Avaya Solution & Interoperability Test Lab

Applications Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet Net-Net 6.2.0 with AT&T IP Toll Free 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 Acme Packet Net-Net (models 3800, 4250, or 4500) with the AT&T IP Toll Free 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 6.0.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Acme Packet Net-Net 6.2.0 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

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

<u>**TABLE OF CONTENTS**</u>

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Acme Packet Net-Net (models 3800, 4250, or 4500) with the AT&T IP Toll Free 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 6.0.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Acme Packet Net-Net 6.2.0 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT[1] transport.

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

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), Acme Packet Net-Net 3800 SBCs, and Avaya Modular Messaging.
- A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise was connected via AVPN transport.

2.1. Interoperability Compliance Testing

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

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

- SIP trunking.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.

[1] MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does support cRTP..

- PBX and AT&T IP Toll Free service features such as hold, resume, conference and transfer. Legacy Transfer Connect and Alternate Destination Routing features were also tested.

2.2. Test Results

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

- Inbound AT&T IP Toll Free service calls to Communication Manager telephones and VDNs/Vectors.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones via the AT&T Toll Free service.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- T.38 fax calls between Communication Manager the AT&T IP Toll Free service/PSTN G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833 between Communication Manager and the AT&T IP Toll Free service/PSTN automated access systems.
- Inbound AT&T IP Toll Free service calls to Communication Manager that 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. If Communication Manager receives an SDP offer with multiple codecs, where at least two of the codecs are supported in the codec set provisioned on Communication Manager, then Communication Manager selects a codec according to the priority order specified in the Communication Manager codec set, not the priority order specified in the SDP offer. For example, if the AT&T IP Toll Free service offers G.711, G.729A, and G.729B in that order, but the Avaya Aura® Communication Manager codec set contains G.729B, G729A, and G.711 in that order, then Avaya Aura® Communication Manager selects G.729A, not G.711. The practical resolution is to provision the Communication Manager codec set to match the expected codec priority order in AT&T IP Toll Free SDP offers.
2. G.726 codec is not supported between Communication Manager and the AT&T IP Toll Free service.
3. G.711 faxing is not supported between Communication Manager and the AT&T IP Toll Free 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. Avaya SIP telephones currently send RTP with a fixed 20ms packet interval. This could cause reduced customer busy-hour bandwidth for AVPN based transport. A fix for this issue is currently being developed by Avaya.

2.3. Support

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

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

3. Reference Configuration

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

- Session Manager 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 communications services for a particular enterprise site. In the reference configuration, Communication Manager runs on an Avaya S8800 Server in a Processor Ethernet (Procr) 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 G450 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.

- Avaya "desk" phones are represented with Avaya A175, 46x0, 96x0, and 96x1 Series IP Telephones running H.323 or SIP software, Avaya 6211 Series Analog Telephones, as well as Avaya PC based softphone: Avaya one-X® Agent. Note – All agent phones are H.323.

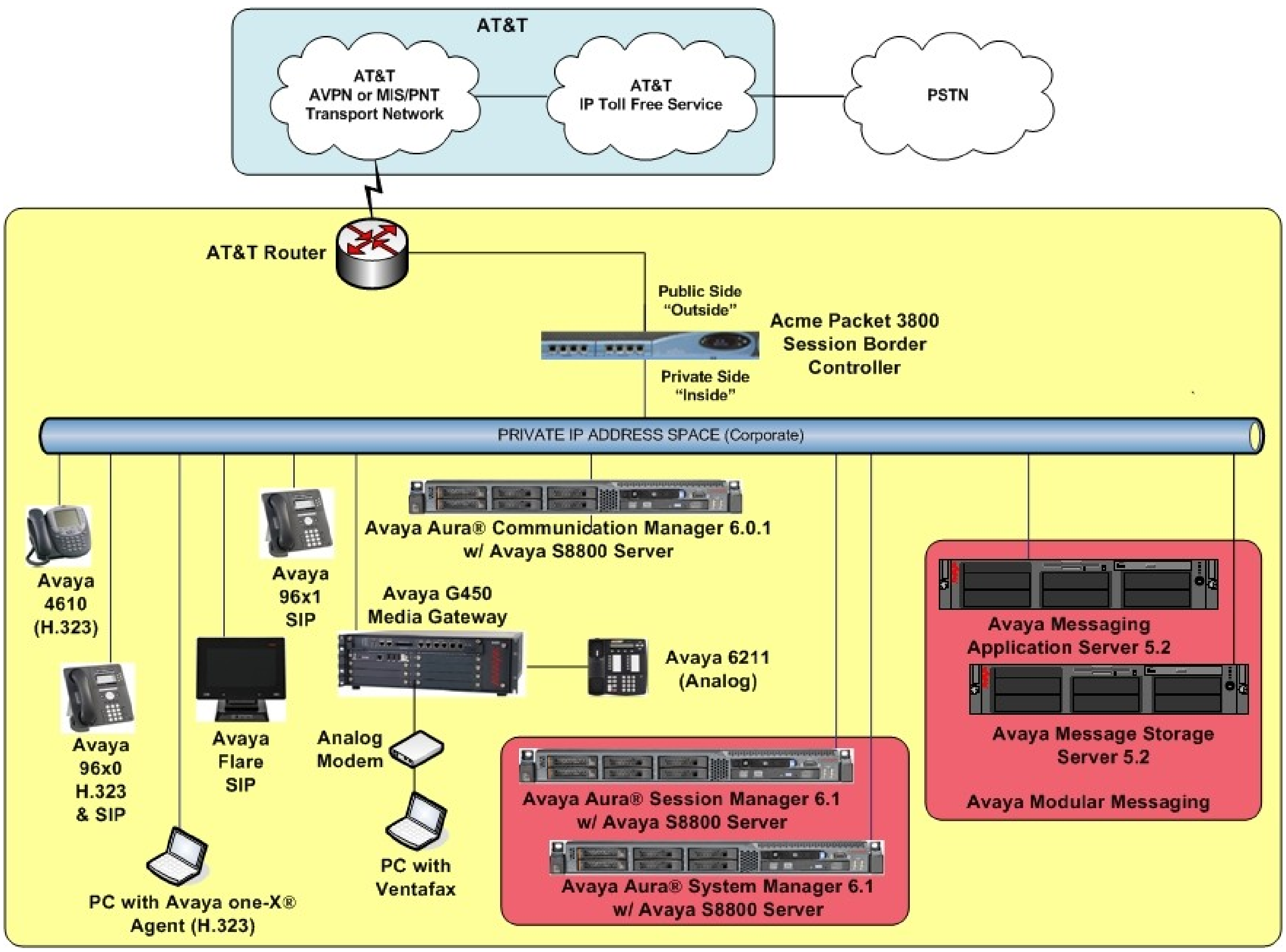
- The Acme Packet Net-Net 3800[2] provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T

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

IP Toll Free service and the enterprise internal network[3]. UDP transport protocol is used between the Acme Packet Net-Net SD and the AT&T IP Toll Free service.

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

- Inbound calls were placed from PSTN via the AT&T IP Toll Free service, through the Acme Packet Net-Net to the Session Manager which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate agent/phone or fax extension. The H.323 phones on the enterprise side registered to the Communication Manager Procr. The SIP phones registered to Session Manager.



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

Figure 1: Reference configuration

3.1. Illustrative Configuration Information

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

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

Component	Illustrative Value in these Application Notes
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	
Procr IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	40xxx = H323 and Analog 41xxx = SIP
Avaya CPE local dial plan	4xxxx
Voice Messaging Pilot Extension	46000
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	1723114xxxx
Acme Packet SBC	
IP Address of "Outside" (Public) Interface (connected to AT&T Access Router/IP Toll Free Service)	192.168.64.130 (active)
IP Address of "Inside" (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.130 (active)
AT&T IP Toll Free Service	
Border Element IP Address	135.25.29.74
AT&T Access router interface (to Acme outside)	192.168.64.254
AT&T Access Router NAT address (Acme outside address)	135.16.170.55

Table 1: Illustrative Values Used in these Application Notes

3.2. Call Flows

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

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

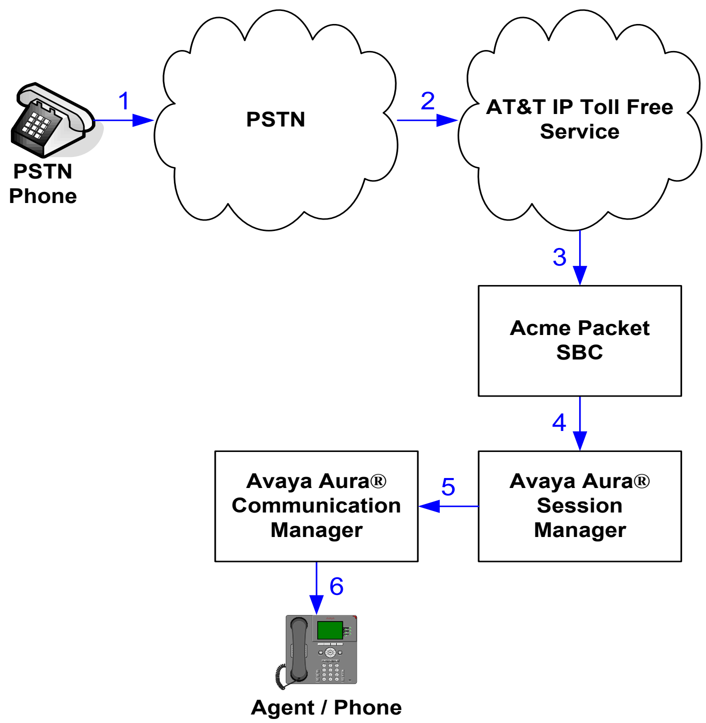


Figure 2: Inbound AT&T IP Toll Free Service Call to VDN / Agent / Phone

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

1. Same as the **Steps 1-5** and **Step 6b** from the first call scenario.
2. The called Communication Manager agent or phone does not answer the call, and the call covers to the agent's or 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 Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Modular Messaging. Modular Messaging answers the call and connects the caller to the called agent's or phone's voice mailbox. Note that the call[5] continues to go through Communication Manager.

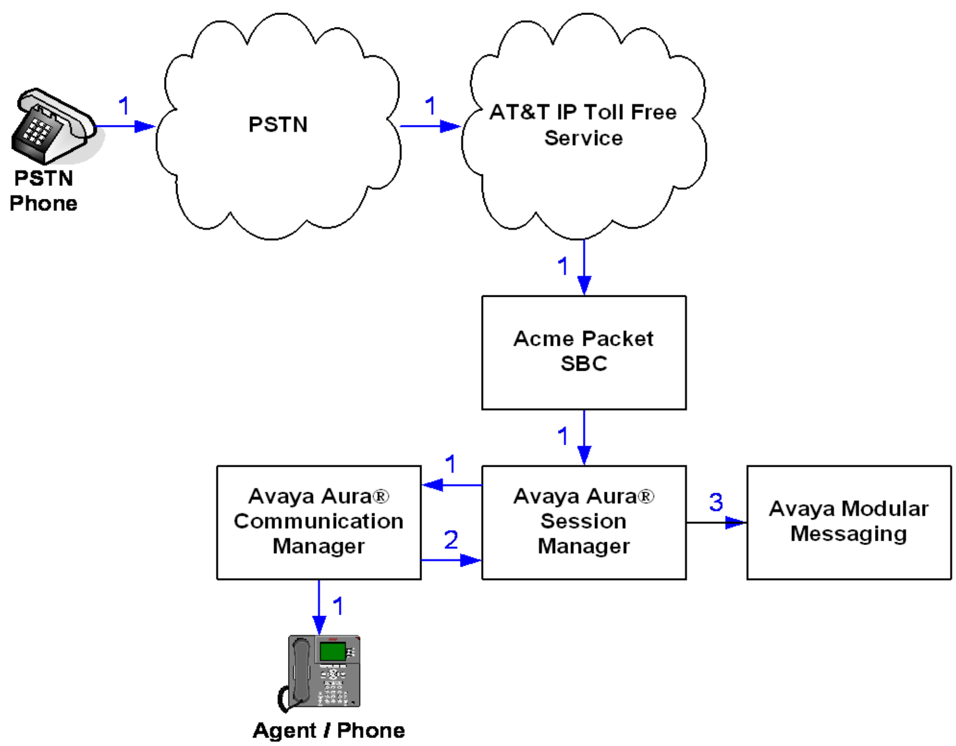


Figure 3: Inbound AT&T IP Toll Free Service Call to Agent / Phone Covered to Avaya Modular Messaging

[4] Communication Manager places a call to Modular Messaging, and then connects the inbound caller to Modular Messaging. SIP redirect methods, e.g., 302, are not used.
[5] The SIP signaling path still goes through Communication Manager. In addition, since the inbound call and Modular Messaging use different codecs (G.729 and G.711, respectively), Communication Manager performs the transcoding, and thus the RTP media path also goes through Communication Manager.

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 SP4 (6.1.0.0.7345-6.1.5.112 update 6.1.8.1.1455) System Platform 6.0.3.1.3
Avaya S8800 Server	Avaya Aura® Session Manager 6.1 (6.1.4.0.614005)
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0.1 SP3 (00.1.510.1-19009) System Platform 6.0.3.1.3
Avaya G450 Media Gateway	31.19.2
MM711 Analog card	HW31 FW094
Avaya 9630 IP Telephone	H.323 Version S3.110b (ha96xxua3_11.bin) SIP Version 2.6.4 (SIP96xx_2_6_4_0.bin)
Avaya 9621 IP Telephone	SIP Version 6.0.1 (S96x1_SALBR6_0_1_V452)
Avaya A175 Desktop Video Device (SIP telephone function)	SIP Version 1.0.3 (SIP_A175_1_0_3_000011)
Avaya one-X® Agent	2.5.00467.09
Avaya 4610SW IP Telephone	H323 Version 2.9.1 (a10d01b2_9_1.bin)
Avaya 6211 Analog phone	-
Avaya Modular Messaging (MAS and MSS) on Avaya S3500 Servers	Release 5.2 – SP5 with Patch 1 (9.0.350.5019)
Fax device	Ventafax Home Version 6.1.59.144
Acme Packet Net-Net 3800	SCX6.2.0m6p3
AT&T IP Toll Free Service using AVPN/MIS-PNT transport service connection	VNI 20 & VNI 21

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] and [2] 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 Acme SBC. In addition, provisioning for calls to Modular Messaging are described.

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

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

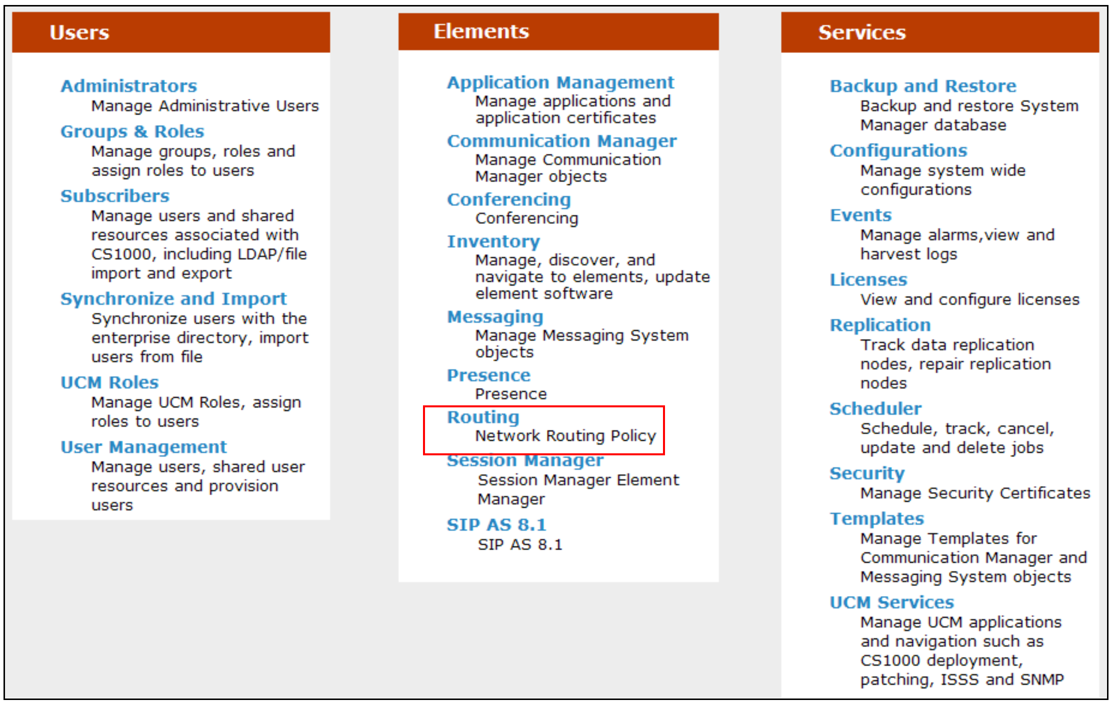
The following administration activities will be described:

- Define SIP Domain
- Define Locations for Communication Manager, the Acme SBC, and Modular Messaging.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Acme SBC, and Modular Messaging.
- Define SIP Entities corresponding to Communication Manager, the Acme 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 Acme SBC, and the SIP trunk between Session manager and Modular Messaging.

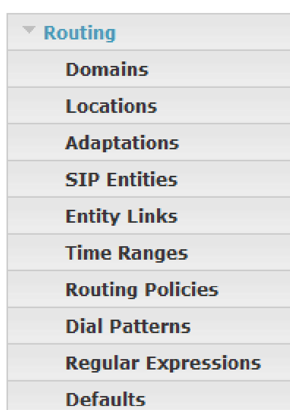
- Define Routing Policies associated with the Communication Manager, the Acme SBC and Modular Messaging.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

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

In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, a Release 6.1 **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.

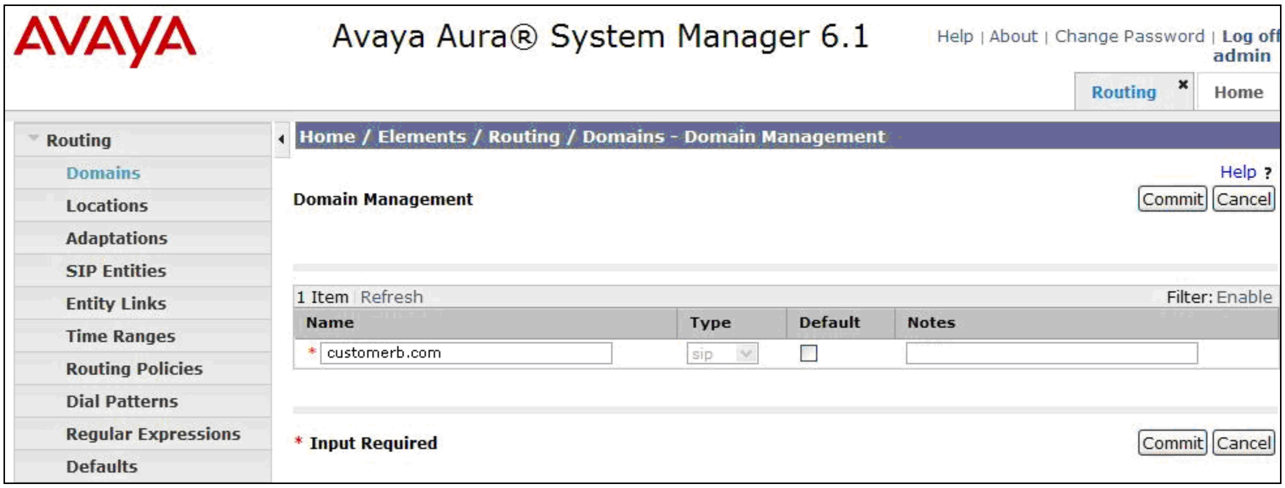


5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration domain "customerb.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, **customerb.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. 192.168.10.x for all devices on a particular subnet), or individual devices (e.g. 192.168.10.10 for a device's IP address). In the reference configuration Communication Manager, Modular Messaging, and the Avaya SBC were each defined as individual Locations.

