



Avaya Solution & Interoperability Test Lab

Applications Notes for Avaya Aura® Communication Manager 6.0, Avaya Aura® Session Manager 6.0 and Acme Packet Net-Net Session Director 6.1.0 with AT&T IP Toll Free SIP Trunk Service – Issue 1.2

Abstract

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

Avaya Aura® Session Manager 6.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.0 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 Session Director (SD) 6.1.0 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. Avaya Aura® Session Manager and Avaya Aura® Communication Manager interaction with the AT&T IP Transfer Connect service option will be addressed in separate Application Notes.

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

TABLE OF CONTENTS

1.	Introduction.....	4
1.1.	Interoperability Compliance Testing	4
1.2.	Support.....	4
1.3.	Known Limitations	5
2.	Reference Configuration.....	5
2.1.	Illustrative Configuration Information.....	8
2.2.	Call Flows	9
3.	Equipment and Software Validated	11
4.	Avaya Aura® Session Manager.....	12
4.1.	Background	12
4.2.	Routing Policies	12
4.3.	SIP Domains	14
4.4.	Locations.....	15
4.5.	Adaptations	16
4.5.1.	Adaptation for calls for Avaya Aura® Communication Manager.....	17
4.5.2.	Adaptation for Avaya Modular Messaging.....	18
4.6.	SIP Entities.....	20
4.6.1.	Avaya Aura® Session Manager SIP Entity	21
4.6.2.	Avaya Aura® Communication Manager SIP Entity	22
4.6.3.	Avaya Aura® Communication Manager SIP Entity – SIP Endpoint Calls.....	24
4.6.4.	Acme Packet SBC SIP Entity	24
4.6.5.	Avaya Modular Messaging SIP Entity	25
4.7.	Entity Links.....	26
4.7.1.	Entity Links to Avaya Aura® Communication Manager	27
4.7.2.	Avaya Aura® Communication Manager Entity Link for SIP Phones.....	27
4.7.3.	Entity Link to AT&T IP Toll Free Service via Acme Packet SBC	28
4.7.4.	Entity Link to Avaya Modular Messaging.....	29
4.8.	Time Ranges	29
4.9.	Routing Policies.....	30
4.9.1.	Routing Policy for Routing to Avaya Aura® Communication Manager	30
4.9.2.	Routing Policy for Routing to Avaya SIP Phones	32
4.9.3.	Routing Policy for Routing to Avaya Modular Messaging	33
4.10.	Dial Patterns.....	35
4.10.1.	Matching Inbound Calls to Avaya Aura® Communication Manager	35
4.10.2.	Matching Inbound Calls to Avaya Modular Messaging Pilot Number via Avaya Aura® Communication Manager.....	39
4.11.	Session Manager Administration.....	42
5.	Avaya Aura® Communication Manager	44
5.1.	System Parameters	44
5.2.	Dial Plan.....	46
5.3.	Alternate Automated Routing (AAR) Table.....	47
5.4.	IP Node Names	47
5.5.	IP Interface for procr.....	48
5.6.	G450 Media Gateway	48

5.6.1.	G450 Provisioning for Registration to Communication Manager	48
5.6.2.	Communication Manager Provisioning for the G450	49
5.7.	IP Network Regions	50
5.7.1.	IP Network Region 1 – Local Region	50
5.7.2.	IP Network Region 2 – AT&T Region	51
5.7.3.	IP Codec Parameters	52
5.8.	SIP Trunks	53
5.8.1.	SIP Trunk for AT&T IP Toll Free Access	54
5.8.2.	Local SIP Trunk (Modular Messaging and Avaya SIP Telephones)	56
5.9.	Private Numbering	59
5.10.	Public Unknown Numbering	60
5.11.	Route Patterns	60
5.11.1.	Calls from AT&T	60
5.11.2.	Calls for Modular Messaging and Avaya SIP Phones	61
5.12.	Call Center Provisioning	61
6.	Avaya Modular Messaging	63
6.1.1.	Hunt Group for Station Coverage to Modular Messaging	63
7.	Configure Acme Packet SBC	65
8.	General Test Approach and Test Results	85
9.	Verification Steps	85
9.1.	General	85
9.2.	Avaya Aura® Communication Manager	86
9.3.	Avaya Aura® Session Manager	87
9.4.	Protocol Traces	89
9.5.	Acme Packet SBC	90
10.	Conclusion	90
11.	References	91
12.	Addendum 1 – Alternate method for suppressing plus signs (“+”) in calling header fields	92
12.1.	Avaya Aura® Communication Manager provisioning	92
12.1.1.	SIP Trunk for AT&T IP Toll Free Access	92
12.1.2.	Route Pattern for Trunk to AT&T	93
12.1.3.	Private Numbering	94
12.1.4.	Public Unknown Numbering	95
12.2.	Acme Packet Net-Net Session Director	95
13.	Addendum 2 – Acme Packet Net-Net Redundancy to Multiple AT&T Border Elements ...	98

1. Introduction

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

Avaya Aura® Session Manager 6.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.0 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 Session Director (SD) 6.1.0 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 MIS/PNT¹ 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.** Avaya Aura® Session Manager and Avaya Aura® Communication Manager interaction with the AT&T IP Transfer Connect service option will be addressed in separate Application Notes.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 2.2** for examples) between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Acme Packet Net-Net Session Director, and the AT&T IP Toll Free service.

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

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

1.2. 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>. The “Connect with Avaya” section provides the worldwide support

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

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

1.3. Known Limitations

1. If Avaya Aura® Communication Manager receives an SDP offer with multiple codecs, where at least two of the codecs are supported in the codec set provisioned on Avaya Aura® Communication Manager, then Avaya Aura® Communication Manager selects a codec according to the priority order specified in the Avaya Aura® 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, G.729A, and G.711 in that order, then Avaya Aura® Communication Manager selects G.729A, not G.711. The practical resolution is to provision the Avaya Aura® Communication Manager codec set to match the expected codec priority order in AT&T IP Toll Free SDP offers.
2. G.726 codec is not supported between Avaya Aura® Communication Manager and the AT&T IP Toll Free service.
3. G.711 faxing is not supported between Avaya Aura® Communication Manager and the AT&T IP Toll Free service. Avaya Aura® Communication Manager does not support the protocol negotiation that AT&T requires to have G.711 fax calls work. T.38 faxing is supported, as is Group 3 and Super Group 3 fax. Fax speeds are limited to 9600 in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Avaya Aura® Communication Manager.
4. Shuffling must be disabled on the Avaya Aura® Communication Manager “local” SIP trunk due to codec negotiation issues with Avaya SIP telephones.
 - Note – 8/30/11 -Subsequent testing performed with Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Avaya one-X® Deskphone Edition SIP telephone firmware 2.6.4 (SIP96xx_2_6_4_0.bin) & 6.0.1 (S96x1_SALBR6_0_1_V452) did *not* encounter this issue.
5. Avaya Aura® Communication Manager 6.0 inserts a leading plus sign to calling number headers by default (e.g. Update, From, PAI, Contact). The AT&T IP Toll Free service does not support the use of digit strings with a leading plus sign (“+”) in headers containing calling numbers (Update in the case of the inbound only AT&T IP Toll Free service). The Avaya Aura® Communication Manager 6.0 provisioning described in **Section 5**, will prevent the insertion of these plus signs. The Addendum in **Section 12**, describes an alternate method, utilizing the Acme Packet Net-Net Session Director to remove the plus signs inserted by Avaya Aura® Communication Manager.

2. Reference Configuration

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

- Avaya Aura® Session Manager provides core SIP routing and integration services that enables communications between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya Aura® Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- Avaya Aura® System Manager provides a common administration interface for centralized management of all Avaya Aura® Session Manager instances in an enterprise.
- Avaya Aura® Communication Manager provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya Aura® 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 Avaya Aura® 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 4600 and 9600 Series IP Telephones running H.323 software, 9600 Series IP Telephones running SIP software, Avaya 6211 Series Analog Telephones, as well as Avaya one-X® Communicator and Avaya one-X® Agent, PC based softphones.
- The Acme Packet Net-Net Session Director (SD) 3800² provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network³. 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 Session Director to the Session Manager which routed the call to Avaya Aura® Communication Manager. Avaya Aura® Communication Manager terminated the call to the appropriate agent/phone or fax extension. The H.323 phones on the enterprise

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

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 Packet SBC and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Acme Packet SBC and Communication Manager.

side registered to the Avaya Aura® Communication Manager Procr. The SIP phones on the enterprise side registered to the Avaya Aura® Session Manager.

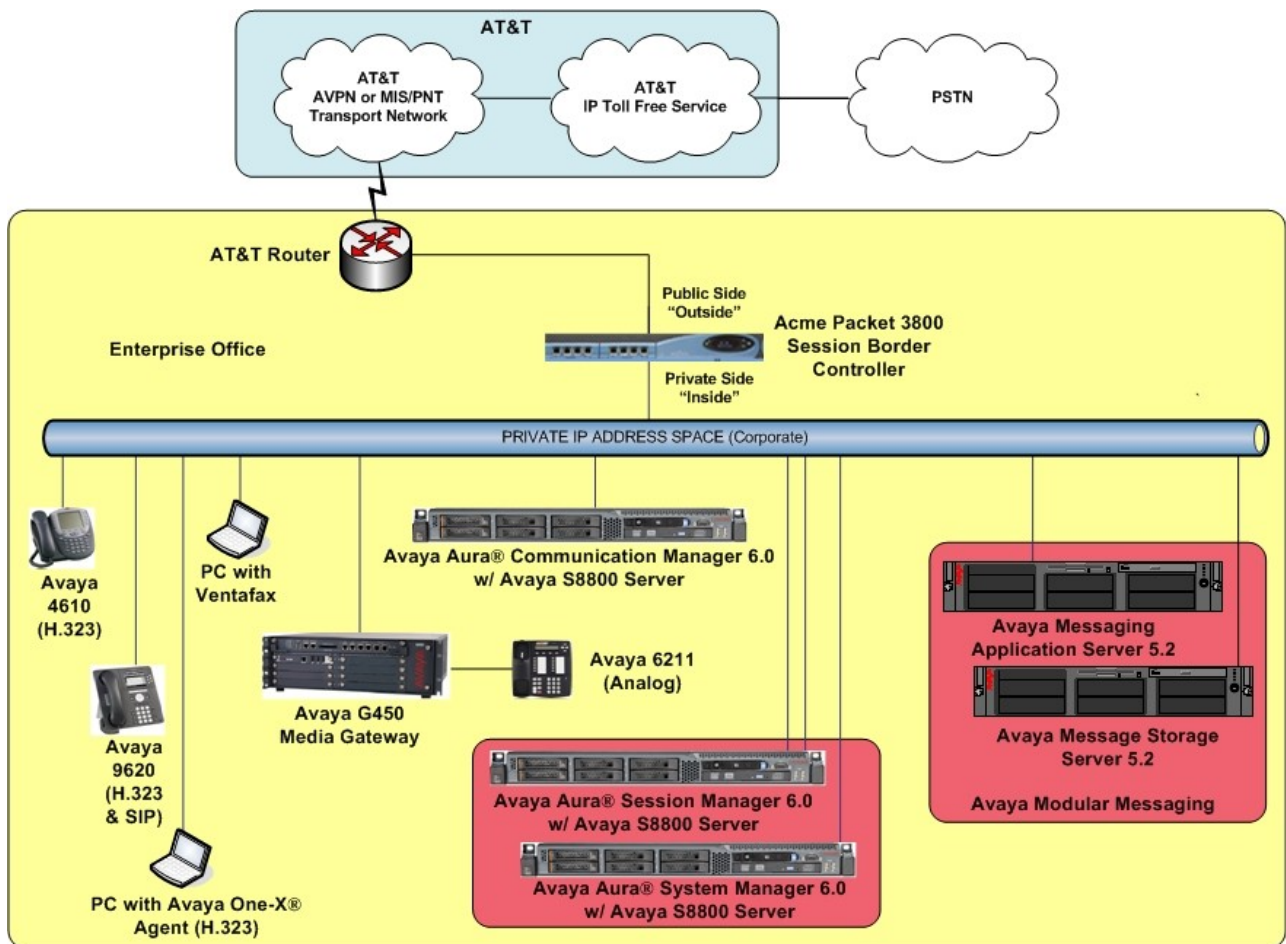


Figure 1: Reference configuration

2.1. Illustrative Configuration Information

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

Note - The AT&T IP 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

2.2. 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.

