

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.

TABLE OF CONTENTS

1. Introduction	4
2. General Test Approach and Test Results	4
2.1. Interoperability Compliance Testing	4
2.2. Test Results	5
2.2.1. Known Limitations	6
2.3. Support	6
3. Reference Configuration	7
3.1. Illustrative Configuration Information	9
3.2. Call Flows	10
3.2.1. Inbound	10
3.2.2. Outbound	11
3.2.3. Call Forward Re-direction	12
3.2.4. Coverage to Voicemail	13
4. Equipment and Software Validated	14
5. Avaya Aura® Communication Manager	15
5.1. System Parameters	15
5.2. Dial Plan	17
5.3. IP Node Names	18
5.4. IP Interface for IP Interface MainCLAN2	18
5.5. IP Network Regions	20
5.5.1. IP Network Region 1 – Local Region	20
5.5.2. IP Network Region 2 – AT&T Trunk Region	21
5.6. IP Codec Parameters	22
5.6.1. Codecs For IP Network Region 1 (local calls)	22
5.6.2. Codecs For IP Network Region 2	23
5.7. SIP Trunks	23
5.7.1. SIP Trunk for AT&T IP Flexible Reach calls	23
5.7.2. Local SIP Trunk (Modular Messaging)	26
5.8. Public Unknown Numbering	28
5.9. Private Numbering	28
5.10. Outbound Call Routing From Avaya Aura® Communication Manager	29
5.10.1. Route Patterns	29
5.10.2. ARS Dialing	30
5.10.3. AAR Dialing \sim	31
5.11. Inbound Calls To Avaya Aura® Communication Manager	31
5.11.1. Calls from A $1 \& 1$	31
5.11.2. Calls from Modular Messaging	32
5.12. Provisioning for Coverage to Modular Messaging	32
5.12.1. Hunt Group for Station Coverage to Modular Messaging	53
5.12.2. Coverage Path for Station Coverage to Modular Messaging	53
5.12.5. Station Coverage Path to Woodular Wessaging	34
 Avaya Iviodullar Iviessaging 6.1 Sotting the DEC2822 Telephone Event Type 	33
0.1. Setting the KI C2033 Telephone Event Type	33

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	2 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

6.2. Disabling Enhanced Security for Outgoing Calls	37
7. Configure Avaya Aura® Session Border Controller (SBC)	38
7.1. Logging into the Avaya Session Border Controller	39
7.2. Network Configuration	41
7.2.1. Verify IP Addressing	41
7.2.2. Transport Protocols	42
7.2.3. Setting the RTP Port Range on Eth2	44
7.2.4. Configuring the SIP-Gateways	45
7.2.5. SIP Header Manipulation	47
7.2.6. Disable Third Party Call Control	50
7.2.7. SIP OPTIONS Messages for AT&T Network Status	51
7.3. Saving and Activating Configuration Changes	53
8. Verification Steps	54
8.1. General	54
8.2. Avaya Aura® Communication Manager	54
8.3. Protocol Traces	55
8.4. Avaya Aura® Session Border Controller Verification	56
8.4.1. Status Tab	56
8.4.2. Call Logs	57
9. Conclusion	60
10. References	61
11. Addendum 1 – Avaya Aura® Session Border Controller Redundancy to Multiple AT&T	
Border Elements	62

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 AVPN¹ or MIS-PNT² transport services.

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

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.

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	5 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

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 Avava 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.

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	6 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

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 network³. 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

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
Avava Aura® Communication Manager	Application Hotes
Control LAN (C-LAN) IP Address	192.168.67.14
Media Processor (MedPro) IP Address	192.168.67.15
Avaya Aura® Communication Manager	26xxx
extensions	
Avaya CPE local dial plan	2xxxx
Modular Messaging Pilot Extension	26000
Avaya Aura® Session Border Controller	
IP Address of "Outside" (Public) Interface	192.168.64.130
(connected to AT&T Access Router/IP Flexible	
Reach Service)	
IP Address of "Inside" (Private) Interface	192.168.67.125
(connected to Avaya Aura® Communication	
Manager)	
Avaya Modular Messaging	
Messaging Application Server (MAS) IP	192.168.67.141
Address	
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®	192.168.64.254
outside)	
AT&T Access Router NAT address (Avaya	135.16.170.55
Aura® outside address)	

 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

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.



JF:Reviewed SPOC 1/4/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 11 of 64 ACM521AASBCIPFR

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 forwards⁴ 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 call⁵ 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	HW02 FW061
(MedPro)	
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)	Release 5.2 – SP5 with Patch 1
on Avaya S3500 Servers	(9.0.350.5019)
Fax device	Ventafax Home Version 6.1.59.144
AT&T IP Flexible Reach Service using	VNI 22
AVPN or MIS-PNT transport service	
connection	

Table 2: Equipment and Software Versions

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 per	rmissio	on change	s.)	