5.2.1. Location for Avaya Aura® Communication Manager

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

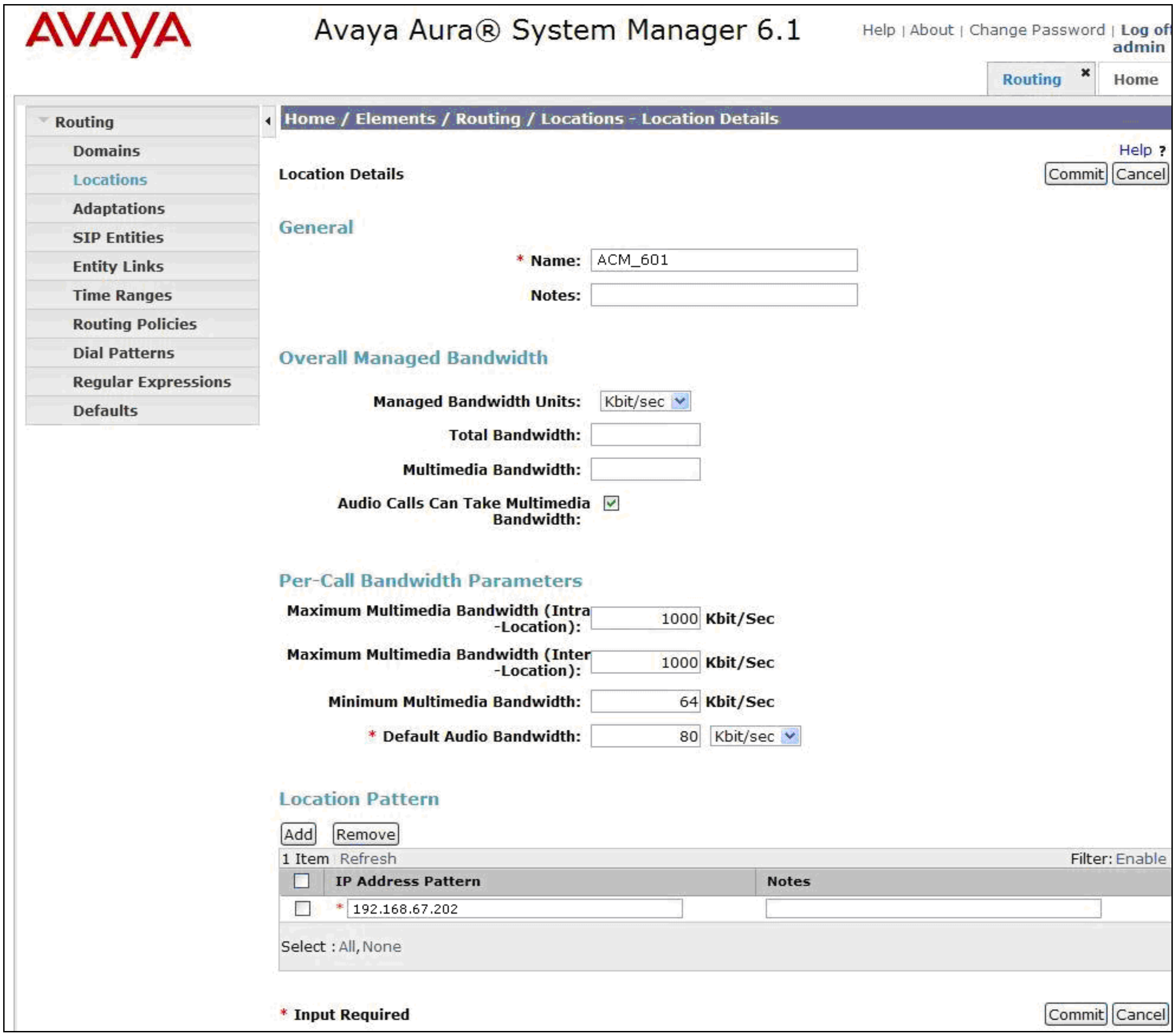
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

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. **192.168.67.202**).
- **Notes** Add a brief description. [Optional]

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

The screen below shows the screen for the Location defined for Communication Manager.



5.2.2. Location for the Acme Session Border Controller

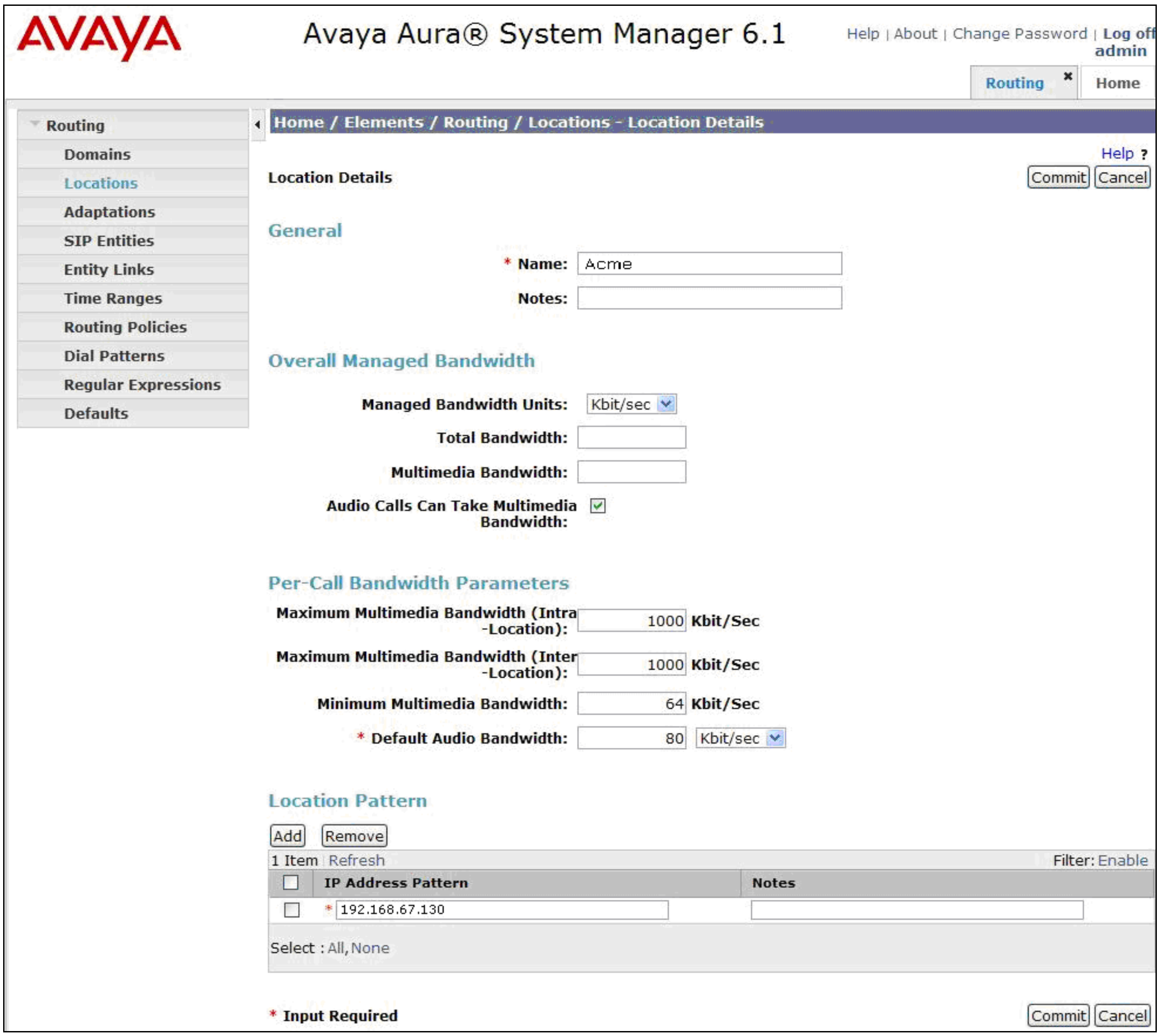
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **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 Acme SBC location (e.g. **192.168.67.130**).
- **Notes:** Add a brief description. [Optional]

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



5.2.3. Location for Modular Messaging

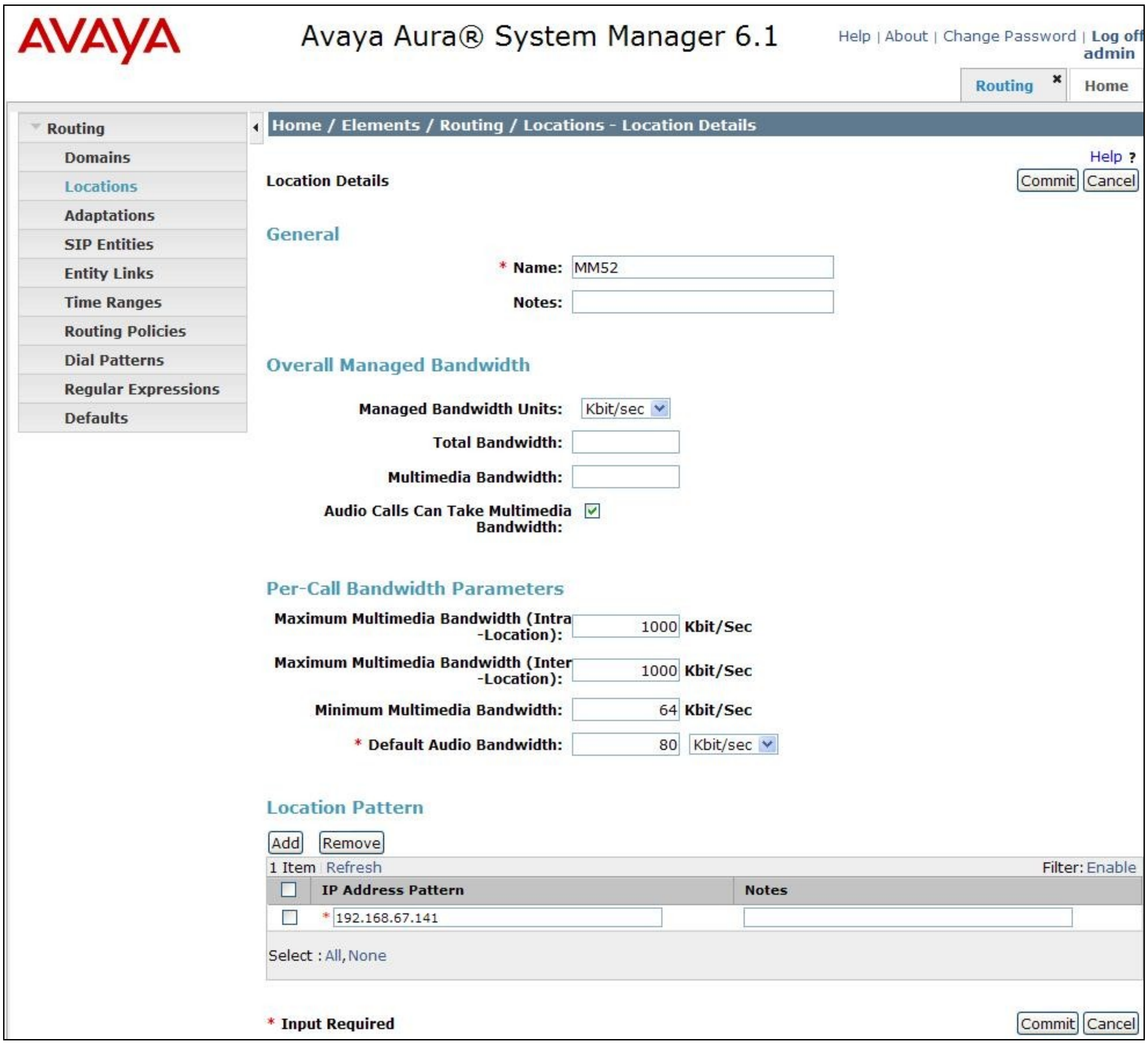
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **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 itself was defined to this location. Note that a specific location like those described in the previous sections could have been used as well.

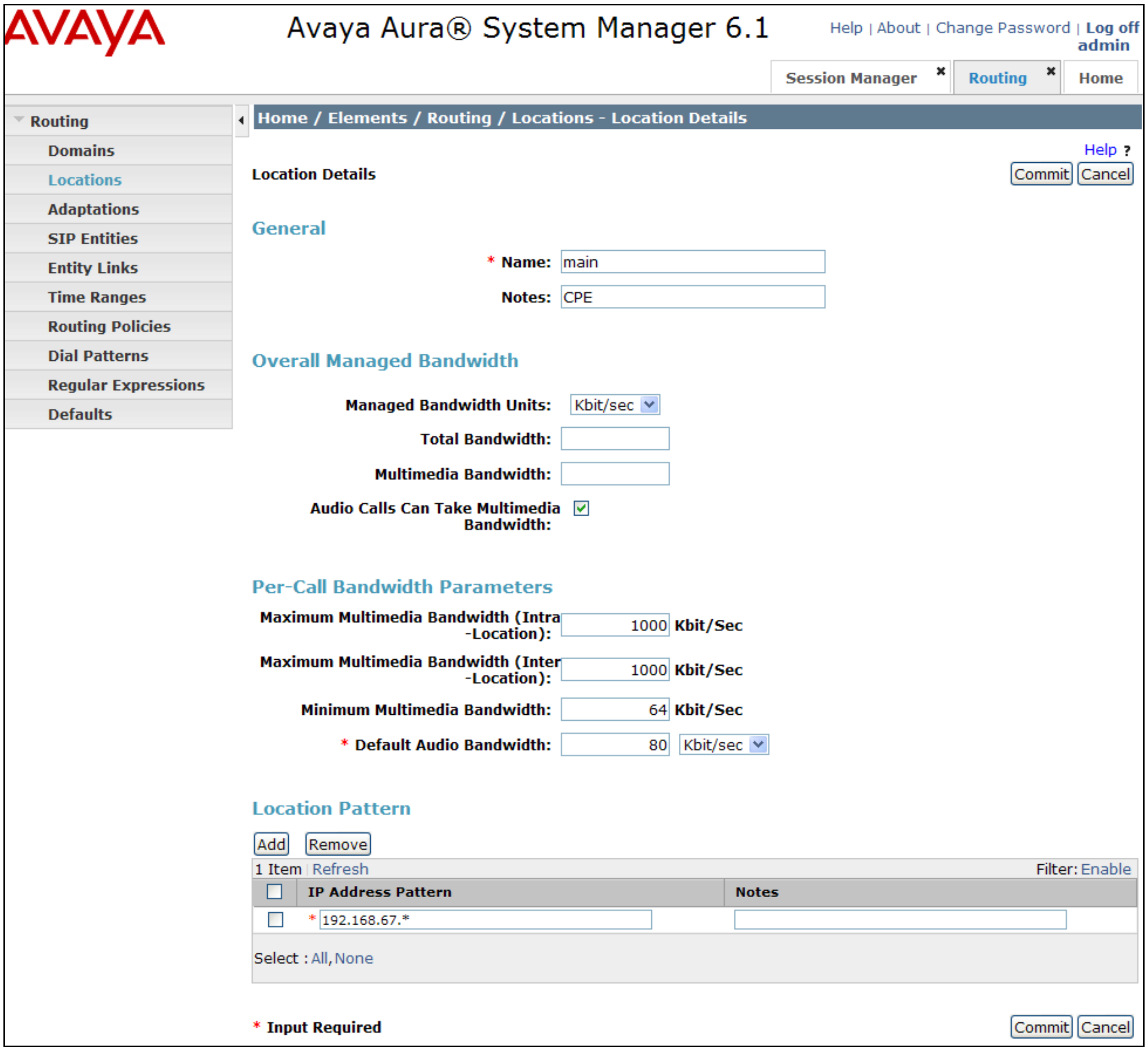
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **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 convert SIP headers in messages sent by AT&T to Communication Manager, and between Communication Manager and Modular Messaging. In the reference configuration the following adaptations were used.

In the reference configuration, Adaptations are administered for the following purposes:

- Calls from AT&T (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager.
  - The IP address of Session Manager (192.168.67.210) is replaced with the Avaya CPE SIP domain **customerb.com** in the Request URI.
  - The AT&T called number digit strings in the Request URI are replaced with their associated Communication Manager extensions/VDNs.
- Calls to/from Modular Messaging (**Section 5.3.2**) - Modification of SIP messages sent to and received from Avaya Modular Messaging.

- From MM (5.3.2) – Modular Messaging 11 digit mailbox numbers are converted to the associated Communication Manager 5 digit extensions.

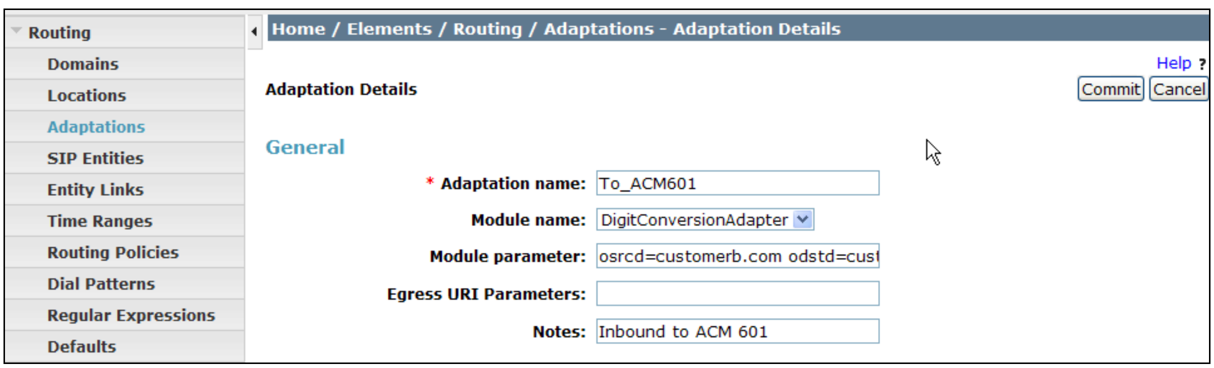
5.3.1. Adaptation for calls to Avaya Aura® Communication Manager

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

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

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

- A descriptive **Name**, (e.g. **To_ACM601**).
- Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select “<click to add module>” and enter **DigitConversionAdapter**).
- In the **Module parameter** field enter **odstd=customerb.com osrcd=customerb.com.** The odstd parameter will replace the IP address of Session Manager (*192.168.67.210*) with *customerb.com* in the *inbound* Request URI, and the osrcd parameter will replace the AT&T border element IP address (*135.25.29.74*) with *customerb.com* in the PAI header.



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

- Example 1: 0000001049 is a digit string sent in the Request URI by AT&T Toll Free service that is associated with Communication Manager extension 40002.
  - Enter **0000001049** in the **Matching Pattern** column.
  - Enter **10** in the **Min/Max** columns.
  - Enter **10** in the **Delete Digits** column.
  - Enter **40002** string in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

- Example 2: 1723114xxxx is the format of the mailboxes sent by Avaya Modular messaging in Notify messages (MWI) to Communication Manager. These mailboxes must be converted to their associated Communication Manager extensions by deleting the first six digits.
  - Enter **1723114** in the **Matching Pattern** column.
  - Enter **11** in the **Min/Max** columns.
  - Enter **6** in the **Delete Digits** column.
  - Leave the **Insert Digits** column blank.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

Step 4 – Repeat **Step 3** for all additional AT&T DID numbers and/.or Modular Messaging mailboxes.

Step 5 - Click on **Commit** (not shown).

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

Digit Conversion for Outgoing Calls from SM

Add Remove

Filter: Enable

☐	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
☐	* 0000001050	* 10	* 10		* 10	44004	destination	IPTF CPN Restrict
☐	* 0000011051	* 10	* 10		* 10	41006	destination	IPTF TCS Agent 3
☐	* 0000021052	* 10	* 10		* 10	44002	destination	IPTF ADR Primary
☐	* 0000031053	* 10	* 10		* 10	44006	destination	IPTF ADR Second
☐	* 0000091049	* 10	* 10		* 10	40002	destination	IPTF CPN Passed
☐	* 1723112	* 11	* 11		* 6		destination	from MM

Select : All, None

5.3.2. Adaptation for Avaya Modular Messaging

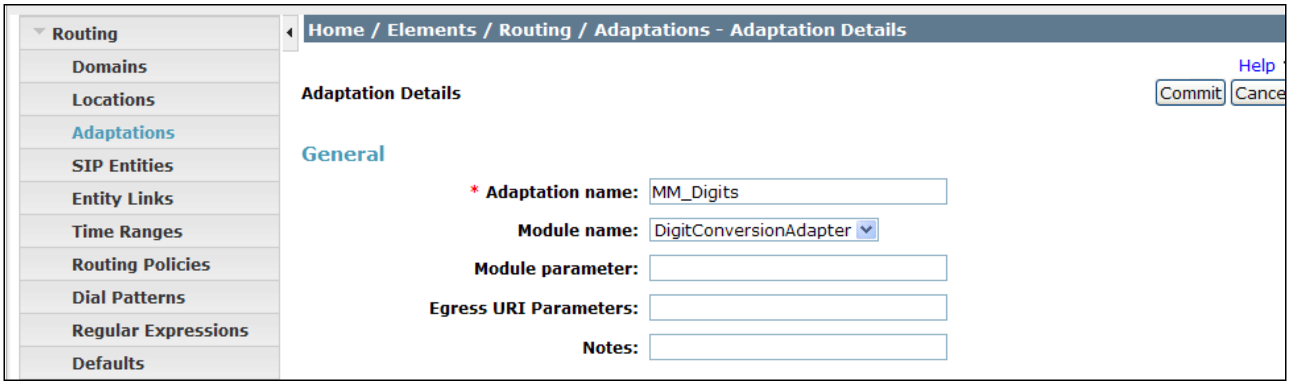
The Adaptation administered in this section is used for digit conversion on SIP messages to and from Avaya Modular Messaging.

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

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

- A descriptive **Name**, (e.g. **MM_Digits**).

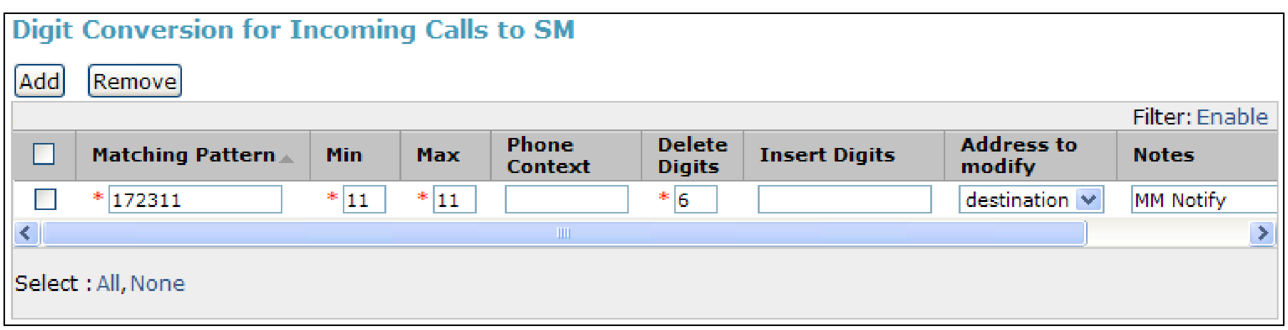
- Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select "<click to add module>" and enter **DigitConversionAdapter**).



Step 3 – Scroll down to the **Digit Conversion for Incoming Calls to SM** section. These are the *inbound* NOTIFY digits Modular Messaging sends to Communication Manager to signal MWI. In the reference configuration, Modular Messaging used 11 digit mailbox numbers (the station extension with a 172311 prefix). This prefix is removed by Session Manager before sending the NOTIFY to Communication Manager..

- Example: 17231140002 is a digit string sent in the NOTIFY by Modular Messaging that is associated with Communication Manager extension 40002.
  - Enter **172311** in the **Matching Pattern** column.
  - Enter **11** in the **Min/Max** columns.
  - Enter **6** in the **Delete Digits** column.
  - Leave the **Insert Digits** column blank.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

Step 4 - Click on **Commit** (not shown).