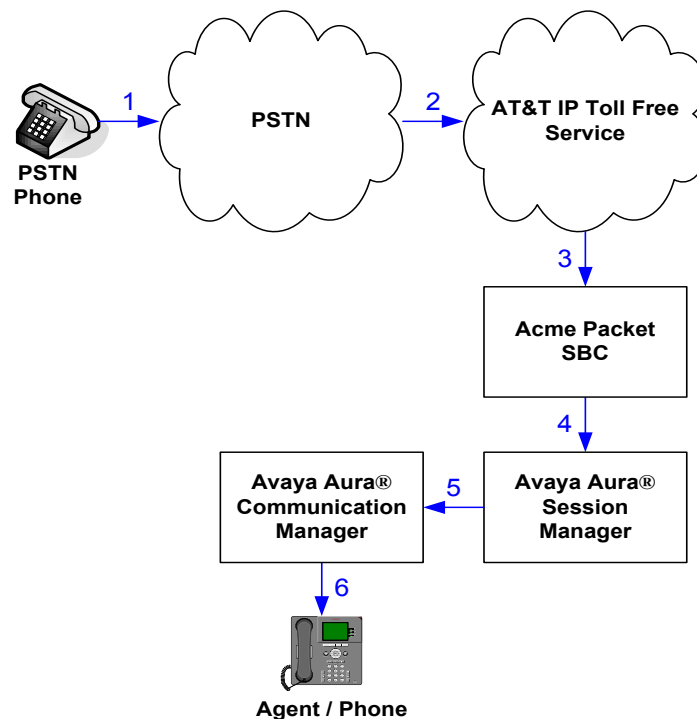


Figure 2: Inbound AT&T IP Toll Free Service Call to VDN / Agent / Phone

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 forwards⁴ 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 call⁵ continues to go through Communication Manager.

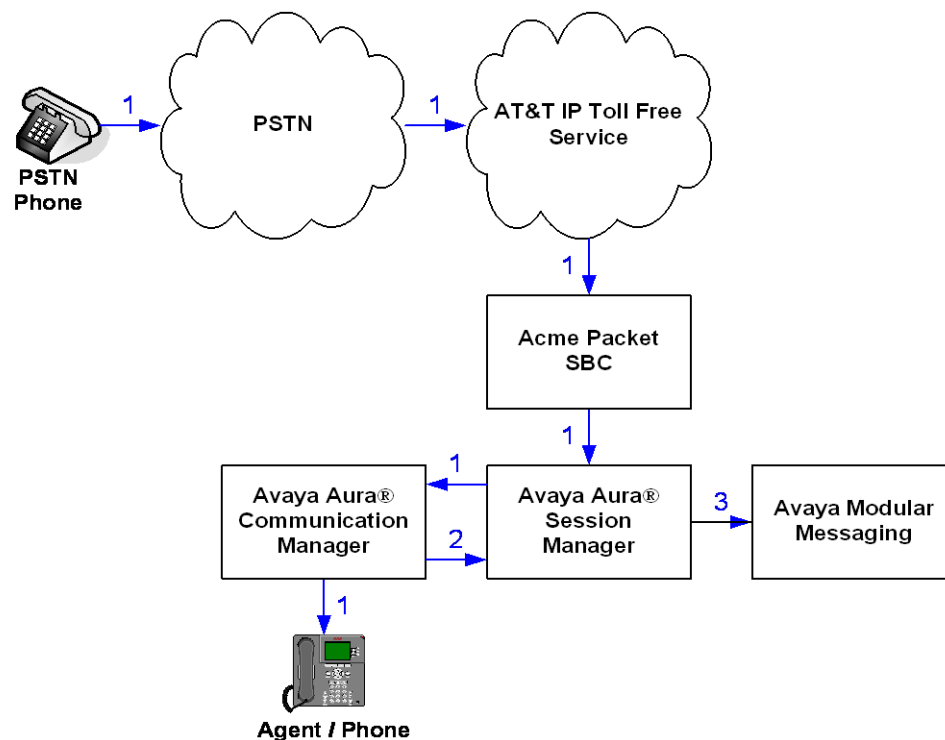


Figure 3: Inbound AT&T IP Toll Free Service Call to Agent / Phone Covered to Avaya Modular Messaging

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.

3. Equipment and Software Validated

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

Component	Version
Avaya S8800 Server	Avaya Aura® System Manager 6.0 (6.0.0.0.556-3.0.6.1)
Avaya S8800 Server	Avaya Aura® Session Manager 6.0 (6.0.0.0.600020)
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with patch 18246
Avaya G450 Media Gateway	30.13.2
MM711 Analog	HW31 FW094
Avaya 9630 IP Telephone	Avaya one-X® Deskphone Edition H.323 Version S3.110b (ha96xxua3_11.bin)
Avaya 9640 IP Telephone	Avaya one-X® Deskphone Edition SIP Version 2.6.0 (sip96xx_2_6_0_0.bin)
Avaya one-X® Communicator	5.2.0.14
Avaya 4610SW IP Telephone	a10d01b2_9_1.bin
Avaya 6211 Analog phone	-
Avaya S3500 Server	Avaya Modular Messaging 5.1-4.0 (9.0.424.1.013)
Fax device	Ventafax Home Version 6.1.59.144
Acme Packet Net-Net Session Director 3800	SCX6.1.0m6
AT&T IP Toll Free Service using MIS/PNT transport service connection	VNI 18

Table 2: Equipment and Software Versions

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1. Avaya agrees to provide service and support for the integration of Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1 with the AT&T IP Toll Free service offer, in compliance with existing support agreements for Avaya Aura® Communication Manager release 6.0 and Avaya Aura® Session Manager 6.0, and in conformance with the integration guidelines as specified in the body of this document.

4. Avaya Aura® Session Manager

These Application Notes assume that basic Avaya Aura® System Manager and Session Manager administration has already been performed. Consult [1] and [2] for further details if necessary. Configuration of Session Manager is performed from Avaya Aura® System Manager. To invoke the Avaya Aura® System Manager Common Console, launch a web browser, enter `https://<IP address of the Avaya Aura® System Manager server>/SMGR` in the URL, and log in with the appropriate credentials.

4.1. Background

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

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

4.2. Routing Policies

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

- SIP Entities – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- Entity Links – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- SIP Domains – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).

- **Locations** – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.
- **Adaptations** – Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities. As an example, basic “Digit Conversion” Adaptations are used in this reference configuration to convert digit strings in “destination” (e.g., Request-URI) and “origination” (e.g. P-Asserted Identity) type headers, of SIP messages sent to and received from SIP Entities.
- **Dial Patterns** – A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one⁶ of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed. Note that Dial Patterns are matched after ingress Adaptations have already been applied.
- **Time Ranges** – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Routing Policy may be associated with one or more Time Ranges during which the Routing Policy is in effect. For example, for a Dial Pattern administered with two Routing Policies, one Routing Policy can be in effect on weekday business hours and the other Routing Policy can be in effect on weekday off-hours and weekends. In the reference configuration no restrictions were placed on calling times.

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

- Use common number formats and uniform numbers in matching called party numbers for routing decisions.
- On ingress to Session Manager, apply any called party number modifications necessary to “normalize” the number to a common format or uniform number as defined in the Dial Patterns.
- On egress from SM, apply any called party number modifications necessary to conform to the expectations of the next-hop SIP Entity. For example, on egress from Session Manager to Communication Manager, modify the called party number such that the number is consistent with the dial plan on Communication Manager.

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

To view the sequenced steps required for configuring network routing policies, click on “**Routing**” in the left pane of the Avaya Aura® System Manager Common Console.

⁶ The Routing Policy in effect at that time with highest ranking is attempted first. If that Routing Policy fails, then the Routing Policy with the next highest rankings is attempted, and so on.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"
- (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

- Step 7: "Routing Policies" are defined
- Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)
- Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

Figure 4: Main Routing Page

4.3. SIP Domains

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

1. In the left pane under **Routing**, click on “**Domains**”. In the **Domain Management** page click on “**New**” (not shown),.
2. Continuing in the **Domain Management** page, enter a SIP domain (e.g. **customerb.com**) for **Name**
3. Select **Type sip**.
4. (Optional) Add notes.
5. Click on “**Commit**”.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 8, 2010 9:47 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Domains

Domain Management Commit Cancel

1 Item | [Refresh](#) Filter: Enable

Name	Type	Default	Notes
* customerb.com	sip	<input type="checkbox"/>	

* Input Required Commit Cancel

Figure 5: Domain Management Page

6. Repeat Steps 1 - 2 to add any additional SIP domains.

4.4. Locations

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

1. In the left pane under **Routing**, click on “**Locations**”. In the **Location** page click on “**New**” (not shown),.
2. In the **Location Details** page, enter a descriptive **Name** (e.g. **main**).
3. [Optional] To limit the number of calls going to and from this Location, i.e., apply CAC, specify the **Managed Bandwidth** and **Average Bandwidth per Call**.

4. [Optional] To identify IP addresses associated with this Location, add **Location Pattern** entries accordingly. In the reference configuration all the Avaya CPE resided in the IP segment 192.168.67.*.
5. Click on “**Commit**”.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 8, 2010 9:47 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Locations / Location Details

Location Details Commit Cancel

General

* Name:
 Notes:
 Managed Bandwidth: Kbit/sec
 * Average Bandwidth per Call: Kbit/sec

Location Pattern
Add Remove

1 Item | [Refresh](#) Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 192.168.67.*	<input type="text"/>

Select : All, None

Figure 6: Location Details Page

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

4.5. Adaptations

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

- Calls from AT&T (4.5.1) - 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 DNIS called number digit strings in the Request URI are replaced with their associated Communication Manager extensions/VDNs.
- Calls to/from Modular Messaging (4.5.2 and 4.5.3) - Modification of SIP messages sent to and received from Avaya Modular Messaging.
 - From MM (4.5.1) – Modular Messaging 11 digit mailbox numbers are converted to the associated Communication Manager 5 digit extensions.
 - To MM (4.5.2) - Convert the Communication Manager extension defined for Modular Messaging access (46000) to the Modular Messaging pilot number (17231146000).

