AVAYA

Avaya Solution & Interoperability Test Lab

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

Abstract

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

Avaya Aura® Communication Manager 5.2.1 is a telephony application server. The Avaya Aura® Session Border Controller 6.0.2 is the point of connection between Avaya Aura® Communication Manager and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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

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

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
1 of 64
ACM521AASBCIPFR

TABLE OF CONTENTS

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
3 of 64
ACM521AASBCIPFR

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 5.2.1 and the Avaya Aura® Session Border Controller 6.0.3 with the AT&T IP Flexible Reach service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Communication Manager 5.2.1 is a telephony application server. In the reference configuration, Avaya Aura® Communication Manager 5.2.1 is provisioned in an Access Element configuration (note that SIP endpoints are not supported in an Aura® Communication Manager 5.2.1 Access Element configuration or when Avaya Aura® Session Manager is not present). An Avaya Aura® Session Border Controller is the point of connection between Avaya Aura® Communication Manager and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. The AT&T IP Flexible Reach service utilizes AVPN[1] or MIS-PNT[2] transport services.

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

2. General Test Approach and Test Results

The test environment consisted of:
- A simulated enterprise with Avaya Aura® Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya Aura® Session Border Controller, and Avaya Modular Messaging.
- A laboratory version of the AT&T IP Flexible Reach service, to which the simulated enterprise was connected via AVPN or MIS-PNT transport.

2.1. Interoperability Compliance Testing

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

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

---

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

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

2.2. Test Results

The main test objectives were to verify the following features and functionality:
- Inbound and outbound calls, and two-way talk path establishment, between PSTN and Communication Manager telephones via the AT&T Flexible Reach service.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- T.38 fax calls between Communication Manager and the AT&T IP Flexible Reach service/PSTN G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833 between Communication Manager and the AT&T IP Flexible Reach service/PSTN automated access systems.
- Inbound AT&T IP Flexible Reach service calls to Communication Manager that are directly routed to stations, and unanswered, can be covered to Avaya Modular Messaging.
- Long duration calls.

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

2.2.1.   Known Limitations

1. SIP stations are not supported by Communication Manager 5.2.1 in an Access Element configuration, or when Session Manager is not present in the configuration.
2. G.722 codec is not supported between Communication Manager and the AT&T IP Flexible Reach service.
3. G.711 faxing is not supported between Communication Manager and the AT&T IP Flexible Reach service. Communication Manager does not support the protocol negotiation that AT&T requires to have G.711 fax calls work. T.38 faxing is supported, as is Group 3 and Super Group 3 fax. Fax speeds are limited to 9600 in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Communication Manager.
4. The AT&T IP Flexible Reach service does not support SIP History-Info headers. However, the AT&T IP Flexible Reach service requires that SIP Diversion Header be sent for certain redirected calls (e.g., Call Forward). Communication Manager will insert the Diversion Header for these types of calls (see **Section 5.7.1)**. For all other calls, the Avaya Aura® Session Border Controller was used in the reference configuration to strip off History-Info headers (see **Section 7.2.5**). Alternatively they may be disabled on the Communication Manager SIP trunk associated with calls to/from AT&T (see **Section 5.7.1**).
5. Emergency 911/E911 Services Limitations and Restrictions – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor.

   While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

2.3. Support

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

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. The "Connect with Avaya" section provides the worldwide support 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.

3. Reference Configuration

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

- Communication Manager provides the voice communications services for a particular enterprise site. In the reference configuration, Communication Manager 5.2.1 runs on an Avaya S8720 Server in a G650/Control LAN (C-LAN) configuration. This solution is extensible to other Avaya S8xxx Servers. The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G650 Media Gateway is used. The G650 contains the system boards such as the Control LAN (C-LAN) and Media Processor (MedPro). This solution is extensible to other Avaya Media Gateways.
- Avaya "desk" phones are represented with Avaya 46x0, 96x0, and 96x1 Series IP Telephones running H.323 firmware, Avaya 6424 Series Digital Telephone, as well Avaya one-X® Communicator PC based softphone running in H.323 mode. The H.323 telephones on the enterprise registered to the Communication Manager C-LANs.
- The Avaya Aura® Session Border Controller provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network[3]. UDP transport protocol is used between the Avaya Aura® SBC and the AT&T IP Flexible Reach service.
- An existing Avaya Modular Messaging system (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.

---

[3] The AT&T IP Flexible Reach service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya Aura® SBC in this sample configuration. Communication Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya Aura® SBC. In the reference configuration, Communication Manager uses SIP over TCP to communicate with the Avaya Aura® SBC.
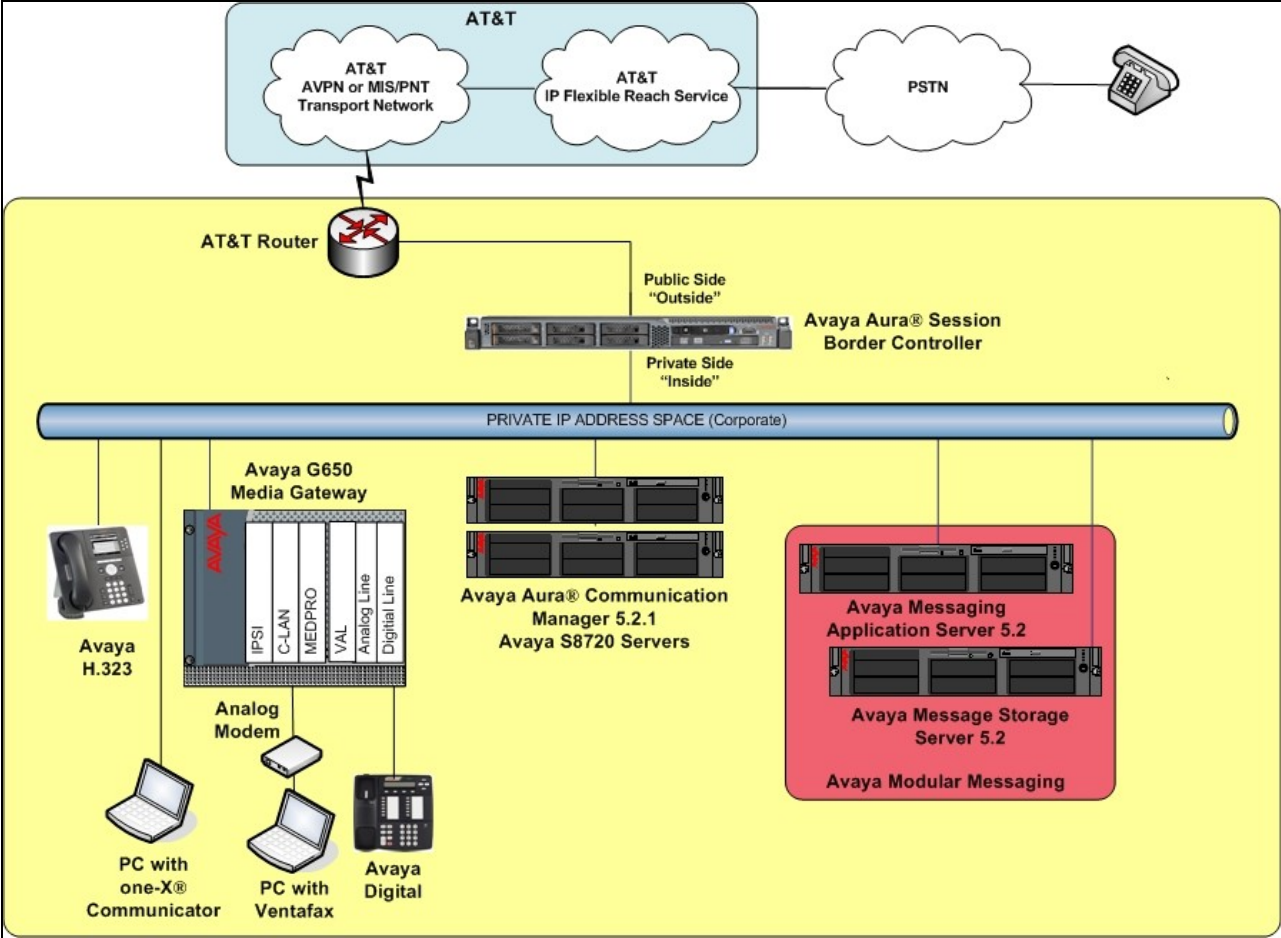
Figure 1: Reference configuration

JF:Reviewed
SPOC 1/4/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

8 of 64
ACM521AASBCIPFR

3.1. Illustrative Configuration Information

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

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

Component	Illustrative Value in these Application Notes
Avaya Aura® Communication Manager	
Control LAN (C-LAN) IP Address	192.168.67.14
Media Processor (MedPro) IP Address	192.168.67.15
Avaya Aura® Communication Manager extensions	26xxx
Avaya CPE local dial plan	2xxxx
Modular Messaging Pilot Extension	26000
Avaya Aura® Session Border Controller	
IP Address of "Outside" (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service)	192.168.64.130
IP Address of "Inside" (Private) Interface (connected to Avaya Aura® Communication Manager)	192.168.67.125
Avaya Modular Messaging	
Messaging Application Server (MAS) IP Address	192.168.67.141
Messaging Server (MSS) IP Address	192.168.67.140
Modular Messaging Dial Plan	1723114xxxx
AT&T IP Flexible Reach Service	
Border Element IP Address	135.25.29.74
AT&T Access router interface (to Avaya Aura® outside)	192.168.64.254
AT&T Access Router NAT address (Avaya Aura® outside address)	135.16.170.55

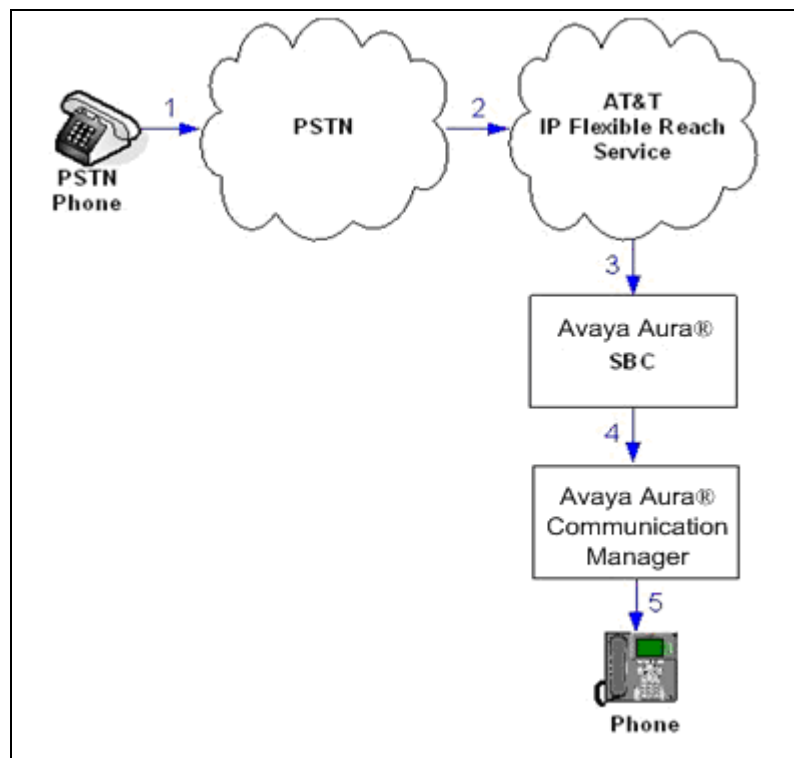**Table 1: Illustrative Values Used in these Application Notes**

3.2. Call Flows

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

3.2.1. Inbound

The first call scenario is an inbound AT&T IP Flexible Reach service call that arrives on the Acme Packet SBC and is routed to Communication Manager, which in turn routes the call to a phone, fax, or a vector.