Note - In the reference configuration no **Digit Conversion for Outgoing Calls from SM** were required.

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 Toll Free 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). In addition, SIP phones will use the "local" trunk for intra-site calls as well as status signaling to Session Manager.
    - 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 Acme Packet SBC. Note that port 5080 is only used between Communication Manager and Session Manager.
    - Communication Manager for local access (**Section 5.4.3**) – This entity, and associated link (using port 5060), is for communication between Avaya SIP phones and Communication Manager.
- Acme SBC to AT&T (**Section 5.4.4**) - This entity, and its associated entity link (using port 5060), is for inbound calls from the AT&T IP Toll Free service via the Acme 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:

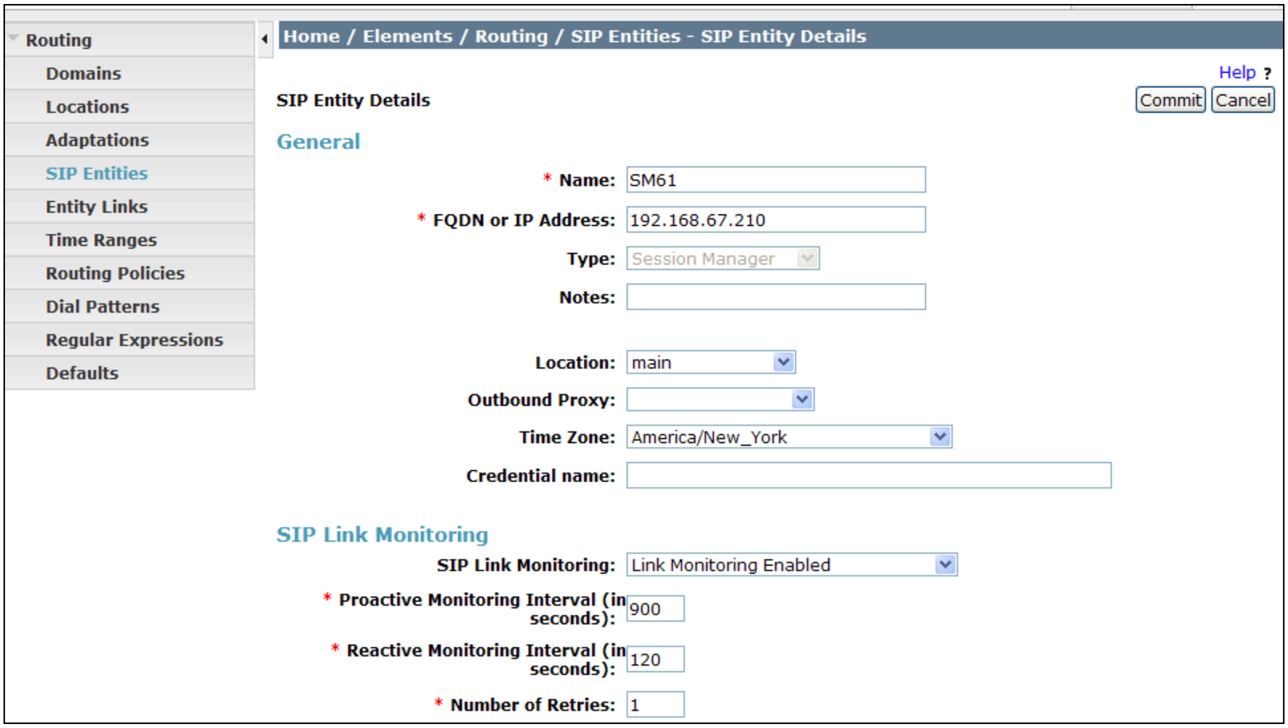
- **Name –** Enter a descriptive name for Session Manager (e.g. **SM61**).
- **FQDN or IP Address –** Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation (e.g. **192.168.67.210**).
- **Type –** Select **Session Manager**.
- **Location** – Select location **Main** (**Section 5.2**).
- **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 (this will correspond to the time ranges specified in **Section 5.6**).

Step 3 - In the **SIP Monitoring** section of the **SIP Entity Details** page select:

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

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

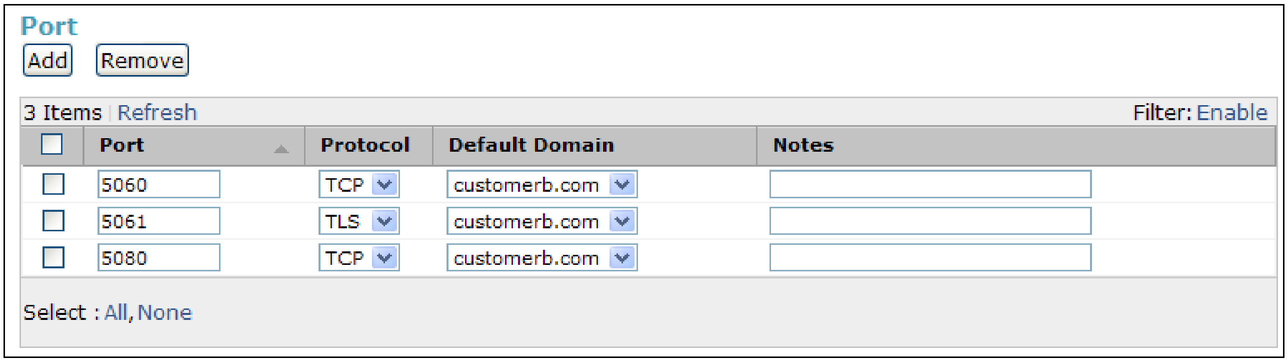


Step 4 - In the **Port** section of the **SIP Entity Details** page, click on **Add** and provision an entry as follows:

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

Step 5 - Repeat **Step 4** to provision another entry 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 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.


Port

Add Remove

3 Items | Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
☐	5060	TCP	customerb.com	
☐	5061	TLS	customerb.com	
☐	5080	TCP	customerb.com	

Select : All, None

Step 6 - 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

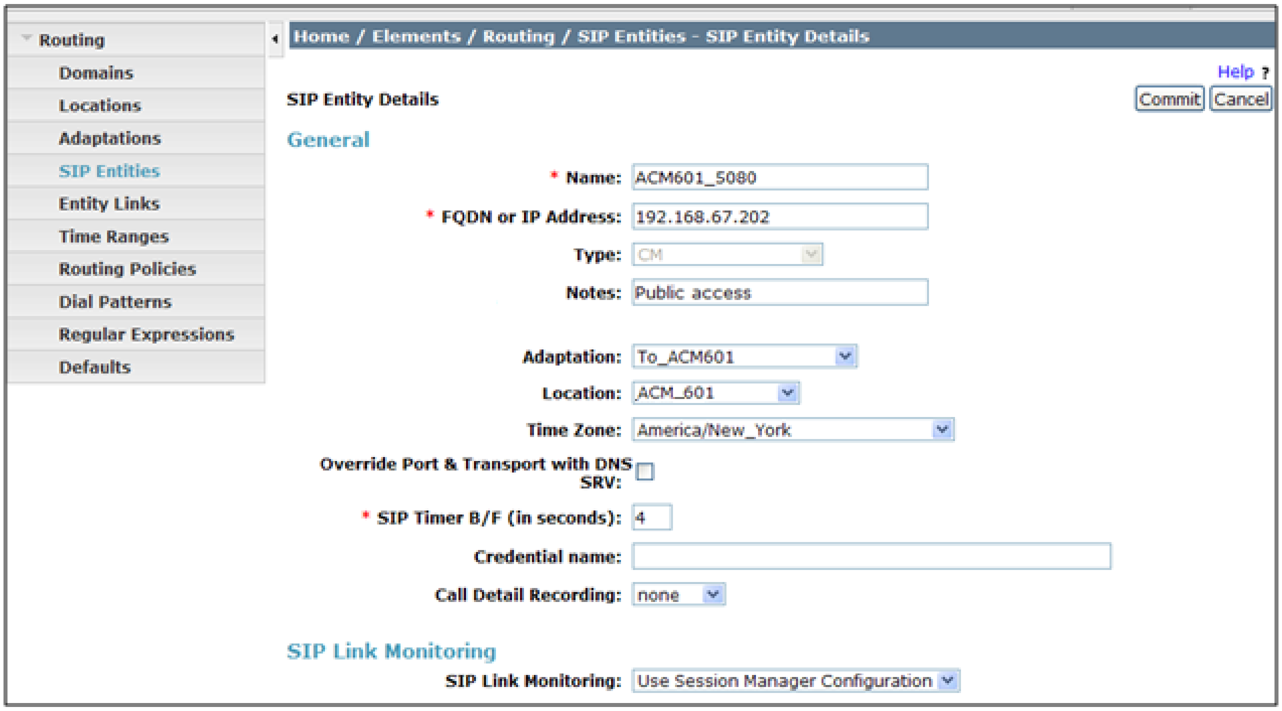
Step 1 - In the **SIP Entities** page, click on **New**.

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.
- **FQDN or IP Address –** Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.4**.
- **Type –** Select **CM**.
- **Adaptation –** Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page:
  - Select **Link Monitoring Enabled** for **SIP Link Monitoring**
  - 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**.

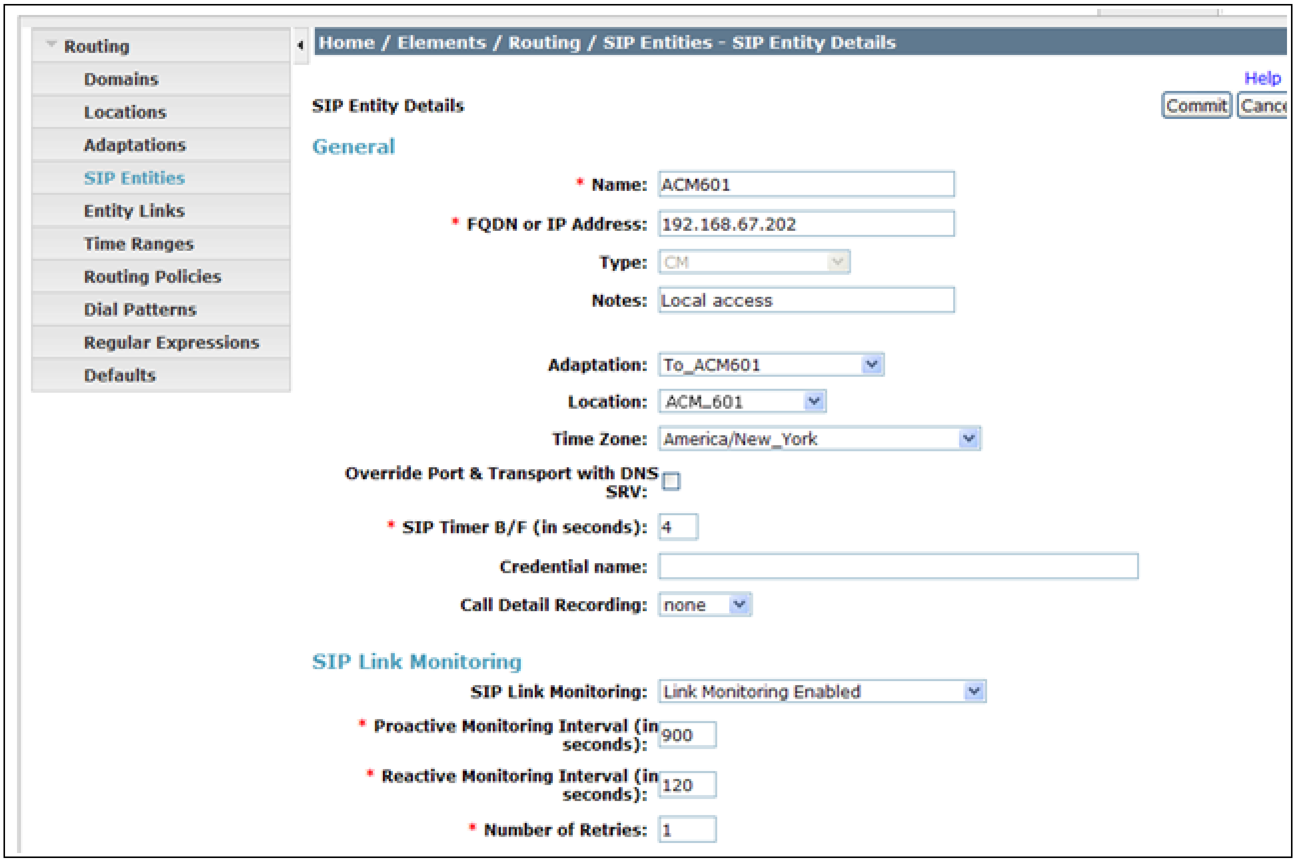
Step 1 - In the **SIP Entities** page, click on **New** (not shown).

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

- **Name –** Enter a descriptive name for the Communication Manager “local” trunk.
- **FQDN or IP Address –** Enter the IP address of the Communication Manager Processor Ethernet (procr) provisioned in **Section 6.3**.
- **Type** – Select **CM**.
- **Adaptation –** Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page:
  - Select **Link Monitoring Enabled** for **SIP Link Monitoring**
  - Use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

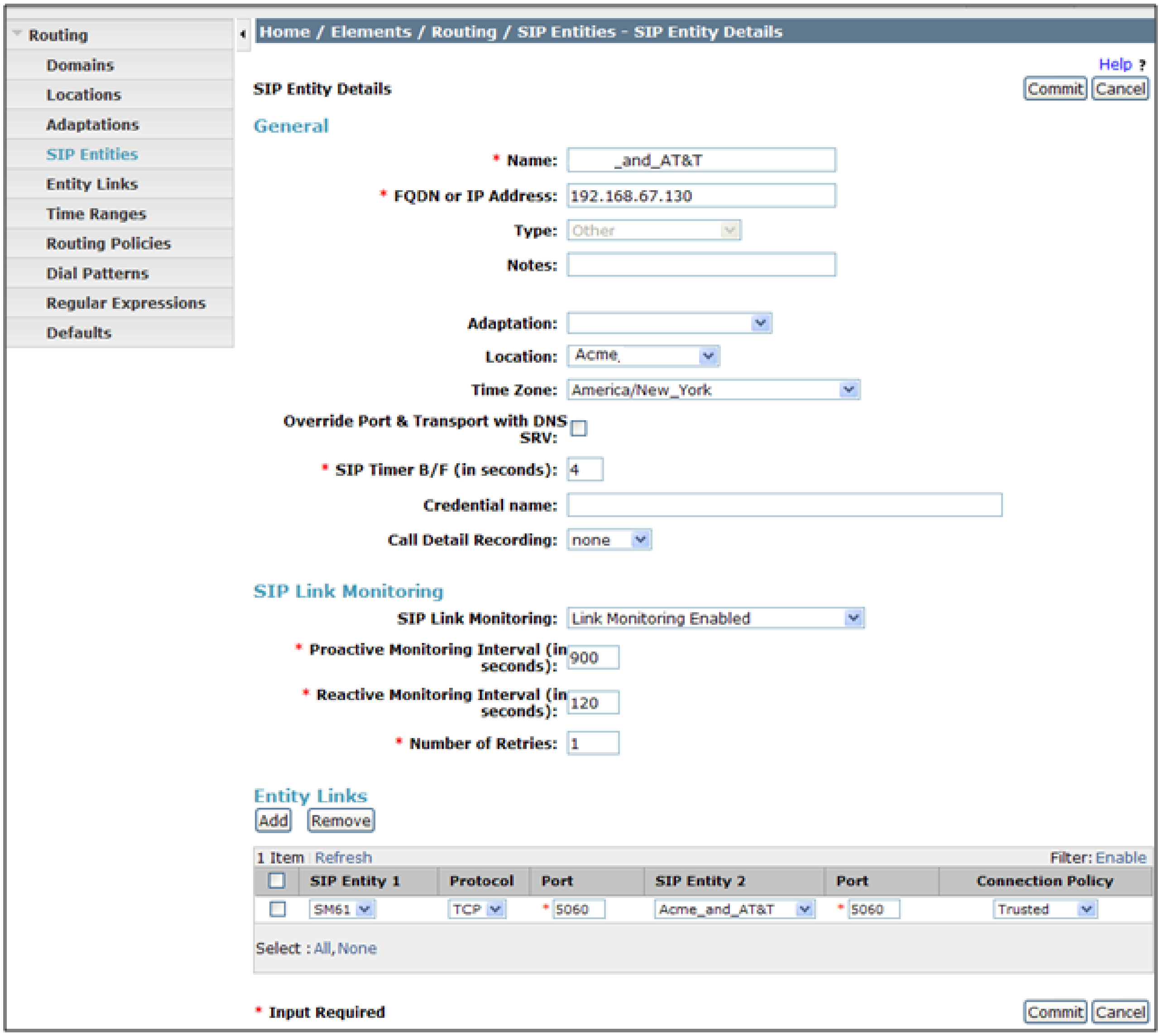
Note that the **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.



5.4.4. Acme Packet SBC SIP Entity

To configure the Session Border Controller entity, repeat the steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of the private (inside) Acme SBC interface configured in **Section 8** and the **Type** field is set to **Other**. See the figure below for the values used in the reference configuration.

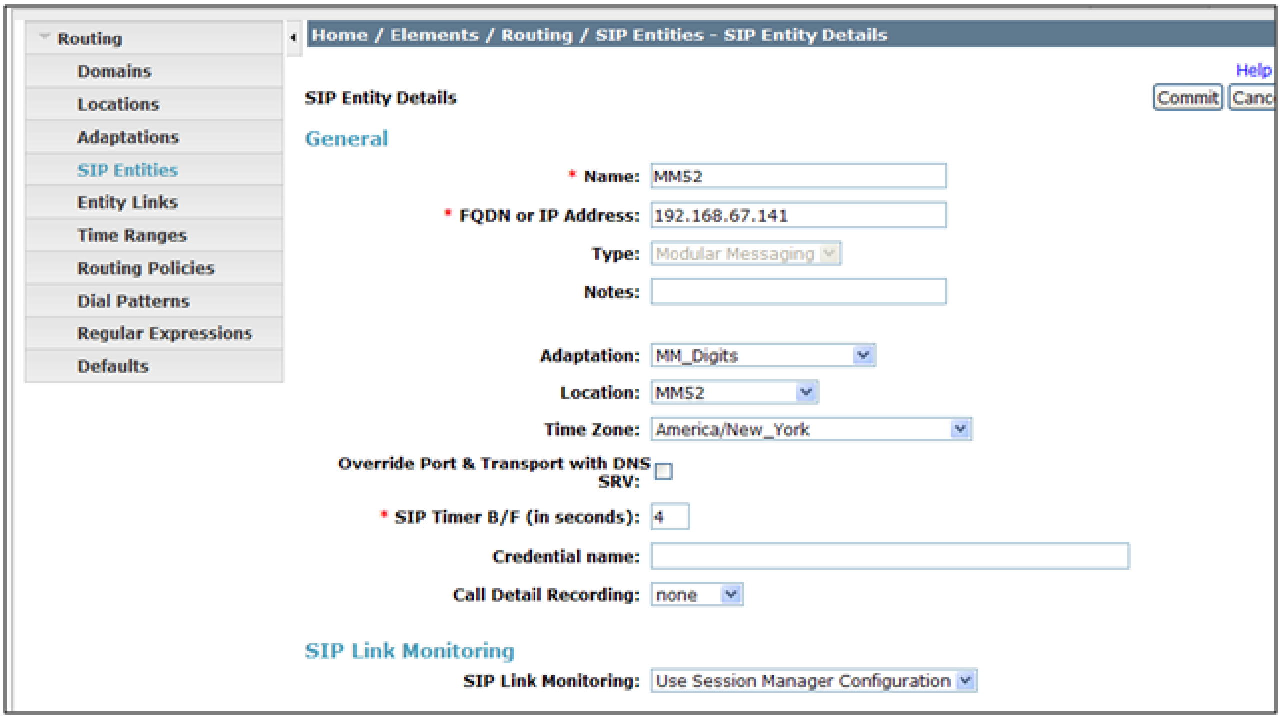
Note that the **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.



5.4.5. Avaya Modular Messaging SIP Entity

To configure the Modular Messaging SIP entity, repeat the steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of the Modular Messaging Application Server (MAS) and the **Type** field is set to **Other**. See the figure below for the values used in the reference configuration.

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**).
- Acme Packet 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 Link to Avaya Aura® Communication Manager - Public

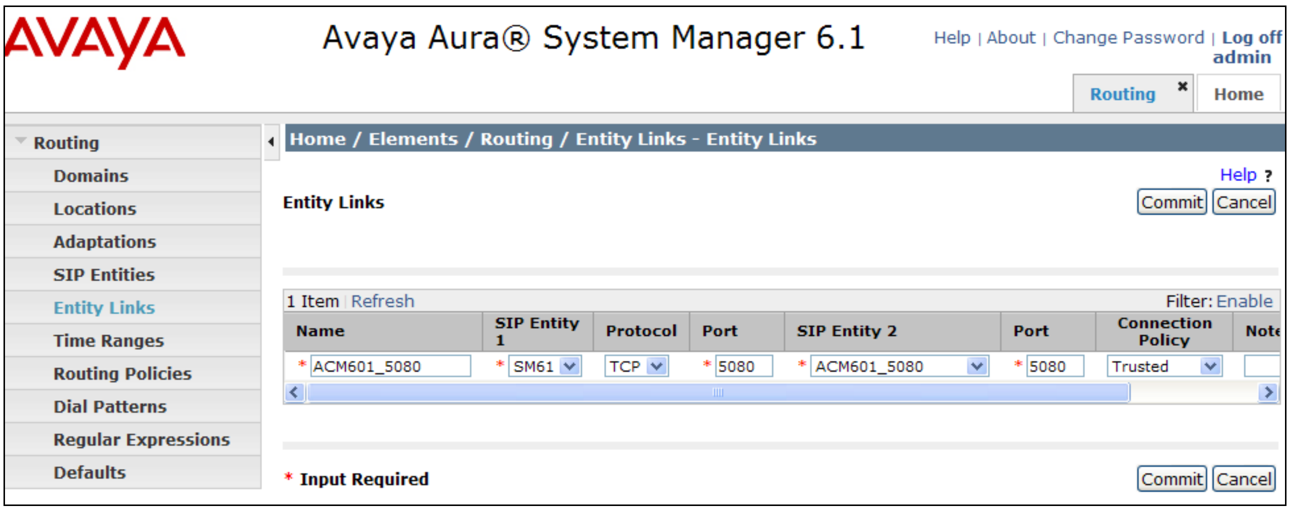
Step 1 - In the left pane under **Routing**, click on **Entity Links**. In the **Entity Links** page click on **New** (not shown).