4.5.1. Adaptation for calls for Avaya Aura® Communication Manager

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

1. In the left pane under **Routing**, click on “**Adaptations**”. In the **Adaptations** page, click on “**New**” (not shown).
2. In the **Adaptation Details** page, enter:
 - a. A descriptive **Name**, (e.g. To_ACM60).
 - b. Select “**DigitConversionAdapter**” from the **Module Name** drop down menu (if no module name is present, select “<click to add module>” and enter **DigitConversionAdapter**).
 - c. In the **Module parameter** field enter **odstd=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 *inbound* PAI.
 - d. In the **Digit Conversion for Outgoing Calls from SM** section, enter the *inbound* DID digits from AT&T that need to be replaced with their associated extensions before being sent to Communication Manager.
 - i. Example 1:
 1. 000001041 is a digit string sent in the Request URI by AT&T Toll Free service that is associated with Communication Manager extension 40002. Enter 000001041 in the **Matching Pattern** column.
 2. Enter **9** in the **Min/Max** columns.
 3. Enter **9** in the **Delete Digits** column.
 4. Enter **40002** string in the **Insert Digits** column.
 5. Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
 6. Enter any desired notes.
 - ii. Example 2:
 1. 1723114xxxx is the format of the mailboxes sent by Avaya Modular messaging. These mailboxes must be converted to their associated Communication Manager extensions by deleting the first six digits. Enter **1723114** in the **Matching Pattern** column.
 2. Enter **11** in the **Min/Max** columns.
 3. Enter **6** in the **Delete Digits** column.
 4. Leave the **Insert Digits** column blank.
 5. Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
 6. Enter any desired notes.
 - e. In the reference configuration no **Digit Conversion for Incoming Calls to SM** are required.
 - f. Click on “**Commit**”.

Avaya Aura™ System Manager

6.0

Welcome, **admin** Last Logged on at July 20, 2010 5:04 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Adaptations / Adaptation Details

▶ Elements

▶ Events

▶ Groups & Roles

Licenses

▼ Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

▶ Security

▶ System Manager Data

▶ Users

Help

Help for Adaptation Details fields

Help for Committing configuration changes

Adaptation Details

Commit Cancel

General

* Adaptation name:

To_ACM60

Module name:

DigitConversionAdapter

Module parameter:

osrcd=customerb.com odstd=customerb.com

Egress URI Parameters:

Notes:

Inbound to ACM

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--	------------------	-----	-----	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

18 Items Refresh

Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 000001041	* 9	* 9	* 9	40002	destination	IPTF
<input type="checkbox"/>	* 000001042	* 9	* 9	* 9	41002	destination	IPTF agent
<input type="checkbox"/>	* 000001043	* 9	* 9	* 9	44002	destination	IPTF agent
<input type="checkbox"/>	* 000001044	* 9	* 9	* 9	47002	destination	IPTF agent
<input type="checkbox"/>	* 000001045	* 9	* 9	* 9	47004	destination	IPTF agent
<input type="checkbox"/>	* 1723114	* 11	* 11	* 6		destination	Convert M

Select : All, None

Figure 7: Adaptation Details Page – Adaptation for Avaya Aura® Communication Manager

4.5.2. 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.

1. In the left pane under **Routing**, click on “**Adaptations**”. In the **Adaptations** page click on “**New**” (not shown).
2. In the **Adaptation Details** page, enter:
 - a. A descriptive **Name**, (e.g. **MM_Digits**).

- b. Select “**DigitConversionAdapter**” from the **Module Name** drop down menu (if no module name is present, select “<click to add module>” and enter **DigitConversionAdapter**).
- c. No **Module parameter** is required.
- d. Inbound calls to the Modular Messaging pilot number (message retrieval).
 - a. In the **Digit Conversion for Outgoing Calls from SM** section, enter **46000** in the **Matching Pattern** column. This is the Modular Messaging pilot extension defined on Communication Manager.
 - b. Enter **5** in the **Min/Max** columns.
 - c. Enter **0** in the **Delete Digits** column.
 - d. Enter **172311** in the **Insert Digits** column. This converts the pilot extension (46000) to the Modular Messaging pilot number (17231146000).
 - e. Specify that this should be applied to the SIP **Destination** headers in the **Address to modify** column.
 - f. Enter any desired notes.
- e. Click on “**Commit**”.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 8, 2010 9:47 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Adaptations / Adaptation Details

Elements
Events
Groups & Roles
Licenses
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Security
System Manager Data
Users

Help
Help for Adaptation Details fields
Help for Committing configuration changes

Adaptation Details
Commit Cancel

General

* Adaptation name:

MM_Digits

Module name:

DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM
Add Remove
Refresh
Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>							

Select : All, None

Digit Conversion for Outgoing Calls from SM
Add Remove
Refresh
Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 46000	* 5	* 5	* 0	172311	destination	to MM pilot

Select : All, None

* Input Required

Commit Cancel

Figure 8: Adaptation Details Page – Adaptation for Avaya Modular Messaging

4.6. SIP Entities

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

- Avaya Aura® Session Manager – **Section 4.6.1**
- Avaya Aura® Communication Manager (AT&T access) – This entity, and its associated entity link (using port 5060), is for calls from AT&T to Communication Manager via the Acme Packet SBC. – **Section 4.6.2**
- Avaya Aura® Communication Manager (Local access) – This entity, and associated link (using port 5080), is for communication between Avaya SIP phones and Communication Manager. – **Section 4.6.3**
- Acme Packet SBC – This entity, and its associated entity link (using port 5060), is for calls between the Acme Packet SBC and AT&T. – **Section 4.6.4**
- Avaya Modular Messaging – This entity, and its associated entity link (using port 5080), is for local calls from Modular Messaging to Communication Manager - **Section 4.6.5**

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

4.6.1. Avaya Aura® Session Manager SIP Entity

1. In the left pane under **Routing**, click on “**SIP Entities**”. In the **SIP Entities** page click on “**New**” (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name for Session Manager (e.g. **SM60**).
 - **FQDN or IP Address** – Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation (e.g. **192.168.67.210**).
 - **Type** – Select “**Session Manager**”.
 - **Location** – Select location “**Main**” (**Section 4.4**).
 - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
 - **Time Zone** – Select the time zone in which Session Manager resides (this will correspond to the time ranges specified in **Section 4.8**).
3. In the **SIP Monitoring** section of the **SIP Entity Details** page select:
 - a. Select **Link Monitoring Enabled** for **SIP Link Monitoring**
 - b. Use the default values for the remaining parameters.
4. In the **Port** section of the **SIP Entity Details** page, click on “**Add**” and provision an entry as follows:
 - **Port** – Enter “**5060**” (see note above).
 - **Protocol** – Select “**TCP**” (see note above).
 - **Default Domain** – (Optional) Select a SIP domain administered in **Section 4.3** with the selected **SIP Default Domain** (e.g. **customerb.com**)
5. Repeat Step 5 to provision another entry, except with “**5080**” for **Port** and “**TCP**” for **Protocol**. This is for local calls from the Avaya SIP phones (and Modular Messaging), to Communication Manager. Since a single Processor Ethernet (procr) was used in this reference configuration, a separate port was configured to separate the outbound SIP endpoint traffic from other traffic. This was done because of the known limitation noted in **Section 1.3**.
6. Click on “**Commit**”.

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

Avaya Aura™ System Manager

6.0

Welcome, **admin** Last Logged on at August 12, 2010 4:29 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

Elements

Events

Groups & Roles

Licenses

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Security

System Manager Data

Users

Help

Help for SIP Entity Details fields

Help for Committing configuration changes

SIP Entity Details

Commit Cancel

General

* Name:

SM60

* FQDN or IP Address:

192.168.67.210

Type:

Session Manager

Notes:

Location:

main

Outbound Proxy:

Time Zone:

America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds):

900

* Reactive Monitoring Interval (in seconds):

120

* Number of Retries:

1

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

Add

Remove

3 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	customerb.com	
<input type="checkbox"/>	5080	TCP	customerb.com	

Select : All, None

* Input Required

Commit Cancel

Figure 9: SIP Entity Details Page – Avaya Aura® Session Manager SIP Entity

4.6.2. Avaya Aura® Communication Manager SIP Entity

1. In the **SIP Entities** page, click on “New”.
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name for Communication Manager.

- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) provisioned in **Section 5.4**.
 - **Type** – Select “CM”.
 - **Adaptation** – Select the Adaptation administered in **Section 4.5.1**.
 - **Location** – Select a Location administered in **Section 4.4**.
 - **Time Zone** – Select the time zone in which Communication Manager resides.
 - In the **SIP Monitoring** section of the **SIP Entity Details** page select:
 - Select **Link Monitoring Enabled** for **SIP Link Monitoring**
 - Use the default values for the remaining parameters.
3. Click on “Commit”.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 12, 2010 4:29 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details [Commit] [Cancel]

General

* Name: ACM60

* FQDN or IP Address: 192.168.67.202

Type: CM

Notes:

Adaptation: To_ACM60

Location: main

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

Entity Links can be modified after SIP Entity is committed.

* Input Required [Commit] [Cancel]

Figure 10: SIP Entity Details Page – Avaya Aura® Communication Manager SIP Entity

4.6.3. Avaya Aura® Communication Manager SIP Entity – SIP Endpoint Calls.

Because of the shuffling limitation noted in **Section 1.3**, a separate SIP Entity was created to handle calls for SIP Endpoints registered with Session Manager. While the same Communication Processor Ethernet (procr) interface is used, a different port number (5080) is used as defined in **Section 4.6.1**. Configuration for this entity is similar to the entity configured in **Section 4.6.2**.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 12, 2010 4:29 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details [Commit] [Cancel]

General

* Name: ACM60_5080

* FQDN or IP Address: 192.168.67.202

Type: CM

Notes: for ACM Local trunk

Adaptation: To_ACM60

Location: main

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links


Entity Links can be modified after SIP Entity is committed.

* Input Required [Commit] [Cancel]

Figure 11: SIP Entity Details Page – Avaya Aura® Communication Manager SIP Entity for SIP Phones

4.6.4. Acme Packet SBC SIP Entity

To configure the Session Border Controller entity, repeat the Steps in **Section 4.6.2**. The **FQDN or IP Address** field is populated with the IP address of the private (inside) interface configured in **Section 7** and the **Type** field is set to “**Other**”. See the figure below for the values used in the reference configuration.



Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at August 12, 2010 4:29 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

Elements
Events
Groups & Roles
Licenses
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Security
System Manager Data
Users

Help
[Help for SIP Entity Details fields](#)
[Help for Committing configuration changes](#)

SIP Entity Details

CommitCancel

General

* Name: Acme_to_AT&T

* FQDN or IP Address: 192.168.67.130

Type: Other

Notes:

Adaptation: AT&T

Location: main

Time Zone: America/New_York

Override Port & Transport with DNS SRV:
☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links
Entity Links can be modified after SIP Entity is committed.


* Input Required

CommitCancel

Figure 12: SIP Entity Details Page – Acme Packet SBC SIP Entity

4.6.5. Avaya Modular Messaging SIP Entity

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



Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at August 12, 2010 4:29 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

▶ Elements
▶ Events
▶ Groups & Roles
Licenses
▼ Routing
 Domains
 Locations
 Adaptations
 SIP Entities
 Entity Links
 Time Ranges
 Routing Policies
 Dial Patterns
 Regular Expressions
 Defaults
▶ Security
▶ System Manager Data
▶ Users

Help
[Help for SIP Entity Details fields](#)
[Help for Committing configuration changes](#)

SIP Entity Details

Commit Cancel

General

* Name: MM52

* FQDN or IP Address: 192.168.67.141

Type: Modular Messaging

Notes:

Adaptation: MM_Digits

Location: main

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

Entity Links can be modified after SIP Entity is committed.

* Input Required

Commit Cancel

Figure 13: SIP Entity Details Page – Avaya Modular Messaging SIP Entity

4.7. Entity Links

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

- Avaya Aura® Communication Manager (4.7.1).
- Avaya Aura® Communication Manager for SIP endpoints (4.7.2).
- Acme Packet SBC (4.7.3).
- Avaya Modular Messaging (4.7.4).