1. A PSTN phone originates a call to an AT&T IP Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service routes the call to the Acme Packet SBC.
4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Communication Manager.
5. Depending on the called number, Communication Manager routes the call to a phone, a fax or a vector.

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
10 of 64
ACM521AASBCIPFR

3.2.2. Outbound

The second call scenario is an outbound call initiated on Communication Manager, and sent to the Acme SBC for delivery to AT&T IP Flexible Reach service.

1. A Communication Manager phone or fax originates a call to an AT&T IP Flexible Reach service number for delivery to PSTN.
2. Communication Manager routes the call to the Acme Packet SBC.
3. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach service.
4. The AT&T IP Flexible Reach service delivers the call to PSTN.
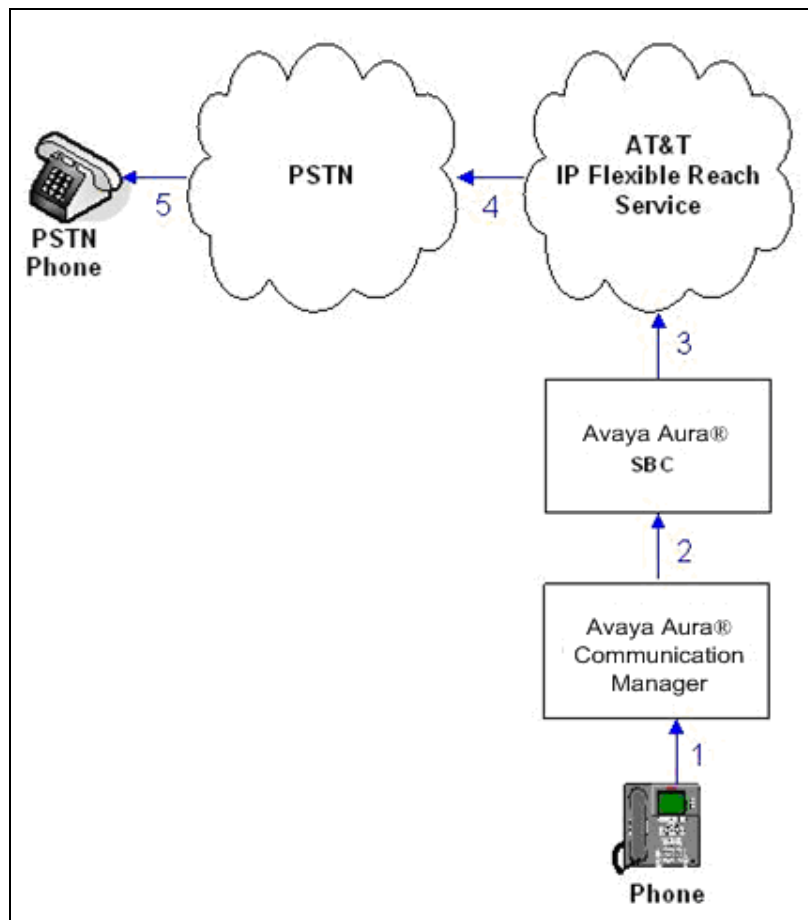
3.2.3. Call Forward Re-direction

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

> **Note** – The AT&T IP Flexible Reach service requires the use of SIP Diversion Header for some redirected calls to complete (see **Section 5.7.1**).

1. Same as the first call scenario in **Section 3.2.1**.
2. Because the Communication Manager phone has set Call Forward to another AT&T IP Flexible Reach service number, Communication Manager initiates a new call back out to the Acme Packet SBC, and to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service places a call to the alternate destination and upon answer, Communication Manager connects the calling party to the target party.
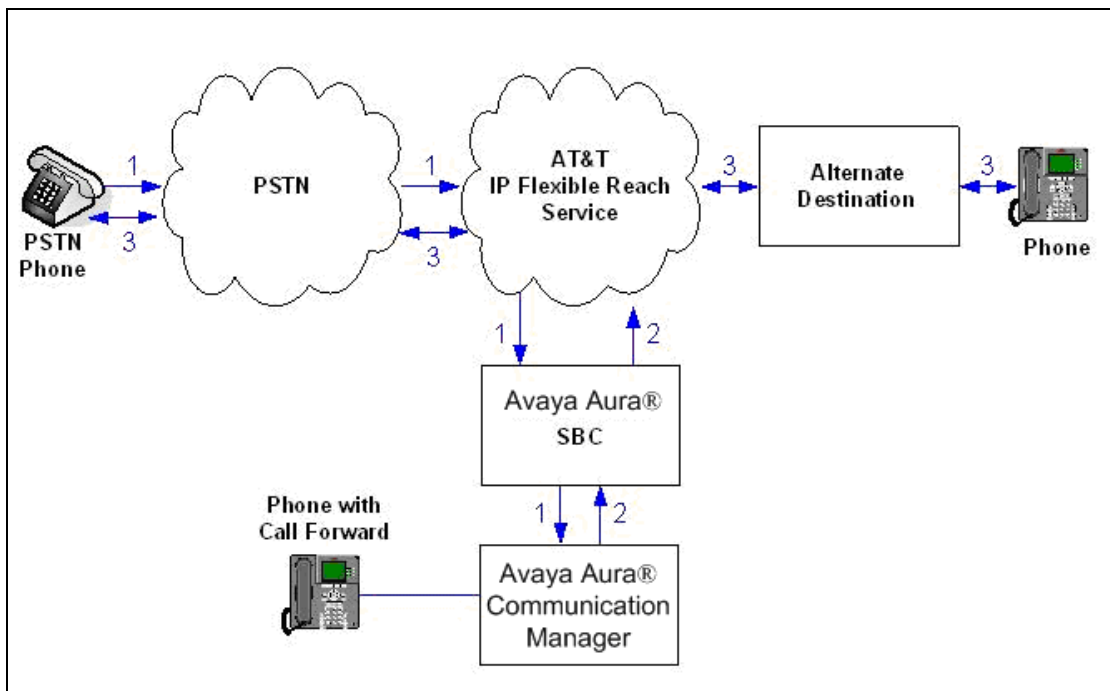
3.2.4. Coverage to Voicemail

This call scenario is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Modular Messaging system connected to Communication Manager.

1. Same as the first call scenario in **Section 3.2.1**.
2. The called Communication Manager phone does not answer the call, and the call covers to the phone's voicemail. Communication Manager forwards[4] the call to Avaya Modular Messaging. Avaya Modular Messaging answers the call and connects the caller to the called phone's voice mailbox. Note that the call[5] continues to go through Communication Manager.

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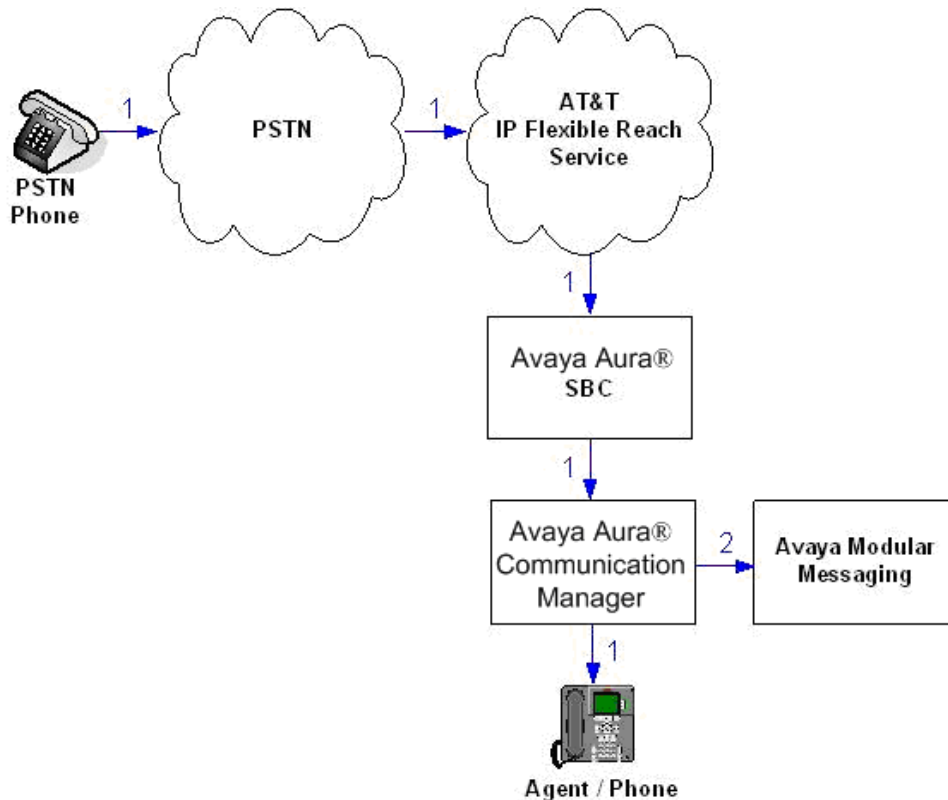
[4] Avaya Aura® Communication Manager places a call to Avaya Modular Messaging, and then connects the inbound caller to Avaya Modular Messaging. SIP redirect methods, e.g., 302, are not used.
[5] The SIP signaling path still goes through Avaya Aura® Communication Manager. In addition, since the inbound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

4. Equipment and Software Validated

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

Component	Version
Avaya S8720 Server	Avaya Aura® Communication Manager 5.2.1 SP10 (02.1.016.4-19191)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW15 FW054
TN799DP Control-LAN (C-LAN)	HW01 FW040
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW061
TN2501AP VAL-ANNOUNCEMENT	HW03 FW021
TN2224CP Digital Line	HW08 FW015
TN793B Analog Line	HW05 FW011
Avaya S8800 Server	Avaya Aura® Session Border Controller Template 6.0.3.0.2
Avaya 9630 IP Telephone	H.323 Version S3.102S
Avaya 9621 IP Telephone	H.323 Version S6.020S
Avaya one-X® Communicator	6.1.1.02-SP1-32858
Avaya 4610SW IP Telephone	H323 Version 2.9.1
Avaya 6424D Digital Telephone	-
Avaya Modular Messaging (MAS and MSS) on Avaya S3500 Servers	Release 5.2 – SP5 with Patch 1 (9.0.350.5019)
Fax device	Ventafax Home Version 6.1.59.144
AT&T IP Flexible Reach Service using AVPN or MIS-PNT transport service connection	VNI 22

Table 2: Equipment and Software Versions

JF:Reviewed
SPOC 1/4/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

14 of 64
ACM521AASBCIPFR

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 [1] and [2] 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.