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

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g. **ACM601_5080**).

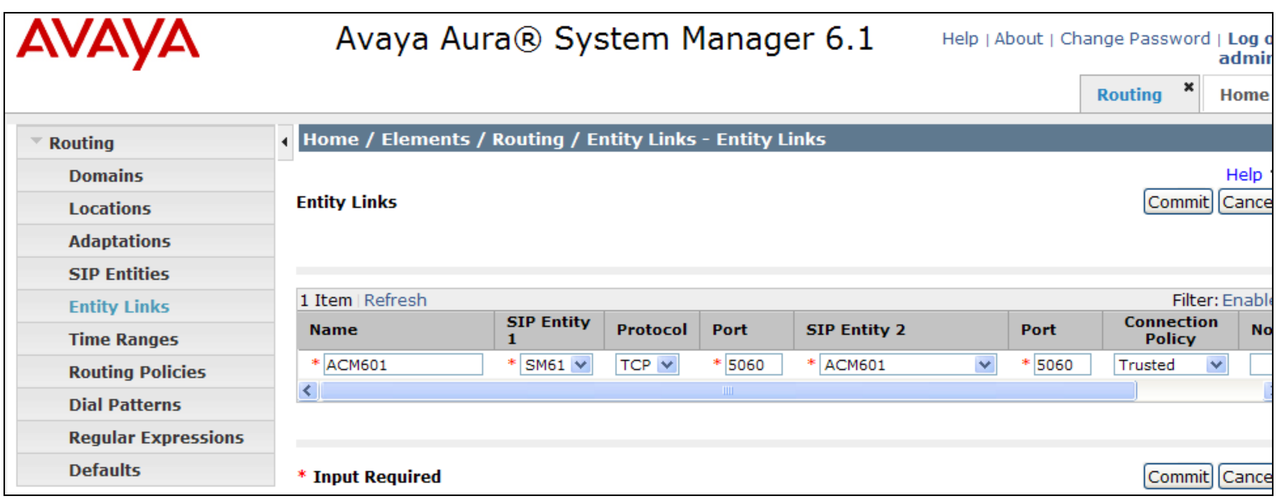
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5080**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager "public" entity.
- **SIP Entity 2 Port** - Enter **5080**.
- **Trusted** – Select **Trusted**.
- **Protocol** – Select **TCP**.

Step 3 - Click on **Commit**.



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

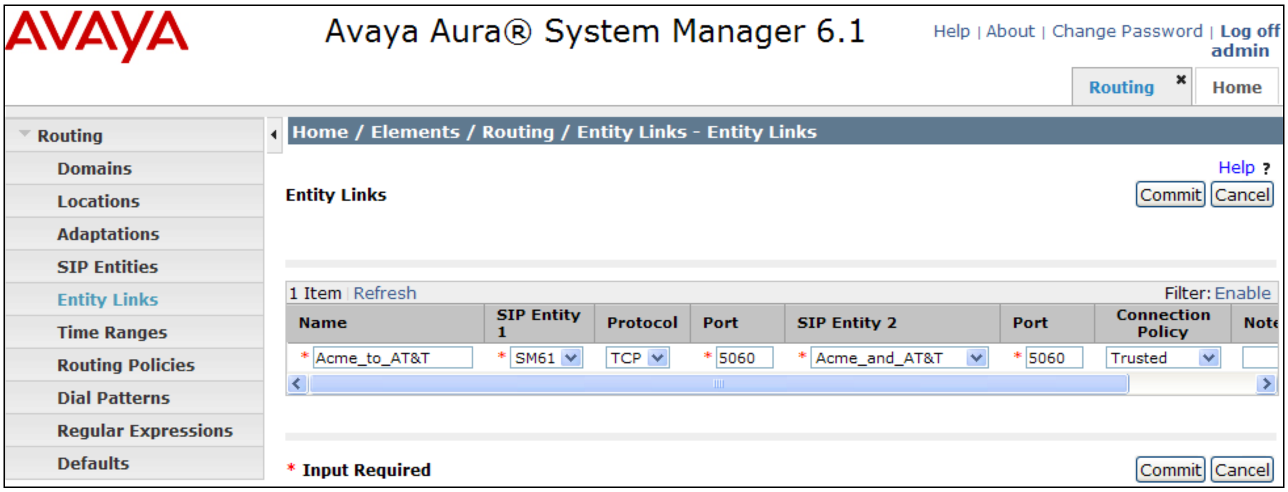
To configure this entity link, repeat the Steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.3** for Communication Manager "local" Entity (e.g. **ACM601**). Note that the **Port** fields are populated with **5060**. See the figure below for the values used in the reference configuration.



5.5.3. Entity Link to AT&T IP Toll Free Service via Acme Packet SBC

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

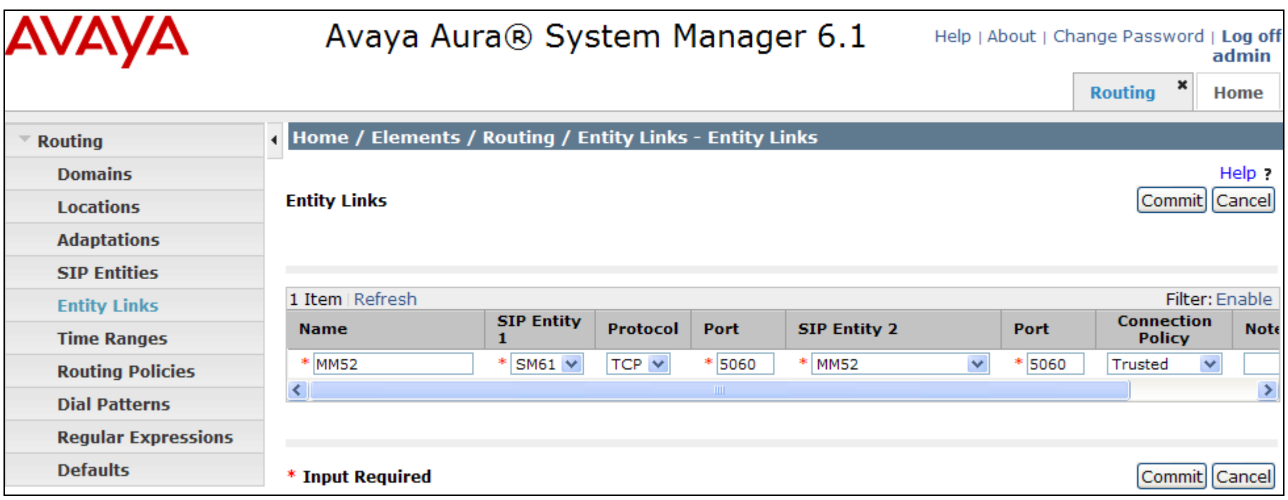
- **Name** – Enter a descriptive name for the link to the AT&T IP Toll Free service, by way of the Acme Packet SBC.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.4** for the Acme Packet SBC.



5.5.4. Entity Link to Avaya Modular Messaging

Repeat **5.5.1** with the following differences:

- **Name** – Enter a descriptive name for the link to Avaya Modular Messaging.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.5** for Avaya Modular Messaging.



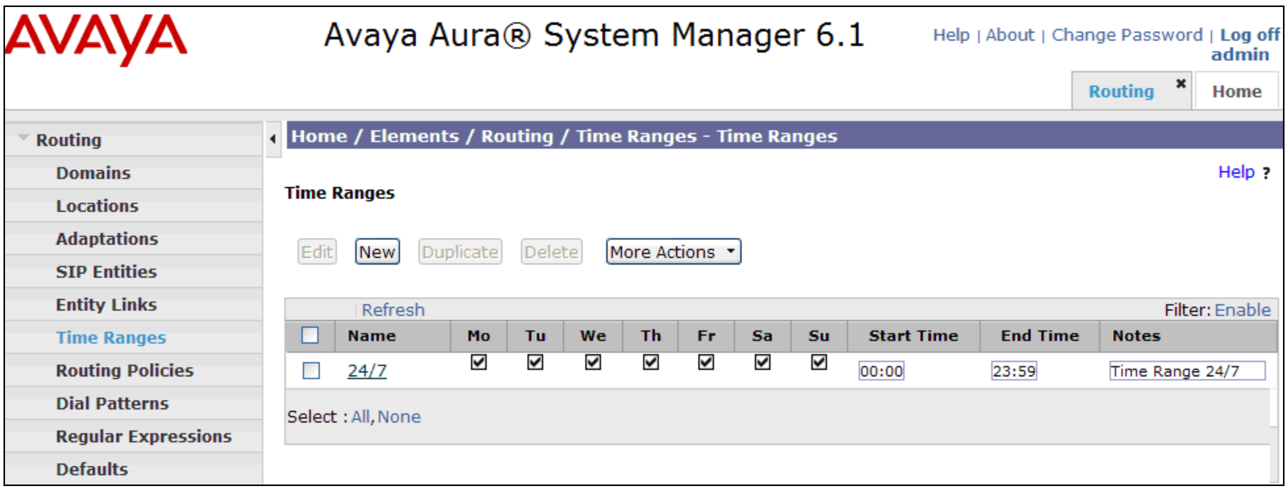
5.6. Time Ranges

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 10 –** 3 to provision additional time ranges.



5.7. Routing Policies

In this section, the following Routing Policies are administered:

- AT&T calls to Communication Manager (**Section 5.7.1**).
- Avaya Modular Messaging MWI notification to Communication Manager (**Section 5.7.2**).
- Communication Manager calls to Avaya Modular Messaging for call coverage (**Section 5.7.3**)

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

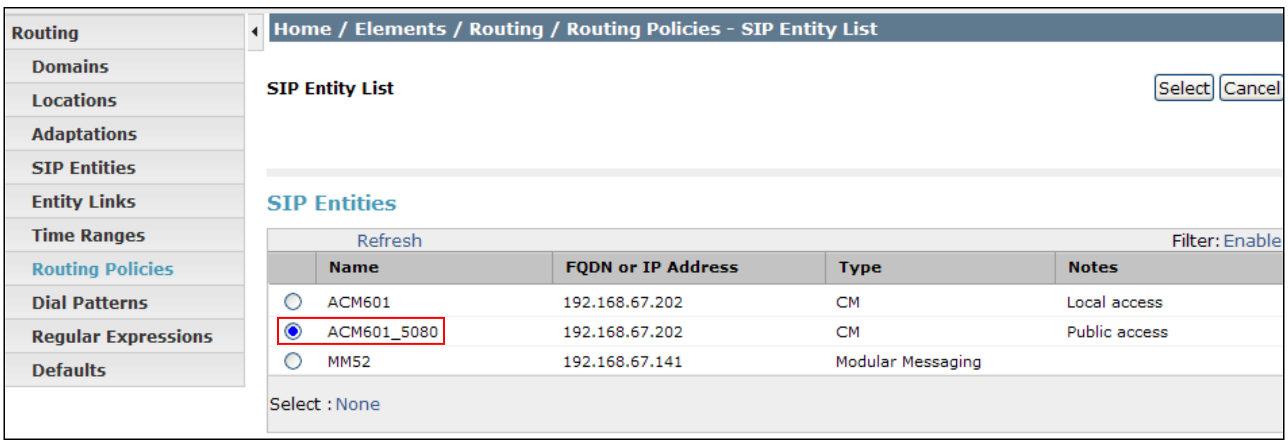
Note that this routing policy will use the "public" SIP Entity ACM601_5080.

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

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g. **To_ACM601_5080**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

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

Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for Communication Manager (**ACM601_5080**), and click on **Select**.



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

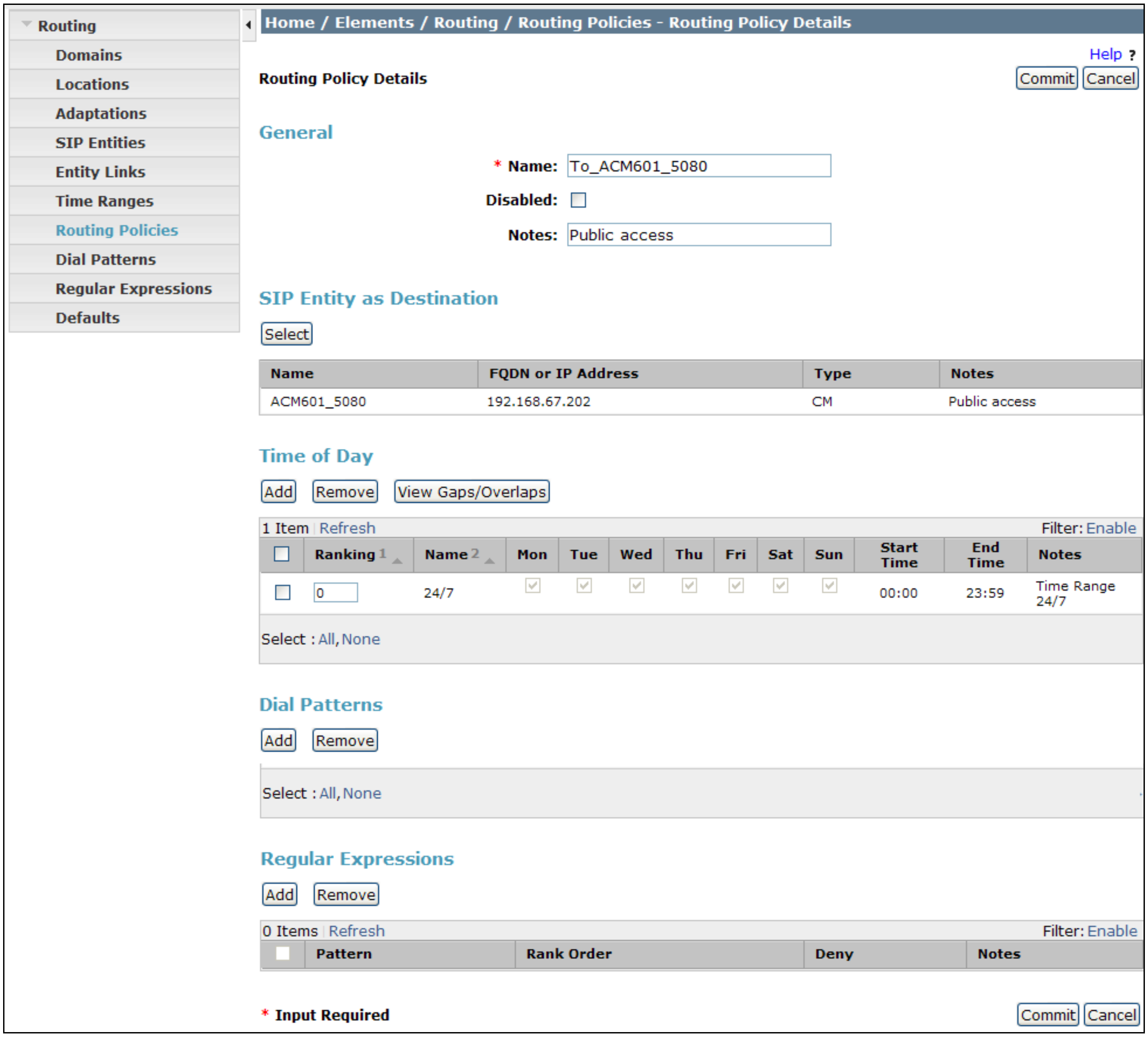
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

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

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

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

Step 10 - Click on **Commit**.

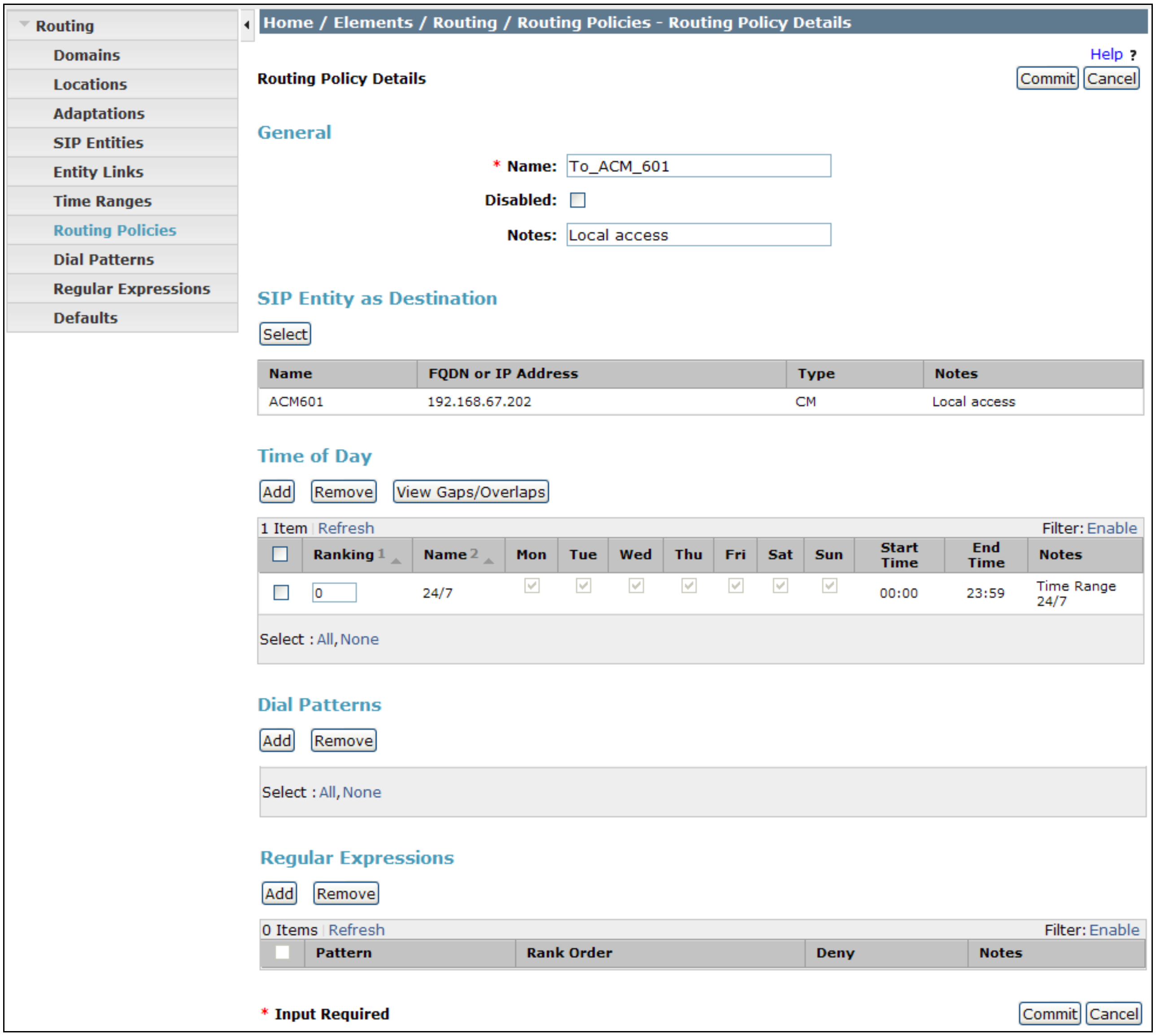


5.7.2. Routing Policy for Routing from Avaya Modular Messaging (MWI) to Avaya Aura® Communication Manager

Note that this routing policy will use the "local" SIP Entity ACM601.