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

display system-parameters customer-opti	ion	s Page 3 of	11
OPTIONA	ΥL	FEATURES	
Abbreviated Dialing Enhanced List?	У	Audible Message Waiting?	У
Access Security Gateway (ASG)?	У	Authorization Codes?	У
Analog Trunk Incoming Call ID?	У	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	У	CAS Main?	n
Answer Supervision by Call Classifier?	У	Change COR by FAC?	n
ARS?	У	Computer Telephony Adjunct Links?	У
ARS/AAR Partitioning?	У	Cvg Of Calls Redirected Off-net?	У
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	У
ASAI Link Core Capabilities?	У	DCS Call Coverage?	У
ASAI Link Plus Capabilities?	У	DCS with Rerouting?	У
Async. Transfer Mode (ATM) PNC?	n		
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	У
ATM WAN Spare Processor?	n	DS1 MSP?	У
ATMS?	У	DS1 Echo Cancellation?	У
Attendant Vectoring?	У		
(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
OPT	IONAL FEATURES
Emergency Access to Attendant? y	IP Stations? y
Enable 'dadmin' Login? y	7
Enhanced Conferencing? y	ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n	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	1
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	7
IP Attendant Consoles? y	7
(NOTE: You must logoff & lo	ogin 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? v
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
                                               Terminal Trans. Init. (TTI)? y
                      PNC Duplication? n
                  Port Network Support? y
                                                Time of Day Routing? y
                      Posted Messages? y
                                              TN2501 VAL Maximum Capacity? y
                                                     Uniform Dialing Plan? y
                                             Usage Allocation Enhancements? y
                    Private Networking? 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 dialp	lan anal	ysis					Page	1 of	12
			DIAL PLA	N ANALYS	SIS TABLE				
			Lo	cation:	all	Pe	rcent Fu	ıll: 1	
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
String	Length	Туре	String	Length	Туре	String	Length	Туре	
1	3 d	lac							
2	5 e	ext							
8	1 f	ac							
9	1 f	ac							
*	3 f	ac							
#	3 f	ac							

JF:Reviewed SPOC 1/4/2012

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			

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**).

7	· · · ·							
list	: ip-in	iteria	ce all					
				IP INTERFACES				
							Net	
ON T	Type	Slot	Code/Sfx	Node Name/	Mask	Gateway Node	Rgn	VLAN
				IP-Address		-	-	
уC	C-LAN	01A02	TN799 D	MainCLAN1	/24	Gateway001	1	n
				192.168.67.13				
y C	C-LAN	01A03	TN799 D	MainCLAN2	/24	Gateway001	1	n
				192.168.67.14				
уM	IEDPRO	01A04	TN2602	MainMP1A04	/24	Gateway001	1	n
				192.168.67.15				
уM	IEDPRO	01A05	TN2602	MainMP1A05	/24	Gateway001	1	n
				192.168.67.16				
y V	7AL	01A06	TN2501	MainVAL1A06	/24	Gateway001		n
				192.168.67.17				

JF:Reviewed SPOC 1/4/2012

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
                                                                           3
                                                                     1 of
                                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:

JF:Reviewed SPOC 1/4/2012

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 RESERVATIO	N PARAM	ETERS				
H.323 IP ENDPOINTS RSVP EN	nabled?	n				
H.323 Link Bounce Recovery? y						
Idle Traffic Interval (sec): 20						
Keep-Alive Interval (sec): 5						
Keep-Alive Count: 5						

JF:Reviewed SPOC 1/4/2012

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.

```
4 of
change ip-network-region 1
                                                                           20
                                                               Page
                     Inter Network Region Connection Management
Source Region: 1
                                                                    Ι
                                                                           М
                                                                    G
                                                                      Α
                                                                           t
dst codec direct WAN-BW-limits Video
                                              Intervening
                                                               Dyn A G
                                                                           С
           WAN Units Total Norm Prio Shr Regions
                                                               CAC R L
ran set
                                                                           е
1
     1
                                                                      all
2
     2
                NoLimit
                                                                    n
                                                                            t
           У
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
                                                                        1 of
                                                                              20
                                                                Page
                               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
```

JF:Reviewed SPOC 1/4/2012

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
                                                                    Ι
                                                                            М
                                                                    G A
                                                                            t
dst codec direct WAN-BW-limits Video
                                              Intervening
                                                               Dyn
                                                                    Α
                                                                      G
                                                                            С
                        Total Norm Prio Shr Regions
rgn set WAN Units
                                                               CAC
                                                                    R
                                                                      L
                                                                            е
1
     2
                NoLimit
                                                                            t
           y
                                                                    n
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
                                 2
                                          20
                      n
                                 2
 2: G.729B
                                          20
                      n
                                 2
 3: G.729A
                                          20
                      n
```

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

change ip-codec-se	et 1			Page	2 of	2
	IP Codec S	Set				
Maxi Maximum Call	Allow mum Call Rate for Rate for Priority	Direct-IP Direct-IP Direct-IP	Multimedia? Multimedia: Multimedia:	y 384:Kbits 384:Kbits		
	Mode	Redunda	ancy			
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
                                                                            2
                                                                    1 of
                                                              Page
                         IP Codec Set
    Codec Set: 2
   Audio
                Silence
                                      Packet
                             Frames
   Codec
                Suppression Per Pkt Size(ms)
1: G.729B
                     n
                               3
                                        30
                                        30
2: G.729A
                               3
                     n
                               2
3: G.711MU
                     n
                                        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
                                        Redundancv
    FAX
                     t.38-standard
                                          0
                                          0
   Modem
                     off
    TDD/TTY
                     off
                                          0
    Clear-channel
                                          0
                     n
```

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					
SIGNALIN	G 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).

