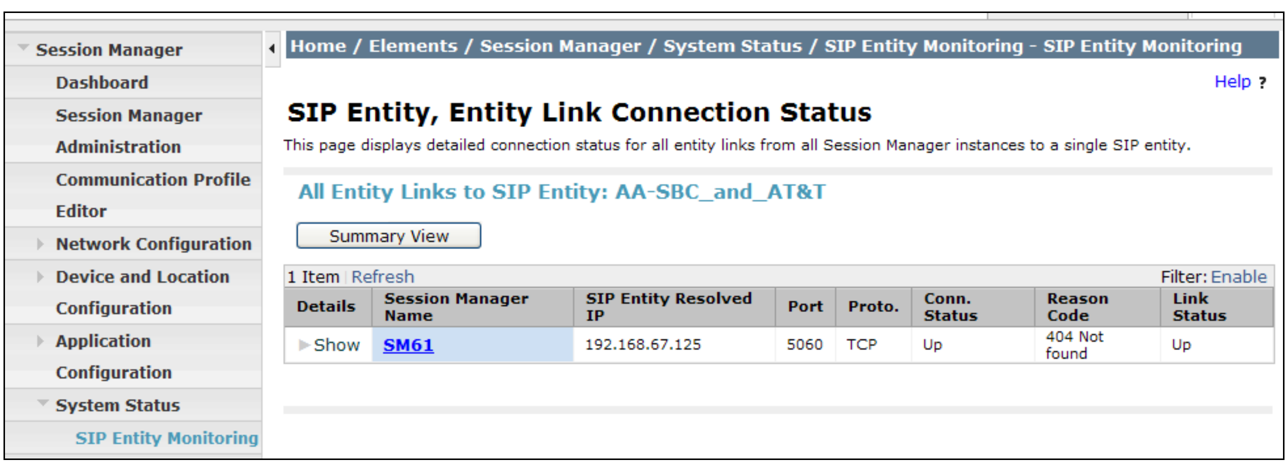
Step 1 - Access the System Manager GUI, using the URL **http://<ip-address>/**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Session Manager**.



Step 2 - Expand **System Status → SIP Entity Monitoring**.



Step – 3 From the list of monitored entities, select an entity of interest, such as **AA-SBC_and_AT&T**. Under normal operating conditions, the **Link Status** should be **Up** as shown in the example screen below. The **Reason Code** column indicates that the SBC has responded to SIP OPTIONS from Session Manager with a SIP 404 message (normal for the Avaya Aura® SBC toAT&T environment), which is sufficient for SIP Link Monitoring to consider the link up.



9.3.1. Call Routing Test

The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, expand **Elements → Session Manager → System Tools → Call Routing Test**. The following example shows an inbound call to Communication Manager from the AT&T IP Flexible Reach service. Note that the Request URI called number was 0000091049 and Session Manager will convert this to Communication Manager extension 26103 before routing the call to Communication Manager.

Step 1 – **Called Party URI** field = the information passed in the Request URI sent by the Avaya Aura® SBC (e.g. **0000091049@customera.com**)

Step 2 – **Calling Party Address** field = the IP address of the inside interface of the Avaya Aura® SBC (e.g. **192.168.67.125**).

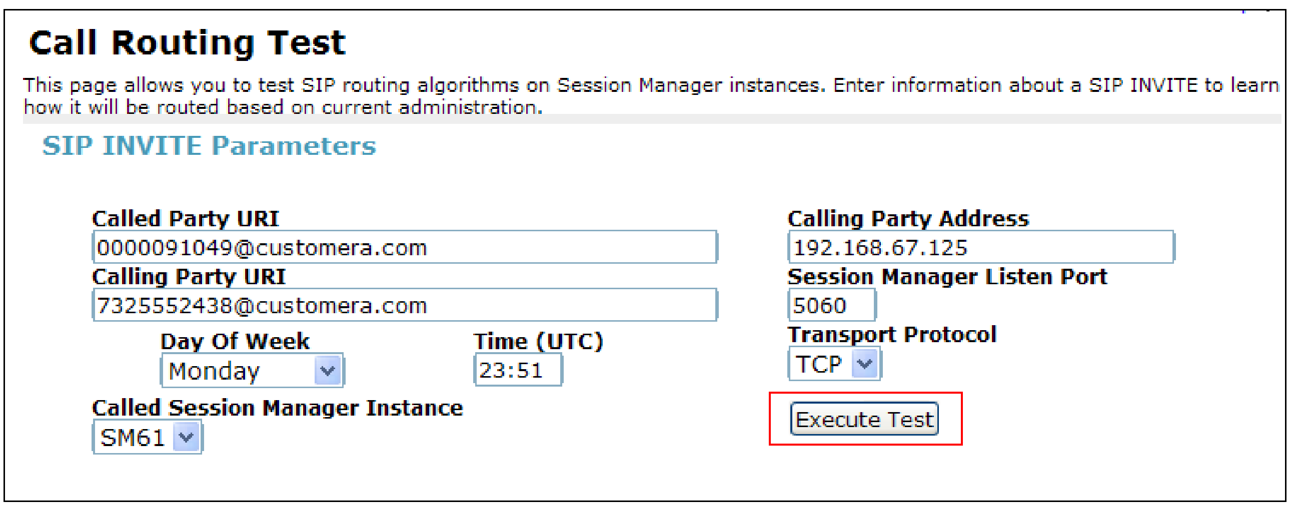
Step 3 – **Calling Party URI** field = The contents of the From header (e.g **7325552438@customera.com**).