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

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

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


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

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

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

Step 3 - On **Page 4** of the **System-Parameters Customer-Options** form, verify that the **Enhanced EC500?** , the **IP Stations?, ISDN-PRI?** and the **IP Trunks?** fields are set to "**y**".

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

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

```
display system-parameters customer-options                       Page   5 of  11
                              OPTIONAL FEATURES
              Multinational Locations? n            Station and Trunk MSP? y
Multiple Level Precedence & Preemption? y       Station as Virtual Extension? y
                   Multiple Locations? n

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

5.2. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. Note that the values shown below are examples used in the reference configuration.

Step 1 - Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings:
- 3-digit dial access codes (indicated with a **Call Type** of "**dac**") beginning with the digit "**1**" (e.g., Trunk Access Codes, TACs, defined for trunk groups in this reference configuration conform to this format).
- 5-digit extensions with a **Call Type** of "**ext**" beginning with the digits "**2xxxxx**" (e.g., Local extensions for Communication Manager stations, agents, and Vector Directory Numbers, VDNs, in this reference configuration conform to this format).
- 1-digit facilities access code (indicated with a **Call Type** of "**fac**") (e.g., "**8**" access code for outbound AAR dialing). Note – AAR is typically used for local trunk calls. In the reference configuration AAR is used for call coverage to Modular Messaging (see **Section 5.10.3**).
- 1-digit facilities access code (indicated with a **Call Type** of "**fac**") (e.g., "**9**" access code for outbound ARS dialing). Note – ARS is typically used for public trunk calls, (e.g., to/from PSTN via the AT&T IP Flexible Reach service).
- 3-digit facilities access codes beginning with ***** and **#** (e.g., for Agent logon/logoff).

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

5.3. IP Node Names

Node names define IP addresses to various Avaya components in the Customer Premise Equipment (CPE) location.

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

Step 2 – Repeat **Step 1** to add node names for Modular Messaging (e.g., **MM**).

Step 3 - Control LAN (C-LAN) signaling boards were used in the reference configuration. These entries appear based on the addresses defined during Communication Manager installation. Make note of their node names and IP addresses (e.g., **MainCLAN2** & **192.168.67.14**). These will be used to define the SIP trunks.

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

5.4. IP Interface for IP Interface MainCLAN2

In the reference configuration, the C-LAN named **MainCLAN2** was used for the SIP trunks.

Step 1 – Enter the **list ip-interface all** command. Note the slot value associated with the C-LAN to be used to define the SIP trunks (e.g., **01a03** for **MainCLAN2**).

```
list ip-interface all
                            IP INTERFACES
                                                             Net
ON Type   Slot  Code/Sfx    Node Name/     Mask  Gateway Node  Rgn  VLAN
                            IP-Address
-- ------ ----- --------    --------------  ----  --------------  ---  ----
 y C-LAN  01A02 TN799  D    MainCLAN1       /24   Gateway001      1    n
                            192.168.67.13
 y C-LAN  01A03 TN799  D    MainCLAN2       /24   Gateway001      1    n
                            192.168.67.14
 y MEDPRO 01A04 TN2602      MainMP1A04      /24   Gateway001      1    n
                            192.168.67.15
 y MEDPRO 01A05 TN2602      MainMP1A05      /24   Gateway001      1    n
                            192.168.67.16
 y VAL    01A06 TN2501      MainVAL1A06     /24   Gateway001           n
                            192.168.67.17
```

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

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

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

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


                              IPV4 PARAMETERS

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

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

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

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

                              ETHERNET OPTIONS
              Slot: 01A03
              Auto? y


                              IPV6 PARAMETERS
           Node Name:
        Subnet Mask: /64
 Gateway Node Name:
  Enable Interface? n


       Ethernet Link:
```

5.5. IP Network Regions

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

5.5.1. IP Network Region 1 – Local Region

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

Step 1 – Enter **change ip-network-region x**, where x is the number of an unused IP network region (e.g., region 1). This IP network region will be used to represent the AT&T IP Flexible Reach service. Populate the form with the following values:
- Enter a descriptive name (e.g., **LOCAL**).
- Enter **customera.com** in the **Authoritative Domain** field.
- Enter **1** for the **Codec Set** parameter.
- **Intra IP-IP Audio Connections** – Set to "**yes**", indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter IP-IP Audio Connections** – Set to "**yes**", indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min**: - Set to **16384 (AT&T requirement).**
- **UDP Port Max**: - Set to **32767 (AT&T requirement).**

```
change ip-network-region 1                                   Page   1 of  20
                            IP NETWORK REGION
  Region: 1
Location: 1          Authoritative Domain: customera.com
     Name: LOCAL
MEDIA PARAMETERS                     Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                   Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 16384                          IP Audio Hairpinning? n
  UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                               RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
          Keep-Alive Count: 5
```

Step 2 - On **Page 4** of the form:
- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region 2 in the **dst rgn** column, enter **2** (this means region 1 is permitted to talk to region 2 and they will use codec set 2 to do so). The **direct WAN** and **WAN-BW-limits Units** columns will self populate with **y** and **NoLimit**.
- Let all other values default for this form.

```
change ip-network-region 1                                      Page    4 of  20

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

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

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

Step 1 - Repeat the steps in **Section 5.5.1** with the following changes:
- **Page 1**
  - Enter a descriptive name (e.g., **AT&T**).
  - Enter **2** for the **Codec Set** parameter.

```
change ip-network-region 2                                      Page    1 of  20
                            IP NETWORK REGION
  Region: 2
Location: 1        Authoritative Domain: customera.com
    Name: AT&T
MEDIA PARAMETERS                      Intra-region IP-IP Direct Audio: yes
      Codec Set: 2                    Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                         IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
       Audio 802.1p Priority: 6
       Video 802.1p Priority: 5     AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                    RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

Step 2 – On **Page 4** of the form:
- Verify that codec **2** is listed for **dst rgn 1** and **2**.

```
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
```

5.6. IP Codec Parameters

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

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

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

```
change ip-codec-set 1                                           Page   1 of   2
                         IP Codec Set
    Codec Set: 1

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

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

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

                         IP Codec Set

                         Allow Direct-IP Multimedia? y
          Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
   Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits


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

5.6.2. Codecs For IP Network Region 2

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

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

```
change ip-codec-set 2                                      Page   1 of   2
                        IP Codec Set

    Codec Set: 2


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

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

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

5.7. SIP Trunks

Two SIP trunks are defined on Communication Manager in the reference configuration:
- AT&T access – SIP Trunk 22
- Local for Modular Messaging access – SIP Trunk 21

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

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

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

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

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

- **Group Type** – Set to "**sip**".
- **Transport Method** – Set to "**tcp**". Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Avaya Aura® SBC and the AT&T IP Flexible Reach service is UDP.
- Verify the **IMS Enabled?** field is set to **n**.
- **Near-end Node Name** – Set to the node name of **MainCLAN2** noted in **Section 5.3** and **5.4**.
- **Far-end Node Name** – Set to the node name of the Avaya Aura® SBC as administered in **Section 5.3** (e.g., **AA-SBC**).
- **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 5.5.2**.
- **Far-end Domain** – Enter **customera.com**. This is the CPE domain used in the reference configuration.
- **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 sends OPTIONS "pings" to the Avaya Aura® SBC to provide link status.

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

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


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

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

- **Group Type** – Set to "**sip**".
- **Group Name** – Enter a descriptive name (e.g., **ATT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **122**).

- **Direction** – Set to "**two-way**".
- **Service Type** – Set to "**public-ntwrk**".
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **22**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g., **10**).

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

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

Step 3 - On **Page 2** of the **Trunk Group** form:
- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900.** This entry will actually cause a value of 1800 to be generated in the SIP header.

```
add trunk-group 22                                          Page   2 of  21

      Group Type: sip

TRUNK PARAMETERS
     Unicode Name: auto
                                         Redirect On OPTIM Failure: 5000
            SCCAN? n                              Digital Loss Group: 18
                   Preferred Minimum Session Refresh Interval(sec): 900

 Disconnect Supervision - In? y  Out? y
```

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

```
add trunk-group 22                                          Page   3 of  21

TRUNK FEATURES
        ACA Assignment? n           Measured: none
                                                        Maintenance Tests? y

                  Numbering Format: public
                                            UUI Treatment: service-provider

                                            Replace Restricted Numbers? n
                                            Replace Unavailable Numbers? n
 Show ANSWERED BY on Display? y
```

Step 5 - On **Page 4** of the **Trunk Group** form:
- Verify that "**Network Call Redirection?**" is set to "**n**" (default).
- Set "**Send Diversion Header?**" to "**y**".
- Set "**Telephone Event Payload Type**" to the RTP payload type required by the AT&T IP Flexible Reach service (e.g., **100**).
- Use default for all other values.

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

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

5.7.2. Local SIP Trunk (Modular Messaging)

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

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **21**), and follow the procedures shown in **Section 5.7.1 Step 1** except:
- **Far-end Node Name** – Set to the node name of Modular Messaging as administered in **Section 5.3** (e.g., **MM**).
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 5.5.1**.

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


 Near-end Node Name: MainCLAN2        Far-end Node Name: MM
 Near-end Listen Port: 5060            Far-end Listen Port: 5060
                                       Far-end Network Region: 1
Far-end Domain: customera.com

                                      Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate           RFC 3389 Comfort Noise? n
        DTMF over IP: rtp-payload        Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3            IP Audio Hairpinning? n
        Enable Layer 3 Test? y                Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n        Alternate Route Timer(sec): 6
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **21**). Follow the procedures shown in **Section 5.7.1 Steps 2-5** except:

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

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

Group Number: 21                        Group Type: sip          CDR Reports: y
  Group Name: Direct_to_MM                    COR: 1      TN: 1         TAC: 121
   Direction: two-way          Outgoing Display? n
 Dial Access? n                                         Night Service:
Queue Length: 0
Service Type: tie                       Auth Code? n


                                                       Signaling Group: 21
                                                     Number of Members: 10
```

Step 3 - On **Page 2** of the **Trunk Group** form: Same as **Section 5.7.1**.