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	24 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

- 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-grou	add trunk-group 22 Page 1 of 21					
		TRUNK GROUP				
Croup Number.	22	Crown Tymes	sin	CDD Dor	orts.	X 7
GIOUP NUMBEL.		Group Type.	stb	CDK Keł	JOILS.	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			
			1	Signaling Gro	oup: 22	2
			Nur	mber of Membe	ers: 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	e:	500	0
SCCAN? n Digital Loss Grou	p:	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:	<pre>public UUI Treatment: service-provider</pre>
Show ANSWERED BY on Display? y	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).
- 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).



5.7.2. Local SIP Trunk (Modular Messaging)

JF:Reviewed

SPOC 1/4/2012

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
                                                                     1 of
                                                                            1
                                                              Page
                                SIGNALING GROUP
 Group Number: 21
                             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
Near-end Node Name: MainCLAN2
                                        Far-end Node Name: MM
                                           Far-end Listen Port: 5060
 Near-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
```

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

26 of 64 ACM521AASBCIPFR **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 Re	ports: 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 Gr	oup: 21
		Nu	mber of Memb	ers: 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	
Redirec	t On OPTIM Failure: 5000
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Ref	resh 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.

char	nge public-unkn	nown-number	ring O			Page	1 of	2
		NUMBEI	RING - PUBLIC/U	NKNOWN FORM	TAN			
				Total				
Ext	Ext	Trk	CPN	CPN				
Len	Code	Grp(s)	Prefix	Len				
5	26101	22	7325554050	10	Total	. Administ	ered:	3
5	26102	22	7325554051	10	Ma	aximum Ent	ries:	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**.

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	28 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

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
                                                                     1 of
                                                               Page
                                                                            2
                           NUMBERING - PRIVATE FORMAT
                             Private
Ext Ext
                  Trk
                                             Total
Len Code
                             Prefix
                                              Len
                  Grp(s)
5 26000
                                               5
                                                    Total Administered: 1
                  21
                                                       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).

					Pat	tern 1	Numbei	:: 22	Pat	tern	Name	: To	ATT					
							SCCAN	l? n	S	ecure	e SIP	? n	_					
	Grp	FRL	NPA	Pfx	Нор	Toll	No.	Inser	ted							DCS/	IXC	
	No			Mrk	Lmt	List	Del	Digit	S							QSIG		
							Dgts									Intw		
1:	22	0														n	user	
2:																n	user	
3:																n	user	
4:																n	user	
	BC	C V	ALUE	TSC	C CA	-TSC	ITC	C BCIE	Ser	vice,	/Feat	ure	PARM	No.	Numb	ering	LAR	
	0 1	2 M	4 W		Req	uest							D	gts	Forma	t		
													Suba	ddre	SS			
1:	УУ	У У	y n	n			rest									I	none	
2:	УУ	У У	y n	n			rest									I	none	
3:	УУ	У У	y n	n			rest									I	none	
4:	УУ	У У	y n	n			rest									1	none	

JF:Reviewed SPOC 1/4/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 29 of 64 ACM521AASBCIPFR

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.

char	nge 1	coute	e-pat	tter	n 1]	Page	1	of	3
			Pá	atte	rn N	umber	: 11	Patte	ern Nam	e: To_MM						
							SCCAI	N? n	Sec	ure SIP?	n					
	${\tt Grp}$	FRL	NPA	Pfx	Нор	Toll	No.	Insei	rted					D	CS/	IXC
	No			Mrk	Lmt	List	Del	Digit	ts					QS	SIG	
							Dgts							ΙI	ntw	
1:	21	0												I	n	user
2:														I	n	user
3:														I	n	user
4:														I	n	user
5:														I	n	user
6:														I	n	user
	BCC	C VAI	LUE	TSC	CA-'	TSC	ITC	BCIE	Servic	e/Feature	PARM	No.	Numbe	eri	ng I	LAR
	0 1	2 M	4 W		Req	uest						Dgts	Forma	at		
											Sub	addr	ess			
1:	У У	У У	y n	n			rest	t					unk-1	ınk	r	none
2:	У У	У У	y n	n			rest	t							r	none
3:	У У	У У	y n	n			rest	t							r	none
4:	УУ	УУ	y n	n			rest	t							r	none
5:	У У	У У	y n	n			rest	t							r	none
6:	УУ	УУ	y n	n			rest	t							r	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

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 1733xxxxxx will be blocked, but calls to 1732xxxxxx will be routed.

change ars analysis 1732						Page 1 of 2
	A	RS DI	GIT ANALYS	IS TABI	ΞE	
			Location:	all		Percent Full: 1
Dialed	Tot	al	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 O						Page	1 of	2
	A	AR DI	GIT ANALY	SIS TABI	E			
			Location:	all		Percent Fu	11: 1	
Dialed	Tot	al	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
```

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	31 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