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

4.7.1. Entity Links to Avaya Aura® Communication Manager

1. In the left pane under **Routing**, click on “**Entity Links**”. In the **Entity Links** page click on “**New**” (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name for this link to Communication Manager (e.g. ACM60).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 4.6.1** for Session Manager. SIP Entity 1 must always be an Session Manager instance.
 - **SIP Entity 1 Port** – Enter “**5060**”
 - **SIP Entity 2** –Select the SIP Entity administered in **Section 4.6.2** for Communication Manager.
 - **SIP Entity 2 Port** - Enter “**5060**”.
 - **Trusted** – Check the checkbox.
 - **Protocol** – Select “**TCP**”.
3. Click on “**Commit**”.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 23, 2010 10:00 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Entity Links

Entity Links Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* ACM60	* SM60	TCP	* 5060	* ACM60	* 5060	<input checked="" type="checkbox"/>

* Input Required Commit Cancel

Figure 14: Entity Links Page – Entity Link to Avaya Aura® Communication Manager – TCP/5060

4.7.2. Avaya Aura® Communication Manager Entity Link for SIP Phones

To configure this entity link, repeat the Steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.3** for Communication Manager SIP Entity (e.g.

ACM60_5080). Note that the **Port** fields are populated with **5080**. See the figure below for the values used in the reference configuration.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 16, 2010 10:05 AM

Help | About | Change Password | **Log off**

Home / Routing / Entity Links

Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Tr
* ACM_5080	* SM60	TCP	* 5080	* ACM60_5080	* 5080	

* Input Required

Commit Cancel

Figure 15: Entity Links Page –Avaya Aura® Communication Manager Entity Link for SIP Phones – TCP/5080

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

Repeat Section 4.7.1 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 4.6.4 for the Acme Packet SBC.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 9:04 AM

Help | About | Change Password | **Log off**

Home / Routing / Entity Links

Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* Acme_to_AT&T	* SM60	TCP	* 5060	* Acme_to_AT&T	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

Figure 16: Entity Links Page – Entity Link to AT&T IP Toll Free Service via Acme Packet SBC

4.7.4. Entity Link to Avaya Modular Messaging

Repeat **Section 4.7.1** 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 4.6.5** for Avaya Modular Messaging.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 10:54 AM

Help | About | Change Password | Log off

Home / Routing / Entity Links

Entity Links

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* MM52	* SM60	TCP	* 5060	* MM52	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

Figure 17: Entity Links Page – Entity Link to Avaya Modular Messaging

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

4.8. Time Ranges

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

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 10:54 AM

Help | About | Change Password | Log off

Home / Routing / Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions Commit

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/Z	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Commit Cancel

Figure 18: Time Ranges Page

4.9. Routing Policies

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

- To Avaya Aura® Communication Manager from AT&T (**Section 4.9.1**).
- To Avaya SIP Phones (**Section 4.9.2**).
- To Avaya Modular Messaging (**Section 4.9.3**).

4.9.1. Routing Policy for Routing to Avaya Aura® Communication Manager

1. In the left pane under **Routing**, click on “**Routing Policies**”. In the **Routing Policies** page click on “**New**” (not shown).
2. In the **General** section of the **Routing Policy Details** page (see **Figure 19**), enter a descriptive **Name** for routing calls to Communication Manager (**To_ACM_6_0**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on “**Select**”.

Commit Cancel

Notes:

Select

Name	FQDN or IP Address	Type	Notes
ACM60	192.168.67.202	CM	

View Gaps/Overlaps

Filter: [Enable](#)

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59

Select : All, None

Remove

Filter: [Enable](#)

Remove

Filter: [Enable](#)

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

*** Input Required**

Commit Cancel

Figure 19: Routing Policy Details Page – Inbound from AT&T to Communication Manager

4. In the **SIP Entity List** page (**Figure 20**), select the SIP Entity administered in **Section 4.6.2** for Communication Manager (**ACM60**), and click on “**Select**”.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 16, 2010 10:05 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details / SIP Entity List

SIP Entity List Select Cancel

SIP Entities

7 Items | [Refresh](#) Filter: [Enable](#)

	Name	FQDN or IP Address	Type	Notes
<input checked="" type="radio"/>	ACM60	192.168.67.202	CM	
<input type="radio"/>	ACM60_5080	192.168.67.202	CM	for ACM Local trunk
<input type="radio"/>	MM52	192.168.67.141	Modular Messaging	
<input type="radio"/>	SM60	192.168.67.210	Session Manager	

Select : [None](#)

Select Cancel

Figure 20: SIP Entity List Page

5. Returning to the Routing Policy Details page in the Time of Day section, click on “Add”.
6. In the **Time Range List** page, check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 4.8**, and click on “**Select**”.
7. Returning to the **Routing Policy Details** page (**Figure 19**), in the **Time of Day** section, enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on “**Commit**”.
8. Note that once the **Dial Patterns** are defined (**Section 4.10**) they will appear in the **Dial Pattern** section.
9. No **Regular Expressions** were used in the reference configuration.
10. Click on **Commit**.

4.9.2. Routing Policy for Routing to Avaya SIP Phones

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

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Avaya Modular Messaging (**ACM_5080**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.6.5** for Avaya Modular Messaging (**ACM60_5080**), and click on “**Select**”.
- Note that once the **Dial Patterns** are defined (**Section 4.10**), they will appear in the **Dial Pattern** section.

4.9.3. Routing Policy for Routing to Avaya Modular Messaging

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

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Avaya Modular Messaging (**To_MM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.6.5** for Avaya Modular Messaging (**MM52**), and click on “**Select**”.
- Note that once the **Dial Patterns** are defined (**Section 4.10**), they will appear in the **Dial Pattern** section.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 23, 2010 10:00 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

Elements
Events
Groups & Roles
Licenses
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Security
System Manager Data
Users

Help

Help for Routing Policy Details fields
Help for SIP Entity List
Help for Time Range List
Help for Pattern List
Help for Regular Expressions List
Help for Committing configuration changes

Routing Policy Details

Commit

Cancel

General

* Name:

ACM_5080

Disabled:

☐

Notes:

ACM Local trunk

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM60_5080	192.168.67.202	CM	for ACM Local trunk

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add

Remove

3 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	4		5	5	<input type="checkbox"/>	-ALL-	main	SIP phone calls
<input type="checkbox"/>	9011		12	15	<input type="checkbox"/>	-ALL-	main	
<input type="checkbox"/>	91		12	12	<input type="checkbox"/>	-ALL-	main	

Select : All, None

Regular Expressions

Add

Remove

0 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

* Input Required

Commit

Cancel

Figure 21: Routing Policy Details Page to Avaya SIP Phones

JF:Reviewed
SPOC 9/9/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

34 of 102
SM60CM60SBCIPTF

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 10:54 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

Elements
Events
Groups & Roles
Licenses
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Security
System Manager Data
Users

Help

Help for Routing Policy Details fields
Help for SIP Entity List
Help for Time Range List
Help for Pattern List
Help for Regular Expressions List
Help for Committing configuration changes

Routing Policy Details

Commit

Cancel

General

* Name:
To_MM

Disabled:
☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
MM52	192.168.67.141	Modular Messaging	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add

Remove

Filter: Enable

Regular Expressions

Add

Remove

0 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

* Input Required

Commit

Cancel

Figure 22: Routing Policy Details Page to Avaya Modular Messaging

4.10. Dial Patterns

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

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

4.10.1. Matching Inbound Calls to Avaya Aura® Communication Manager

In this example inbound calls from the AT&T IP Toll Free service with the called digit pattern 00000104x are defined.

1. In the left pane under **Routing**, click on “**Dial Patterns**”. In the **Dial Patterns** page click on “**New**” (not shown).
2. In the **General** section of the **Dial Pattern Details** page, provision the following:
 - **Pattern** – In the reference configuration, AT&T sends 9 digit called numbers with the format 00000104x. Enter **00000104**. Note - The adaptation defined for Communication Manager in **Section 4.5.1** will convert the various 00000104x numbers into their corresponding extensions.
 - **Min** and **Max** – Enter **9**.
 - **SIP Domain** – Select one of the SIP Domains defined in **Section 4.3** or “**-ALL-**”, to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if “**-ALL-**” is selected) can match this Dial Pattern.

Avaya Aura™ System Manager

6.0

Welcome, **admin** Last Logged on at July 21, 2010 9:21 AM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details

Elements

Events

Groups & Roles

Licenses

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Security

System Manager Data

Users

Help

Help for Dial Pattern Details fields

Help for Location and Routing Policy Lists

Help for Denied Location fields

Help for Committing configuration changes

Dial Pattern Details

Commit Cancel

General

* Pattern: 00000104

* Min: 9

* Max: 9

Emergency Call: ☐

SIP Domain: -ALL-

Notes: IPTF

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	main		To_ACM_6_0	0	<input type="checkbox"/>	ACM60

Select : All, None

Denied Originating Locations

Add Remove

0 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit Cancel

Figure 23: Dial Pattern Details Page - Matching Inbound AT&T IP Toll Free Service Calls

- In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on “Add”.
- In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Main** to which Communication Manager is assigned is assigned (see **Section 4.6.2**). 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.
- 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 Communication Manager in **Section 4.9.2**.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 10:58 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details / Locations and Policy List

▶ Elements

▶ Events

▶ Groups & Roles

Licenses

▼ Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

▶ Security

▶ System Manager Data

▶ Users

Help

Originating Location and Routing Policy List

Select
Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item
Refresh
Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	main	

Select : All, None

Routing Policies

5 Items
Refresh
Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input checked="" type="checkbox"/>	To_ACM_6_0	<input type="checkbox"/>	ACM60	
<input type="checkbox"/>	To_MM	<input type="checkbox"/>	MM52	

Select : All, None

Select
Cancel

Figure 24: Originating Location and Routing Policy List Page - Matching Inbound AT&T IP Toll Free Service Calls

6. In the **Originating Location and Routing Policy List** page, click on “**Select**”.
7. Returning to the **Dial Pattern Details** page (Figure 24), click on “**Commit**”.

JF:Reviewed
SPOC 9/9/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

38 of 102
SM60CM60SBCIPTF

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 21, 2010 9:21 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns

Dial Patterns

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) [Commit](#)

23 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	00000104	9	9	<input type="checkbox"/>	-ALL-	IPTF

Select : [All](#), [None](#)

Figure 25: Dial Pattern Details - Matching Inbound AT&T IP Toll Free Service Calls

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

Avaya Aura® Communication Manager stations cover to Avaya Modular Messaging using a pilot extension (46000 in the reference configuration). Additionally stations may dial this extension to retrieve messages or modify mailbox settings. Note – Extension 46000 is converted to the Modular Messaging mailbox format 17321146000 in the adaptation defined in **Section 4.5.2**.

1. In the left pane under **Routing**, click on “**Dial Patterns**”. In the **Dial Patterns** page click on “**New**” (not shown).
2. In the **General** section of the **Dial Pattern Details** page, 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 4.3** or “**-ALL-**”, to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if “**-ALL-**” is selected) can match this Dial Pattern.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 10:58 AM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details

Elements
Events
Groups & Roles
Licenses
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Security
System Manager Data
Users

Help

Help for Dial Pattern Details fields
Help for Location and Routing Policy Lists
Help for Denied Location fields
Help for Committing configuration changes

Dial Pattern Details

Commit
Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:
☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add
Remove

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To MM	0	<input type="checkbox"/>	MM52	

Select : All, None

Denied Originating Locations

Add
Remove

0 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit
Cancel

Figure 26: Dial Pattern Details – Matching Avaya Modular Messaging Pilot Number

3. In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on “Add”.
4. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Main** to which Modular Messaging is assigned (see **Section 4.6.5**). Note that only those calls that originate from the selected Location(s), or all administered Locations if “-ALL-” is selected, can match this Dial Pattern.
5. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy administered for routing calls to Modular Messaging in **Section 4.9.2**.