```
add trunk-group 21                                           Page   2 of  21

  Group Type: sip

TRUNK PARAMETERS

    Unicode Name: auto
                                          Redirect On OPTIM Failure: 5000
           SCCAN? n                                Digital Loss Group: 18
                  Preferred Minimum Session Refresh Interval(sec): 900
Disconnect Supervision - In? y  Out? y
```

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

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

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

Step 5 - On **Page 4** of the **Trunk Group** form:
- Verify that "**Network Call Redirection?**" is set to "**n**" (default).
- Verify that "**Send Diversion Header?"** is set to "**n**" (default).
- Verify that "**Support Request History?**" is set to "**y**" (default).
- Set "**Telephone Event Payload Type**" to the RTP payload type required by the AT&T IP Flexible Reach service (e.g., **100**).

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

                            PROTOCOL VARIATIONS


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

5.8. Public Unknown Numbering

In the public unknown numbering form, Communication Manager local extensions are converted to AT&T Flexible Reach numbers (previously identified by AT&T) and directed to the "public" trunk defined in **Section 5.7.1**.

Step 1 - Using the **change public-unknown-numbering 0** command, enter.
- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter a Communication Manager extension (e.g., **26101**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g., **22**).
- **CPN Prefix** – Enter the AT&T P Flexible Reach number (e.g., **7325554050**) that corresponds to the Communication Manager extension.
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

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

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

5.9. Private Numbering

The private-numbering form is used for calls to Modular Messaging (call coverage/retrieval) via the "local" trunk defined in **Section 5.7.2**.

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

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension (e.g., **26000**).assigned to the Modular Messaging coverage hunt group defined in **Section 5.12**.
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **21**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

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

5.10. Outbound Call Routing from Avaya Aura® Communication Manager

5.10.1. Route Patterns

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

5.10.1.1   Route Pattern for Calls to AT&T

This form defines the "public" SIP trunk, based on the route-pattern selected by the ARS table in **Section 5.10.2** (e.g., calls to the AT&T IP Flexible Reach service).

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

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

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

5.10.1.2 Route Pattern for Calls to Modular Messaging

This form defines the "local" SIP trunk, based on the route-pattern selected by the AAR table in **Section 5.10.3** (e.g., calls to the Modular messaging pilot number 26000).

> **Step 1** – Enter the **change route-pattern x** command where "x" is an available route-pattern (e.g., **21**) and enter the following:
>
> - In the **Pattern Name** field, enter a descriptive name (e.g., **To_MM**).
> - In the **Grp No** column, enter **21** for SIP trunk 21 ("local" trunk).
> - In the **FRL** column, enter **0** (zero).
> - In the **1:** row near the bottom of the form, enter **unk-unk** under the **Numbering Format** column.

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

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

5.10.2. ARS Dialing

Automatic Route Selection (ARS) is used to direct calls to AT&T via the route pattern defined in **Section 5.10.1**.1.

> **Step 1** – Enter the change **ars analysis x** command where "x" is a digit string dialed to AT&T . In the following example calls to PSTN using an 11 digit number and beginning with 1732 are defined.
>
> - **Dialed String** enter **1732**
> - **Min** & **Max** enter **11**
> - **Route Pattern** enter **22**
> - **Call Type** enter **ars**

JF:Reviewed
SPOC 1/4/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

30 of 64
ACM521AASBCIPFR

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

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

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


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

5.10.3. AAR Dialing

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

Step 1 – Enter the change **aar analysis 0** command and for the Modular Messaging coverage hunt group extension enter the following:
- **Dialed String** enter **26000**
- **Min** & **Max** enter **5**
- **Route Pattern** enter **21**
- **Call Type** enter **aar**

```
change aar analysis 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
     26000             5    5       21        aar         n
```

5.11. Inbound Calls to Avaya Aura® Communication Manager

5.11.1. Calls from AT&T

The AT&T IP Flexible Reach service will assign DNIS digits that will be inserted in the Request URI of inbound calls. These DNIS digit strings must be converted to extensions defined on Communication Manager.

Step 1 – Enter the change **incoming-call-handling-treatment trunk x** command where x is the "public" trunk defined in **Section 5.7.1** (e.g., **22**). Given that a 10 digit DNIS string of 7325554383 is sent by AT&T, and that the call should be sent to extension 26101, enter the following:
- **Number Len** – **10**

- **Number Digits** – **7325554383**
- **Del** – **10**
- **Insert** – **26101**

Step 2 – Repeat **Step 1** for every AT&T DNIS/Communication Manager extension association.

```
change inc-call-handling-trmt trunk-group 22              Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/         Number    Number       Del Insert
 Feature          Len       Digits


 public-ntwrk    10 7325554383         10   26101
 public-ntwrk    10 7325554384         10   26102
 public-ntwrk    10 7325554385         10   26103
```

5.11.2. Calls from Modular Messaging

Modular Messaging supports an outbound calling feature called "Find Me". This feature has Modular Messaging call a remote number (previously defined by the user) to notify the user that someone is trying to reach them when the call goes to coverage. Typically a 10 or 11 digit public number will be defined. In order for Communication Manager to route this call over the "public" trunk to AT&T, the ARS access code defined in **Section 5.2** (e.g., **9**) must be added to the dialed string sent by Modular Messaging.

Step 1 – Enter the change **incoming-call-handling-treatment trunk x** command where x is the "local" trunk defined in **Section 5.7.2** (e.g., **21**). Given that a 10 digit DNIS string of 17325551234 is sent by Modular Messaging, and that the call should be sent to AT&T, enter the following:
- **Number Len** – **11**
- **Number Digits** – **17325551234**
- **Del** – **<leave blank>**
- **Insert** – **9**

Communication Manager will then route the call as though a local station had dialed 917325551234.

```
change inc-call-handling-trmt trunk-group 21              Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/         Number    Number       Del Insert
 Feature          Len       Digits


 public-ntwrk    11 17325551234          9
```

5.12. Provisioning for Coverage to Modular Messaging

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

5.12.1. Hunt Group for Station Coverage to Modular Messaging

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

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

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

              Group Number: 1                            ACD? n
                Group Name: MM                          Queue? n
           Group Extension: 26000                      Vector? n
                Group Type: ucd-mia            Coverage Path:
                        TN: 1        Night Service Destination:
                       COR: 1                  MM Early Answer? n
             Security Code:                Local Agent Preference? n
    ISDN/SIP Caller Display: mbr-name
```

Step 2 – On **Page 2** of the form enter the following:
- **Message Center –** Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Modular Messaging pilot number (e.g., **26000**).
- **Voice Mail Handle** - Enter the Modular Messaging pilot number (e.g., **26000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 5.2** (e.g., **8**).

```
change hunt-group 1                                            Page    2 of  60
                               HUNT GROUP

                 Message Center: sip-adjunct          Routing Digits
       Voice Mail Number       Voice Mail Handle   (e.g., AAR/ARS Access Code)
            26000                   26000                      8
```

5.12.2. Coverage Path for Station Coverage to Modular Messaging

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

Step 1 – Enter the command **add coverage path x**, where x is an available coverage path (e.g., **1**).
- **Point1** – Specify the hunt group defined in the previous section (e.g., **h1**).
- **Rng** – Enter the number of rings before the stations go to coverage (e.g., **4**).
- Let all other fields default.

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

5.12.3. Station Coverage Path to Modular Messaging

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

> **Step 1** – Enter the command **cha station xxxxx**, where xxxxx is a previously defined station or agent extension (e.g., station **26102**).
> - **Coverage path** – Specify the coverage path defined in **Section 5.12.2** (e.g., **1**). Note that the coverage path field will appear at different positions on the form depending on whether agent or station extensions are being provisioned.

```
change station 26102                                         Page   1 of   5
                                STATION

Extension: 26102                      Lock Messages? n             BCC: 0
    Type: 9630                        Security Code: 123456         TN: 1
    Port: S00000                      Coverage Path 1: 1           COR: 1
    Name: Keith Richards              Coverage Path 2:             COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
            Loss Group: 19        Personalized Ringing Pattern: 1
                                          Message Lamp Ext: 26102
        Speakerphone: 2-way           Mute Button Enabled? y
    Display Language: english           Button Modules: 0
 Survivable GK Node Name:
        Survivable COR: internal       Media Complex Ext:
  Survivable Trunk Dest? y                   IP SoftPhone? n

                                      Customizable Labels? y
```

6. Avaya Modular Messaging

In this reference configuration, Avaya Modular Messaging is used to verify DTMF, Message Wait Indicator (MWI), as well as basic call coverage functionality. The Avaya Modular Messaging used in the reference configuration is provisioned for Multi-Site mode. Multi-Site mode allows Avaya Modular Messaging to serve subscribers in multiple locations. The administration for Modular Messaging is beyond the scope of these Application Notes, (consult [3] and [4] for further details). However, two settings are pertinent to the correct functionality of Modular Messaging Find-Me calls in the reference configuration.

- Setting the RFC2833 Telephone Event Type (**Note** – As shown in the reference configuration software list (**Section 4**), Modular Messaging 5.2 SP 5 is required for this feature).
- Disabling Modular Messaging Enhanced Security for outbound calls to Communication Manager (required to allow Communication Manager and Modular Messaging to be connected directly via a SIP trunk).

6.1. Setting the RFC2833 Telephone Event Type

The AT&T IP Flexible Reach service requires the use of SIP RFC2833 telephone event type 100. In cases where Modular Messaging originates outbound calls to AT&T (e.g., Find-Me calls), Modular Messaging must use 100.

> **Step 1** - Log into the Modular Messaging Messaging Application Server (MAS) using appropriate credentials.

> **Step 2** - Open the Voice Mail System Configuration tool and select the PBX defined for Communication Manager (e.g., **ACM521**).
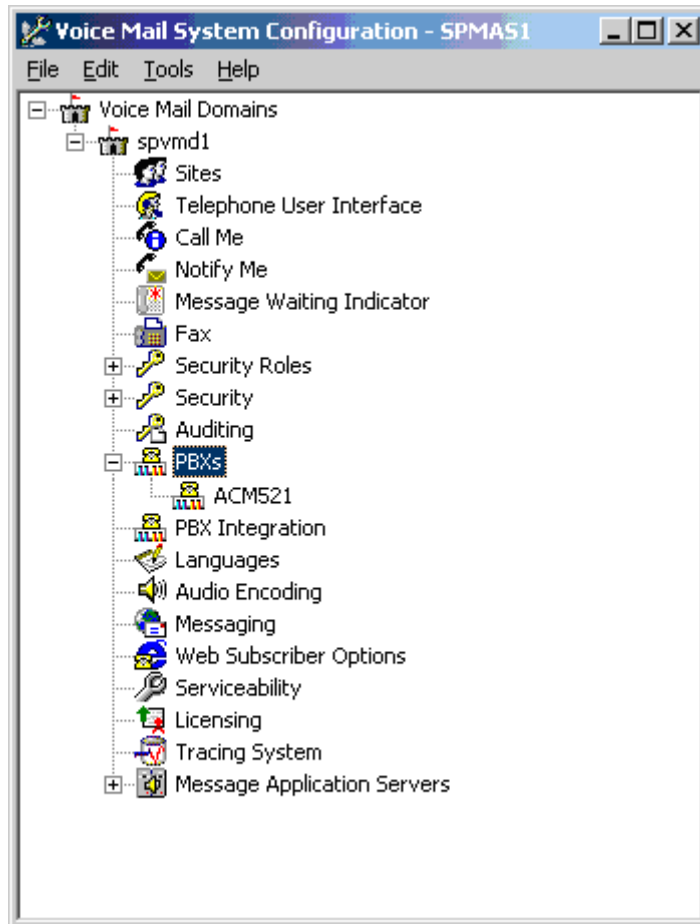
Step 3 - In the **General** tab, set the **Payload Type for RFC2833 RTP Event** to **100**.