- 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 22Page1 of30INCOMING CALL HANDLING TREATMENTService/NumberNumberDelInsertFeatureLenDigitsDigits026101public-ntwrk10732555438310261020public-ntwrk10732555438510261030
```

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-cal	l-handli:	ng-trmt tru	unk-group 21		Page	1 of	30
		INCOMING (CALL HANDLING 7	TREATMENT			
Service/ Feature	Number Len	Number Digits	Del Insert				
public-ntwrk	11 17	325551234	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**).

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	32 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

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-grou	ıp 1		Page	2 of	60
		HUNT GROUP			
	Message	Center: sip-adjunct	Routing Digi	ts	
Voice Mail	Number	Voice Mail Handle	(e.g., AAR/ARS Acc	ess Coc	de)
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
Next Path Number:
                                          Hunt after Coverage? n
                                            Linkage
COVERAGE CRITERIA
   Station/Group Status Inside Call Outside Call
           Active?
                         n
                                          n
            Busy?
                            У
                                           У
                            У
      Don't Answer?
                                                   Number of Rings: 4
                                           У
             All?
                             n
                                           n
                            У
DND/SAC/Goto Cover?
                                          У
  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
                                     Lock Messages? n
Security Code: 123456
Coverage Path 1: 1
Extension: 26102
                                                                      BCC: 0
    Type: 9630
                                                                       TN: 1
    Port: S00000
                                                                       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
       Speakerphone: 2-way
Display Language: english
able GK Node Name:
                                               Message Lamp Ext: 26102
 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.

ACM521 PBX Configuration - Voice Mail Domain		×
General Transfer/Outcall Tone Detection SIP		
		_
PBX <u>N</u> ame	ACM521	
DTMF Inter-Digit Delay during Dialing (ms)	80 📫	
DTM <u>F</u> Length during Dialing (ms)	80 🔅	
DIMF Length during Detection (ms)	50 📮	
Payload Type for RFC2833 RTP Event	100 📫	
Call Setup <u>D</u> elay for Media Re-direct (ms)	500 🗦	
ОК	Cancel He	lp

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.

General	Transfer/Outcall Tone Deter	ction SIP		
<u>T</u> ransfe	er Mode	F	ull	•
Enable	Music on hold	<u> </u>	f.	
<u>E</u> nable	Enhanced Security for Outgoin	g Calls 🛛 🗖		
<u>U</u> se Hi	unt Group Over Asserted ID		1	
Tranfer	<u>D</u> elay (ms)	1	000 🛨	

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.

avaya		Avaya Aura [™] System Platforn Web Conso
		?Hel
	Login User Id Continue	
	Copyright © 2009-2010 Avaya Inc. All Rights Reserved	

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

Αναγα		Avaya Aura™ System Platforı ^{Web Conso}
	Login User Id admin Password Reset Log On	?Hel
	Copyright © 2009-2010 Avaya Inc. All Rights Reserved.	

The **Virtual Machine List** will show the SBC Template. Click on the \mathcal{P} to access the Avaya Aura® SBC GUI interface.

							Avaya Aur	a™ Sy	stem
AVAYA Previous successful log							s successful login	n: Wed Jun 29 15:3 Failed login at	
							Fa	ilover st	tatus: <u>N</u>
<u>Home</u>								Abo	out H
 Virtual Machine Management 	Virt	ual Mac	hine Ma	nagement					
✓ Server Management	Virtu	al Machine	e List						
 User Administration 	Syste	m Domain	Uptime: 64 d	days, 5 hours, 3	7 minutes	, 9 seconds			
	Curre	ent template	e installed: 9	5BCT <mark>6.0.2.0.3</mark> (sbc E362P	4) Refresh			
		Name	Version	IP Address	Maximum	n Memory Maximum Virtual CPUs	CPU Time	State	Appli
	0	Domain	n-0 <u>6.0.3.0.3</u>	192.168.67.123	512.0 MB	8	3d 8h 44m 1s	Running	
	Ø	the sbc	E362P4	192.168.67.125	4.0 GB	4	1d 7h 35m 50s	Running	-
	Ø	<u>cdom</u>	6.0.3.0.3	192.168.67.124	1024.0 MB	1	1d 4h 57m 50s	Running	100
			Copyr	ight © 2009-2010	Avaya Inc.	All Rights Reserved.			

Enter appropriate Username and Password and click Login.

Acme Packet Net-Net OS-E								
To access the NNOS-E management int	erface, you must first log in. Please provide your user name							
	Username:							
	Password:							
	Login							

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

AVAYA acme packet powered Logout admin	Home Configuration	Status Call Logs E	vent Logs Actions Services	Keys Access Tools
(c) 2005-2010 Acme Packet, Inc. All rights	Get summary for: Box 1 💌	Refresh		<u>Help</u>
reserved. [www.acmepacket.com]	box-identifier	017b-92c9-6442-35d9		
	box-status	IPAddress State build-version build-number	LocalBox (65.206.67.93) Connected E362P1 47121	
	master-services	database		
	up-time	time timezone uptime	13:44:08 Wed 2011-05-11 EDT 7 days 16:07:38	

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** \rightarrow **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**.