JF:Reviewed
SPOC 9/9/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

40 of 102
SM60CM60SBCIPTF

Avaya Aura™ System Manager

6.0

Welcome, **admin** Last Logged on at July 21, 2010 9:21 AM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns

▶ Elements

▶ Events

▶ Groups & Roles

Licenses

▼ Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Dial Patterns

Edit

New

Duplicate

Delete

More Actions ▼

Commit

23 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Notes
<input type="checkbox"/>	00000104	9	9	<input type="checkbox"/>	-ALL-	IPTF
<input type="checkbox"/>	46000	5	5	<input type="checkbox"/>	-ALL-	IPTF

Select : All, None

Figure 28: Dial Pattern Details – AT&T Inbound and Modular Messaging Pilot number Calls

4.11. Session Manager Administration

1. In the left pane under **Session Manager**, click on **Elements → Session Manager Administration**. In the **Session Manager Administration** page click on “**New**” (not shown).
2. In the **General** section of the **Add Session Manager** page, provision the following:
 - **SIP Entity Name** – Select the SIP Entity administered for Session Manager in **Section 4.6.1**.
 - **Management Access Point Host Name/IP** – Enter the IP address of the management interface on Session Manager as defined during installation, (*not* the network interface). E.g. **192.168.67.209**
3. In the **Security Module** section of the **Add Session Manager** page, enter the **Network Mask** and **Default Gateway** of the Session Manager network interface as defined during installation (e.g. **255.255.255.0** and **192.168.67.1**).
4. In the **Monitoring** section, verify that the **Enable Monitoring** box is checked.
5. Use the default values for the remaining fields.
6. Click on “**Commit**”.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 9, 2010 10:58 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Session Manager / Session Manager Administration / Edit Session Manager

Elements

Conferencing
Presence
Application Management
Endpoints
SIP AS 8.1
Feature Management
Inventory
Templates
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Events
Groups & Roles
Licenses
Routing
Security
System Manager Data
Users

Help
Editing Session Manager Settings
Page Fields
About NIC Bonding
Session Manager Administration

Add Session Manager

Commit
Cancel

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

General

SIP Entity NameSM60
Description
*Management Access Point Host Name/IP192.168.67.209
*Direct Routing to EndpointsEnable

Security Module

SIP Entity IP Address192.168.67.210
*Network Mask255.255.255.0
*Default Gateway192.168.67.1
*Call Control PHB46
*QOS Priority6
*Speed & DuplexAuto
VLAN ID

NIC Bonding

Enable Bonding
Driver Monitoring ModeARP Monitoring
ARP Interval (msecs)100Link Monitoring Frequency (msecs)100
ARP Target IPDown Delay (msecs)200
ARP Target IPUp Delay (msecs)200
ARP Target IP

Monitoring

Enable Monitoring
*Proactive cycle time (secs)900
*Reactive cycle time (secs)120
*Number of Retries1

CDR

Enable CDR
UserCDR_User
Password
Confirm Password

Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection
*Maximum Connection per PPM Client3
PPM Packet Rate Limiting
*PPM Packet Rate Limiting Threshold200

Event Server

Clear Subscription on Notification FailureNo

*Required
Commit
Cancel

Figure 29: Add Session Manager Page

5. Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [3] and [4] for further details if necessary.

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

5.1. System Parameters

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

1. Enter the **display system-parameters customer-options** command. On Page 2 of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks (e.g. 5000).

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		8000	0
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		0	0
Maximum Concurrently Registered Remote Office Stations:		0	0
Maximum Concurrently Registered IP eCons:		0	0
Max Concur Registered Unauthenticated H.323 Stations:		0	0
Maximum Video Capable H.323 Stations:		0	0
Maximum Video Capable IP Softphones:		0	0
Maximum Administered SIP Trunks:		5000	250
Maximum Administered Ad-hoc Video Conferencing Ports:		0	0
Maximum Number of DS1 Boards with Echo Cancellation:		0	0
Maximum TN2501 VAL Boards:		10	1
Maximum Media Gateway VAL Sources:		0	0
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	2
Maximum Number of Expanded Meet-me Conference Ports:		0	0
(NOTE: You must logoff & login to effect the permission changes.)			

Figure 30: System-Parameters Customer-Options Form – Page 2

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

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? y		

Figure 31: System-Parameters Customer-Options Form – Page 3

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

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y	ISDN Feature Plus? y	
Enhanced Conferencing? y	ISDN/SIP Network Call Redirection? n	
Enhanced EC500? y	ISDN-BRI Trunks? y	
Enterprise Survivable Server? n	ISDN-PRI? y	
Enterprise Wide Licensing? n	Local Survivable Processor? n	
ESS Administration? n	Malicious Call Trace? n	
Extended Cvg/Fwd Admin? y	Media Encryption Over IP? n	
External Device Alarm Admin? n	Mode Code for Centralized Voice Mail? n	
Five Port Networks Max Per MCC? n	Multifrequency Signaling? y	
Flexible Billing? n	Multimedia Call Handling (Basic)? y	
Forced Entry of Account Codes? n	Multimedia Call Handling (Enhanced)? y	
Global Call Classification? n	Multimedia IP SIP Trunking? n	
Hospitality (Basic)? y		
Hospitality (G3V3 Enhancements)? n		
IP Trunks? y		
IP Attendant Consoles? n		

Figure 32: System-Parameters Customer-Options Form – Page 4

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

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

Figure 33: System-Parameters Customer-Options Form – Page 5

5.2. Dial Plan

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

- 3-digit dial access codes (indicated with a **Call Type** of “**dac**”) beginning with the digit “1” (e.g. Trunk Access Codes (TACs) defined for trunk groups in this reference configuration conform to this format).
- 5-digit extensions with a **Call Type** of “**ext**” beginning with the digits “4xxxxx” (e.g. Local extensions for Communication Manager stations, agents, and Vector Directory Numbers (VDNs) in this reference configuration conform to this format).
- 1-digit facilities access code (indicated with a **Call Type** of “**fac**”) (e.g. “9” access code for outbound ARS dialing and “8” for AAR local dialing).
- 3-digit facilities access codes (e.g. * and # for Agent logon/logoff).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	3	dac						
4	5	ext						
8	1	fac						
9	1	fac						
*	3	fac						
#	3	fac						

Figure 34: Dialplan Analysis Form

5.3. Alternate Automated Routing (AAR) Table

The AAR table is selected based on the caller dialing the AAR access code (e.g. “8”) as defined in **Section 5.2**. The access code is removed and the AAR table matches the remaining dialed digits and sends then to the designated route-pattern (see **Section 5.11**).

1. In the **Dialed String** column enter **17231146000**.
2. In the **Min** and **Max** columns enter the corresponding matching digit lengths, (e.g. **11** and **11**).
3. In the Route Pattern column select a route-pattern to be used for these calls (e.g. **2**).
4. In the **Call Type** column enter **unku**.
5. Repeat steps 1 through 5 using pilot extension **46000** and a length of **5**.
6. In the reference configuration Avaya SIP phones use the extension range 41xxx. Repeat steps 1 through 5 using Avaya SIP phone extension **46** and a length of **5**.

In the example below outbound calls to Modular Messaging pilot number (17231146000) or pilot extension (46000), and calls to Avaya SIP phones (41xxx) are sent to route-pattern 2 (see **Section 5.11**).

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	
17231146000	11	11	2	unku		n	
41	5	5	2	unku		n	
46000	5	5	2	unku		n	

Figure 35: AAR Analysis Form

5.4. IP Node Names

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

1. Enter the **change node-names ip** command, and add a node name and the IP address for the Session Manager network interface (e.g. **ASM60**)
2. As described in **Section 2**, 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		
ASM60	192.168.67.210		
default	0.0.0.0		
procr	192.168.67.202		
procr6	::		

Figure 36: Node-Names Form

5.5. IP Interface for procr

The “add ip-interface procr” or “change ip-interface procr” command can be used to configure 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.

change ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCr	Target socket load: 19660	
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 192.168.67.202	
Subnet Mask: /24		

Figure 37: IP-Interface Procr Form

5.6. G450 Media Gateway

In the reference configuration an Avaya G450 Media Gateway is used for media resources and to support various interface cards (e.g. MM711 Analog card). The G450 registers to Communication Manager. This requires provisioning on both Communication Manager and the G450.

Note – Only the G450 provisioning required to register to Communication Manager is described here. Other G450 provisioning including network provisioning, is beyond the scope of this document. Additional G450 provisioning documents are available at www.support.avaya.com.

5.6.1. G450 Provisioning for Registration to Communication Manager

1. Log into the G450 (via console or network connections) using appropriate credentials. Note that the console prompt will appear similar to **G450-???#**, where ??? means the G450 is not registered. Once the G450 registers, the prompt will change to **G450-001#** (where 001 is the Media Gateway reference number provisioned in Communication Manager (see **Section 5.6.2**).
2. Enter **set mgc list x.x.x.x**, where x.x.x.x is the IP address of the Communication Manager Procr (e.g. 192.168.67.202)
3. Enter Show System and note the G450 serial number. This will be used to provision the G450 on Communication Manager.

```
G450-001(super)# show system
System Name      :
System Location  :
System Contact   :
Uptime (d,h:m:s) : 34,05:49:29
Call Controller Time : 15:33:15 13 JUL 2010
Serial No      : 09IS53298916
Model           : G450
HW Ready for FIPS : No
Chassis HW Vintage : 1
Chassis HW Suffix : A
Mainboard HW Vintage : 2
Mainboard HW Suffix : B
```

Figure 38: G450 Show System Command

5.6.2. Communication Manager Provisioning for the G450

1. Enter add media gateway x, where x is the next available Media Gateway reference number (e.g. 1).
2. Enter **Type: G450**
3. Enter a descriptive name.
4. Enter the G450 Serial Number from **Section 5.6.1**.
5. Enter a network Region (e.g. 1).
6. Leave other values to default (these other values may be changed for other configurations beyond the scope of this document).

Once the G450 is registered the **Registered?** field will change from “n” to “y” and other fields will self-populate.

```
add media-gateway 1                                     Page 1 of 2
                                          MEDIA GATEWAY 1

      Type: g450
      Name: ES-CM-G450
      Serial No: 09IS53298916
      Encrypt Link? y                                Enable CF? n
      Network Region: 1                               Location: 1
                                                    Site Data:

      Recovery Rule: none

      Registered? y
      FW Version/HW Vintage: 30 .13 .2 /1
      MGP IPV4 Address: 192.168.67.203
      MGP IPV6 Address:
      Controller IP Address: 192.168.67.202
      MAC Address: 00:1b:4f:3e:53:68
```

Figure 39: Communication Manager Add Media-Gateway form

5.7. 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.

5.7.1. 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. Modular Messaging) are assigned to ip-network-region 1.