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

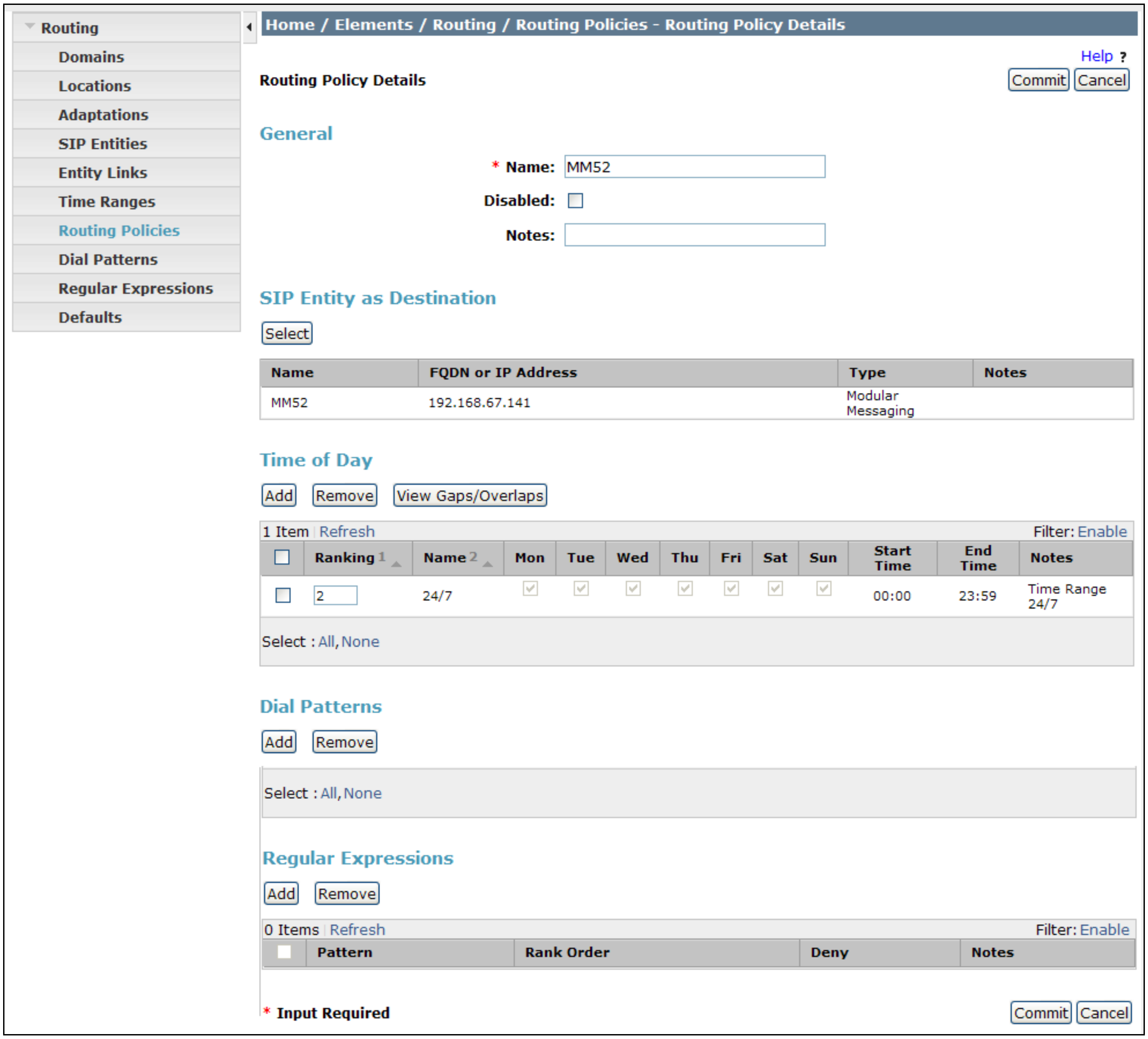
- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing local calls to Communication Manager (**To_ACM610**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for Communication Manager (**ACM610**), and click on **Select**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



5.7.3. Routing Policy for Routing to Avaya Modular Messaging (Call Coverage) from Avaya Aura® Communication Manager

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



5.8. Dial Patterns

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

- Inbound PSTN calls via AT&T IP Toll Free service to Communication Manager.
- Call Coverage/retrieval calls to Modular Messaging from Communication Manager to the Modular Messaging pilot number.
- Notifications from Avaya Modular Messaging (MWI) to Communications Manager 5 digit local extensions.

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

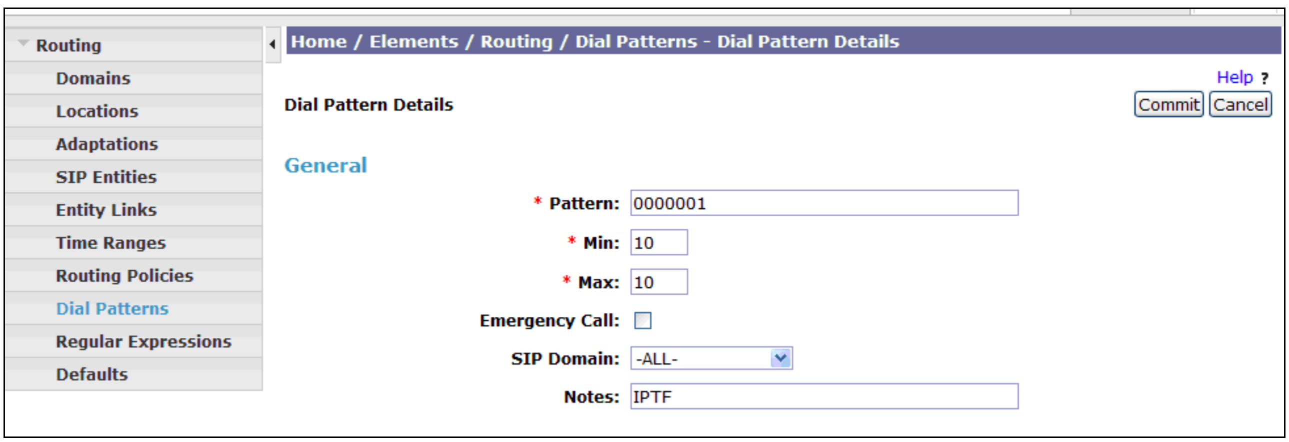
In the reference configuration inbound calls from the AT&T IP Toll Free service used the called digit pattern 0000001xxx in the SIP Request URI. This pattern is matched for further call processing.

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

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

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

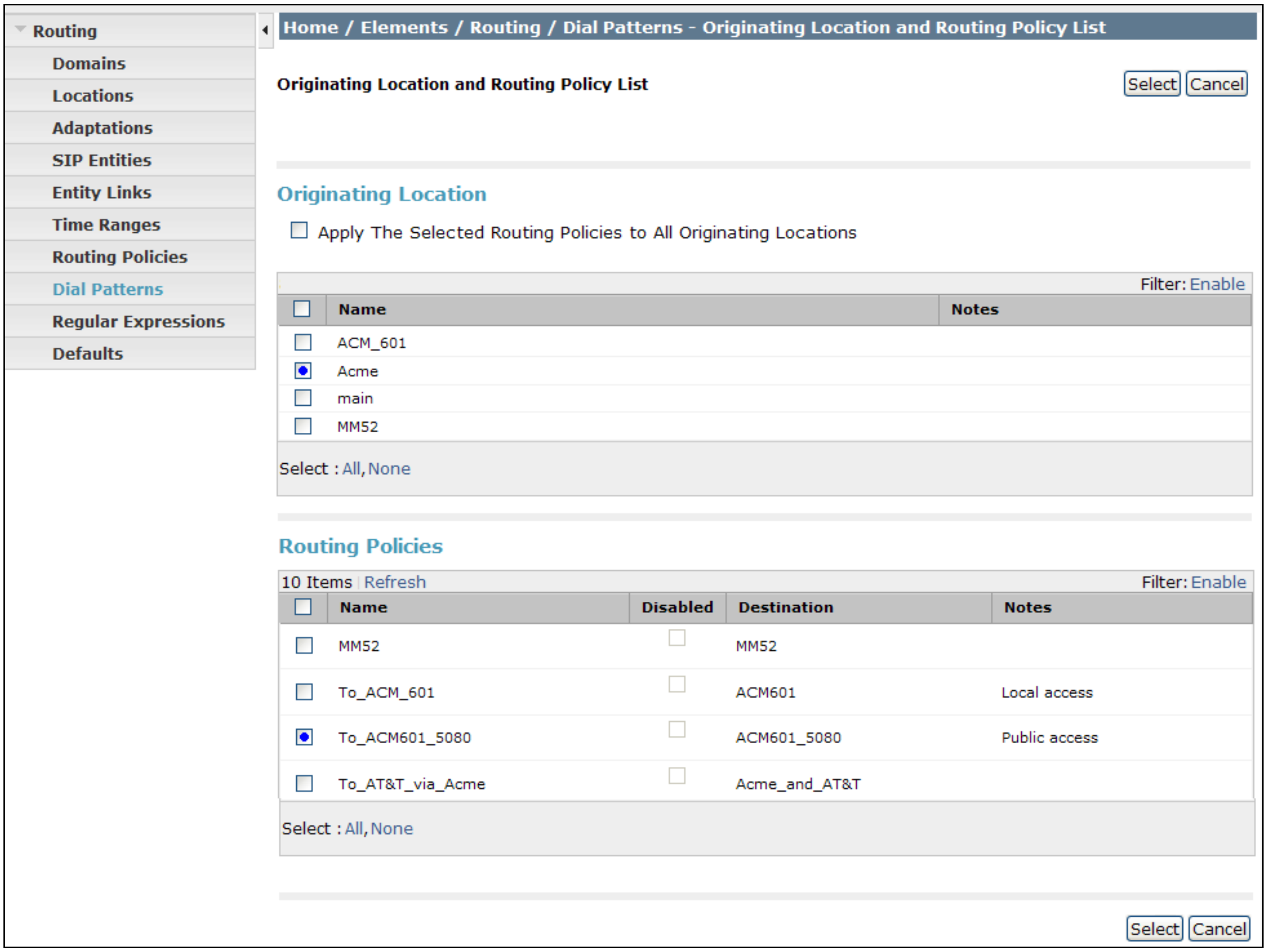
- **Pattern** – In the reference configuration, AT&T sends a 10 digit number in the Request URI with the format 0000001xxx. Enter **0000001**. Note - The adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 0000001xxx numbers into their corresponding extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or "**-ALL-**", to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if "**-ALL-**" is selected) can match this Dial Pattern.



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

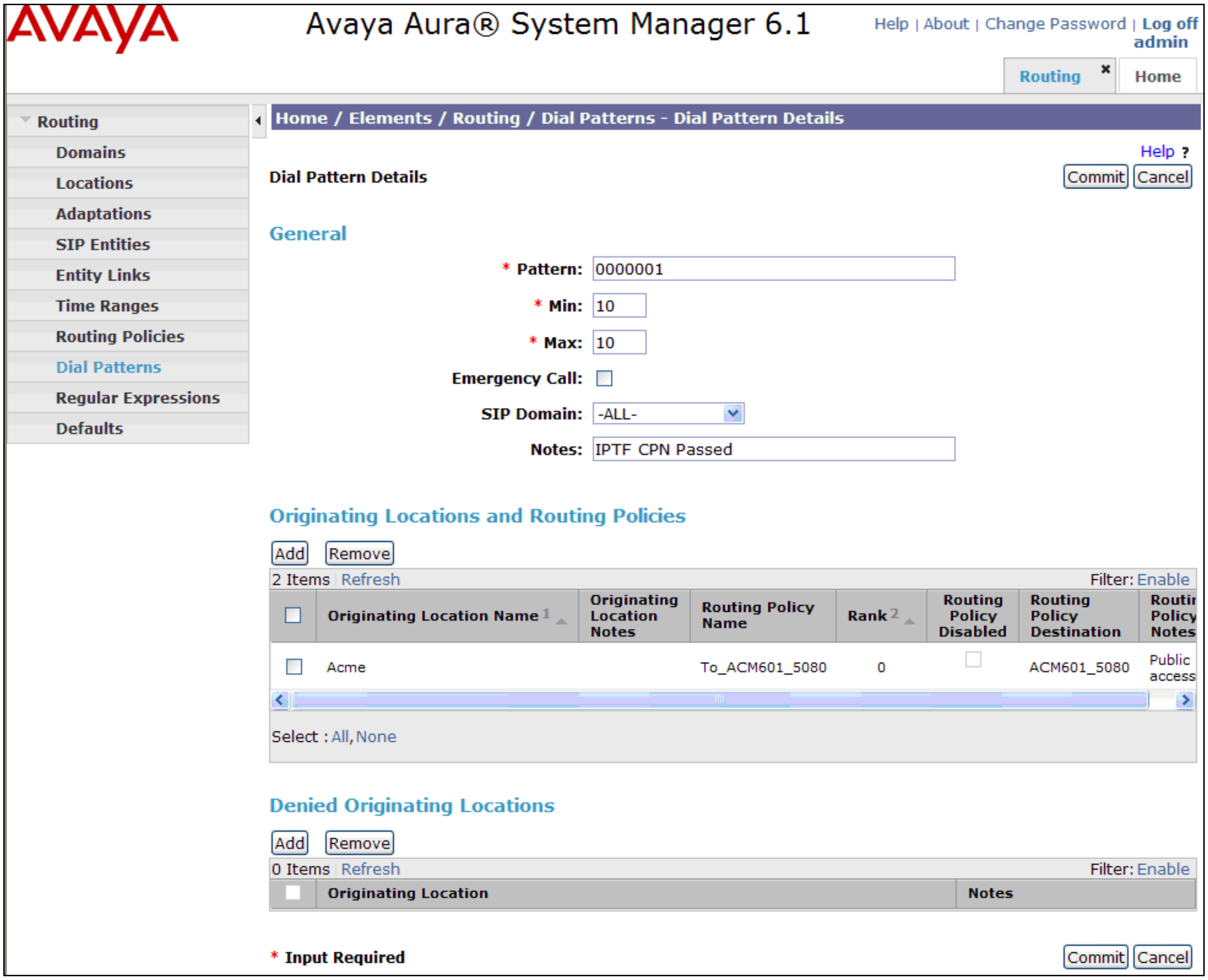
Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Acme** (see **Section 5.2.3**). Note that only those calls that originate from the selected Location(s), or all administered Locations if "**-ALL-**" is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager "Public" trunk 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**.



5.8.2. Matching Inbound Calls to Avaya Modular Messaging Pilot Number via Avaya Aura® Communication Manager

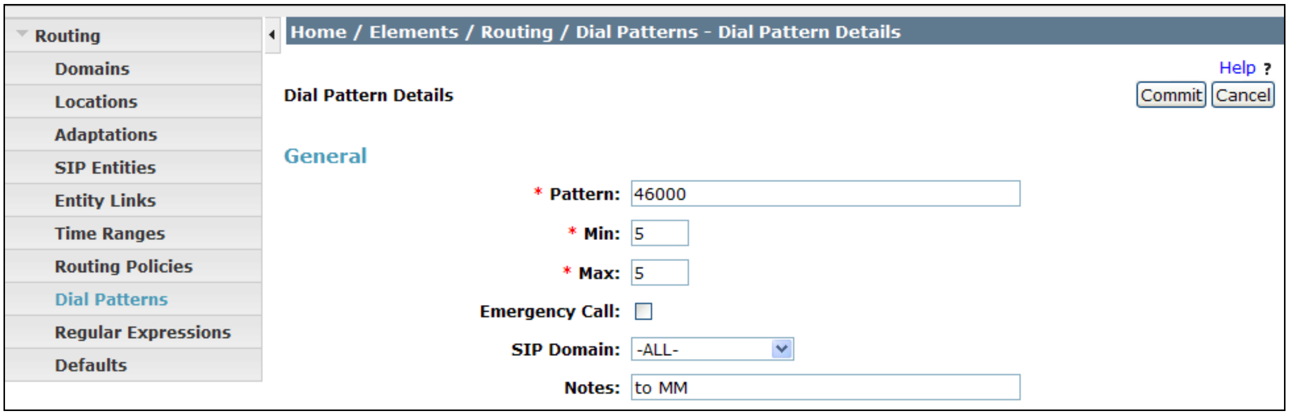
Communication Manager stations cover to Avaya Modular Messaging using a pilot extension (46000 in the reference configuration). Additionally stations may dial this pilot extension to retrieve messages or modify mailbox settings.

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 the Avaya Modular Messaging pilot extension (e.g. **46000**)
- **Min** and **Max** – Enter **5**.
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or "**-ALL-**", to select all of those administered SIP Domains. Only those calls with the same

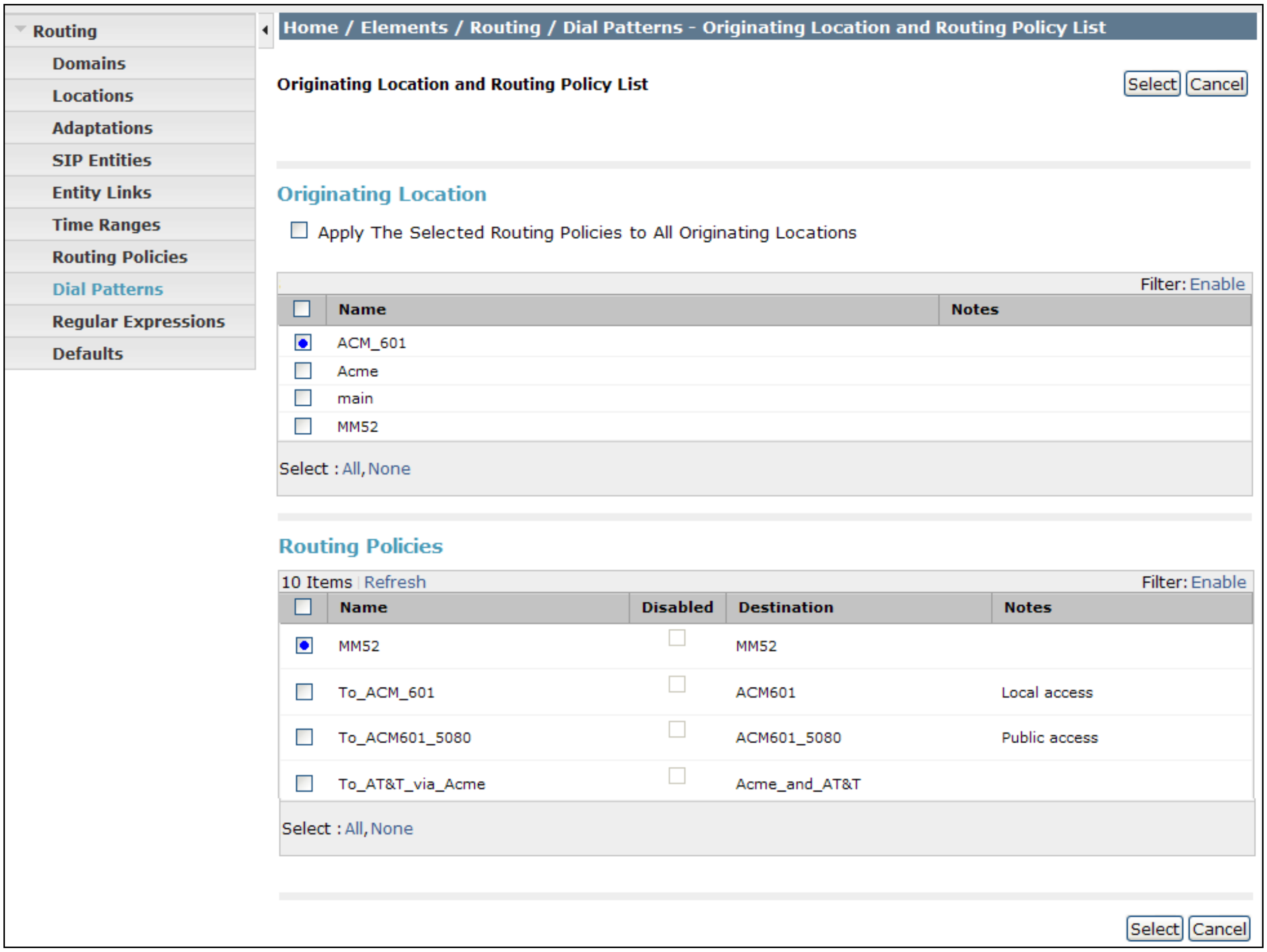
domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if "**-ALL-**" is selected) can match this Dial Pattern.



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

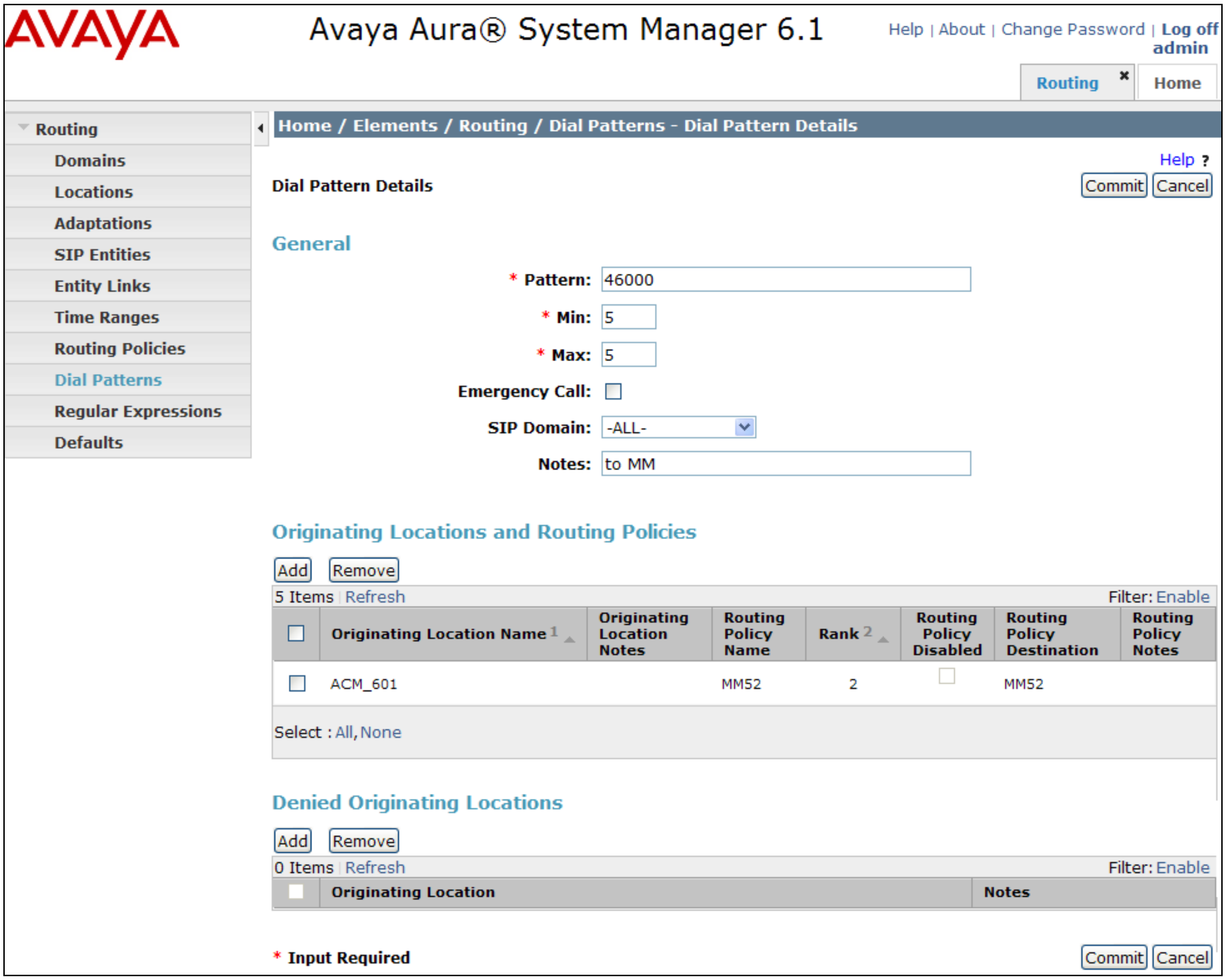
Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **ACM_601** (see **Section 5.2.1**). Note that only the calls that originate from the selected Location(s), or all administered Locations if "**-ALL-**" is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **MM52** administered for routing calls to Modular Messaging in **Section 5.7.3**.