acmer packet								Cont	figura	tion	
Status Summary Logout admin	Home C	onfiguration	Status	Call L	ogs Event Logs	Actions S	ervices	Keys A	ccess	Tools	
Configuration: all	duplex	full 💌 (Fu	ull duplex)								
Configuration Setup View	autoneg	enabled 💌	(Resou	rce is act	ive)						
E cluster E box:AA-SBC	ip		ip	admin	ip-address	geolocation	security- domain	address- scope	filter- intf	media- ports	metr
E ip inside E ip outside cli E vsp E default-session-config E tls		Edit Delete	ip inside	enabled	static 192.168.67.125/24	0			disabled	enabled 20000 5000 enabled <u>Edit</u>	1
 ⇒ session-contig-pool ⊕ entry ToTelco ⊕ entry ToPBX ⊕ entry Discard 		Add ip									
 dial-plan enterprise servers e sip-gateway PBX e sip-gateway Telco e dns settings 	Vlan Set Re Help Inc	Add Vlan set Back]								
	<	10									>

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 \rightarrow box <name defined during install> \rightarrow interface eth0 \rightarrow ip inside.

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

<mark>⊟sip</mark> [Delete]	admin	enabled 🚩	(Resource i	active)	1				
	nat- translation	disabled 🗸	(Resource i	s inactiv	e)				
	nat-add- received- from	disabled 💙	(Resource is	s inactiv	e)				
	nat-add-X- Remote- Info	enabled 🔽	(Resource is	s active)	1				
	load- balance- head-end	false 💙							
	udp-port		udp-port	from- serve	r serv	trans	port ren	note- rt	certificate
		Edit Delete	udp-port 5060	<u>Edit</u>	Edit	any	0		Edit
		Add udp-por	<u>t</u>						
	tcp-port		tcp-port	from- server	to- serv	transp er	oort ren por	note- t	certificate
		Edit Delete	tcp-port 5060	<u>Edit</u>	<u>Edit</u>	any	0		Edit
		Add tcp-port	E I						
	tls-port		tls-port	from- server	to- server	transport	remote port	- cert	ificate
		Edit Delete	<u>tls-port 5061</u>	<u>Edit</u>	<u>Edit</u>	TLS	0	vsp\t aast	tls\certificate pc.p12
1									

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 \rightarrow box <name defined during install> \rightarrow interface eth2 \rightarrow ip outside.

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

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	43 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

⊟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	<u>Edit</u>	Edit	any	0	Edit
		Add udp-por	t					

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 \rightarrow box <name defined during install> \rightarrow interface eth2 \rightarrow ip outside to display the eth2 configuration toward AT&T. Select Media Ports from either the menu or from the display.

AVAYA acme/Epacket				C	onfiguration
Status Summary Logout admin	Home Configura	ttion Status Call L	ogs Event Logs Act	ions Services Keys	Access Tools
Configuration: all	Set Reset Add allow rule, Add d	Back Copy	Delete		
□ cluster □ box:AA-SBC.customerb.com □ interface eth0	general: * name	outside			metr
ip inside interface eth2 ip outside ip outside	admin	enabled 💌 (Resou	rce is active)		1
sip icmp ■ media-ports ■ routing ■ kernel-filter	ip address	* type * address/mask	static (static IP add 192.168.64.130/24	dress) (n.n.n.n/n)	
cli ⊡ vsp	geolocation	0			
derauit-session-config	security-domain	enter	or select from	<not configured=""> 💌</not>	
entry ToTelco entry ToPBX	address-scope	enter	or select from	<not configured=""> 💌</not>	
. entry Discard	filter-intf	disabled 💙 (Resou	rce is inactive)		
enterprise Servers	⊞media-ports [Delete]				>

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

<mark>⊡media-ports</mark> [Delete]	admin	enabled 💌 (Resource is	s active)
	base-port	16384	(at minimum 1,default=20000)
	count	16383	(from 0 to 65,535)
	idle-monitor	enabled 🖌 (Resource is	s active)

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** \rightarrow **enterprise** \rightarrow **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** \rightarrow **servers** \rightarrow **server-pool** \rightarrow **server Telco1** and the Telco1 sip-gateway configuration will be displayed.

AVAYA acme/Epacket				Configuration
Status Summary Logout admin	Home Configu	ration Status Call Lo	gs Event Logs Actions hervices	Keys Access Tools
Configuration: all	Configure vsp\ Show advance	enterprise\servers\sig	o-gateway Telco\server-pool\se	rver Telco1
Configuration Setup View Cluster Vsp	Set Reset	Back Copy	Delete	
 default-session-config tls session-config-pool 	General: * server-name	Telco1		
⊞ dial-plan ⊡ enterprise	admin	enabled 🖌 (Resource	is active)	
	* host	135.25.29.74	(host name or n.n.n.n)	
 € vsp\session-config-pc server-pool Server Telco1 	transport	transport UDP V	User Datagram Protocol)	
. dns settings	port	5060	(at minimum 1,default=5060)	
	Policy:			
	outbound-norm	alization Add outbound	-normalization	
<	inbound-norma	lization Add inbound-r	normalization	

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	Solution & Interoperability Test Lab Application Notes	46 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	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 $vsp \rightarrow session-config-pool \rightarrow entry ToTelco \rightarrow header-settings. In the resultant screen, click$ **Edit blocked-header**.



Step 2 – Enter History-Info into the selection box.

Configure vsp\session-config-pool\entry ToTelco\keader-settings blocked-header
Back
History-info X
Add Remove All
OK