Step 4 - Click **OK.**
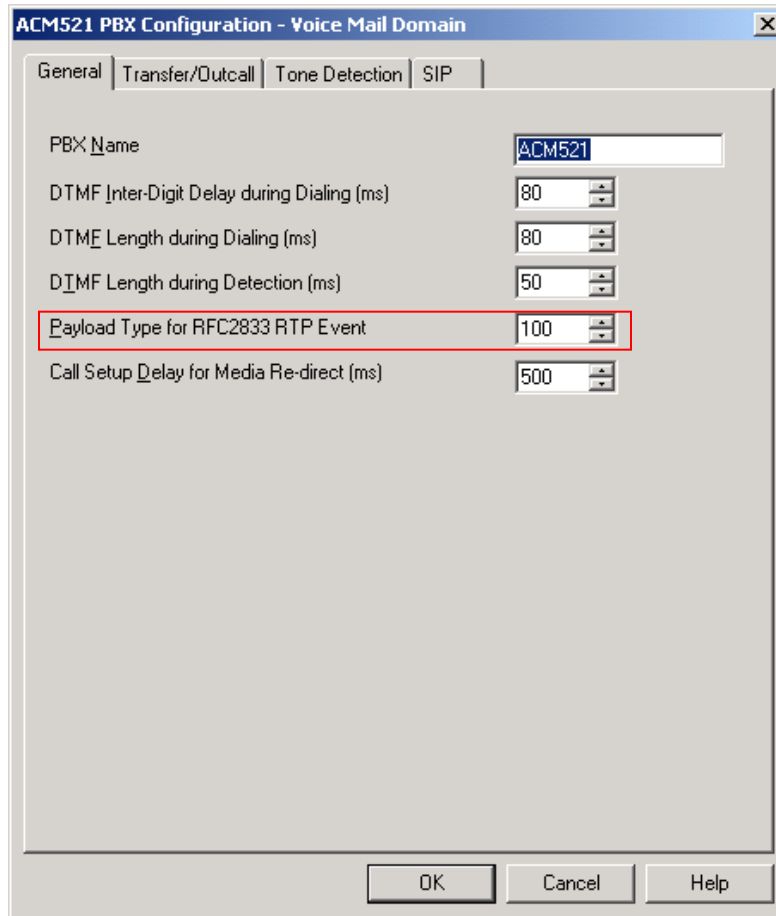
6.2. Disabling Enhanced Security for Outgoing Calls

When Modular Messaging is connected directly to Communications Manager via a SIP trunk, the Modular Messaging **Enhanced Security for Outgoing Calls** option must be disabled.

> **Step 1** – Repeat **Steps 1** and **2** from **Section 6.1**.
>
> **Step 2** - Select the **Transfer/Outcall** tab and *uncheck* the **Enabled Enhanced Security for Outbound Calls** box.
>
> **Step 3** - Click **OK**.
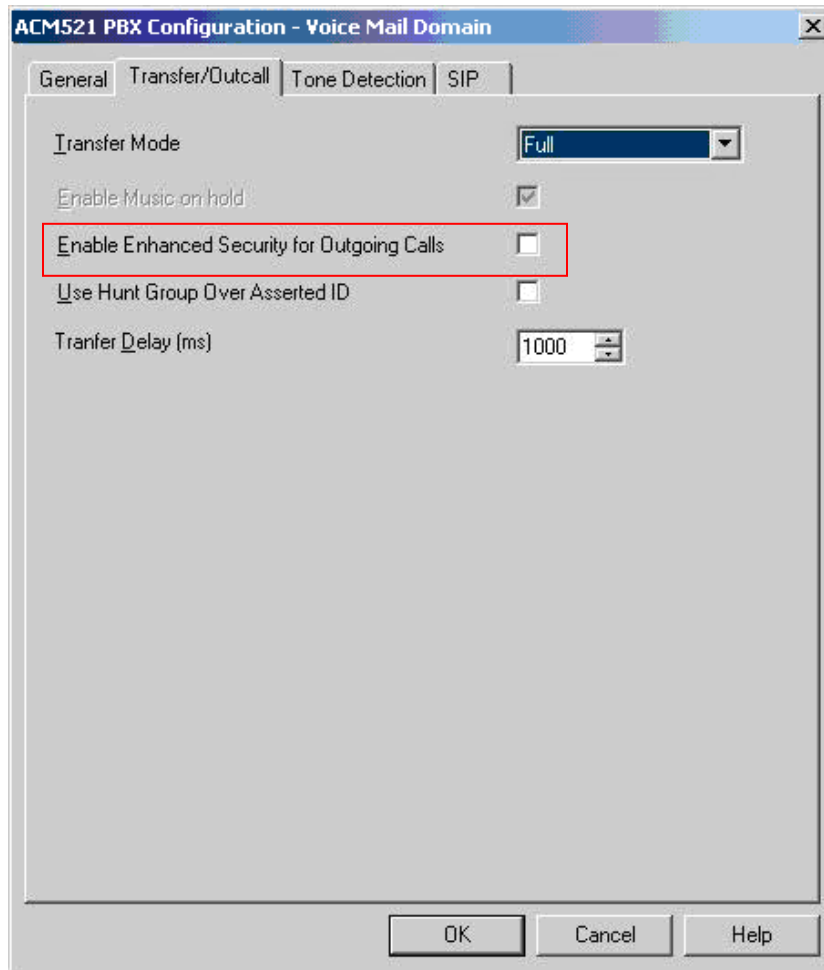
7. Configure Avaya Aura® Session Border Controller (SBC)

This section illustrates an example configuration of the Avaya Aura® SBC. In the sample configuration, the Avaya Aura® SBC resides on its own S8800 Server as an application template running on System Platform The application template defines basic functionality for the SBC such as IP addressing, SIP domains, etc. The installation of the System Platform and application template is assumed to have been previously completed (see the Avaya Aura® SBC references [5] and [6]) for additional information on the Avaya Aura® SBC installation.

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

7.1. Logging into the Avaya Aura® Session Border Controller

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

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

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

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

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

7.2. Network Configuration

As described previously much of the network information is defined during installation of the SBC application template (see [5] through [7]). However there may be occasions where these parameters need to be modified. Therefore these values are described below.

In the reference configuration, the Avaya S8800 Server has four physical network interfaces, labeled 1 through 4. The port labeled "1" (virtual "eth0") is used for the management and private (inside) network interface of the SBC (toward the customer equipment). The port labeled "4" (virtual "eth2") is used for the public (outside) network interface of the SBC (toward AT&T). These can be verified by checking the "interface eth0" and interface eth2" settings (see **Section 7.2.1**).

The AT&T requires that RTP media traffic use UDP port range 16384-32767. This range is defined as part of "interface eth2" (see **Section 7.2.3**).

SIP-Gateways are defined for corresponding to the private and public interfaces. In the reference configuration, the private interface is defined as "**PBX**" and the public interface is defined as "**Telco1**" (see **Section 7.2.4**).

7.2.1. Verify IP Addressing

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

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

7.2.2. Transport Protocols

7.2.2.1 Private Interface – Eth0

The private interface, eth0, was provisioned to support UDP, TCP, and TLS transport protocols. However, TCP (port 5060) was used in the reference configuration for the connection to Communication Manager (see **Section 5.7.1**). This can be displayed by the following:

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

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

sip
[Delete]

admin	enabled ▾	(Resource is active)
nat-translation	disabled ▾	(Resource is inactive)
nat-add-received-from	disabled ▾	(Resource is inactive)
nat-add-X-Remote-Info	enabled ▾	(Resource is active)
load-balance-head-end	false ▾	

udp-port

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

Add udp-port

tcp-port

	tcp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	tcp-port 5060	Edit	Edit	any	0	Edit

Add tcp-port

tls-port

	tls-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	tls-port 5061	Edit	Edit	TLS	0	vsp\tls\certificate aasbc.p12