Step 4 – **Session Manager Listening Port** = **5060** and **Transport protocol** = **TCP** (see the note in **Section 5.5** regarding the use of TCP).

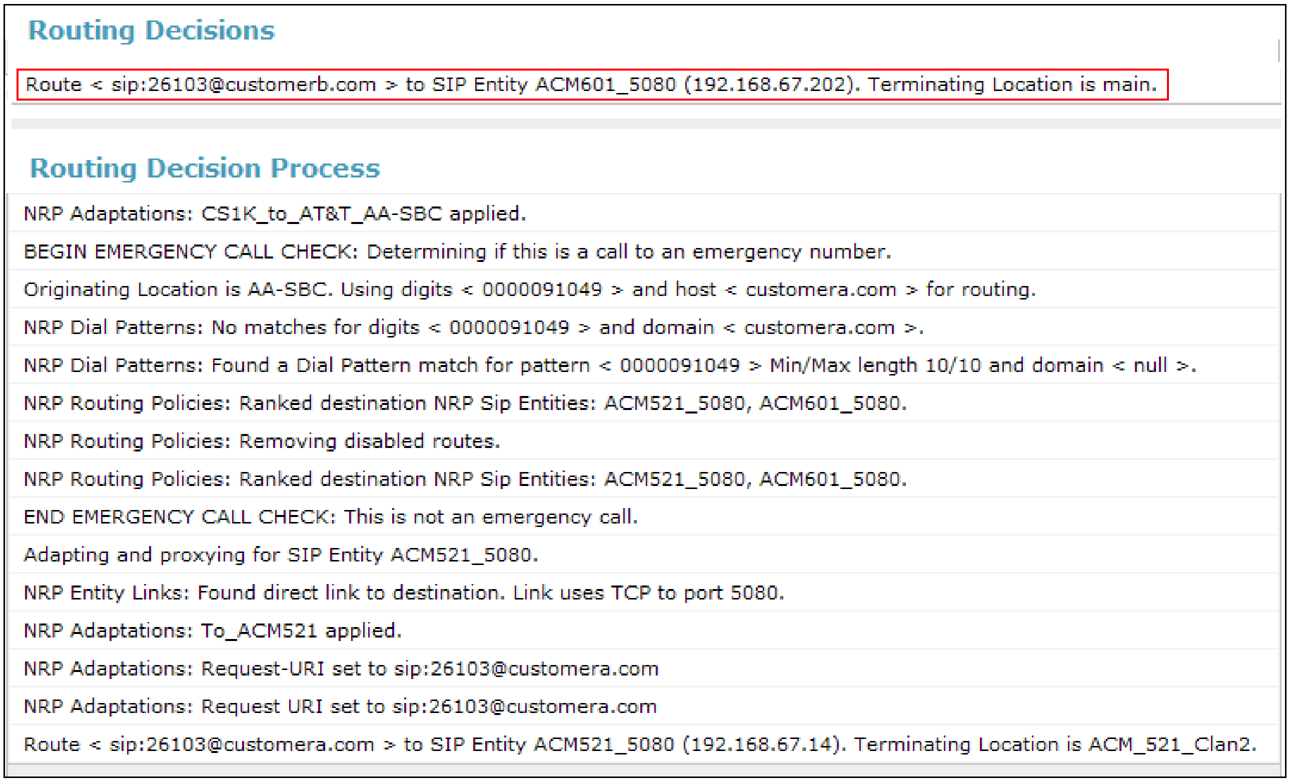
Step 5 – Populate the **Day of Week** and **Time (UTC)** fields, or let them default to current.

Step 6 – Verify that the **Called Session Manager** instance is correct (if multiple ones are defined).

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



The results of the test are shown below**.** The ultimate routing decision is displayed under the heading **Routing Decisions.** The example shows that a PSTN call to AT&T IP Flexible Reach service, delivering 0000091049 in the Request URI, is sent to Communication Manager extension **26103**. Further down, the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated).Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 5**.



Routing Decisions

Route < sip:26103@customerb.com > to SIP Entity ACM601_5080 (192.168.67.202). Terminating Location is main.

Routing Decision Process

NRP Adaptations: CS1K_to_AT&T_AA-SBC applied.

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Originating Location is AA-SBC. Using digits < 0000091049 > and host < customera.com > for routing.

NRP Dial Patterns: No matches for digits < 0000091049 > and domain < customera.com >.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 0000091049 > Min/Max length 10/10 and domain < null >.