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 \rightarrow session-config-pool \rightarrow entry ToPBX \rightarrow header-settings \rightarrow 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.

Please provide some basic information for reg-ex-header 0. Then press "Create".			
* number	1		
* destination	enter P-Asserted-Identity or select from P-Asserted-Identity V		
Create Reset Cancel			

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.

⊡create	* source	enter P-Asserted-Identity or select from P-Asserted-Identity
	* expression	<pre><sip:(.*)@135.25.29.74(.*) (regular="" expression)<="" pre=""></sip:(.*)@135.25.29.74(.*)></pre>
	* replacement	<sip:\1@customera.com\2< th=""></sip:\1@customera.com\2<>

Step 5 – Enter the following in the remaining fields:

- admin enabled
- apply-to-methods INVITE
- Let all other fields default.

Set Reset B	ack Copy Delete			
admin	enabled 💌 (Resource is active)			
* number	6			
* destination	enter P-Asserted-Identity or select from P-Asserted-Identity V			
⊡create	* source enter P-Asserted-Identity or select from P-Asserted-Identity			
	* expression <pre><sip:(.*)@135.25.29.74(.*) (regular="" expression)<="" pre=""></sip:(.*)@135.25.29.74(.*)></pre>			
	* replacement <sip:\1@customera.com\2< td=""></sip:\1@customera.com\2<>			
append	Add append			
apply-to-methods	INVITE A REFER MESSAGE INFO V			
	Select All Unselect All			
apply-to- responses	* type no 💌 (Do not apply to responses (requests only))			
apply-to-dialog	both (Apply to both inbound and outbound dialogs.)			
session-persistent	disabled 💙 (Resource is inactive)			
Set Reset Ba	ck Copy			

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.

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	49 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

Set Reset E	Copy Delete
admin	enabled 💙 (Resource is active)
* number	5
* destination	enter From or select from From
⊟create	* source enter From or select from From
	* expression <pre><sip:(.*)@135.25.29.74(.*) (regular="" expression)<="" pre=""></sip:(.*)@135.25.29.74(.*)></pre>
	* replacement <pre><sip:\1@customera.com\2< pre=""></sip:\1@customera.com\2<></pre>
append	Add append
apply-to-methods	INVITE
	Select All Unselect All
apply-to- responses	* type no 💌 (Do not apply to responses (requests only))
apply-to-dialog	both (Apply to both inbound and outbound dialogs.)
session-persistent	disabled 💙 (Resource is inactive)
Set Reset Ba	ck Copy

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** \rightarrow **default-session-config** \rightarrow **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.

aura acme (packet	Configuration			
Status Summary Logout admin	Home Configuration Status Call Log	s Event Logs Actions Services Keyle Access Tools		
Configuration: all	Configure vsp\default-session-configure Index Set Reset Back Deleter	g\third-party-call-control Show advanced <u>Help</u>		
 Box:AA-SBC.customerb.com interface eth0 Ip inside Interface eth2 	admin	disabled V (Resource is inactive)		
ip outside sip icmp ≡ media-ports	handle-refer-locally	both (both call-legs) disabled (Resource is inactive)		
 ∎ routing ternel-filter 	refer-maintain-identity	false 💌		
cli ⊡vsp	ringback-file	Browse System Files		
□ default-session-config media	busy-file	Browse System Files		
sip-directive	pre-call-announcement	Browse System Files		
header-settings	terminate-after-pre-call-announcement	disabled 💌 (Resource is inactive)		
⊞ tls	handle-replaces-locally	disabled 🔍 (Recource is inactive)		

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 \rightarrow enterprise \rightarrow servers \rightarrow 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.

Configure vsp\enterprise\servers\sip-gateway Telco					
Set Reset B	ack Copy Delete				
Manage connections, Log instant messages, Record media, Record files, Set up accounting, Change from: URI, Change to: URI					
general:					
* name	Telco				
peer-identity					
admin	enabled 💌 (Resource is active)				
domain					
directory	Create				
failover-detection	ping 💉 (Use OPTIONS to detect failures)				

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

routing:				
routing-setting	normalization auto-tag-match auto-domain-match pstn-backup			
	Select All Unselect All			
domain-alias	Edit domain-alias			
domain-subnet	Edit domain-subnet			
loop-detection	tight 💉 (Compare source and destination address/port/transport)			
service-type	provider 🖌 (Provider peer)			
ping-interval	60 seconds			

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** \rightarrow **Update and save configuration** from the upper left hand side of the user interface, as shown below.

Configuration: all				
Configuration	Setup	View	1	
Update and sav Reloa Update and Validate coningu Analyze configu	e configura I save the cu ration ration	tion Irrent cor	nfigu	
Search configura	ation			
Save as XML Load from XML				

Step 2 - Click OK to update the live configuration.

Microsof	t Internet Explore	r	×		
?	Do you want to update the live configuration?				
	ОК	Cancel			

Step 3 - Click OK to save the live configuration.



A screen that includes the following should appear.



JF:Reviewed SPOC 1/4/2012

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. Avava 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
```