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

7.2.2.2 Public Interface – Eth2

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

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

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

JF:Reviewed
SPOC 1/4/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

43 of 64
ACM521AASBCIPFR

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

7.2.3. Setting the RTP Port Range on Eth2

Step 1 - Go to **cluster → box <name defined during install> → interface eth2 → ip outside** to display the eth2 configuration toward AT&T. Select Media Ports from either the menu or from the display.
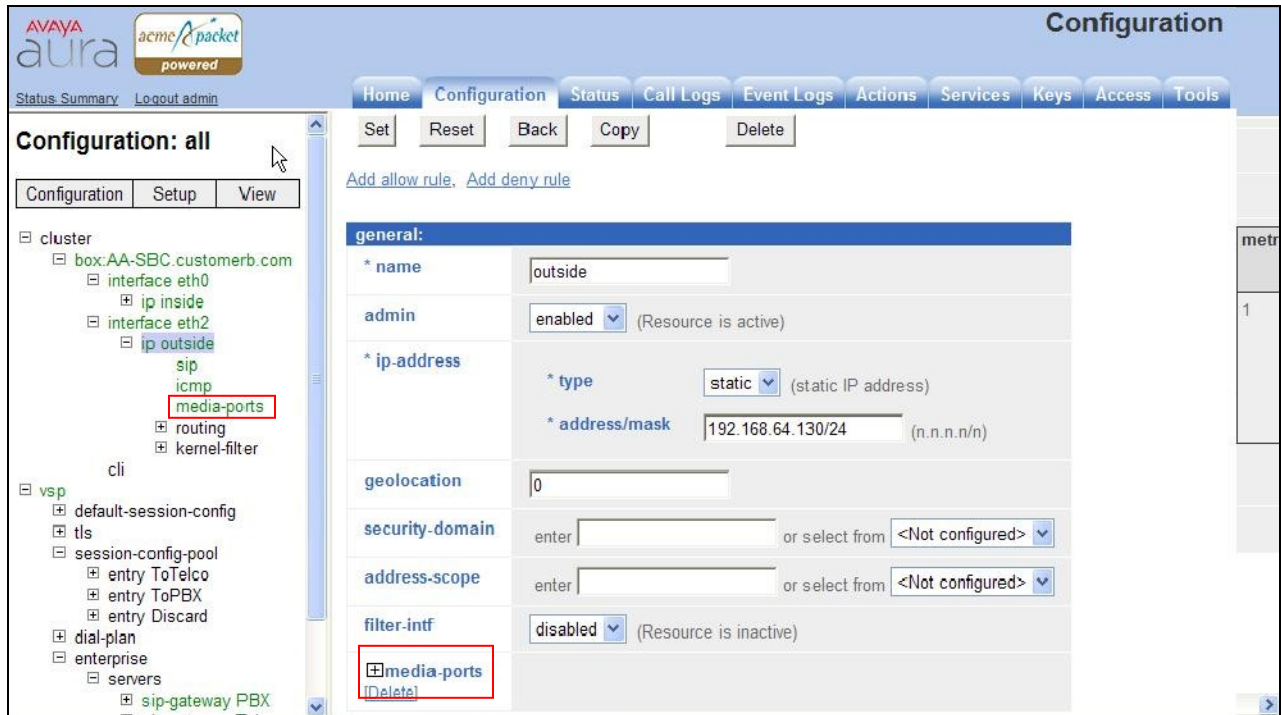
Step 2 - The media port section will be displayed. Enter **16384** in the **base-port** field and **16383** in the **count** field.
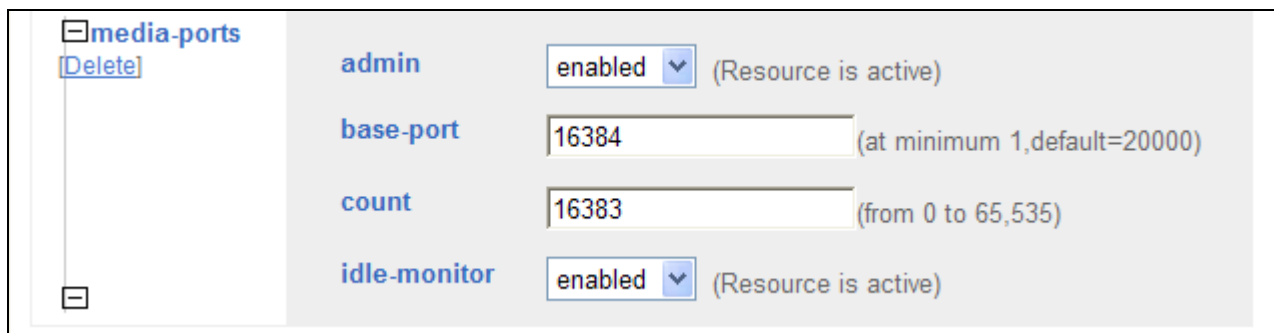
Step 3 - Click on the **Set** button to save.

Step 4 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.4. Configuring the SIP-Gateways

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

7.2.4.1 Telco1

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

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

Step 3 - Verify the following:
- admin state is **enabled**.
- host address is the IP address of the AT&T IP Flexible Reach border element (e.g., **135.25.29.74**).
- transport protocol is **UDP**.
- port is **5060**.

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

Step 5 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.4.2 PBX

Repeat the steps in **Section 7.2.4.1** and verify the following:
- admin state is **enabled**.
- host address is the IP address of the Communication Manager C-LAN **MainCLAN2** defined in **Section 5.4** and **5.7.1** (e.g., **192.168.67.14**).

JF:Reviewed
SPOC 1/4/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

46 of 64
ACM521AASBCIPFR

- transport protocol is **TCP**. Note that TCP was used in the reference configuration to facilitate protocol trace verification and troubleshooting. TLS may be used as well.
- port is **5060**.

7.2.5. SIP Header Manipulation

The Avaya Aura® SBC can be used to change or remove SIP headers that are not required or supported by AT&T. For headers that have relevance only within the enterprise, it may be desirable to prevent the header from being sent to the public SIP Service Provider. For example, by default Communication Manager uses History-Info headers. If these headers are not disabled in Communication Manager (see **Section 5.7.1 Step 5**), they may be removed by the Avaya Aura® SBC.

7.2.5.1 Removing SIP Headers

Undesired headers may be removed via the session-config-pool. For example, during installation, two session-config-pools were created, "To-Telco" and "To-PBX". Specified headers sent to AT&T are removed session-config-pool "**To-Telco**".

> **Step 1** - Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. In the resultant screen, click **Edit blocked-header.**
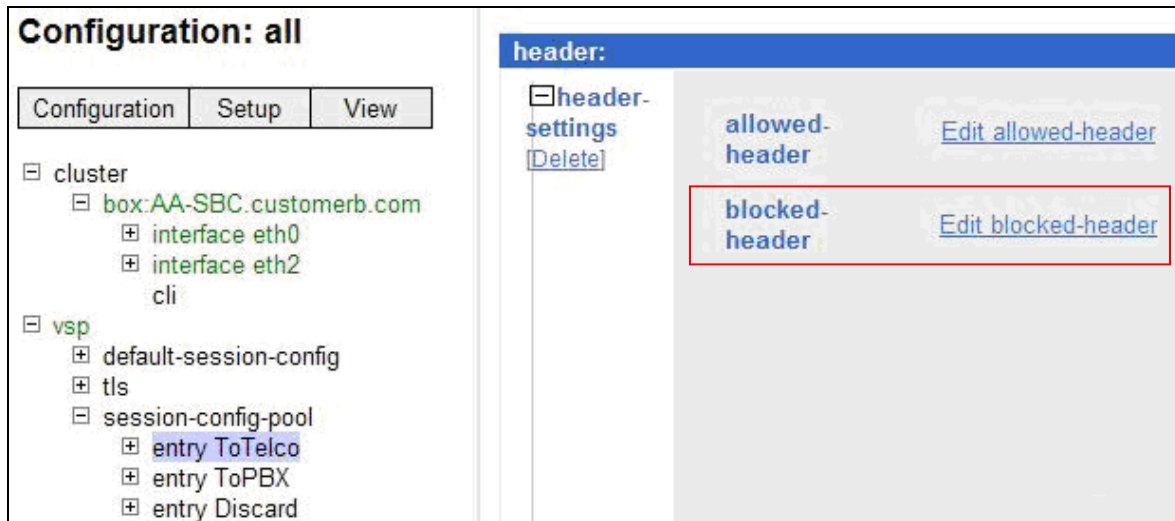
> **Step 2** – Enter **History-Info** into the selection box.
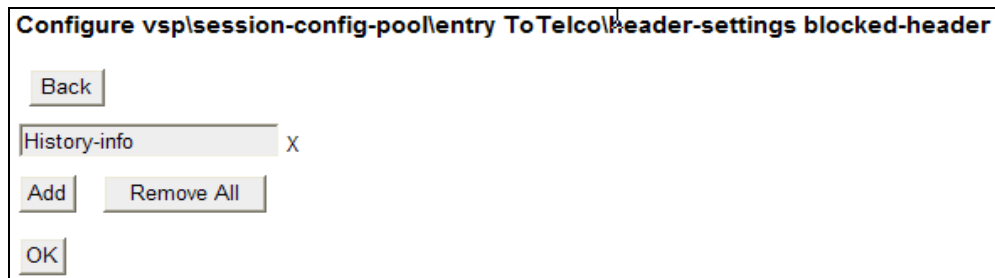
Step 4 – If additional headers need to be blocked, click on the **Add** button.

Step 5 – When all headers are entered, click on **OK**.

Step 6 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.5.2 Modifying SIP Headers
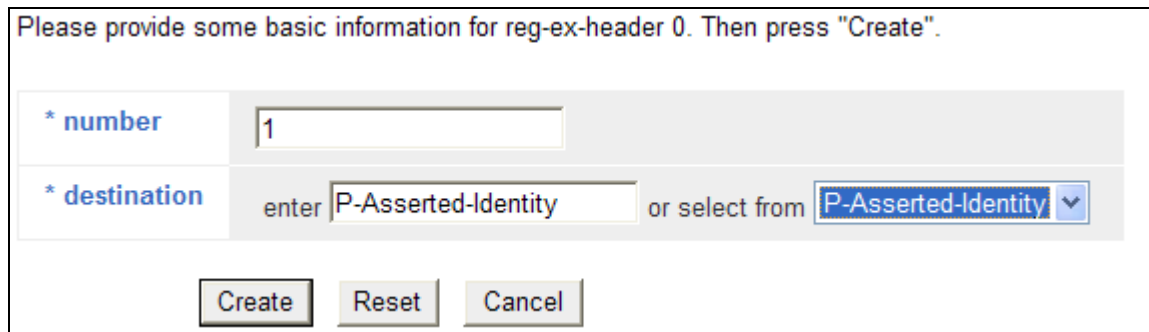
Some SIP headers may require modification to meet local or network content requirements. For example, for inbound calls the AT&T IP Flexible Reach network with include the IP address of the IP Flexible Reach Border Element (e.g., **135.25.29.74**) in the From and PAI headers. Communication Manager expects its local domain (e.g., **customera.com**) in these headers.

Step 1 - Navigate to **vsp → session-config-pool → entry ToPBX → header-settings → reg-ex-header**. Click **Add reg-ex-header.**

Step 2 – In the resultant screen enter the following:
- **number** – Enter an available number designation (e.g., **1**).
- **destination** – Select **P-Asserted-Identity** from the drop-down menu, or type that value into the **enter** field if P-Asserted-Identity is not a menu option.

Step 3 – Click on **Create**.

Step 4 – Returning to the reg-ex screen, click on Create and enter the following:
- **source** – Enter **P-Asserted-Identity** from the drop-down menu.
- **expression** – enter   **<sip:(.*)@135.25.29.74(.*)>**   , where 135.25.29.74 is the IP address of the IP Toll Free Border Element. Note the the first (.*) will store all user values preceeding the @, and the second (.*) will store all values after the host IP address.
- **replacement** – Enter   **<sip:\1@customera.com\2>**   , where customera.com is the domain of Communication Manager. Note that the \1 will insert the values stored by the first (.*) in the Expression field, and the \2 will insert the values stored by the second (.*) in the Expression field.

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
48 of 64
ACM521AASBCIPFR

Step 5 – Enter the following in the remaining fields:
- **admin** – **enabled**
- **apply-to-methods** – **INVITE**
- Let all other fields default.

Step 6 – Click on **Set**.

Step 7 – Repeat **Steps 2** through **6** to modify the **From** headers, with the following changes:
- In **Step 2**
  - Enter a new **number** designation (e.g., **5**).
  - For **destination** select or enter **From**.
- In **Step 4**
  - For **source** select **From**.