NRP Routing Policies: Ranked destination NRP Sip Entities: ACM521_5080, ACM601_5080.

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP Sip Entities: ACM521_5080, ACM601_5080.

END EMERGENCY CALL CHECK: This is not an emergency call.

Adapting and proxying for SIP Entity ACM521_5080.

NRP Entity Links: Found direct link to destination. Link uses TCP to port 5080.

NRP Adaptations: To_ACM521 applied.

NRP Adaptations: Request-URI set to sip:26103@customera.com

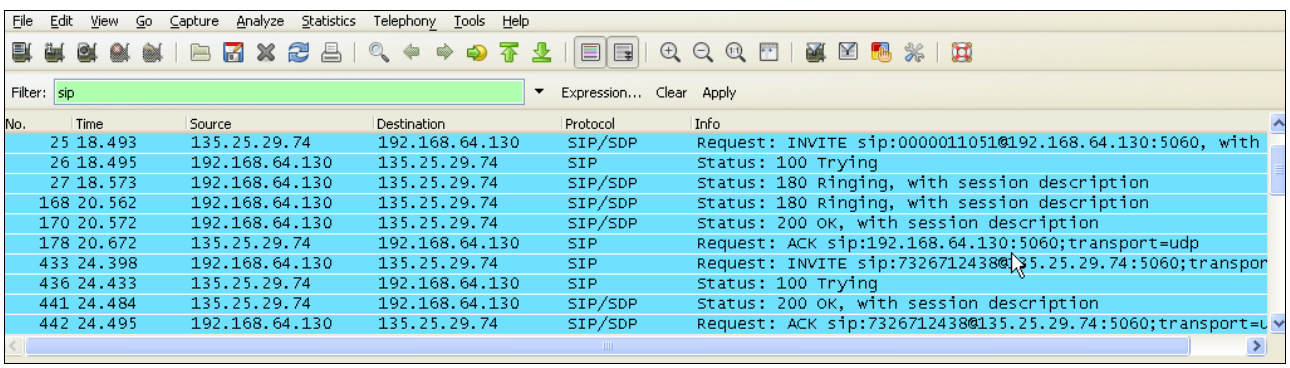
NRP Adaptations: Request URI set to sip:26103@customera.com

Route < sip:26103@customera.com > to SIP Entity ACM521_5080 (192.168.67.14). Terminating Location is ACM_521_Clan2.

9.4. Protocol Traces

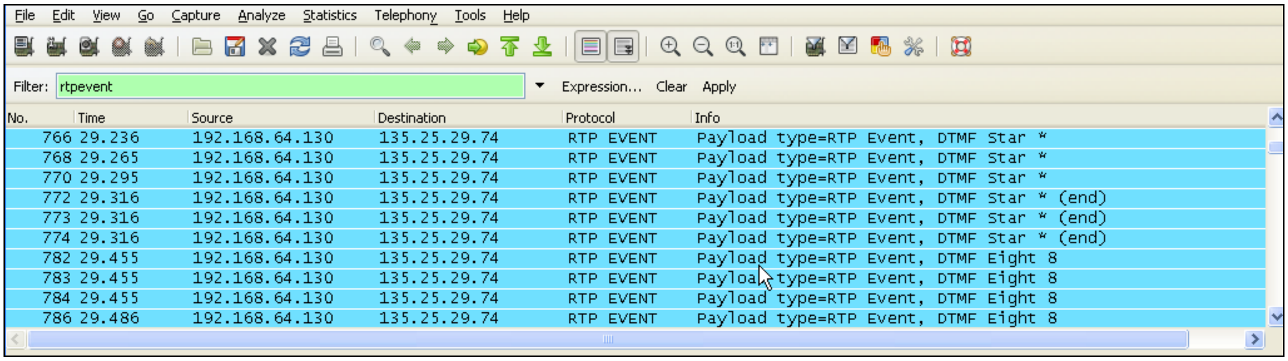
Using a SIP protocol analyzer (e.g. Wireshark), monitor the SIP traffic at the Avaya Aura® SBC public "outside" interface connection to the AT&T IP Flexible Reach service.

The following are examples of calls filtering on the SIP protocol.