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**.



5.8.3. Matching Inbound Calls to Avaya Aura® Communication Manager from Avaya Modular Messaging (MWI Notify).

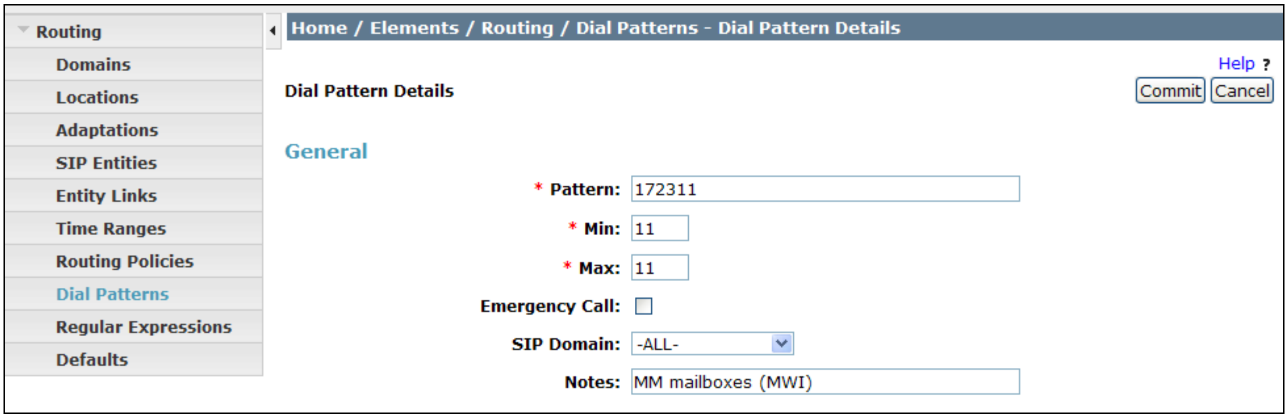
Avaya Modular Messaging will send SIP Notify messages to Communication Manager stations to indicate waiting messages (MWI). In the reference configuration, Modular Messaging uses 11 digit mailboxes. These 11 digit mailboxes use the format **172311xxxxx** where xxxxx is the Communication Manager extension. Note that these 11 digits are converted to the Communication Manager 5 digit extension in the Modular Messaging Adaptation defined in **Section 5.3.2**.

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 the first 6 digits of the Modular Messaging mailbox number format (e.g. 1**72311**)
- **Min** and **Max** – Enter **11**.

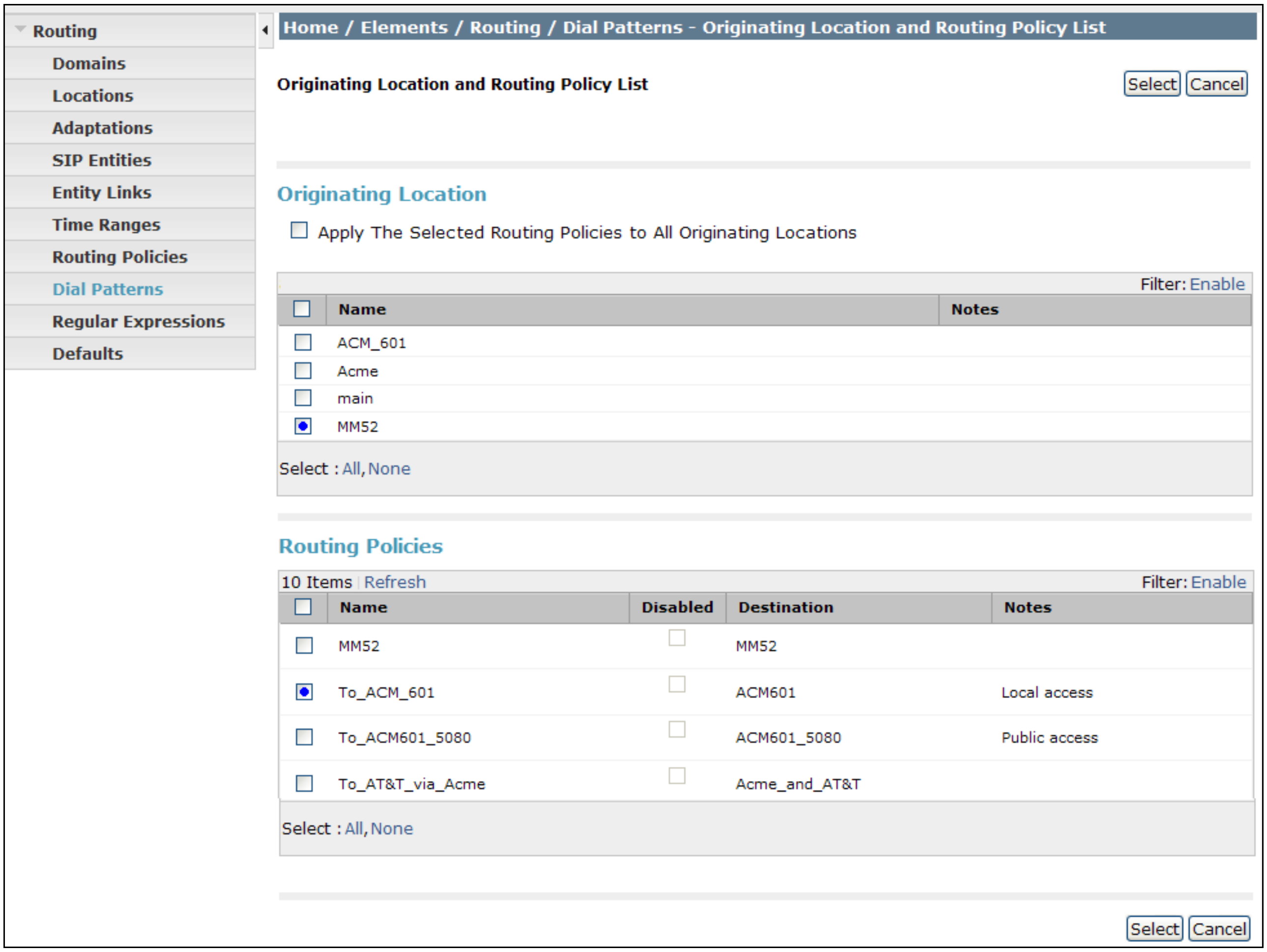
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or "**-ALL-**", to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if "**-ALL-**" is selected) can match this Dial Pattern.



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

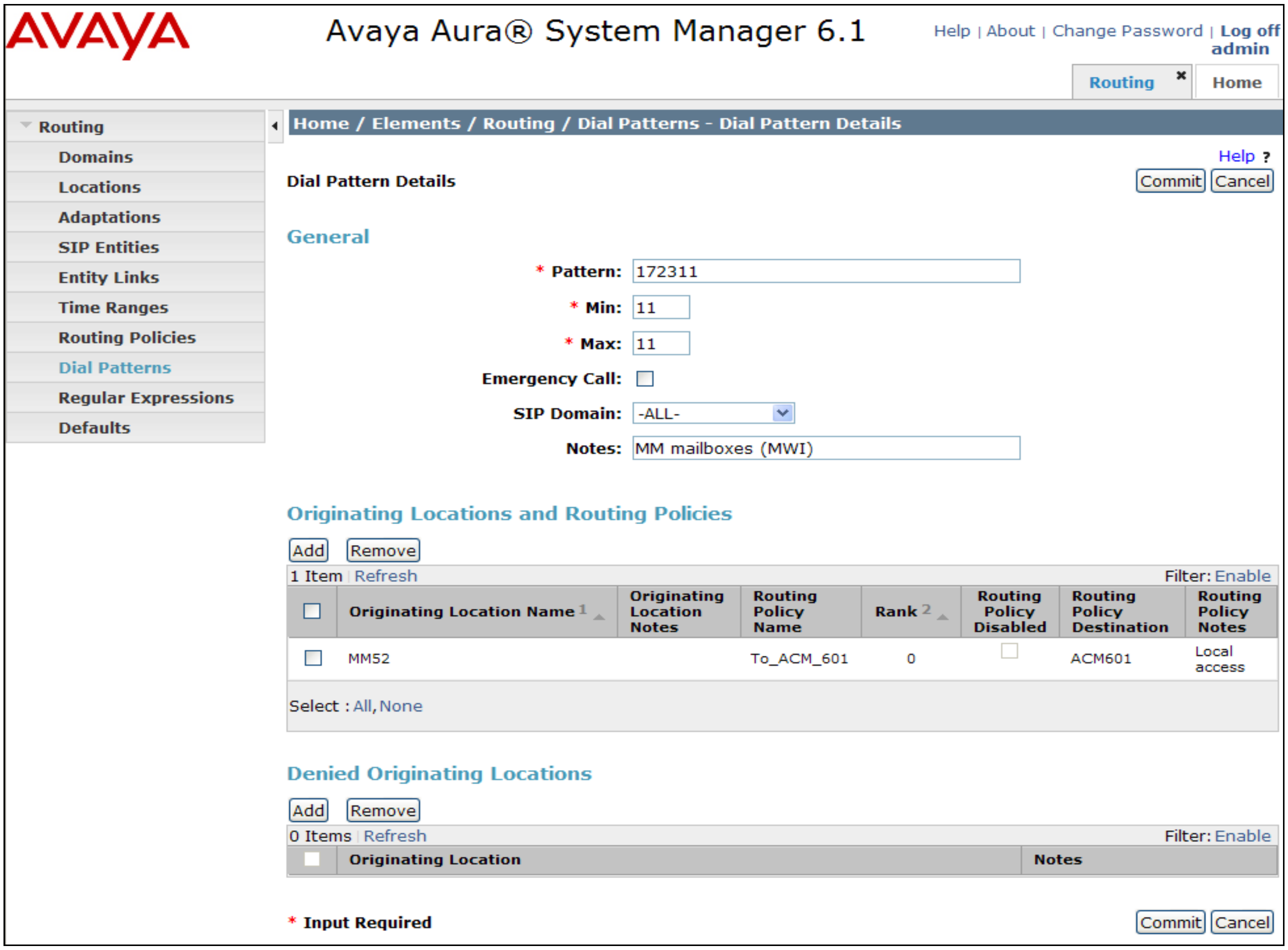
Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **MM52** (see **Section 5.2.3**). Note that only those calls that originate from the selected Location(s), or all administered Locations if "**-ALL-**" is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **To_ACM_601** administered for routing calls to the Communication Manager "Local" trunk in **Section 5.7.2**.



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**.



6. Avaya Aura® Communication Manager

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

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

6.1. System Parameters

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

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

IP PORT CAPACITIES                                             USED
                    Maximum Administered H.323 Trunks: 12000 0
          Maximum Concurrently Registered IP Stations: 18000 4
            Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
             Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 18000 1
                  Maximum Video Capable IP Softphones: 18000 2
                      Maximum Administered SIP Trunks: 24000 24
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                            Maximum TN2501 VAL Boards: 128   0
                    Maximum Media Gateway VAL Sources: 250   1
          Maximum TN2602 Boards with 80 VoIP Channels: 128   0
         Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

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

```
display system-parameters customer-options                        Page   3 of  11
                                OPTIONAL FEATURES
    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? y               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
        (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?** , the **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? y
     External Device Alarm Admin? y               Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n    Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                Multifrequency Signaling? y
      Global Call Classification? y        Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y     Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y              Multimedia IP SIP Trunking? y
                       IP Trunks? y
           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

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

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

6.2. Dial Plan

The dial plan defines how digit string will be used locally by Communication manager.

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**. 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 **4xxxx** . 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. access code **8** for outbound AAR dialing).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g. access code **9** for outbound ARS dialing).
  - Note – ARS is typically used for outbound dialing, which the AT&T IP Toll Free service does not support. It is shown here for informational purposes only.
- 3-digit facilities access codes beginning with ***** and **#** for Agent logon/logoff (e.g.*66 or #76).

```
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
   4            5   ext
   8            1   fac
   9            1   fac
   *            3   fac
   #            3   fac
```

6.3. IP Node Names

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

Step 1 - Enter the **change node-names ip** command, and add a node name and the IP address for the Session Manager network interface (e.g. **ASM61**)

Step 2 – Repeat **Step 1** to add node names for the Acme and for Modular Messaging.

Step 3 - A Processor Ethernet (procr) based Communication Manager platform is used in the reference configuration. Make note of the Processor Ethernet node name and IP Address (**procr** & **192.168.67.202**). These entries appear automatically based on the address defined during Communication Manager installation.

```
change node-names ip                                               Page   1 of   2
                                    IP NODE NAMES
    Name                  IP Address
ASM61                   192.168.67.210
Acme                    192.168.67.130
MM52                    192.168.67.141
default                 0.0.0.0
procr                   192.168.67.202
procr6                  ::
```

6.4. IP Interface for procr

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

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

```
display ip-interface procr                                  Page   1 of   2
                                  IP INTERFACES


                  Type: PROCR
                                                  Target socket load: 19660

      Enable Interface? y                      Allow H.323 Endpoints? y
                                                Allow H.248 Gateways? y
        Network Region: 1                        Gatekeeper Priority: 5


                                 IPV4 PARAMETERS
             Node Name: procr                     IP Address: 192.168.67.202


           Subnet Mask: /24
```

6.5. IP Network Regions

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

6.5.1. IP Network Region 1 – Local Region

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

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

- Enter a descriptive name (e.g. **LOCAL**).
- Enter **customerb.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: customerb.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**.
- 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
 3
```

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 6.5.1** 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: customerb.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**

```
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**, **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 AT&T IP Toll Free 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 **30** for **Packet Size(ms)**. Let **G711MU** default to **20**.

Note – See **Section 2.1.1 item 4** for an issue regarding SIP telephone packet sizes.

```
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 2
    - Note that this trunk will use TCP port 5080 as described in **Section 5.5.1**.
- Local for Modular Messaging and Avaya SIP phone access – SIP Trunk 1
    - Note that this trunk will use TCP port 5060 as described in **Section 5.5.2**.

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

Note – In the reference configuration TCP ports 5060 and 5080 are 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 in customer environments whenever possible.

6.7.1. SIP Trunk for AT&T IP Toll Free calls

This section describes the steps for administering the SIP trunk used for AT&T IP Toll Free calls. This trunk corresponds to the **ACM601_5080** Entity defined in **Section 5.4.2**.

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp**. Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Acme Packet SBC and the AT&T IP Toll Free service is UDP.
- Verify the **IMS Enabled?** Is set to **n**.
- Verify that **Peer Detection Enabled** is **y** and that **Peer Server** is **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.3**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g. **ASM61**).
- **Near-end Listen Port** and **Far-end Listen Port** – set to **5080** (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 **customerb.com**. This is the domain used by Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized to reduce the use of media resources on the Avaya media gateway when possible (known as “shuffling”).
- **Enable Layer 3 Test** – Set to **y**. This initiates Communication Manager to send OPTIONS “pings” to Session Manager to provide link status.

```
add signaling-group 2                                           Page   1 of   1
                                SIGNALING GROUP
 Group Number: 2             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: procr                  Far-end Node Name: ASM61
 Near-end Listen Port: 5080                 Far-end Listen Port: 5080
                                         Far-end Network Region: 2
                                   Far-end Secondary Node Name:
Far-end Domain: customerb.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y               Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

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

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g. **ATT**).

- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **102**).
- **Direction** – Set to **incoming**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g. **2**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g. **20**).

```
add trunk-group 2                                           Page   1 of  21
                                TRUNK GROUP
Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: ATT                         COR: 1        TN: 1        TAC: 102
   Direction: incoming       Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? N
                                              Member Assignment Method: auto
                                              Signaling Group: 2
                                              Number of Members: 20
```

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

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

```
add trunk-group 2                                           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
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

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

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

```
add trunk-group 2                                           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
                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
 DSN Term? n
```

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

- Set **Telephone Event Payload Type** to the RTP payload type required by the AT&T IP Toll Free service (e.g. **100**).
- Use default for all other values.

```
add trunk-group 2                                                Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 100
       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                            Enable Q-SIP? n
```

6.7.2. Local SIP Trunk (Modular Messaging and Avaya SIP Telephones)

This section describes the steps for administering the local SIP trunk for Avaya Modular Messaging and Avaya SIP station calls. This trunk corresponds to the **ACM601** Entity defined in **Section 5.4.3**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **1**), and 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 Acme Packet SBC and the AT&T IP Toll Free service is UDP.
- Verify the **IMS Enabled?** Is set to **n**.
- Verify that **Peer Detection Enabled** is **y** and that **Peer Server** is **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.3**
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g. **ASM61**).
- **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 **1**, as defined in **Section 6.5.1**.
- **Far-end Domain** – Enter **customerb.com**. This is the domain used by Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized to reduce the use of media resources on the Avaya media gateway when possible (known as "shuffling").

- **Enable Layer 3 Test** – Set to **y**. This initiates Communication Manager to send OPTIONS "pings" to Session Manager to provide link status.

```
add signaling-group 1                                          Page   1 of   1
                                SIGNALING GROUP
 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: procr                  Far-end Node Name: ASM61
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain: customerb.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

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

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g. **Local**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **101**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step** 1 (e.g. **1**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g. **20**).

```
add trunk-group 1                                              Page   1 of  21
                                TRUNK GROUP
Group Number: 1                    Group Type: sip            CDR Reports: y
  Group Name: Local                       COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? N
                                              Member Assignment Method: auto
                                              Signaling Group: 1
                                              Number of Members: 20
```

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

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

```
add trunk-group 1                                              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
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

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

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

```
add trunk-group 1                                              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
                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
 DSN Term? n
```

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

- Set **Telephone Event Payload Type** to the RTP payload type required by the AT&T IP Toll Free service (e.g. **100**).
- Use default for all other values.

```
add trunk-group 2                                              Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 100
       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

6.8. Public Unknown Numbering

In the public unknown numbering form, Communication Manager local extensions are converted to AT&T Toll Free numbers (previously identified 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 the Communication Manager extension (e.g. **40001**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g. **2**).
- **CPN Prefix** – Enter the corresponding AT&T P Toll Free number (e.g. **7325554050**).
- **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 Toll Free 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  40001         2         7325554050    10         Total Administered: 3
 5  40002         2         7325554051    10            Maximum Entries: 9999
 5  41001         2         7325554052    10
```

6.9. Private Numbering

The private-numbering form is used to direct calls to Avaya SIP phones and calls to Modular Messaging (call coverage/retrieval) to the "local trunk defined in **Section 6.7.2**.

Step 1 - Using the **change private-unknown-numbering 0** command, enter the Modular Messaging pilot number 46000.

- **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. **46000**).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. **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g. **5**).

Step 2 – Repeat **Step 1** to direct calls to Avaya SIP phones (the Communication Manager extension range 41xxx was used for SIP phones) to the "local" trunk.

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. **5**).
- **Ext Code –** Enter the Avaya SIP phone extension range (e.g. **41**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g. **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g. **5**).

```
change private-numbering 0                                       Page   1 of   2

                           NUMBERING - PRIVATE FORMAT

Ext Ext            Trk        Private           Total
Len Code           Grp(s)     Prefix            Len
 5  46000          1                            5     Total Administered: 2
 5  41             1                            5       Maximum Entries: 540
```

6.10. Route Patterns

The AT&T IP Toll Free service does not support outbound dialing, so a route pattern is not required to direct calls to the "public" trunk. However a route pattern is used to direct calls to the "local" trunk.

6.10.1. Route Pattern for Modular Messaging and Avaya SIP Phones

This form defines the "local" SIP trunk, based on the route-pattern selected by the AAR table in **Section 6.11** (e.g. calls to the Modular messaging pilot number 46000 or calls to Avaya SIP phones 41xxx).

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

- In the **Grp No** column enter **1** for SIP trunk 1 ("local" trunk).
- In the **FRL** column enter **0** (zero).

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name:
                             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: 1    0                                                            n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user
    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
   0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                        next
 2: y y y y y n  n            rest                                        none
 3: y y y y y n  n            rest                                        none
 4: y y y y y n  n            rest                                        none
 5: y y y y y n  n            rest                                        none
 6: y y y y y n  n            rest                                        none
```

6.11. AAR Dialing

Automatic Alternate Routing (AAR) is used to direct coverage calls for Modular Messaging (46000) or calls to the Avaya SIP phones (41xxx) to the route pattern defined in **Section 6.10**.

Step 1 – Enter the **change aar analysis 0** command and for the SIP phone extensions enter the following:

- **Dialed String** enter **41**
- **Min** & **Max** enter **5**
- **Route Pattern** enter **1**
- **Call Type** enter **aar**

Step 2 – For the Modular Messaging coverage hunt group extension enter the following:

- **Dialed String** enter **46000**

- **Min** & **Max** enter **5**
- **Route Pattern** enter **1**
- **Call Type** enter **aar**

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1
          Dialed            Total      Route     Call    Node  ANI
          String           Min  Max  Pattern     Type    Num   Reqd
    41                     5    5       1        aar            n
    46000                  5    5       1        aar            n
```

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. **46000**), as well as a coverage path that is defined to the various stations

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**), and on **Page 1** of the form enter the following:

- **Group Name** – Enter a descriptive name (e.g. **MM**).
- **Group Extension** – Enter an available extension (e.g. **46000**). 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: 46000                            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. **46000**).
- **Voice Mail Handle** - Enter the Modular Messaging pilot number (e.g. **46000**).
- **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)
         46000                     46000                       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**), and on **Page 1** of the form enter the following:

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

```
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:
  Point5:                        Point6:
```

6.12.3. Station Coverage Path to Modular Messaging

The coverage path configured in the previous section is then defined on the stations.