1. Enter a descriptive name (e.g. **Local**).
2. Enter the **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g. **region 1**). This IP network region will be used to represent the AT&T IP Toll Free service.
 - 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	
Codec Set: 1	Intra-region IP-IP Direct Audio: yes
UDP Port Min: 16384	Inter-region IP-IP Direct Audio: yes
UDP Port Max: 32767	IP Audio Hairpinning? n
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	
H.323 Link Bounce Recovery? y	
Idle Traffic Interval (sec): 20	
Keep-Alive Interval (sec): 5	
Keep-Alive Count: 5	
RSVP Enabled? n	

Figure 40: IP-Network-Region 1 Form– Page 1

3. 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 **No Limit**.
 - 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 rgn	codec set	direct WAN	Units	WAN-BW-limits	Video	Intervening		Dyn	A	G	c	
				Total Norm	Prio Shr	Regions		CAC	R	L	e	
1	1									all		
2	2	y	NoLimit						n		t	
3												

Figure 41: IP-Network-Region 1 Form– Page 3

5.7.2. IP Network Region 2 – AT&T Region

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

1. Repeat the steps in **Section 5.7.1** with the following changes:
 - Page 1
 - a. Enter a descriptive name (e.g. **AT&T**)
 - b. 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			
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 Link Bounce Recovery? y		RSVP Enabled? n	
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			
Keep-Alive Count: 5			

Figure 42: IP-Network-Region 2 Form– Page 1

- Page 4
 - a. 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		
3												

Figure 43: IP-Network-Region 2 Form– Page 4

5.7.3. IP Codec Parameters

5.7.3.1 Codecs For IP Network Region 1

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

1. Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used only for internal calls. On Page 1 of the **ip-codec-set** form, ensure that “**G.711MU**”, “**G.729B**”, and “**G.729A**” are included in the codec list.

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

Figure 44: IP-Codec-Set Form for Internal Calls – Page 1

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

change ip-codec-set 1			Page 2 of 2	
IP Codec Set				
Allow Direct-IP Multimedia? n				
FAX	Mode	Redundancy		
	t.38-standard	0		
Modem	off	0		
TDD/TTY	off	0		
Clear-channel	n	0		

Figure 45: IP-Codec-Set 1 Form for External Calls – Page 2

5.7.3.2 Codecs For IP Network Region 2

In the reference configuration IP Network Region 2 uses codec set 2.

1. Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g. **2**). This IP codec set will be used for inbound and outbound AT&T IP 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 **30ms** for the Packet Size). Let G711MU default to **20**.

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

Figure 46: IP-Codec-Set 2 Form for External Calls – Page 1

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

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

Figure 47: IP-Codec-Set 2 Form for External Calls – Page 2

5.8. SIP Trunks

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

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

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

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

5.8.1. SIP Trunk for AT&T IP Toll Free Access

This section describes the steps for administering the SIP trunk from Session Manager used for AT&T access. This trunk corresponds to the **ACM60** Entity defined in **Section 4.6.2**.

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 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 5.4**
 - **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g. **ASM60**).
 - **Near-end Listen Port** and **Far-end Listen Port** – set to “**5060**” (see Transport Method note above).
 - **Far-end Network Region** – Set to the IP network region **2**, as defined in **Section 5.7.2**.
 - **Far-end Domain** – Enter **customerb.com**. This is the domain inserted by Session Manager in **Section 4.5.1**.
 - **DTMF over IP** – Set to “**rtp-payload**” to enable Communication Manager to use DTMF according to RFC 2833.
 - **Direct IP-IP Audio Connections** – Set to “**y**”, indicating that the RTP paths should be optimized to reduce the use of MedPro resources 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: ASM60	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 2	
Far-end Domain: customerb.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Figure 48: Signaling-Group 1 Form for AT&T IP Toll Free Calls

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. 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. **ASM_6_0**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **101**).
- **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. 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: ASM_6_0	COR: 1	TN: 1	TAC: 101
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: 1			
Number of Members: 20			

Figure 49: Trunk-Group 1 Form for AT&T IP Toll Free Calls – Page 1

3. On Page 2 of the **Trunk Group** form:

- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900**. This entry will actually cause a value of 1800 to be generated in the SIP header. 1800 is the value required by AT&T IP Toll Free service.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
SCCAN? n		Redirect On OPTIM Failure: 5000	
		Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 900			
Delay Call Setup When Accessed Via IGAR? n			

Figure 50: Trunk-Group 1 Form for AT&T IP Toll Free Calls – Page 2

4. On Page 3 of the **Trunk Group** form:
 - Set **Numbering Format:** to **private**

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

Figure 51: Trunk-Group 1 Form for AT&T IP Toll Free Calls – Page 3

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**). Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Toll Free service to determine this value.
 - Use default for all other values.

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 100	
Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? n	
Enable Q-SIP? n	

Figure 52: Outbound Voice Trunk Group 51 – Page 4

5.8.2. 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 Telephone calls.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **2**), and follow the same procedures described in **Section 5.8.1, Step 1**, except:
 - **Near-end Port** – Set to **5080**.
 - **Far-end Port** – Set to **5080**.
 - **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 5.7.1**.

- **Direct IP-IP Audio Connections** – Set to “n”. As described in **Section 1.3**, shuffling needs to be disabled for Avaya SIP telephones.
- **Enable Layer 3 Test** – Set to “n”.

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: ASM60	
Near-end Listen Port: 5080	Far-end Listen Port: 5080	
Far-end Network Region: 1		
Far-end Domain: customerb.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? n	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
Alternate Route Timer(sec): 6		

Figure 53: Signaling-Group 2 Form for Local Modular Messaging and Avaya SIP Phone Calls

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

change trunk-group 2		Page 1 of 21
TRUNK GROUP		
Group Number: 2	Group Type: sip	CDR Reports: y
Group Name: MM_and_SIP_Phones	COR: 1	TN: 1 TAC: 102
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: 2		
Number of Members: 20		

Figure 54: Trunk-Group 2 Form for Local Calls – Page 1

3. Repeat **Section 5.8.1, Steps 3 and 4** for pages 2 and 3 of the form.

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	
Delay Call Setup When Accessed Via IGAR? n	

Figure 55: Trunk-Group 2 Form for Local Calls – Page 2

add trunk-group 2	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UII Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

Figure 56: Trunk-Group 2 Form for Local Calls – Page 3

4. 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**). Contact AT&T to examine a SIP trace of an inbound call from the AT&T IP Toll Free service to determine this value.
- Let all other values default.

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? y	
Always Use re-INVITE for Display Updates? n	
Enable Q-SIP? n	

Figure 57: Trunk-Group 2 Form for Local Calls – Page 4

5.9. Private Numbering

For AT&T Toll Free service call admission control purposes, calling number origination SIP header contents (e.g. From, Contact, and PAI) are converted to public numbers (previously identified by AT&T), instead of Communication Manager local extensions. However, Avaya Modular Messaging looks for Communication Manager extensions in these headers for mail-box processing. These function may be accomplished using the Communication Manager *private-numbering* form.

1. Converting Communication Manager extensions to AT&T DID.
Using the **change private-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. **1**).
 - **CPN Prefix** – Enter the corresponding AT&T DID (e.g. **7323204050**) used for the specified extension (e.g. **40001**).
 - **CPN Len** – Enter the total number of digits after the digit conversion (e.g. **10**).
2. Repeat Step 1 for each extension/DID conversion required.
3. Passing Communication Manager extensions to Modular Messaging.
 - **Ext Len** – Enter the total number of digits in the local extension range (e.g. **5**).
 - **Ext Code** – Enter the broadest wildcard match necessary to cover extensions with coverage to Modular Messaging (e.g. **4** to cover the provisioned extension range 4xxxx).
 - **Trk Grp(s)** – Enter the number of the Local trunk group (e.g. **2**).
 - **CPN Prefix** – Leave blank.
 - **CPN Len** – Enter the total number of extension digits (e.g. **5**).

For example, in **Figure 57**, any extension beginning with 4 and 5 digits long will remain unchanged for trunk 2 (Modular Messaging processing). However when 5 digit extension 41001 calls out to Session Manager, the originating number will be converted to 7323204052.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	4	2		5	Total Administered: 4
5	40001	1	7323204050	10	Maximum Entries: 540
5	40002	1	7323204051	10	
5	41001	1	7323204052	10	

Figure 58: Public- Numbering Form

5.10. Public Unknown Numbering

Use the same procedures described in **Section 5.9**, Steps 1 and 2 , to populate this form. Note that only local extension conversions to AT&T DIDs are specified on this form.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
5	40001	1	7323204050	10	Total Administered: 3 Maximum Entries: 9999
5	40002	1	7323204051	10	
5	41001	1	7323204052	10	

Figure 59: Public- Numbering Form

5.11. Route Patterns

Although the AT&T IP Toll Free service does not support outbound dialing, the provisioning of this form insures the use of private numbering as described in **Section 1.3 Item 5**.

5.11.1. Calls from AT&T

1. In the **Grp No** column enter **1** for SIP trunk 1.
2. In the **FRL** column enter **0** (zero).
3. In the **Pfx Mrk** column enter **1**
4. In the **Numbering Format** column enter **unk-unk**
5. In the **LAR** column enter **next** in the row corresponding to **1**.

change route-pattern 1													Page 1 of 3
Pattern Number: 1 Pattern Name: To_AT&T													
SCCAN? n Secure SIP? n													
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts	DCS/ QSIG Intw	IXC				
1: 1	0		1					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. Dgts	Numbering Format	LAR			
0	1 2 M 4 W		Request										
1:	y y y y y n	n		rest					unk-unk	next			
2:	y y y y y n	n		rest						none			
3:	y y y y y n	n		rest						none			
4:	y y y y y n	n		rest						none			
5:	y y y y y n	n		rest						none			
6:	y y y y y n	n		rest						none			

Figure 60: Route-pattern 1 form

5.11.2. Calls for Modular Messaging and Avaya SIP Phones

This form defines the SIP trunk to be used based on the route-pattern selected by the AAR table (see **Section 5.3 and 5.8.2**).

1. In the **Grp No** column enter **2** for SIP trunk 2.
2. In the **FRL** column enter **0** (zero).
3. In the **LAR** column enter **next** in the row corresponding to **1:**.

change route-pattern 2															Page 1 of 3			
Pattern Number: 2 Pattern Name: MM_&_SIP_phones																		
SCCAN? n Secure SIP? n																		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/	IXC		
No				Mrk	Lmt	List	Del	Digits								QSIG		
									Dgts								Intw	
1:	2	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			Dgts	Format		
						Request		Subaddress			
1:	y	y	y	y	y	n	n			rest	next
2:	y	y	y	y	y	n	n			rest	none
3:	y	y	y	y	y	n	n			rest	none
4:	y	y	y	y	y	n	n			rest	none
5:	y	y	y	y	y	n	n			rest	none
6:	y	y	y	y	y	n	n			rest	none

Figure 61: Route-pattern 2 form

5.12. 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 [3], [4], [5], and [6] for further details if necessary. The samples that follow are provided for reference purposes only.

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:				
3:				18:				33:				48:				

Figure 62: Agent form – page 2

display hunt-group 2		Page 1 of 4
HUNT GROUP		
Group Number: 2	ACD? y	
Group Name: Skill12	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 :	

Figure 63: Skill 2 Hunt Group form – page 1

display vdn 44002		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 44002		
Name*: Skill12		
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		

Figure 64: Skill 2 VDN form – page 1

display vector 2		Page 1 of 6
CALL VECTOR		
Number: 2	Name: Skill12	
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		

Figure 65: Skill 2 Vector 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		

Figure 66: Agent form – page 1

6. Avaya Modular Messaging

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

6.1.1. Hunt Group for Station Coverage to Modular Messaging

Hunt group 1 is used in the reference configuration to verify Modular Messaging coverage functionality. The hunt group (e.g. 1) is defined with the 5 digit Modular Messaging pilot number (e.g. 46000). The hunt group is associated with a coverage path (e.g. **h1** in **Figure 69**) and the coverage path is assigned to a station (e.g. 40002 in **Figure 70**). Communication Manager will use the AAR access code “8” (defined in **Section 5.2**) to dial Modular Messaging (e.g. 846000).

display 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		

Figure 67: Hunt Group 1Form – Page 1

display hunt-group 1		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits
46000	46000	(e.g., AAR/ARS Access Code) 8

Figure 68: Hunt Group 1 Form – Page 2

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

Figure 69: Coverage Path 1 Form

display station 40002		Page 1 of 5
STATION		
Extension: 40002	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 123456	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: 9630_H323	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 40002	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Figure 70: Station 40002 Form

7. Configure Acme Packet SBC⁷

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 [11] 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.