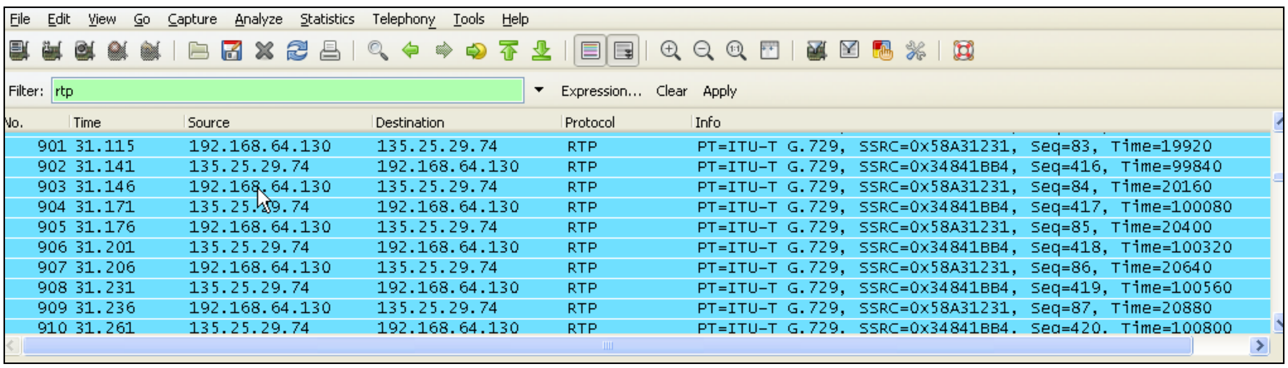


No.	Time	Source	Destination	Protocol	Info
25	18.493	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:0000011051@192.168.64.130:5060, with
26	18.495	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying
27	18.573	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
168	20.562	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
170	20.572	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description
178	20.672	135.25.29.74	192.168.64.130	SIP	Request: ACK sip:192.168.64.130:5060;transport=udp
433	24.398	192.168.64.130	135.25.29.74	SIP	Request: INVITE sip:7326712438@135.25.29.74:5060;transpor
436	24.433	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
441	24.484	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
442	24.495	192.168.64.130	135.25.29.74	SIP/SDP	Request: ACK sip:7326712438@135.25.29.74:5060;transport=u

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



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



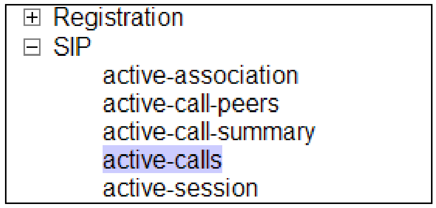
9.5. Avaya Aura® Session Border Controller Verification

This section contains verification steps that may be performed using the Avaya Aura® Session Border Controller.

9.5.1. Status Tab

Avaya SBC status information is available via the **Status** tab.

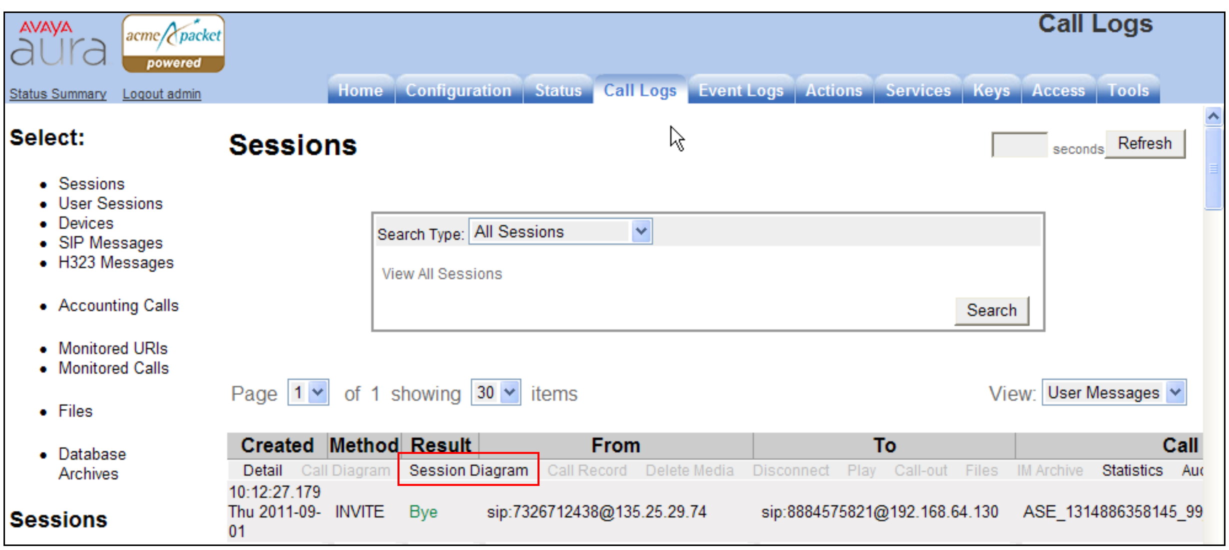
For example, there is a SIP heading on the left menu that can be expanded as shown below.