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

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

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

     WARNING:  Agent must log in again before changes take effect
```

6.13. Call Center Provisioning

The administration of Communication Manager Call Center elements – agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult [6] and [7] for further details if necessary. The samples that follow are provided for reference purposes only.

- Agent form – page 1

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

- Agent form – page 2

```
display agent-loginID 47002                                          Page   2 of   3
                                   AGENT LOGINID
      Direct Agent Skill:                                      Service Objective? n
Call Handling Preference: skill-level                      Local Call Preference? n
    SN   RL SL          SN   RL SL          SN   RL SL          SN   RL SL
 1: 2       1       16:                 31:                 46:
 2:                 17:                 32:                 47:
```

- Skill 2 Hunt Group form – page 1

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

- Skill 2 VDN form – page 1

```
display vdn 44002                                                    Page   1 of   3
                             VECTOR DIRECTORY NUMBER

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

- Skill 2 Vector form – page 1

```
display vector 2                                               Page   1 of   6
                                  CALL VECTOR

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

7. Avaya 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 server subscribers in multiple locations. The administration for Modular Messaging is beyond the scope of these Application Notes. Consult [8] and [9] for further details.

8. Configure Acme Packet SBC[6]

These Application Notes assume that basic Acme Packet SBC administration has already been performed. In the reference configuration two Acme Packet SBCs are implemented in a High Availability (HA) configuration. The Acme Packet SBC configuration used in the reference configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Consult with Acme Packet Support [9] for further details and explanations on the configuration below.

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

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

8.1. Local Policies

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

```
local-policy
      from-address
                               *
      to-address
                               *
      source-realm
                               INSIDE
      description
      activate-time            N/A
      deactivate-time          N/A
      state                    enabled
      policy-priority          none

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

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

```
local-policy
      from-address
                               *
      to-address
                               *
      source-realm
                               OUTSIDE
      description
      activate-time            N/A
      deactivate-time          N/A
      state                    enabled
      policy-priority          none
```

```
policy-attribute
      next-hop                      SAG:ENTERPRISE
      realm                         INSIDE
      action                        none
      terminate-recursion           disabled
      carrier
      start-time                    0000
      end-time                      2400
      days-of-week                  U-S
      cost                          0
      app-protocol                  SIP
      state                         enabled
      methods
      media-profiles
```

8.2. Network Interfaces

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

```
network-interface
      name                          s0p0
      sub-port-id                   0
      description
      hostname
      ip-address                    192.168.64.130
      pri-utility-addr              192.168.64.131
      sec-utility-addr              192.168.64.132
      netmask                       255.255.255.0
      gateway                       192.168.64.1
      sec-gateway
      gw-heartbeat
            state                         disabled
            heartbeat                     0
            retry-count                   0
            retry-timeout                 1
            health-score                  0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                   11
        hip-ip-list                   192.168.64.130
      ftp-address
        icmp-address                  192.168.64.130
      snmp-address
      telnet-address
```

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

```
network-interface
```

```
name                          s0p1
sub-port-id                   0
description
hostname
ip-address                    192.168.67.130
pri-utility-addr              192.168.67.131
sec-utility-addr              192.168.67.132
netmask                       255.255.255.0
gateway                       192.168.67.1
sec-gateway
gw-heartbeat
      state                         disabled
      heartbeat                     0
      retry-count                   0
      retry-timeout                 1
      health-score                  0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout                   11
  hip-ip-list                   192.168.67.130
ftp-address                   192.168.67.130
  icmp-address                  192.168.67.130
snmp-address
telnet-address
```

8.3. Realms

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

```
realm-config
      identifier                    OUTSIDE
      description
      addr-prefix                   0.0.0.0
      network-interfaces
                                    s0p0:0
      mm-in-realm                   enabled
      mm-in-network                 enabled
      mm-same-ip                    enabled
      mm-in-system                  enabled
      bw-cac-non-mm                 disabled
      msm-release                   disabled
      generate-UDP-checksum         disabled
      max-bandwidth                 0
      fallback-bandwidth            0
      max-priority-bandwidth        0
      max-latency                   0
      max-jitter                    0
      max-packet-loss               0
      observ-window-size            0
      parent-realm
```

```
    dns-realm
    media-policy
    in-translationid
    out-translationid
    in-manipulationid
    out-manipulationid              NAT_IP
    manipulation-string
    class-profile
    average-rate-limit              0
    access-control-trust-level      medium
    invalid-signal-threshold        4
    maximum-signal-threshold        3000
    untrusted-signal-threshold      10
    nat-trust-threshold             0
    deny-period                     60
    ext-policy-svr
    symmetric-latching              disabled
    pai-strip                       disabled
    trunk-context
    early-media-allow
    enforcement-profile
    additional-prefixes
    restricted-latching             none
    restriction-mask                32
    accounting-enable               enabled
    user-cac-mode                   none
    user-cac-bandwidth              0
    user-cac-sessions               0
    icmp-detect-multiplier          0
    icmp-advertisement-interval     0
    icmp-target-ip
    monthly-minutes                 0
    net-management-control          disabled
    delay-media-update              disabled
    refer-call-transfer             disabled
    codec-policy
    codec-manip-in-realm            disabled
    constraint-name
    call-recording-server-id
    stun-enable                     disabled
    stun-server-ip                  0.0.0.0
    stun-server-port                3478
    stun-changed-ip                 0.0.0.0
    stun-changed-port               3479
    match-media-profiles
    qos-constraint
```

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

```
realm-config
    identifier                      INSIDE
    description
```



```
addr-prefix                    0.0.0.0
network-interfaces
                               s0p1:0
mm-in-realm                    enabled
mm-in-network                  enabled
mm-same-ip                     enabled
mm-in-system                   enabled
bw-cac-non-mm                  disabled
msm-release                    disabled
generate-UDP-checksum          disabled
max-bandwidth                  0
fallback-bandwidth             0
max-priority-bandwidth         0
max-latency                    0
max-jitter                     0
max-packet-loss                0
observ-window-size             0
parent-realm
dns-realm
media-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
class-profile
average-rate-limit             0
access-control-trust-level     high
invalid-signal-threshold       0
maximum-signal-threshold       0
untrusted-signal-threshold     0
nat-trust-threshold            0
deny-period                    30
ext-policy-svr
symmetric-latching             disabled
pai-strip                      disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching            none
restriction-mask               32
accounting-enable              enabled
user-cac-mode                  none
user-cac-bandwidth             0
user-cac-sessions              0
icmp-detect-multiplier         0
icmp-advertisement-interval    0
icmp-target-ip
monthly-minutes                0
net-management-control         disabled
delay-media-update             disabled
refer-call-transfer            disabled
codec-policy
```

```
codec-manip-in-realm           disabled
constraint-name
call-recording-server-id
stun-enable                    disabled
stun-server-ip                 0.0.0.0
stun-server-port               3478
stun-changed-ip                0.0.0.0
stun-changed-port              3479
match-media-profiles
qos-constraint
```

8.4. Session Agents

ANNOTATION: The **session agent** below represents the AT&T IP Toll Free service network border element. The Acme will attempt to send calls to the border element based on successful responses to the OPTIONS "ping-method". The AT&T IP Toll Free service border element is also specified in the **session-group** section below. Redundant network session-agents may be defined (see **Addendum 1**).

NOTE – The ***ping-method OPTIONS;hops=20*** parameter shown below was a setting used in the reference test environment. Acme Packet best practices recommends a setting of ***OPTIONS;hops=0*** in customer deployments.

```
session-agent
      hostname                       135.25.29.74
      ip-address                     135.25.29.74
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       OUTSIDE
      egress-realm-id
      description                    AT&T_BE
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
```

```
    proxy-mode
    redirect-action
    loose-routing                  enabled
    send-media-session             enabled
    response-map
    ping-method                    OPTIONS;hops=20
    ping-interval                  60
    ping-send-mode                 keep-alive
    ping-in-service-response-codes
    out-service-response-codes
    media-profiles
    in-translationid
    out-translationid
    trust-me                       disabled
    request-uri-headers
    stop-recurse
    local-response-map
    ping-to-user-part
    ping-from-user-part
    li-trust-me                    disabled
    in-manipulationid
    out-manipulationid
    manipulation-string
    p-asserted-id
    trunk-group
    max-register-sustain-rate      0
    early-media-allow
    invalidate-registrations       disabled
    rfc2833-mode                   none
    rfc2833-payload                0
    codec-policy
    enforcement-profile
    refer-call-transfer            disabled
    reuse-connections              NONE
    tcp-keepalive                  none
    tcp-reconn-interval            0
    max-register-burst-rate        0
    register-burst-window          0
```

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

```
session-agent
    hostname                       192.168.67.210
    ip-address                     192.168.67.210
    port                           5060
    state                          enabled
    app-protocol                   SIP
    app-type
    transport-method               staticTCP
    realm-id                       INSIDE
    egress-realm-id
    description                    Session Manager_6_1
```

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

```
tcp-keepalive                  none
tcp-reconn-interval            0
max-register-burst-rate        0
register-burst-window          0
```

8.5. Session Groups

ANNOTATION: The **session group** below specifies the AT&T IP Toll Free service border element (see **session-agent 135.25.29.74** above). This session-group is specified in the local-policy with source-realm IN**SIDE.**

Note - Multiple session-agents may be specified in a session-group. The *strategy* parameter may be used to select how these multiple session-agents are used (e.g. *Hunt* and *RoundRobin*). See **Addendum 1** for an example of redundant session agents.

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

ANNOTATION: The session group below represents Avaya Session Manager(see **session-agent 192.168.67.210** above). This session-group is specified in the local-policy with source-realm **OUTSIDE.**

```
session-group
      group-name                     ENTERPRISE
      description
      state                          enabled
      app-protocol                   SIP
      strategy                       Hunt
      dest
                                     192.168.67.210
      trunk-group
      sag-recursion                  disabled
      stop-sag-recurse               401,407
```

8.6. SIP Configuration

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

```
sip-config
      state                          enabled
      operation-mode                 dialog
```

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

8.7. SIP Interfaces

ANNOTATION: The SIP interface below is used to communicate with the AT&T IP Toll Free service, and specifies the "**OUTSIDE**" realm. Note that the connection between the Acme SBC and the AT&T border element uses UDP.

```
sip-interface
      state                          enabled
      realm-id                       OUTSIDE
      description
      sip-port
            address                        192.168.64.130
            port                           5060
            transport-protocol             UDP
            tls-profile
            allow-anonymous                agents-only
            ims-aka-profile
```

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

```
     add-sdp-invite                 disabled
     add-sdp-profiles
```

ANNOTATION: The SIP interface below is used to communicate with the Avaya elements and references the "**INSIDE**" realm. Note that TCP is used between the Acme SBC and Session Manager. See the note in **Section 5.5** regarding the use of TCP and TLS.

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

```
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
refer-call-transfer            disabled
route-unauthorized-calls
tcp-keepalive                  none
add-sdp-invite                 disabled
add-sdp-profiles
```

8.8. SIP Manipulations

ANNOTATION: The **NAT_IP** sip-manipulation below performs address translation and topology hiding for SIP messages between the AT&T IP Toll Free services and the Avaya elements. The NAT function is comprised of the header rules **manipFrom** and **manipTo.**

In the header-rule **manipFrom** the Acme will convert this value to the "outside" IP address of the Acme (**$Local_IP**). In the header-rule **manipTo,** the Acme will convert this value to the IP address of the AT&T IP Toll Free border element (**$Remote_IP**).

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

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

ANNOTATION: OPTIONAL – The Acme may be used to remove unnecessary SIP headers before they are passed to AT&T. In the reference configuration the following headers were removed – P-Site, P-Location, and Alert-Info. Since there is no value in sending these headers to AT&T, and they only increase the overall packet size, the headers are removed by the Acme. Calls can still be completed successfully if the configuration in this section is not performed. This information is included to allow the reader to delete the headers if desired.

```
header-rule
            name                           deletePSITE
            header-name                    P-Site
            action                         delete
            comparison-type                pattern-rule
            msg-type                       request
            methods
            match-value
            new-value
header-rule
            name                           deletePlocation
            header-name                    P-Location
            action                         delete
            comparison-type                pattern-rule
            msg-type                       any
            methods
            match-value
            new-value
header-rule
            name                           deleteAlertInfo
            header-name                    Alert-Info
            action                         delete
            comparison-type                pattern-rule
```

```
            msg-type                         request
            methods
            match-value
            new-value
```

ANNOTATION: Avaya Communication Manager will insert a plus (+) into calling number strings. These leading plus signs may cause issue to the AT&T IP Toll Free service. The Acme may be used to remove the plus signs before they are passed to AT&T. In the reference configuration the following headers were monitored to remove any plus signs – PAI, Contact, From, and Update.

```
header-rule
            name                             modPAIPlus
            header-name                      P-Asserted-Identity
            action                           manipulate
            comparison-type                  pattern-rule
            msg-type                         any
            methods                          INVITE
            match-value
            new-value
            element-rule
                  name                             modVal
                  parameter-name
                  type                             uri-user
                  action                           find-replace-all
                  match-val-type                   any
                  comparison-type                  case-sensitive
                  match-value                      \+(.*)
                  new-value                        $modPAI.$modVal.$1
header-rule
            name                             modContactPlus
            header-name                      Contact
            action                           manipulate
            comparison-type                  pattern-rule
            msg-type                         any
            methods                          INVITE
            match-value
            new-value
            element-rule
                  name                             modVal
                  parameter-name
                  type                             uri-user
                  action                           find-replace-all
                  match-val-type                   any
                  comparison-type                  case-sensitive
                  match-value                      \+(.*)
                  new-value                        $modContact.$modVal.$1
header-rule
            name                             modFromPlus
            header-name                      From
            action                           manipulate
            comparison-type                  pattern-rule
            msg-type                         any
```

```
            methods                          INVITE
            match-value
            new-value
            element-rule
                  name                             modVal
                  parameter-name
                  type                             uri-user
                  action                           find-replace-all
                  match-val-type                   any
                  comparison-type                  case-sensitive
                  match-value                      \+(.*)
                  new-value                        $modFrom.$modVal.$1
header-rule
            name                             modUpdatePlus
            header-name                      Update
            action                           manipulate
            comparison-type                  pattern-rule
            msg-type                         any
            methods
            match-value
            new-value
            element-rule
                  name                             modVal
                  parameter-name
                  type                             uri-user
                  action                           find-replace-all
                  match-val-type                   any
                  comparison-type                  case-sensitive
                  match-value                      \+(.*)
                  new-value                        $modUpdate.$modVal.$1
```

ANNOTATION: The **Mod_Inbound** sip-manipulation below modifies the To header to the local domain (customerb.com) instead of Acme outside address (192.168.67.130), and modify the From header from AT&T BE address (135.25.29.74) to Acme inside address (192.168.67.130).

- **sip-manipulation**

```
      name                             Mod_Inbound
      description
      split-headers
      join-headers

            header-rule
                  name                             Inbound_To
                  header-name                      To
                  action                           manipulate
                  comparison-type                  case-sensitive
                  msg-type                         request
                  methods
                  match-value
```

```
            new-value
            element-rule
                  name                              To
                  parameter-name
                  type                              uri-host
                  action                            replace
                  match-val-type                    any
                  comparison-type                   case-sensitive
                  match-value                       192.168.64.130
                  new-value                         customerb.com
      header-rule
            name                              Inbound_From
            header-name                       From
            action                            manipulate
            comparison-type                   case-sensitive
            msg-type                          request
            methods
            match-value
            new-value
            element-rule
                  name                              From
                  parameter-name
                  type                              uri-host
                  action                            replace
                  match-val-type                    any
                  comparison-type                   case-sensitive
                  match-value
                  new-value                         $LOCAL_IP
```

8.9. Steering Pools

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

```
steering-pool
      ip-address                        192.168.64.130
      start-port                        16384
      end-port                          32767
      realm-id                          OUTSIDE
      network-interface

steering-pool
      ip-address                        192.168.67.130
      start-port                        16384
      end-port                          32767
      realm-id                          INSIDE
      network-interface
```

8.10. Additional Acme Provisioning

The following Acme configuration parameters were part of the initial Acme installation provisioning and not specifically for interoperability with the AT&T IP Toll Free service. The parameters are included here as a reference.

```
media-manager
      state                          enabled
      latching                       enabled
      flow-time-limit                86400
      initial-guard-timer            300
      subsq-guard-timer              300
      tcp-flow-time-limit            86400
      tcp-initial-guard-timer        300
      tcp-subsq-guard-timer          300
      tcp-number-of-ports-per-flow   2
      hnt-rtcp                       disabled
      algd-log-level                 NOTICE
      mbcd-log-level                 NOTICE
      red-flow-port                  1985
      red-mgcp-port                  1986
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      media-policing                 enabled
      max-signaling-bandwidth        775880
      max-untrusted-signaling        80
      min-untrusted-signaling        20
      app-signaling-bandwidth        0
      tolerance-window               30
      rtcp-rate-limit                0
      min-media-allocation           2000
      min-trusted-allocation         4000
      deny-allocation                64000
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      dnsalg-server-failover         disabled

network-interface
      name                           wancom1
      sub-port-id                    0
      description
      hostname
      ip-address
      pri-utility-addr               169.254.1.1
      sec-utility-addr               169.254.1.2
      netmask                        255.255.255.252
      gateway
```

```
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list
      ftp-address
        icmp-address
      snmp-address
      telnet-address

network-interface
      name                           wancom2
      sub-port-id                    0
      description
      hostname
      ip-address
      pri-utility-addr               169.254.2.1
      sec-utility-addr               169.254.2.2
      netmask                        255.255.255.252
      gateway
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list
      ftp-address
        icmp-address
      snmp-address
      telnet-address

ntp-config
      server                         135.8.139.1

phy-interface
      name                           s0p1
      operation-type                 Media
      port                           1
      slot                           0
```

```
        virtual-mac                    00:08:25:a0:f3:69
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100

phy-interface
        name                           s0p0
        operation-type                 Media
        port                           0
        slot                           0
        virtual-mac                    00:08:25:a0:f3:68
        admin-state                    enabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100

phy-interface
        name                           s1p0
        operation-type                 Media
        port                           0
        slot                           1
        virtual-mac                    00:08:25:a0:f3:6e
        admin-state                    disabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100

phy-interface
        name                           s1p1
        operation-type                 Media
        port                           1
        slot                           1
        virtual-mac                    00:08:25:a0:f3:6f
        admin-state                    disabled
        auto-negotiation               enabled
        duplex-mode                    FULL
        speed                          100

phy-interface
        name                           wancom1
        operation-type                 Control
        port                           1
        slot                           0
        virtual-mac
        wancom-health-score            8

phy-interface
        name                           wancom2
        operation-type                 Control
        port                           2
        slot                           0
        virtual-mac
        wancom-health-score            9
```

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

sip-feature
      name                          Replaces
      realm
      support-mode-inbound          Pass
      require-mode-inbound          Pass
      proxy-require-mode-inbound    Pass
      support-mode-outbound         Pass
      require-mode-outbound         Pass
      proxy-require-mode-outbound   Pass

system-config
      hostname                      acmesbc
```

```
description
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled                   enabled
enable-snmp-auth-traps         disabled
enable-snmp-syslog-notify      disabled
enable-snmp-monitor-traps      disabled
enable-env-monitor-traps       disabled
snmp-syslog-his-table-length   1
snmp-syslog-level              WARNING
system-log-level               WARNING
process-log-level              NOTICE
process-log-ip-address         0.0.0.0
process-log-port               0
collect
      sample-interval                5
      push-interval                  15
      boot-state                     disabled
      start-time                     now
      end-time                       never
      red-collect-state              disabled
      red-max-trans                  1000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      push-success-trap-state        disabled
call-trace                     disabled
internal-trace                 disabled
log-filter                     all
default-gateway                135.8.139.1
restart                        enabled
exceptions
telnet-timeout                 0
console-timeout                0
remote-control                 enabled
cli-audit-trail                enabled
link-redundancy-state          disabled
source-routing                 enabled
cli-more                       disabled
terminal-height                24
debug-timeout                  0
trap-event-lifetime            0
```

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 [3] for more information.

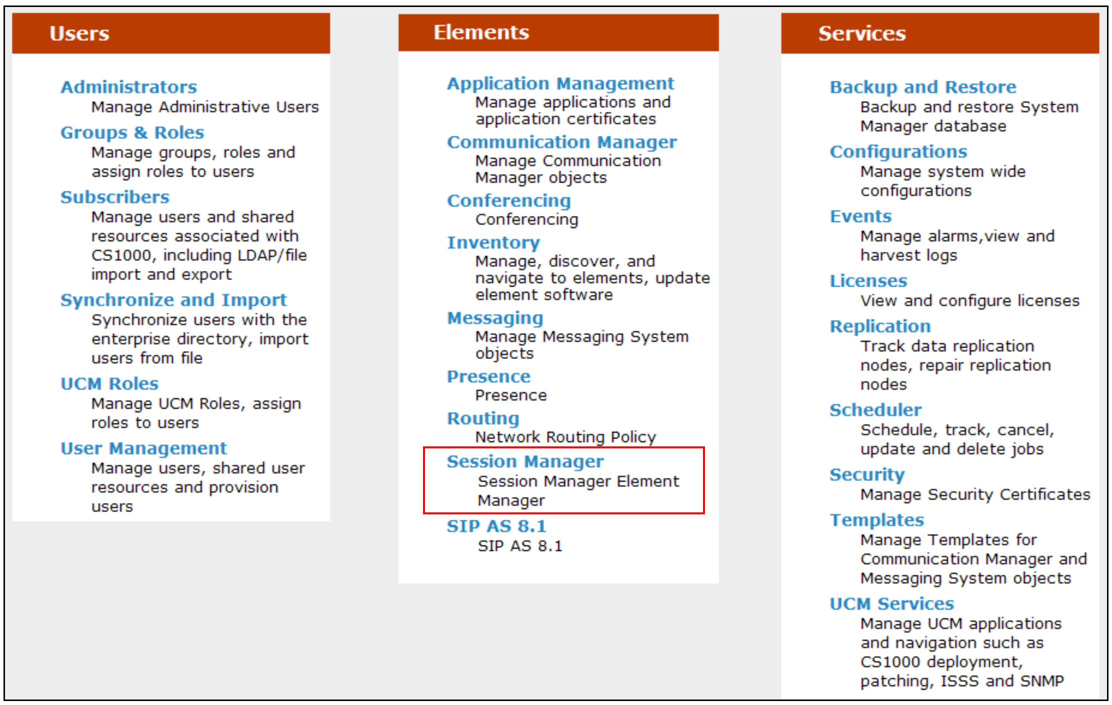
1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where xxx is a trunk access code defined for the SIP trunk to AT&T (e.g. 101). Note that in the trace below Session Manager has already converted the AT&T digits sent in the Request URI, to the Communication Manager extension 40002, before sending the INVITE to Communication Manager.