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
  last-modified-by      admin@console
  last-modified-date    2009-11-05 17:50:26

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

⁷ Although an Acme Net-Net SD 3800 was used in the reference configuration, these configurations also apply to the 4250 and 4500 platforms

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
last-modified-by	admin@console
last-modified-date	2009-11-04 00:56:55
policy-attribute	
next-hop	SAG:ENTERPRISE
realm	INSIDE
action	none
terminate-recursion	disabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	

media-manager

state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000

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

network-interface

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

network-interface

name	wancom2
------	---------

```

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

```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the AT&T IP 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	
last-modified-by	admin@console
last-modified-date	2009-11-06 13:33:09

<p>ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.</p>
--

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

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

phy-interface	
name	s0p1
operation-type	Media
port	1
slot	0
virtual-mac	00:08:25:a0:f3:69

admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
last-modified-by	admin@console
last-modified-date	2009-11-04 00:24:39

```

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

```

```

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

```

```

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

```

```

phy-interface
  name          wancom1
  operation-type Control
  port          1
  slot          0

```

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

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

<p>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.</p>
--

realm-config	
identifier	OUTSIDE
description	
addr-prefix	0.0.0.0
network-interfaces	
s0p0:0	
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	NAT_IP
manipulation-string	
class-profile	
average-rate-limit	0
access-control-trust-level	medium
invalid-signal-threshold	4
maximum-signal-threshold	3000

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

<p>ANNOTATION: The realm configuration "INSIDE" below represents the internal network on which the Avaya elements reside.</p>
--

realm-config

identifier	INSIDE
description	
addr-prefix	0.0.0.0
network-interfaces	
	s0p1:0
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
generate-UDP-checksum	disabled

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

last-modified-date 2009-11-04 00:49:58

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

ANNOTATION: The **session agent** below represents the AT&T IP Flexible Reach service border element. The Acme will attempt to send calls to the border element based on successful responses to the OPTIONS "ping-method". The AT&T IP Flexible Reach service border element is also specified in the **session-group** section below. Note - See Addendum 2 for an example of redundant session agents.

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

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

ANNOTATION: The session agent below represents the 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_0
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	

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

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

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

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

135.25.29.74

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

ANNOTATION: The session group below represents Session Manager. This session-group is specified in the local-policy source-realm "OUTSIDE".

session-group

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

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the 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
last-modified-by	admin@console
last-modified-date	2009-11-04 00:34:23

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

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

sip-interface	
state	enabled
realm-id	OUTSIDE
description	
sip-port	
address	192.168.64.130
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	agents-only
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30

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

<p>ANNOTATION: The SIP interface below is used to communicate with the Avaya elements.</p>

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

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

ANNOTATION: The NAT_IP SIP manipulation below performs address translation and topology hiding for SIP messages between the AT&T IP 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 **match-val-type** value **any** allows the either the IP address or SIP Domain of Session Manager to be specified in the far-end domain field of the Communication Manager signaling group 1 (see **Section 5.8.1**). In either case the Acme will convert this value to the "outside" IP address of the Acme (**\$Local_IP**).

In the header-rule **manipTo**, the **match-val-type** value **any** allows the either the IP address or SIP Domain of Session Manager to be specified in the far-end domain field of the Communication Manager signaling group 1 (see **Section 5.8.1**). In either case 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 - In addition to manipulating the From and To headers, the NAT_IP SIP manipulation also is used to delete a P-Site header inserted by Session Manager. Session Manager Release 6 inserts a P-Site header which contains the IP-Address of System Manager as a parameter. Since there is no value in sending this header to AT&T in the sample configuration, the header is stripped by the Acme. Calls can still be completed successfully if the configuration in this section is not performed and the P-Site header is sent to AT&T. This information is included to allow the reader to delete the P-Site header if desired so that the private IP address of System Manager is not revealed on the public side of the SBC.

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

ANNOTATION: The steering pools below define the IP Addresses and RTP port ranges on the respective realms. The "OUTSIDE" realm IP Address will be used as the CPE media traffic IP Address to communicate with AT&T. **The "OUTSIDE" realm RTP port range is an AT&T IP 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	
last-modified-by	admin@console
last-modified-date	2009-11-04 00:49:36

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

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

link-redundancy-state	disabled
source-routing	enabled
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
last-modified-by	admin@console
last-modified-date	2009-11-04 00:27:17

8. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya phones, fax machines (Ventafax application), Acme Packet 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 MIS/PNT transport.

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

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

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

9. Verification Steps

The following steps may be used to verify the configuration:

9.1. General

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

9.2. Avaya Aura® Communication Manager

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 converted the AT&T DID dialed by PSTN (732-320-5050) 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
```

Figure 71: Communication Manager *list trace tac 101* – Inbound call.

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

9.3. Avaya Aura® Session Manager

The following commands are issued from the System Manager console.

1. Verify the call routing administration on Session Manager.
 - a. In the left pane of the Avaya Aura® System Manager Common Console, under Elements/Session Manager/System Tools, click on “Call Routing Test”. The **Call Routing Test** page shown in **Figure 72** will open.
 - b. In the **Call Routing Test** page, enter the appropriate parameters of the test call. **Figure 73** shows a routing test for an inbound call from PSTN to AT&T DID **7323204384**. The call arrives from the Acme Packet SBC and the calling number **7326712438**.
 - c. Click on “Execute Test”.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 16, 2010 1:32 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Session Manager / System Tools / Call Routing Test

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI: 7323204384@192.168.67.210
 Calling Party URI: 7326712438@135.25.29.74
 Day Of Week: Monday
 Time (UTC): 14:59
 Called Session Manager Instance: SM60

Calling Party Address: 192.168.67.130
 Session Manager Listen Port: 5060
 Transport Protocol: TCP

Execute Test

Figure 72: Session Manager Call Routing Test Page

- d. The results of the test are displayed as shown in **Figure 73**. The ultimate routing decision is displayed under the heading **Routing Decisions**. The example test shows that the PSTN call to **7323204384** is sent by Session Manager to the Communication Manager extension **40002**. Under that section the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated). Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 4**.

Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at July 16, 2010 1:32 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Session Manager / System Tools / Call Routing Test

Elements

- Conferencing
- Presence
- Application Management
- Endpoints
- SIP AS 8.1
- Feature Management
- Inventory
- Templates
- Session Manager
 - Dashboard
 - Session Manager
 - Administration
 - Communication Profile Editor
 - Network Configuration
 - Device and Location Configuration
 - Application Configuration
 - System Status
 - System Tools
 - Maintenance Tests
 - SIP Tracer
 - Configuration
 - SIP Trace Viewer
 - Call Routing Test
 - Events
 - Groups & Roles
 - Licenses
 - Routing
 - Security
 - System Manager Data
 - Users

Help

- Call Routing Testing
- Page Fields

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI <input type="text" value="7323204384@192.168.67.210"/>	Calling Party Address <input type="text" value="192.168.67.130"/>
Calling Party URI <input type="text" value="7326712438@135.25.29.74"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Monday"/>	Time (UTC) <input type="text" value="14:59"/>
Called Session Manager Instance <input type="text" value="SM60"/>	Transport Protocol <input type="text" value="TCP"/>

Routing Decisions

Route < sip:40002@customerb.com > to SIP Entity ACM60 (192.168.67.202). Terminating Location is main.

Routing Decision Process

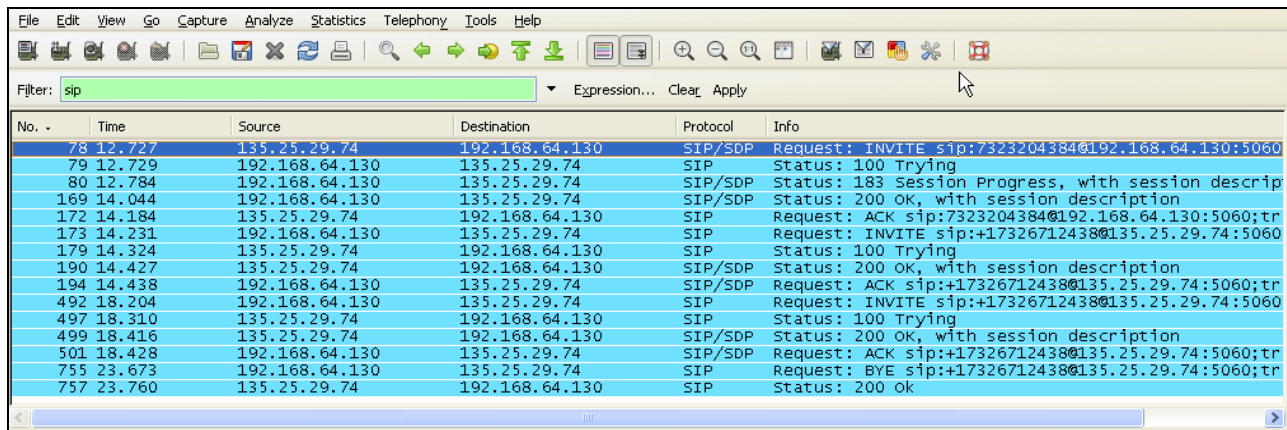
NRP Sip Entities: Replacing Session Manager FQDN/IP address < 192.168.67.210 > with < customerb.com > in request URI.
NRP Adaptations: AT&T applied.
NRP Adaptations: P-Asserted-Identity set to sip:7326712438@135.25.29.74
BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.
Originating Location is main. Using digits < 7323204384 > and host < customerb.com > for routing.
NRP Dial Patterns: No matches for digits < 7323204384 > and domain < customerb.com >.
NRP Dial Patterns: Found a Dial Pattern match for pattern < 732320 > Min/Max length 10/10 and domain < null >.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACM60.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACM60.
END EMERGENCY CALL CHECK: This is not an emergency call.
Adapting and proxying for SIP Entity ACM60.
NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.
NRP Adaptations: To_ACM60 applied.
NRP Adaptations: P-Asserted-Identity set to sip:7326712438@customerb.com
NRP Adaptations: Request-URI set to sip:40002@customerb.com
Route < sip:40002@customerb.com > to SIP Entity ACM60 (192.168.67.202). Terminating Location is main.

Figure 73: Call Routing Test Page -Completed

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.

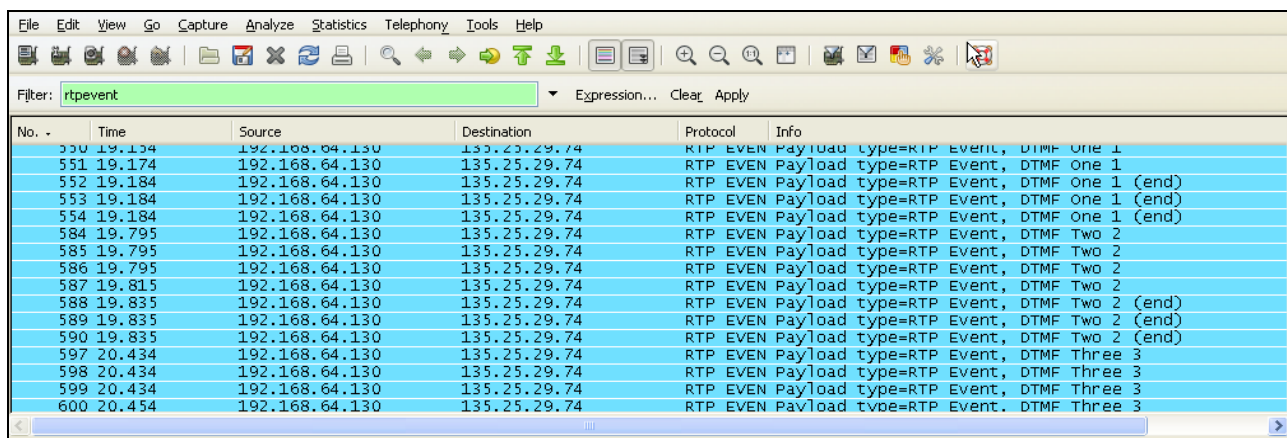
1. The following are examples of calls filtering on the SIP protocol.



No. -	Time	Source	Destination	Protocol	Info
78	12.727	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:73232043840192.168.64.130:5060
79	12.729	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying
80	12.784	192.168.64.130	135.25.29.74	SIP/SDP	Status: 183 Session Progress, with session description
169	14.044	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description
172	14.184	135.25.29.74	192.168.64.130	SIP	Request: ACK sip:73232043840192.168.64.130:5060;tr
173	14.231	192.168.64.130	135.25.29.74	SIP	Request: INVITE sip:+173267124380135.25.29.74:5060
179	14.324	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
190	14.427	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
194	14.438	192.168.64.130	135.25.29.74	SIP/SDP	Request: ACK sip:+173267124380135.25.29.74:5060;tr
492	18.204	192.168.64.130	135.25.29.74	SIP	Request: INVITE sip:+173267124380135.25.29.74:5060
497	18.310	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
499	18.416	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
501	18.428	192.168.64.130	135.25.29.74	SIP/SDP	Request: ACK sip:+173267124380135.25.29.74:5060;tr
755	23.673	192.168.64.130	135.25.29.74	SIP	Request: BYE sip:+173267124380135.25.29.74:5060;tr
757	23.760	135.25.29.74	192.168.64.130	SIP	Status: 200 OK

Figure 74: –SIP Protocol trace – Inbound call from AT&T

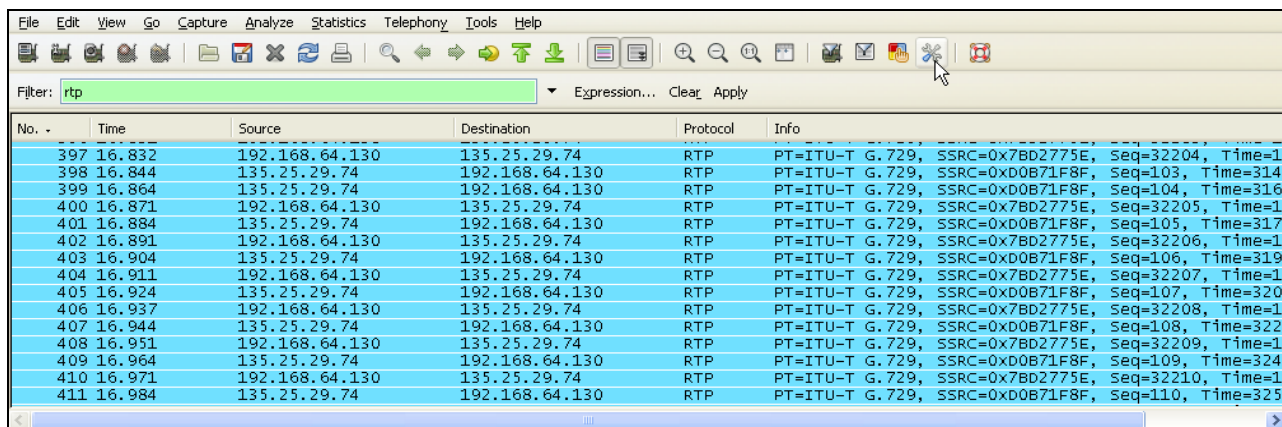
2. The following is an example of a call filtering on DTMF.



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

Figure 75: – RTPEvent (DTMF) trace

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



The image shows a Wireshark network packet capture window. The filter is set to 'rtp'. The packet list shows 13 packets (397-411) of RTP protocol. The packet details pane shows the RTP header and payload. The payload is identified as G.729, SSRC=0x7BD2775E, Seq=32204, Time=1. The packet bytes pane shows the raw data.

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

Figure 76: – RTP trace (showing codec used)

9.5. Acme Packet SBC

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

10. Conclusion

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

Acme Packet Support (login required):

- [11] <http://support.acmepacket.com>

AT&T IP Toll Free Service Descriptions:

- [12] *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 – Alternate method for suppressing plus signs (“+”) in calling header fields.

As described in **Section 1.3**, Avaya Aura® Communication Manager 6.0 inserts a leading plus sign to calling number headers (e.g. Update, From, PAI, Contact) when public numbering processing is used (the typical default configuration). The AT&T IP Toll Free service does not support the use of digit strings with a leading plus sign (“+”) in the calling number headers (Update in the case of the inbound AT&T IP Toll Free service). The Avaya Aura® Communication Manager 6.0 provisioning described in **Sections 5.3, 5.8, 5.9, 5.10, and 5.11**, will prevent the insertion of these plus signs by using private numbering processing. However, an alternate method is shown here utilizing the Acme Packet Net-Net Session Director to strip off the plus signs inserted by Avaya Aura® Communication Manager when public number processing is used.

12.1. Avaya Aura® Communication Manager provisioning.

This section shows the typical Avaya Aura® Communication Manager provisioning, in contrast to the provisioning shown in **Section 5**. Only those parameters having impact on the plus sign insertion are described.

12.1.1. SIP Trunk for AT&T IP Toll Free Access

This section describes the typical provisioning for the SIP trunk used for AT&T access. This trunk corresponds to the trunk defined in **Section 5.8.1**.

1. Enter the **display signaling-group x** command, where **x** is the number of an unused signaling group (e.g. 1), and verify the following:
 - Verify that **Peer Detection Enabled** is “y” and that **Peer Server** is **SM**.

display 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: ASM60		
Near-end Listen Port: 5060		Far-end Listen Port: 5060		
		Far-end Network Region: 2		
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		

Figure 77: Signaling-Group 1 Form for AT&T IP Toll Free Calls

2. Enter the **display 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, verify the following:
 - Verify **Direction** is set to “**two-way**”.
 - Verify the **Service Type** is set to “**public-ntwrk**”.

display trunk-group 1		Page 1 of 21
TRUNK GROUP		
Group Number: 1	Group Type: sip	CDR Reports: y
Group Name: To ASM_6_0	COR: 1	TN: 1 TAC: 101
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? N	
Member Assignment Method: auto		
Signaling Group: 1		
Number of Members: 20		

Figure 78: Trunk-Group 1 Form for AT&T IP Toll Free Calls – Page 1

3. On Page 3 of the **Trunk Group** form:
 - Verify the **Numbering Format** is set to **public**

display trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

Figure 79: Trunk-Group 1 Form for AT&T IP Toll Free Calls – Page 3

12.1.2. Route Pattern for Trunk to AT&T

Since the AT&T IP Toll Free service does not support outbound dialing, there should be no need for a route-pattern directing calls to the AT&T SIP trunk (e.g. trunk 1). However if such a trunk exists (possibly to support other call scenarios), verify the following:

1. There is no entry in the **Numbering Format** column.

display route-pattern 1													Page 1 of 3	
Pattern Number: 1 Pattern Name: To_AT&T														
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		1										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			<blank>	next		
2:	y	y	y	y	y	n	n	rest				none		
3:	y	y	y	y	y	n	n	rest				none		
4:	y	y	y	y	y	n	n	rest				none		
5:	y	y	y	y	y	n	n	rest				none		
6:	y	y	y	y	y	n	n	rest				none		

Figure 80: Route-pattern 1 form

12.1.3. Private Numbering

Typically the Private Numbering form is used for digit handling/manipulation internal to the CPE (not to AT&T). In the reference configuration Communication Manager extensions are passed to Modular Messaging in the calling number fields. However no Communication Manager to AT&T DID number conversions are performed here.

1. Verify the passing of Communication Manager extensions to Modular Messaging.
 - **Ext Len** – Enter the total number of digits in the local extension range (e.g. 5).
 - **Ext Code** – Enter the broadest wildcard match necessary to cover extensions with coverage to Modular Messaging (e.g. 4 to cover the provisioned extension range 4xxxx).
 - **Trk Grp(s)** – Enter the number of the Local trunk group (e.g. 2).
 - **CPN Prefix** – Leave blank.
 - **CPN Len** – Enter the total number of extension digits (e.g. 5).

For example, in **Figure 80**, any extension beginning with 4 and 5 digits long will remain unchanged for trunk 2 (Modular Messaging processing).

display private-numbering 0										Page 1 of 2	
NUMBERING - PRIVATE FORMAT											
Ext	Ext	Trk		Private		Total					
Len	Code	Grp (s)		Prefix		Len					
5	4	2				5		Total Administered: 1			
								Maximum Entries: 540			

Figure 81: Public- Numbering Form – Modular Messaging digits

12.1.4. Public Unknown Numbering

Typically the Public Unknown Numbering form is used for digit handling/manipulation external to the CPE (e.g. to AT&T). In the reference configuration Communication Manager extensions are converted to AT&T DID numbers in the calling number fields.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp (s)	Prefix	CPN	
				Len	
5	40001	1	7323204050	10	Total Administered: 3
5	40002	1	7323204051	10	Maximum Entries: 9999
5	41001	1	7323204052	10	

Figure 82: Public- Numbering Form

The combination of these parameters shown in **Section 12.1** results in Avaya Aura® Communication Manager 6.0 using public numbering and inserting a leading plus sign (“+”) to calling number fields. For example, if 7323204050 is specified in the public-unknown-numbering form, the string +7323204050 will be inserted in the Update, From, Contact, and PAI headers.

12.2. Acme Packet Net-Net Session Director⁸

The following provisioning was added to an existing sip-manipulation *NAT_IP* as shown in **Section 7**. These additional parameters remove plus signs (“+”) from the Update, From, Contact, and PAI headers, before sending the frames to the AT&T IP Toll Free service. Although only the Update header manipulation is required (the AT&T IP Toll Free service is an inbound only service), the other header manipulations are shown for completeness.

sip-manipulation		NAT_IP
name		Topology hiding for TO and FROM headers
description		
split-headers		
join-headers		
header-rule		
name		manipFrom
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

⁸ Although an Acme Net-Net SD 3800 was used in the reference configuration, these configurations also apply to the 4250 and 4500 platforms.

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
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	
new-value	\$REMOTE_IP
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	modPAI
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	modContact
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	modFrom
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	modUpdate
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
last-modified-by	admin@console

13. Addendum 2 – Acme Packet Net-Net Redundancy to Multiple AT&T Border Elements

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

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

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

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

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

session-agent

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

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

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

```

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

```

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

```

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

```

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ® are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.