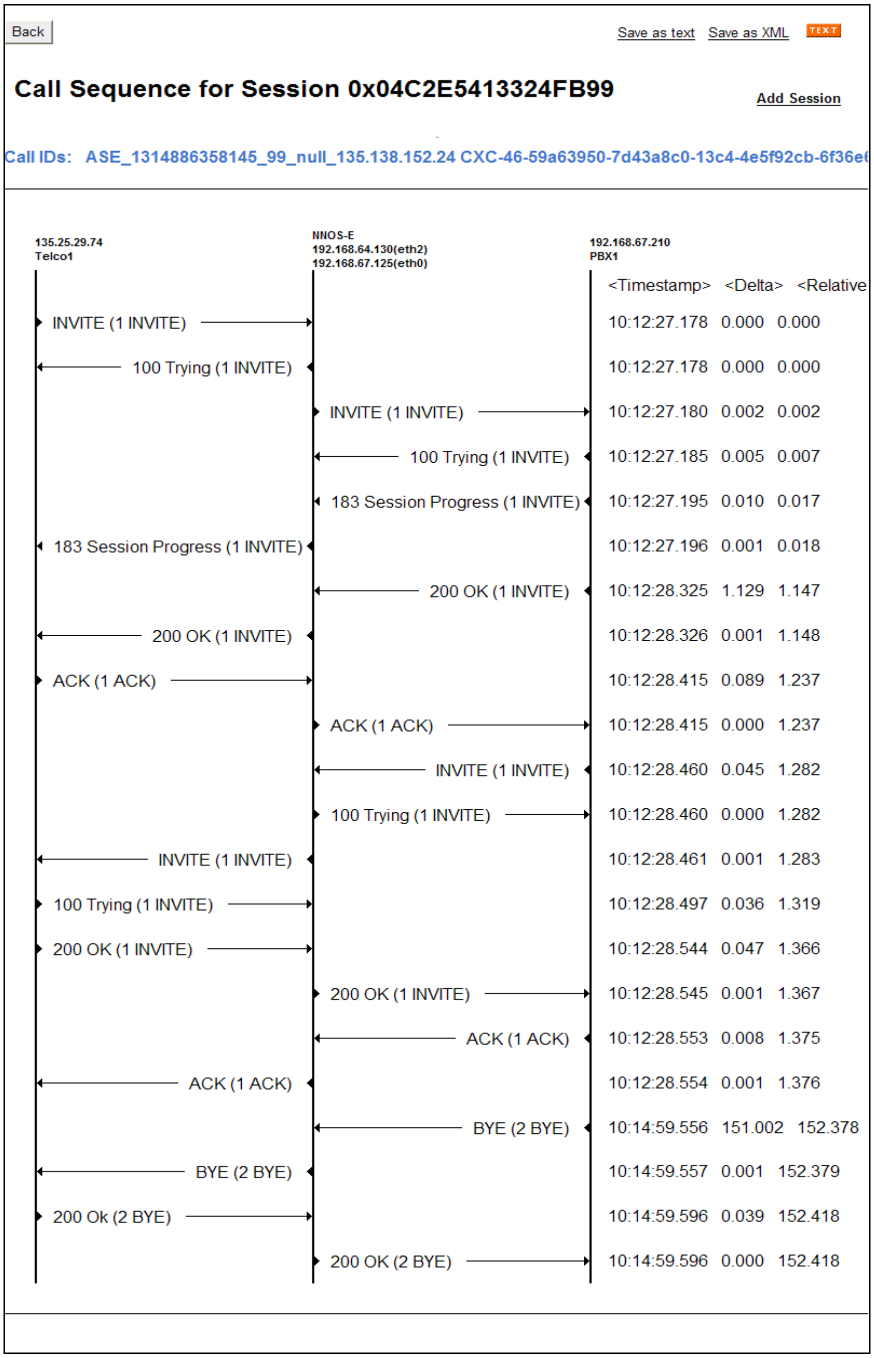
In the example below, **active-calls** was selected from the left, revealing details about an active inbound call from PSTN. Additional information about the call is available by moving the bottom scroll bar to the right (not shown).

9.5.2. Call Logs

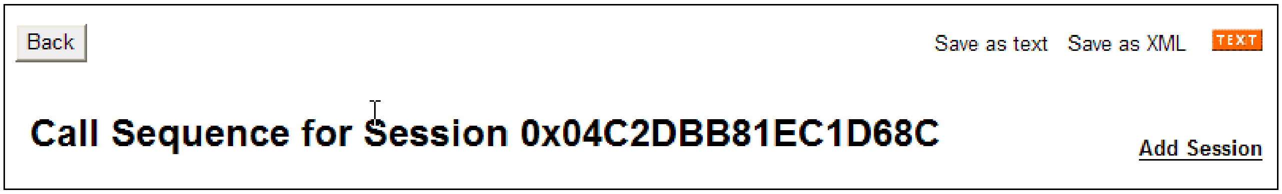
The **Call Logs** tab can provide useful diagnostic or troubleshooting information. In the following screen, the **SIP Messages** search capability can be observed. The following screen shows a portion of the **Call Logs** tab selected after an inbound call from PSTN.