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	54 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

```
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.

Eile	Edit <u>V</u> iew	Go Capture Analyze Statistic	s Telephon <u>y T</u> ools <u>H</u> elp			
		🕷 🖻 🖬 🗙 🎅 🖴	🔍 🍬 🔿 🛧 🖞		2, 0, 12 🖼 🗹 褐 % 💢	
Filt	er: sip			Expression Cle	ear Apply	
No.	Time	Source	Destination	Protocol	Info	^
	25 18.493	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:0000011051@192.168.64.130:5060, wi	th
	26 18.495	5 192.168.64.130	135.25.29.74	SIP	Status: 100 Trying	
	27 18.573	3 192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description	
	168 20.562	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description	
	170 20.572	2 192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description	
	178 20.672	2 135.25.29.74	192.168.64.130	SIP	Request: ACK sip:192.168.64.130:5060;transport=udp	
	433 24.398	3 192.168.64.130	135.25.29.74	SIP	Request: INVITE sip:7326712438@135.25.29.74:5060;trans	por
	436 24.433	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying	
	441 24.484	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description	
	442 24.495	5 192.168.64.130	135.25.29.74	SIP/SDP	Request: ACK sip:73267124380135.25.29.74:5060;transpor	t=u∨
<						>

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

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

Eile	Ēc	lit ⊻iew	<u>Go C</u> apture <u>A</u> nalyze	Statistics Telephony Tools	Help			
	ĕ	. 🖼 🕷	🕷 🖿 🛃 🗶 (2 占 🔍 🍬 🔶 🖄	7 ⊉ 🔳 🗐 🔍	Q Q 🖭 🎬 🖬 🕵 %		
Filte	r: r	tpevent			Expression Clear	r Apply		
No.		Time	Source	Destination	Protocol	Info		~
	76	6 29.236	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Star *	
	768	8 29.265	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Star *	
	77(0 29.295	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Star *	
	777	2 29.316	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Star * (end)	
	773	3 29.316	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Star * (end)	
	774	4 29.316	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Star * (end)	
	782	2 29.455	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Eight 8	
	783	3 29.455	192.168.64	4.130 135.25.29.74	RTP EVENT	Payloa type=RTP Event,	DTMF Eight 8	
	784	4 29.455	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Eight 8	
	78	6 29.486	192.168.64	4.130 135.25.29.74	RTP EVENT	Payload type=RTP Event,	DTMF Eight 8	×
<								>

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

Eile	e <u>E</u> dit	<u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> Statistics	Telephony <u>T</u> ools <u>H</u> elp		
		o 10 10	x 🖻 🛃 🗙 🎅 占	이, 🗢 🛸 🌍 ዥ 👱		Q. Q. 🖾 🚟 🔟 🍢 🎇
Filt	er: rtp)		-	Expression Clea	r Apply
No.		Time	Source	Destination	Protocol	Info
	901	31.115	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=83, Time=19920
	902	31.141	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=416, Time=99840
	903	31.146	192.168,64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=84, Time=20160
	904	31.171	135.25.39.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=417, Time=100080
	905	31.176	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=85, Time=20400
	906	31.201	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=418, Time=100320
	907	31.206	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=86, Time=20640
	908	31.231	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=419, Time=100560
	909	31.236	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=87, Time=20880
	910	31.261	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729. SSRC=0x34841BB4. Sea=420. Time=100800
<						>

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.



JF:Reviewed	
SPOC 1/4/2012	

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

Registration
⊟ SIP
active-association
active-call-peers
active-call-summary
active-calls
active-session

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).

aura 🔐	nc/packet				Status
Status Summary Log	out admin	Home C	onfiguration Status Call Logs Event Logs	Actions Services Keys Ac	cess Tools
 	^		active-calls - currently	vactive calls	
 Memory Messaging Netfilter Policy Presence 			View: Basic 💌 Search		seconds Refresh
		session-id	from	to	state
 	ciation	0x04C2E5413324FB99	<sip:7326712438@135.25.29.74>;tag=ds895bbb08</sip:7326712438@135.25.29.74>	<sip:8884575821@192.168.64.130></sip:8884575821@192.168.64.130>	B2B_CONNECTED
active-call-p active-call-s active-calls active-sess audit-trail	beers summary ion		Page 1 v of 1 showing 25	Taken Sep 1, 2	2011 10:13:34 AM XML

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.

aura acme/tpacket			Call Logs
Status Summary Logout admin Select:	Sessions	Configuration Status Call Logs Event Logs Actions S	ervices Keys Access Tools
 Sessions User Sessions Devices SIP Messages H323 Messages 	Sea	rch Type: All Sessions	
Accounting Calls			Search
Monitored URIs Monitored Calls Files	Page 1 v of 1 s	howing 30 v items	View: User Messages 💌
Database Archives	Created Method Detail Call Diagram 10:12:27.179	Result From To Session Diagram Call Record Delete Media Disconnect Play	Call Call-out Files IM Archive Statistics Auc
Sessions	Thu 2011-09- INVITE 01	Bye sip://326/12438@135.25.29.74 sip:8884575821@1	92.168.64.130 ASE_1314886358145_99

JF:Reviewed SPOC 1/4/2012

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.