```
list trace tac 101                                   Page   1

                        LIST TRACE

time          data

10:50:35 TRACE STARTED 07/19/2010 CM Release String cold-00.0.345.0-18246
10:50:49 SIP<INVITE sip:40002@customerb.com:5060;transport=tcp S
10:50:49 SIP<IP/2.0
10:50:49     active trunk-group 1 member 1  cid 0x270
10:50:49 SIP>SIP/2.0 183 Session Progress
10:50:49     dial 40002
10:50:49     ring station    40002 cid 0x270
10:50:49     G711MU ss:off ps:20
          rgn:1 [192.168.67.80]:17382
          rgn:1 [192.168.67.203]:16390
10:50:49     G729B ss:off ps:20
          rgn:2 [192.168.67.130]:16480
          rgn:1 [192.168.67.203]:16386
10:50:49     xoip options: fax:T38 modem:off tty:US  uid:0x50001
          xoip ip: [192.168.67.203]:16386
10:50:50 SIP>SIP/2.0 200 OK
10:50:50     active station    40002 cid 0x270
10:50:50 SIP<ACK sip:7323204384@192.168.67.202;transport=tcp SIP
10:50:50 SIP</2.0
10:50:50 SIP>INVITE sip:7326712438@192.168.67.130:5060;transport
10:50:50 SIP>=tcp SIP/2.0
10:50:50 SIP<SIP/2.0 100 Trying
10:50:51 SIP<SIP/2.0 200 OK
10:50:51 SIP>ACK sip:7326712438@192.168.67.130:5060;transport=tc
10:50:51 SIP>p SIP/2.0
10:50:51     G729AB ss:off ps:20
          rgn:2 [192.168.67.130]:16480
          rgn:1 [192.168.67.80]:17382
10:50:51     G729B ss:off ps:20
          rgn:1 [192.168.67.80]:17382
          rgn:2 [192.168.67.130]:16480
10:50:54 SIP>BYE sip:7326712438@192.168.67.130:5060;transport=tc
10:50:54 SIP>p SIP/2.0
10:50:54     idle station    40002 cid 0x270
```

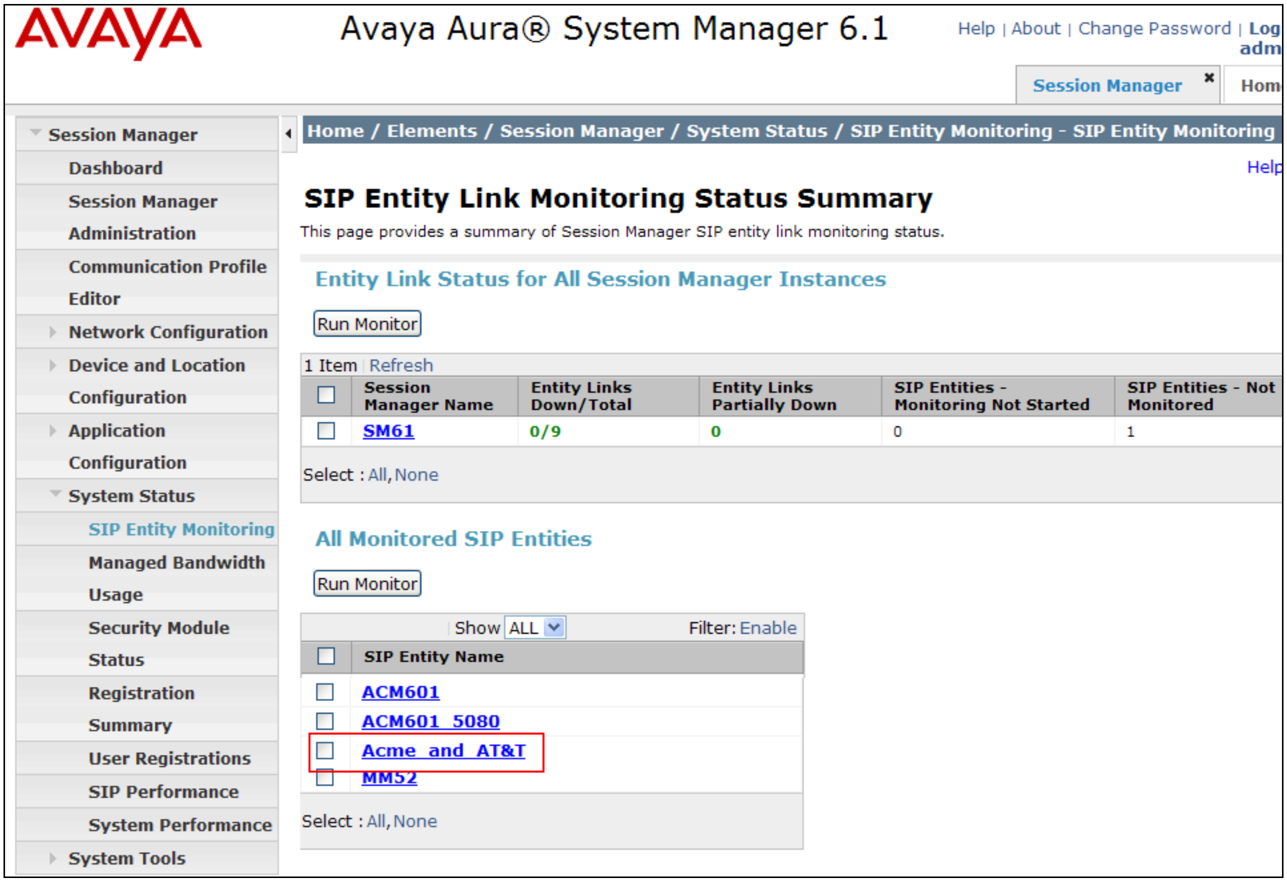
2. Similar Communication Manager commands are, ***list trace station***, ***list trace vdn***, and ***list trace vector***. Other useful commands are ***status trunk*** and ***status station***.

9.3. Avaya Aura® Session Manager

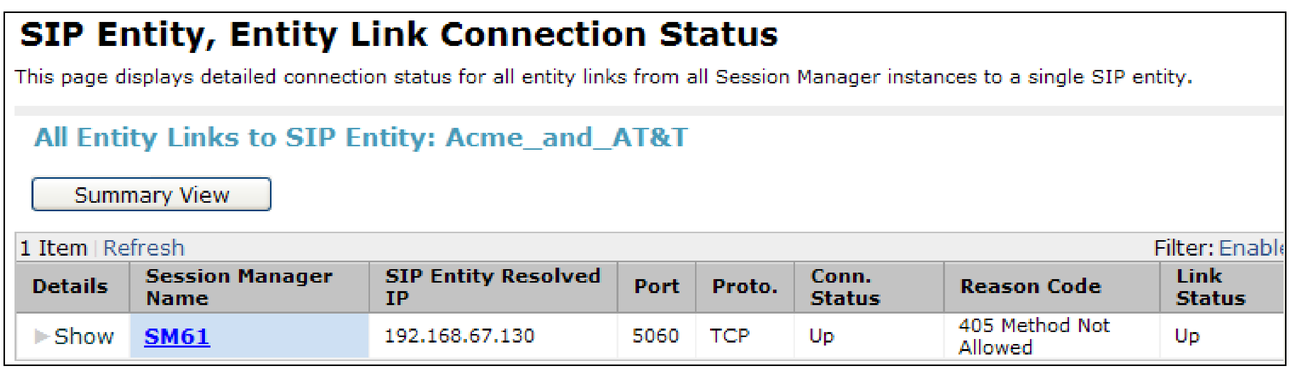
Step 1 - Access the System Manager GUI, using the URL "**http://<ip-address>/SMGR**", where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. Once logged in, the **Home** screen is displayed. Under the **Elements** heading in the center, select **Session Manager**.



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



Step – 3 From the list of monitored entities, select an entity of interest, such as **Acme_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 405 message (normal for the AT&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 Toll Free service. Note that the Request URI called number was 0000001050 and Session Manager converts this to Communication Manager extension 41006 before routing the call to Communication Manager

Step 1 – **Called Party URI** field = the information passed in the Request URI sent by the Acme SBC (e.g. **0000001050@customerb.com**)

Step 2 – **Calling Party Address** field = the IP address of the inside interface of the Acme (e.g. **192.168.67.130**).

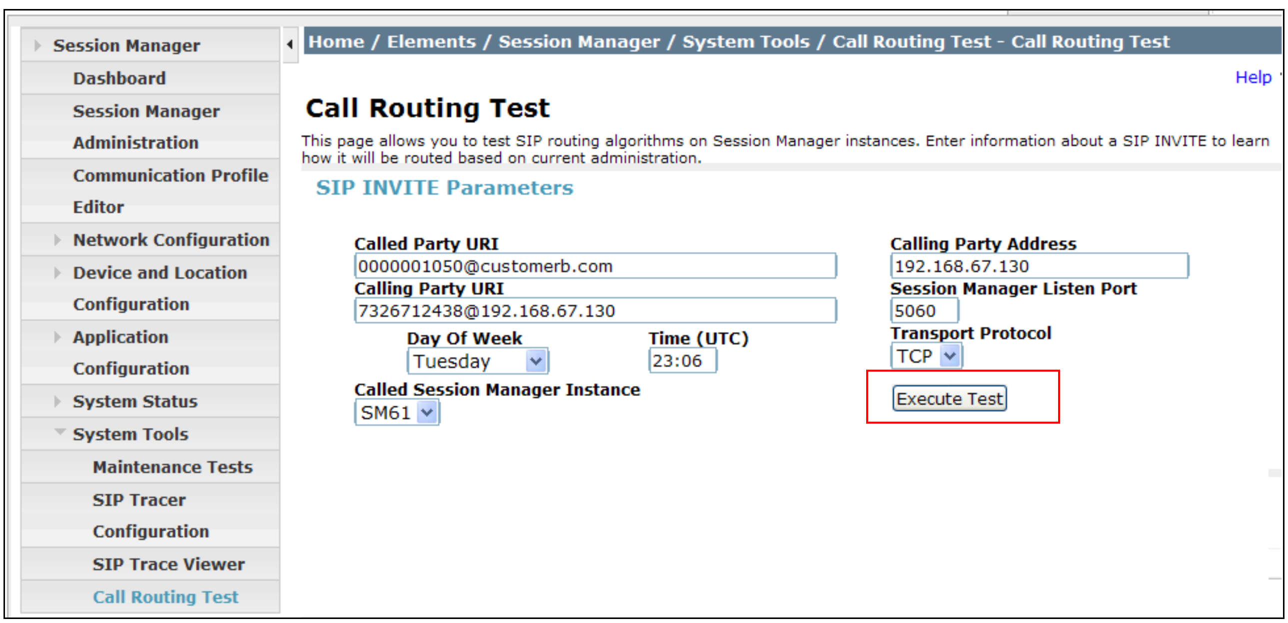
Step 3 – **Calling Party URI** field = The contents of the From header (e.g. **7326712438@192.168.67.130**).

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

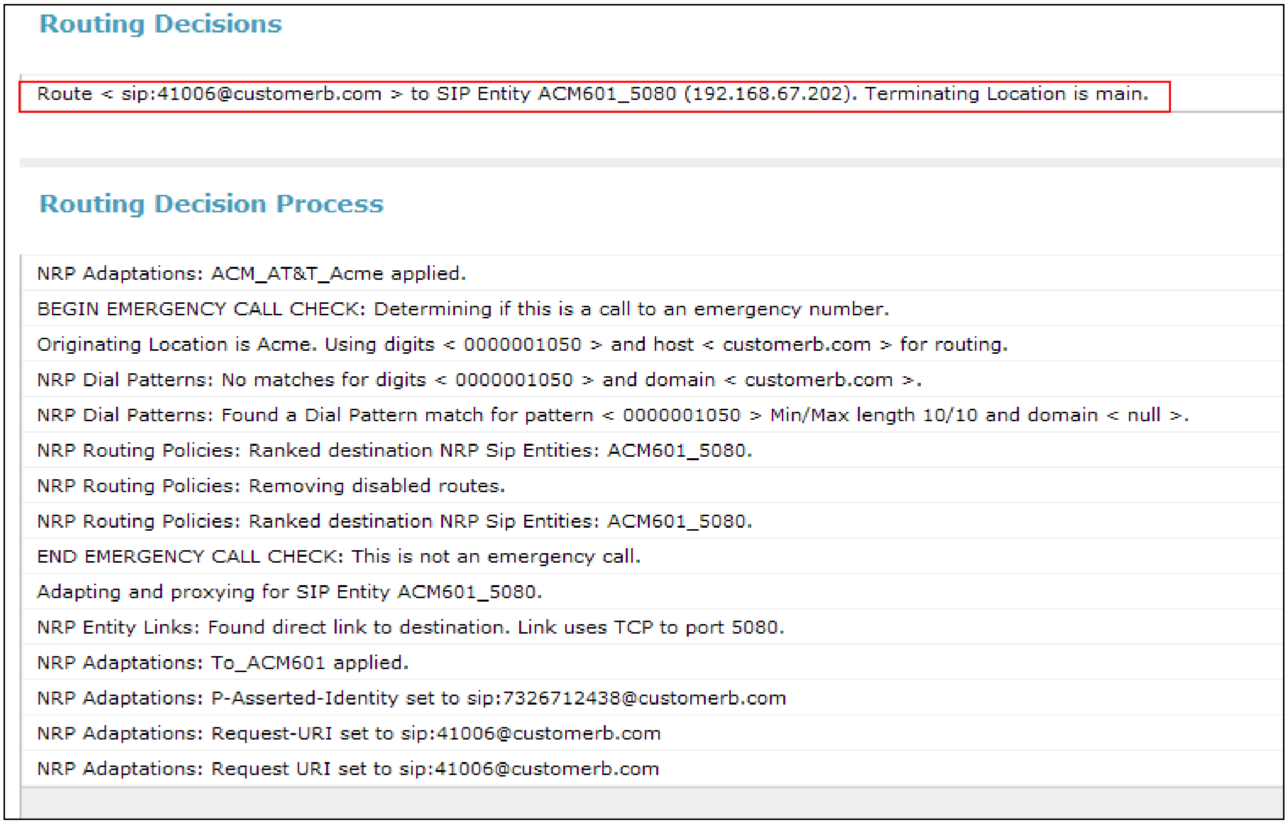
Step 5 – Populate the **Day of Week** and **Time (UTC)** fields, or let them default to current.

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

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



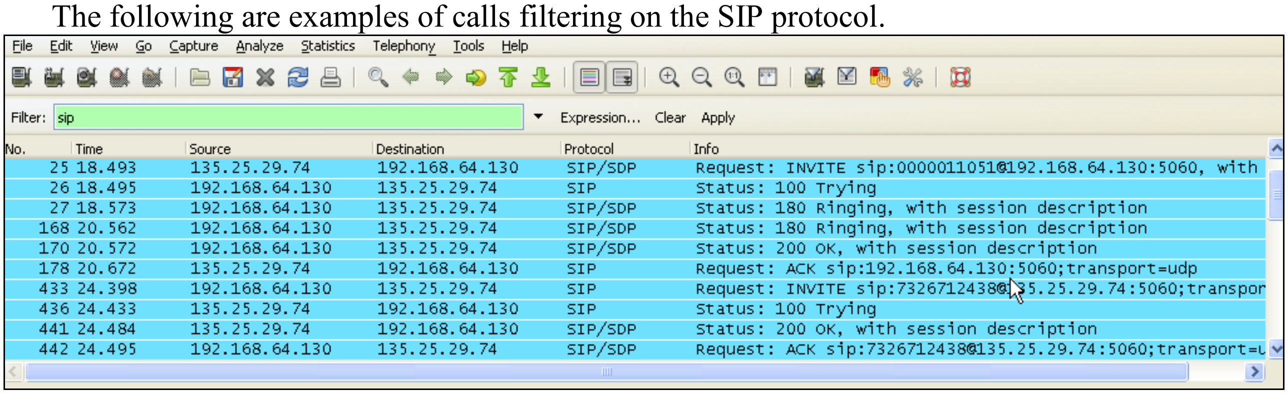
The results of the test are shown below**.** The ultimate routing decision is displayed under the heading **Routing Decisions.** The example shows that a PSTN call to AT&T IP Toll Free service, delivering 0000001050 in the Request URI, is sent to Communication Manager extension **41006**. Further down, 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**.



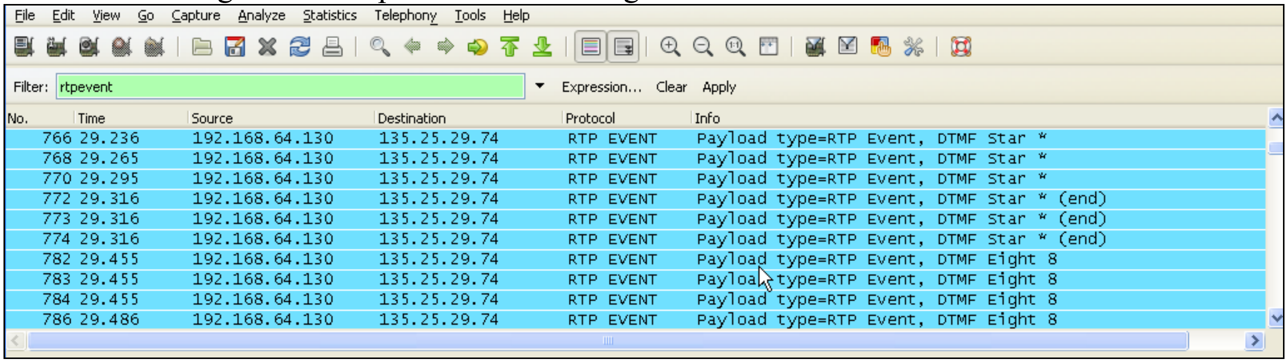
9.4. Protocol Traces

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

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

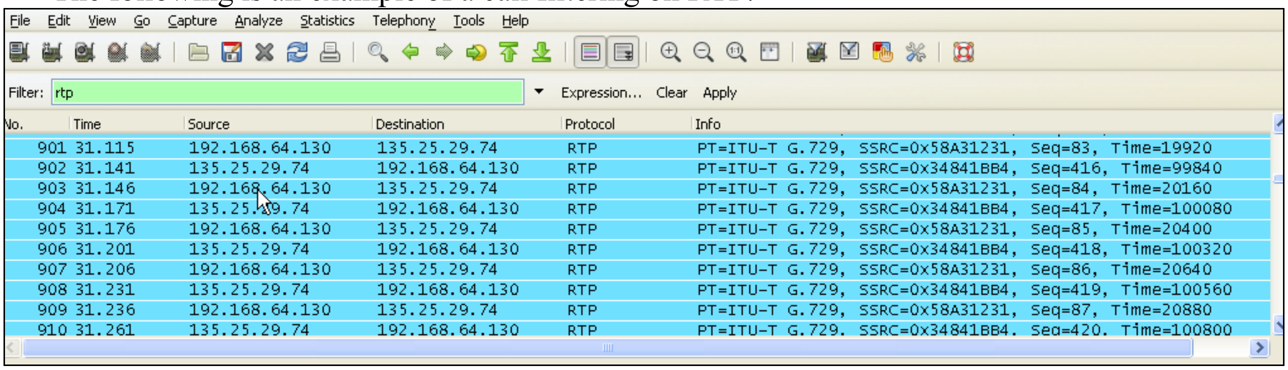


The following is an example of a call filtering on DTMF.



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

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



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

9.5. Acme Packet SBC

The Acme Packet SBC provisioning can be checked by entering the command "***verify-config***". Acme maintenance manuals may be found at [10]

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Acme Packet Net-Net can be configured to interoperate successfully with the AT&T IP Toll Free service. This solution provides users of Avaya Aura® Communication Manager the ability to support inbound toll free calls over an AT&T IP Toll Free SIP trunk service connection.

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

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

11. References

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

[1] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Issue 4, May 2011
[2] Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Issue 2.2, April 2011
[3] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, Issue 4.1, March 2011
[4] Administering Avaya Aura® System Manager 6.1, November 2010
[5] Administering Avaya Aura® Communication Manager, Release 6.0, Doc ID 03-300509, Issue 6.0, June 2010
[6] *Administering Avaya Aura® Call Center Features*, Release 6.0, November 2010
[7] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010
[8] *Modular Messaging Multi-Site Guide Release 5.2*, October 2010
[9] *Modular Messaging Messaging Application Server (MAS) Administration Guide,* July 2011

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

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

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

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

Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, and building on the configuration shown in **Section 8**, the Acme Packet Net-Net SBC is provisioned as follows.

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

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

```
        response-map
        ping-method                     OPTIONS;hops=20
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0


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

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

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

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

ANNOTATION: - The following header-rule is added to the "**NAT_IP**" sip-manipulation shown in **Section 8.8.** This header-rule inserts the IP address of the AT&T BE being used for the call (determined by the session-group above) into the SIP Request-URI header.

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

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.