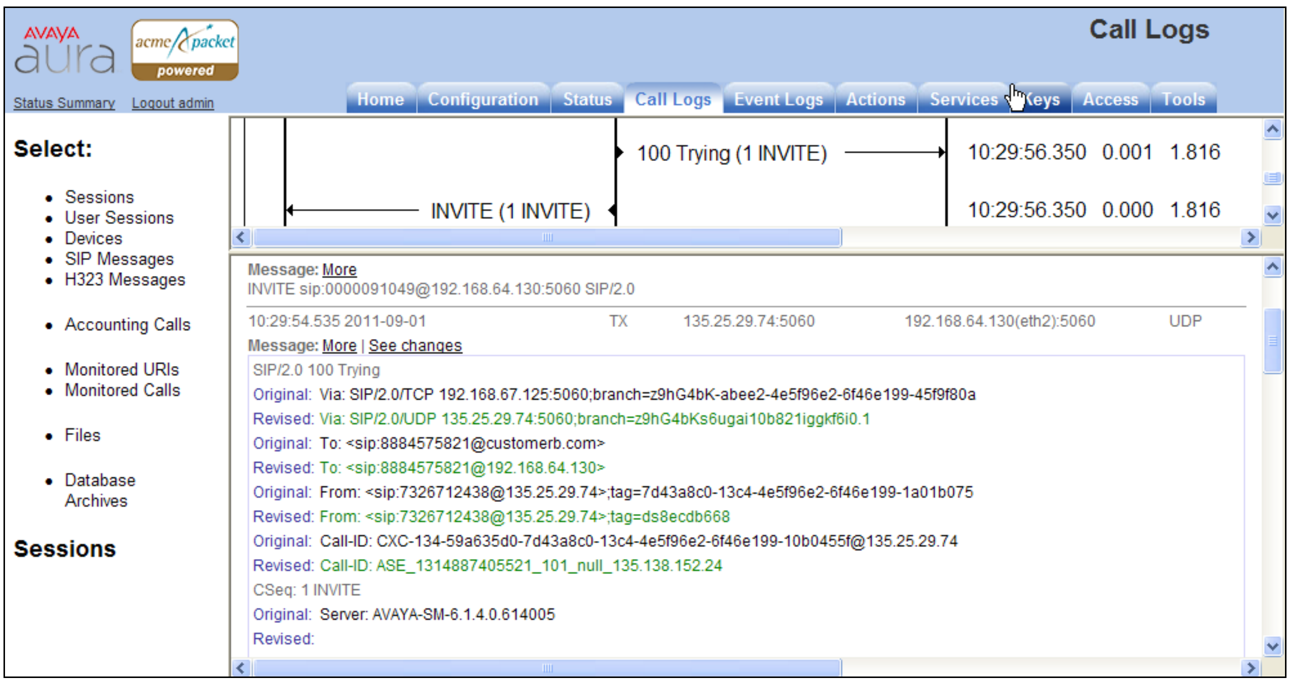
As shown below, to view a ladder diagram for the session, select the **Session Diagram** link. When the session window opens, expand the upper portion of the screen under the "Call Sequence" heading to display the ladder diagram. The following screen shows the ladder diagram for the inbound call. Note that the activity for both the inside private and outside public side of the SBC can be seen.



At the top right of the screen, the session may be saved as a text or XML file. If the session is saved as an XML file, using the **Save as XML** link, the xml file can be provided to support personnel that can open the session on another Avaya SBC for analysis.



The **Call Logs** tab also provides the capability to see modifications made to SIP headers by the SBC. Below the ladder diagram area is another screen section. Using the same Session Diagram as shown above, Scrolling down to the INVITE message sent by the SBC to AT&T. The **More** and **See changes** links was selected to expand the SIP message display and enable observation of the changes made by the SBC to the **Revised** message, as compared to the **Original** INVITE received from Session Manager.



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Avaya Aura® SBC can be configured to interoperate successfully with the AT&T IP Flexible Reach service using either AVPN or MIS-PNT transport. 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.

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

11. References

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

Avaya Aura® Session Manager/System Manager

[1] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Issue 4, Feb 2011
[2] Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Issue 2, November 2010
[3] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, Issue 3.1, March 2011
[4] Administering Avaya Aura® System Manager, Document Number 03-603324, June 2010

Avaya Aura® Communication Manager

[5] Administering Avaya Aura® Communication Manager, Issue 5.0, Release 5.2, May 2009, Document Number 03-300509
[6] Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent Selection (EAS) Reference, Release 5.2, April 2009, Document Number 07-600780

Avaya Modular Messaging

[7] Modular Messaging Multi-Site Guide Release 5.1, June 2009
[8] Modular Messaging Messaging Application Server (MAS) Administration Guide, July 2011

Avaya Aura® Session Border Controller

[9] Installing and Configuring Avaya Aura® Session Border Controller, Release 6.0.1, November 2010 available at: http://support.avaya.com/css/P8/documents/100134970
[10] Avaya Aura™ SBC System Administration Guide, V.6.0, 2010 available at: http://support.avaya.com/css/P8/documents/100111137

AT&T IP Flexible Reach Service Descriptions:

[11] AT&T IP Flexible Reach Service description - http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-toll-free-enterprise/