Call Sequence for Sessic	Don 0x04C2E5413324FB II_135.138.152.24 CXC-46-59a639(INOS-E 92.168.64.130(eth2) 92.168.64.130(eth2) 92.168.64.130(eth2)	99 <u>Add Session</u> 50-7d43a8c0-13c4-4e5f92cb-6f36e(
Call IDs: ASE_1314886358145_99_nu 	II_135.138.152.24 CXC-46-59a6394 NOS-E 92.168.64.130(eth2) 92.168.67.125(eth0)	50-7d43a8c0-13c4-4e5f92cb-6f36e(
SanDS. ASE_1014000000140_00_110	NOS-E 92.168.64.130(eth2) 92.168.67.125(eth0)	402.459.87.240
	NOS-E 92.168.64.130(eth2) 92.168.67.125(eth0)	403 469 67 340
135.25.29.74 N Telco1 1		192.100.07.210 PBX1
ĺ		<timestamp> <delta> <relative< th=""></relative<></delta></timestamp>
► INVITE (1 INVITE)		10:12:27.178 0.000 0.000
100 Trying (1 INVITE)		10:12:27.178 0.000 0.000
	· INVITE (1 INVITE)	10:12:27.180 0.002 0.002
	100 Trying (1 INVITE)	10:12:27.185 0.005 0.007
4	183 Session Progress (1 INVITE)	10:12:27.195 0.010 0.017
 183 Session Progress (1 INVITE) 		10:12:27.196 0.001 0.018
	200 OK (1 INVITE)	10:12:28.325 1.129 1.147
← 200 OK (1 INVITE) ◆		10:12:28.326 0.001 1.148
ACK (1 ACK)		10:12:28.415 0.089 1.237
	• ACK (1 ACK)→	10:12:28.415 0.000 1.237
	INVITE (1 INVITE)	10:12:28.460 0.045 1.282
	100 Trying (1 INVITE)	10:12:28.460 0.000 1.282
•	, ., ,	10:12:28.461 0.001 1.283
100 Trying (1 INVITE)		10:12:28.497 0.036 1.319
200 OK (1 INVITE)		10:12:28 544 0 047 1 366
		10:12:28 545 0.001 1.367
		10:12:20.553 0.009 1.275
	ACK (TACK)	10:12:28:555 0:008 1:575
ACK (1 ACK)		10:12:28:554 0:001 1:376
	BYE (2 BYE)	10:14:59.556 151.002 152.378
BYE (2 BYE)		10:14:59.557 0.001 152.379
▶ 200 Ok (2 BYE) →		10:14:59.596 0.039 152.418
	200 OK (2 BYE)	10:14:59.596 0.000 152.418

JF:Reviewed SPOC 1/4/2012

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.

Back	Save as text	Save as XML	TEXIT
Call Sequence for Session 0x04C2DBB81EC1D68C	•	Add S	ession

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 <u>http://support.avaya.com</u> 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: <u>http://support.avaya.com/css/P8/documents/100134970</u>
- [6] Avaya Aura® SBC System Administration Guide, V.6.0, 2010 available at: <u>http://support.avaya.com/css/P8/documents/100111137</u>
- [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 -<u>http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-toll-free-enterprise/</u>

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 \rightarrow enterprise \rightarrow servers \rightarrow sip-gatewayTelco \rightarrow server-pool and the previously defined sip-gateway Telco1 defined in Section 7.2.4.1 will be displayed.

AVAYA acme/Epacket								Configu	ration	
Status Summary Loqout admin	Home	Configuration St	atus Call Log	s Event	Logs Actio	ns Serv	ices	Access	Tools	
Configuration: all	Configure	vsp\enterprise\s	servers\sip-g	ateway	Telco\serve	er-pool	S	how advanced	Help	^
Configuration Setup View Configuration Setup View Configuration box:AA-SBC.customerb.com	Set Re	Back	Delete							
 vsp 	server		server	admin	host	transport	port	outbound- normalization	inbound- normalization	
 enterprise servers Bip-gateway PBX sip-gateway Zelco 		Add server	ete server Telco1	enabled	135.25.29.74	UDP	5060	Configure	<u>Configure</u>	İ
l sip-gateway reico	handle- response	Add handle-respo	nse							
⊞ dns settings	Set Res	Back								*

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.

lease provide som	e basic information	for server. Then press "Create".
General:	7	
* server-name	Telco2	
* host	135.25.29.74	(host name or n.n.n.n)
Cr	eate Reset	Cancel

JF:Reviewed SPOC 1/4/2012

Step 4 – Enter the following:

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

aura acme (packet		Configuration
Status Summary Logout admin	Home Configu	ration Status Call Logs Event Logs Actions Services Keys Access Tools
Configuration: all	Configure vsp\e Show advance	enterprise\servers\sip-gateway Telco\serverrpool\server Telco2
 Cluster E box:AA-SBC.customerb.com 	Set Reset	Back Copy Delete
vsp tetault-session-config	General:	
E tis	* server-name	Telco2
 	admin	enabled 💽 (Resource is active)
□ servers I sip-gateway PBX	* host	135.25.29.75 (host name or n.n.n.n)
 ⇒ sip-gateway Telco ⊕ vsp\session-config-r ⊖ server-pool ⊕ server-pool 	transport	transport UDP 🖌 (User Datagram Protocol)
	port	(at minimum 1,default=5060)

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

AVAVA acme/Ypacket								Configur	ation	
aura powered										
Status Summary Logout admin	Home Co	onfiguration Sta	us Call Logs	Event	Logs Action	is Servic	ces	Keys Access	Tools	
Configuration: all	Configure v	/sp\enterprise\s	ervers\sip-ga	iteway	Telco\serve	er∄pool	S	how advanced	Help	>
Configuration Setup View										
□ cluster	Set Res	set Back	Delete							
 vsp 	server		server	admin	host	transport	port	outbound- normalization	inbound- normalization	
session-config-pool										
 		Edit Dele	te server Telco1	enabled	135.25.29.74	UDP	5060	Configure	Configure	
⊟ servers		Edit Dele	etel server Telco2	enabled	135.25.29.75	UDP	5060	Configure	Configure	
I sip-gateway PD∧ □ sip-gateway Telco				ondered	100.20120110	001		<u>bonnga.c</u>		
	c	Add server								
 	handle- response	Add handle-respo	nse							
e dns settings	Set Rese	et Back							i.	~

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

JF:Reviewed	Solution & Interoperability Test Lab Application Notes	63 of 64
SPOC 1/4/2012	©2012 Avaya Inc. All Rights Reserved.	ACM521AASBCIPFR

©2012 Avaya Inc. All Rights Reserved.

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

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