Step 8 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.6. Disable Third Party Call Control

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

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

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
50 of 64
ACM521AASBCIPFR
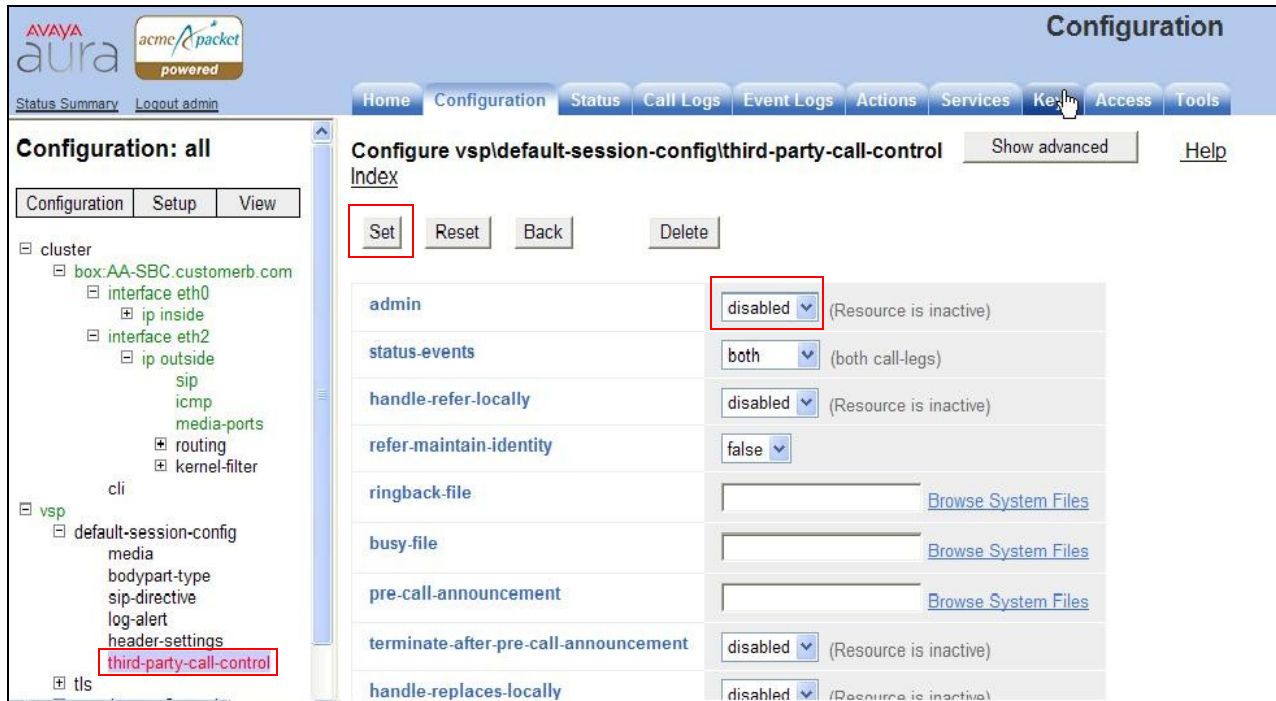
Step 3 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.2.7. SIP OPTIONS Messages for AT&T Network Status

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

Step 1 - Navigate to **vsp → enterprise → servers → sip-gateway Telco**. Click on the **Show Advanced** button at the top of the page (not shown).

Step 2 – In the **general:** section set **failover-detection** and select **ping** from the menu.

JF:Reviewed
SPOC 1/4/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

51 of 64
ACM521AASBCIPFR

Configure vsp\enterprise\servers\sip-gateway Telco

Step 3 – Scroll down to the **routing**: section and set the **ping-interval** as desired (e.g., **60**).

Step 4 - Scroll to the bottom of the screen and click **Set**.

Step 5 - Proceed to save and activate the configuration as described in **Section 7.3**.

7.3. Saving and Activating Configuration Changes

Step 1 - To save and activate configuration changes, select **Configuration → Update and save configuration** from the upper left hand side of the user interface, as shown below.
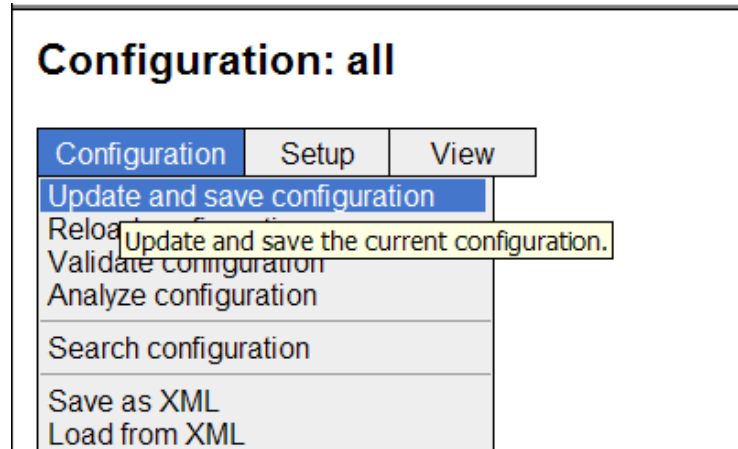
Step 2 - Click **OK** to update the live configuration.
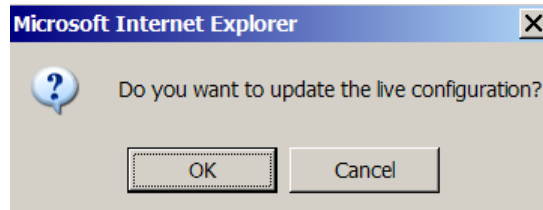
Step 3 - Click **OK** to save the live configuration.
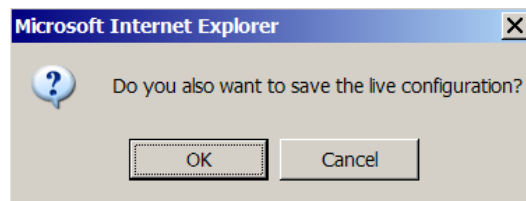
A screen that includes the following should appear.
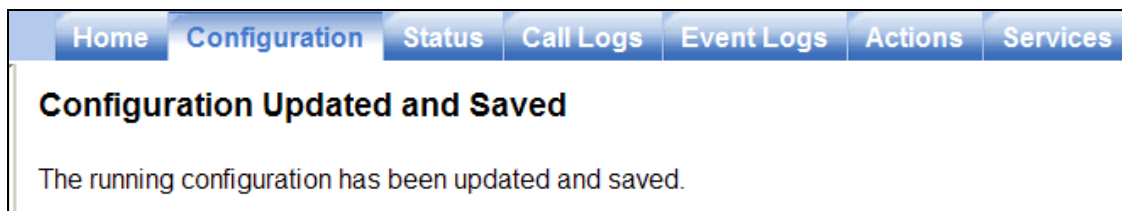
8. Verification Steps

The following steps may be used to verify the configuration:

8.1. 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.

8.2. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See [1] for more information.

1. From the Communication Manager console connection enter the command *list trace tac xxx*, where xxx is a trunk access code defined for the SIP trunk to AT&T (e.g., **122**). Note that Communication Manager has previously converted the AT&T IP Flexible Reach DNIS dialed by the PSTN (732-555-4384) to the Communication Manager extension 26103, before processing the INVITE.

```
list trace tac 122

                  LIST TRACE

time        data

14:31:44 SIP<INVITE sip:26103@customera.com:5060  SIP/2.0
14:31:44    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:44    2-6f328733@135.25.29.74
14:31:44    active trunk-group 22 member 1    cid 0xb4
14:31:44 SIP>SIP/2.0 180 Ringing
14:31:44    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:44    2-6f328733@135.25.29.74
14:31:44    dial 26103
14:31:44    ring station     26103 cid 0xb4
14:31:44    G711MU ss:off ps:20
       rgn:1 [192.168.67.81]:31202
       rgn:1 [192.168.67.16]:16588
14:31:44    G729 ss:off ps:30
       rgn:2 [192.168.67.125]:28536
       rgn:1 [192.168.67.16]:16580
14:31:44    xoip options: fax:T38 modem:off tty:US  uid:0x5000a
       xoip ip: [192.168.67.16]:16580
14:31:45 SIP>SIP/2.0 200 OK
14:31:45    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45    2-6f328733@135.25.29.74
14:31:45    active station     26103 cid 0xb4
14:31:45 SIP<ACK sip:7323204302@192.168.67.14:5080;transport=tcp  SI
14:31:45 SIP<P/2.0
14:31:45    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
```

```
14:31:45    2-6f328733@135.25.29.74
14:31:45 SIP>INVITE sip:7326712438@135.25.29.74:5060;maddr=192.168.6
14:31:45 SIP>7.125;transport=tcp SIP/2.0
14:31:45    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45    2-6f328733@135.25.29.74
14:31:45 SIP<SIP/2.0 100 Trying
14:31:45    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45    2-6f328733@135.25.29.74
14:31:45 SIP<SIP/2.0 200 OK
14:31:45    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45    2-6f328733@135.25.29.74
14:31:45 SIP>ACK sip:7326712438@135.25.29.74:5060;maddr=192.168.67.1
14:31:45 SIP>25;transport=tcp SIP/2.0
14:31:45    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:45    2-6f328733@135.25.29.74
14:31:45    G729A ss:off ps:30
        rgn:2 [192.168.67.125]:28536
        rgn:1 [192.168.67.81]:31202
14:31:45    G729 ss:off ps:30
        rgn:1 [192.168.67.81]:31202
        rgn:2 [192.168.67.125]:28536
14:31:48 SIP>BYE sip:7326712438@135.25.29.74:5060;maddr=192.168.67.1
14:31:48 SIP>25;transport=tcp SIP/2.0
14:31:48    Call-ID: CXC-15-5aa3d9a8-8240a8c0-13c4-4e8a0b2a-151d2d4
14:31:48    2-6f328733@135.25.29.74
14:31:48    idle station    26103 cid 0xb4
```

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

8.3. Protocol Traces

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

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

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

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

8.4. Avaya Aura® Session Border Controller Verification

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

8.4.1. Status Tab

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

For example, there is a SIP heading on the left menu that can be expanded as shown below.
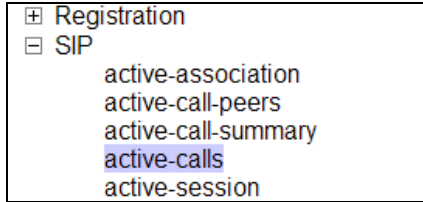
In the example below, **active-calls** was selected from the left, revealing details about an active inbound call from the PSTN. Additional information about the call is available by moving the bottom scroll bar to the right (not shown).
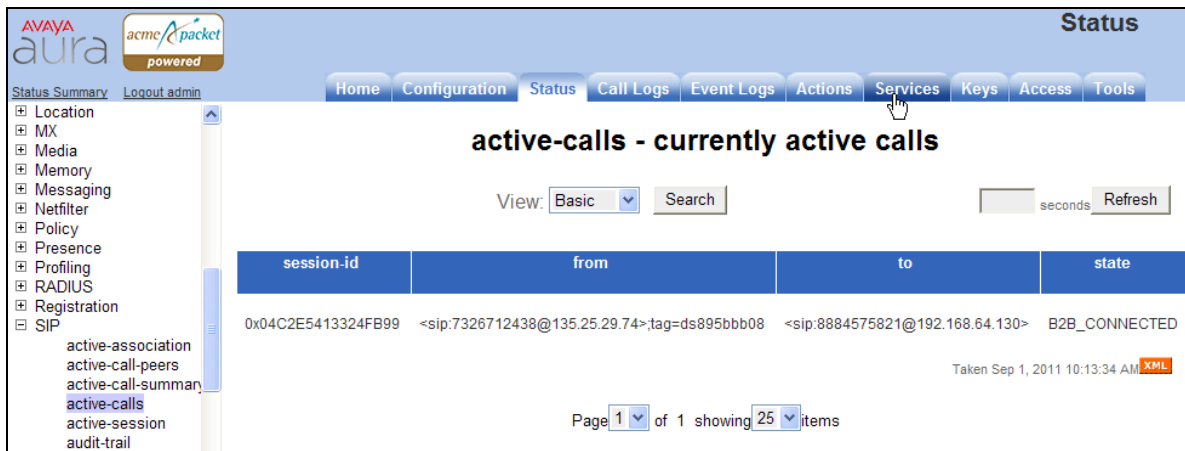
8.4.2. Call Logs