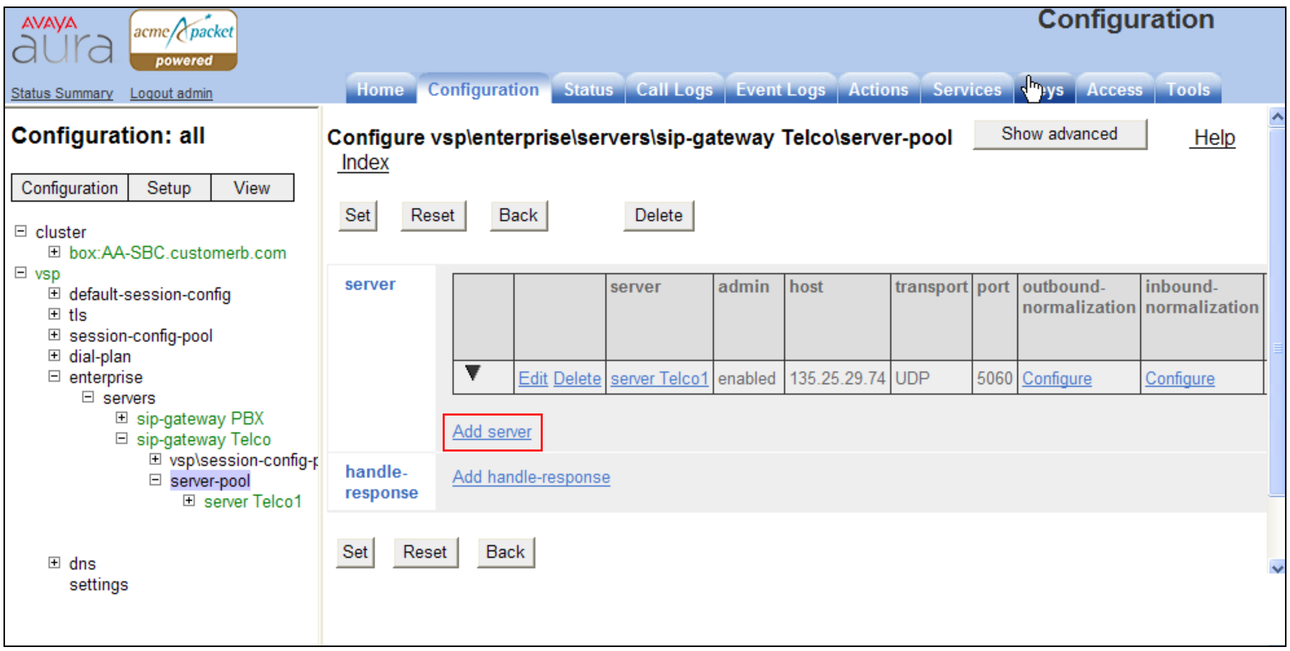
12. Addendum 1 – Avaya Aura® Session Border Controller Redundancy to Multiple AT&T Border Elements

AT&T may provide multiple network border elements for redundancy purposes. The Avaya Aura® SBC can be provisioned to support this redundant configuration.

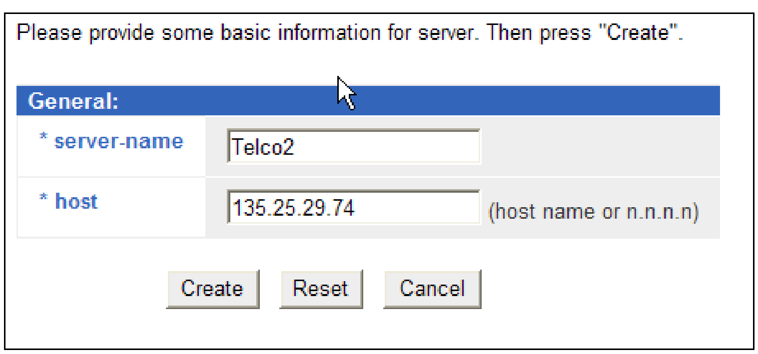
Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, and building on the sip gateway configuration shown in **Section 8.2.4.1**, the Avaya Aura® SBC is provisioned as follows.

Step 1 - Go to **vsp → enterprise → servers → sip-gatewayTelco → server-pool** and the previously defined sip-gateway **Telco1** defined in **Section 8.2.4.1** will be displayed.

Step 2 – Click on **Add server**.