The **Call Logs** tab can provide useful diagnostic or troubleshooting information. In the following screen, the **SIP Messages** search capability can be observed. The following screen shows a portion of the **Call Logs** tab selected after an inbound call from the PSTN.
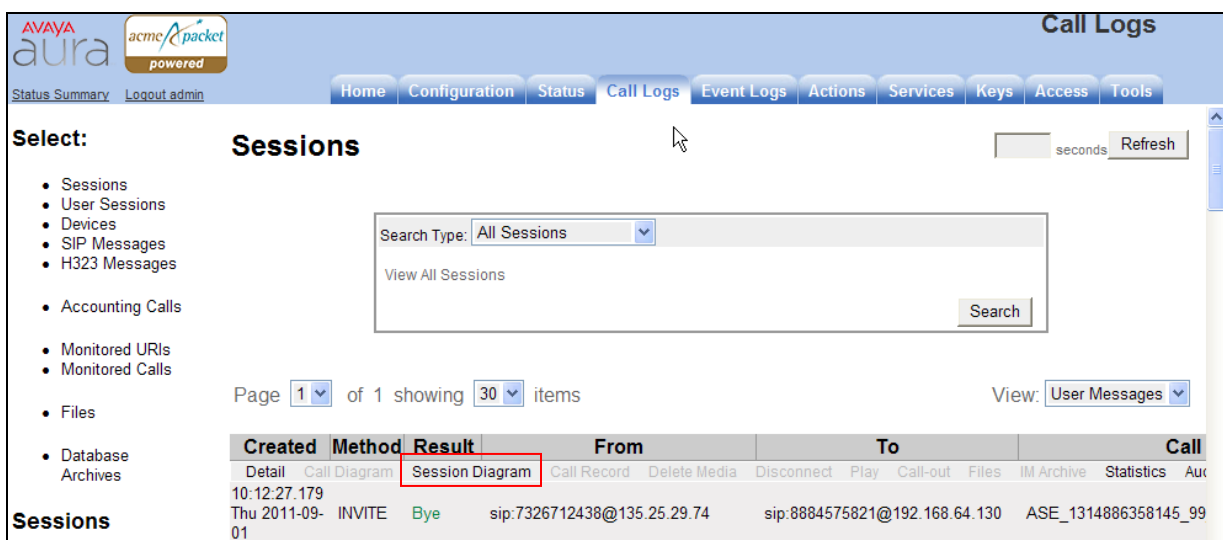
As shown below, to view a ladder diagram for the session, select the **Session Diagram** link. When the session window opens, expand the upper portion of the screen under the "Call Sequence" heading to display the ladder diagram. The following screen shows the ladder diagram for the inbound call. Note that the activity for both the inside private and outside public side of the SBC can be seen.

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
58 of 64
ACM521AASBCIPFR
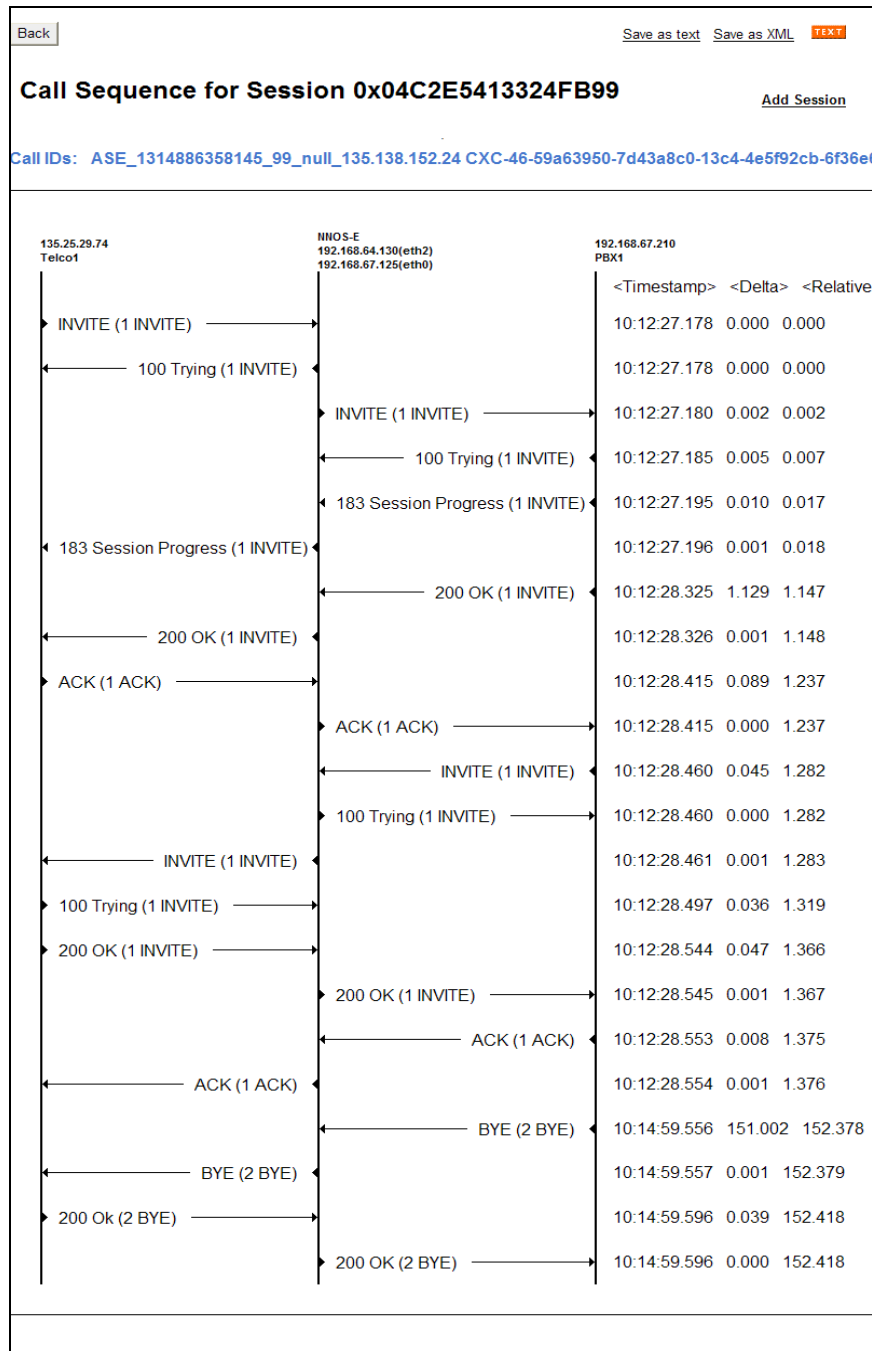
At the top right of the screen, the session may be saved as a text or XML file. If the session is saved as an XML file, using the **Save as XML** link, the xml file can be provided to support personnel that can open the session on another Avaya Aura® SBC for analysis.
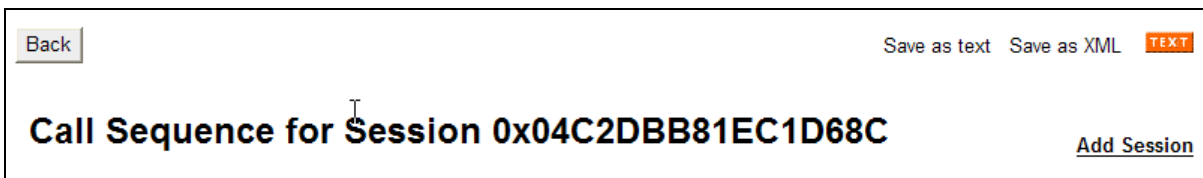
The **Call Logs** tab also provides the capability to see modifications made to SIP headers by the SBC. Below the ladder diagram area is another screen section. Using the same Session Diagram as shown above, scroll down to the INVITE message sent by the SBC to AT&T. The **More** and **See changes** links have been selected to expand the SIP message display and enable observation of the changes made by the SBC to the **Revised** message, as compared to the **Original** INVITE received from Session Manager. In the example below the From and PAI SIP header modifications described in **Section 7.2.5.2** can be seen.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager, and the Avaya Aura® Session Border Controller can be configured to interoperate successfully with the AT&T IP Flexible Reach service using either AVPN or MIS-PNT transport. This solution provides users of Avaya Aura® Communication Manager the ability to support inbound and outbound calls over an AT&T IP Flexible Reach SIP trunk service connection.

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

10. References

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

Avaya Aura® Communication Manager

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

Avaya Modular Messaging

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

Avaya Aura® Session Border Controller

[5] Installing and Configuring Avaya Aura® Session Border Controller, Release 6.0.1, November 2010 available at: http://support.avaya.com/css/P8/documents/100134970
[6] Avaya Aura® SBC System Administration Guide, V.6.0, 2010 available at: http://support.avaya.com/css/P8/documents/100111137
[7] Applications Notes for Avaya Aura® Communication Manager 6.0, Avaya Aura® Session Manager 6.0 and Avaya Aura® Session Border Controller with AT&T IP Flexible Reach SIP Trunk Service, Issue 1.1 available at: https://devconnect.avaya.com/public/download/dyn/CMSMAASBC60IPFR.pdf

AT&T IP Flexible Reach Service Descriptions:

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

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
61 of 64
ACM521AASBCIPFR

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

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

Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, and building on the sip gateway configuration shown in **Section 7.2.4.1**, the Avaya Aura® SBC is provisioned as follows.

Step 1 - Go to **vsp → enterprise → servers → sip-gatewayTelco → server-pool** and the previously defined sip-gateway **Telco1** defined in **Section 7.2.4.1** will be displayed.

Step 2 – Click on **Add server**.

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

Step 4 – Enter the following:

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

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

Step 5 - Proceed to save and activate the configuration as described in **Section 7.3**.

JF:Reviewed
SPOC 1/4/2012
Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.
64 of 64
ACM521AASBCIPFR