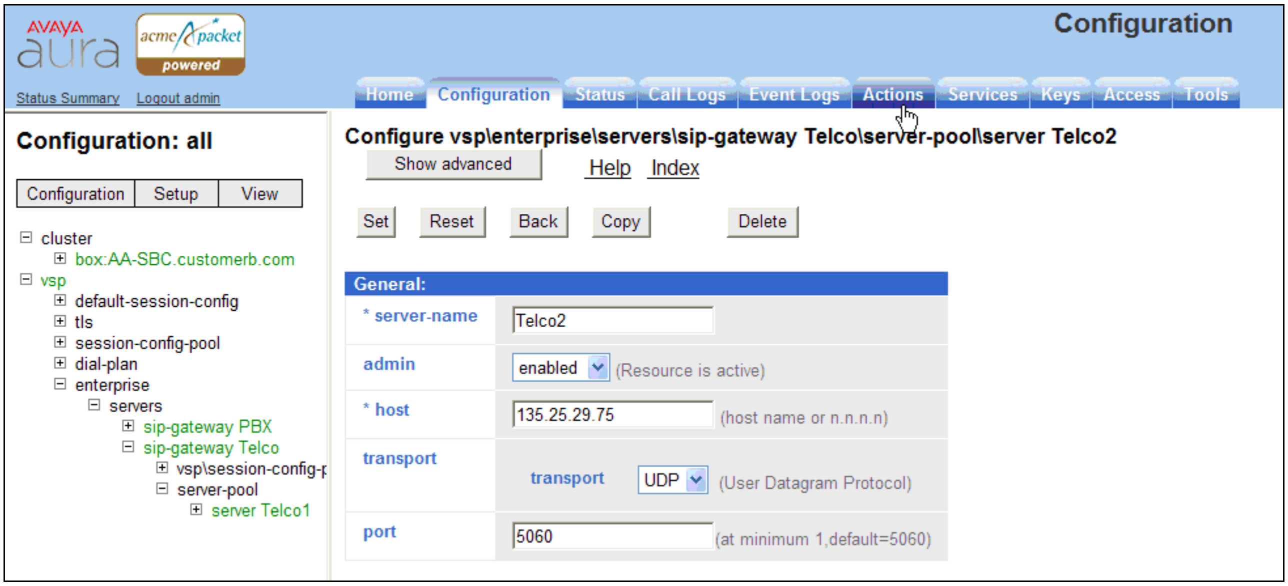


Step 3 – Enter a name in the server-name field (e.g **Telco2**) and enter the second AT&T border element IP address in the host field (e.g.**135.25.29.75**). Click on **Create**.

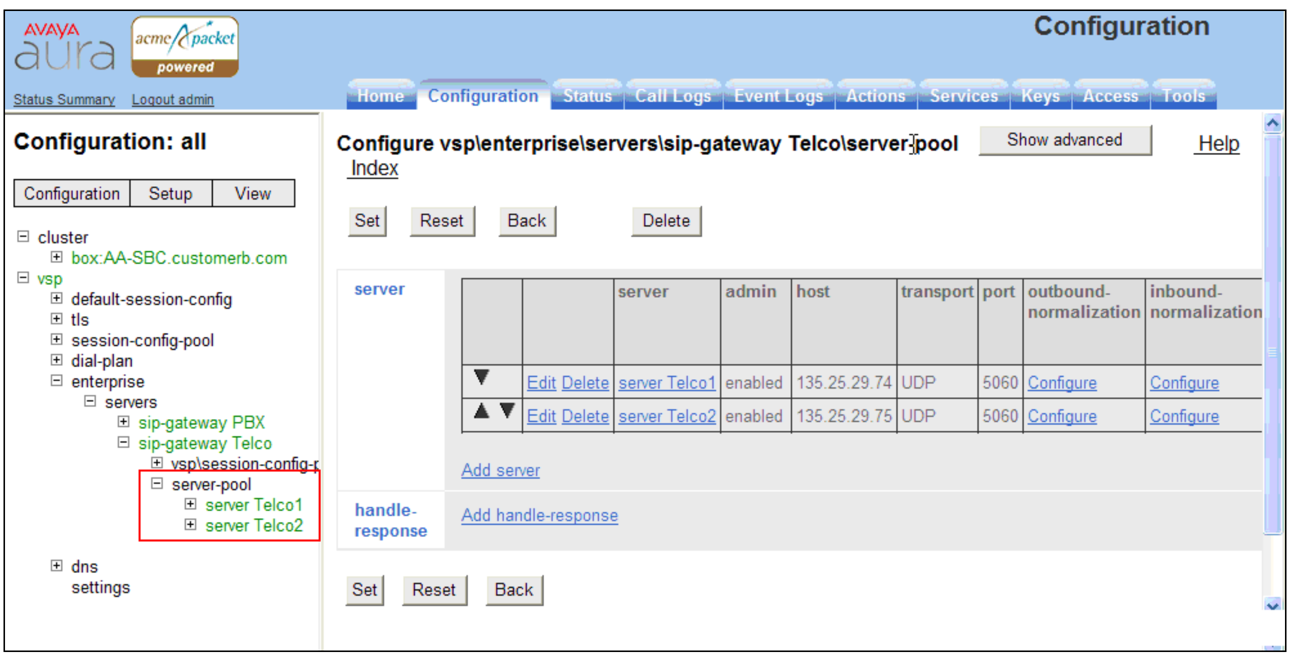


Step 4 – Enter the following:

- Admin is **enabled**.
- Transport protocol is **UDP**.
- Port is **5060**.



Step 5 - Click on the **Set** button to save. **Telco1**and **Telco2** will be displayed in the server-pool.



Step 5 - Proceed to save and activate the configuration as described in **Section 8.3**.

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