



Avaya Solution & Interoperability Test Lab

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

Abstract

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

Avaya Aura™ Session Manager 6.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura™ Communication Manager 6.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura™ Session Manager. An Avaya Aura™ Session Border Controller is the point of connection between Avaya Aura™ Session Manager and the AT&T IP Flexible Reach service and is used not only to 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.

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

TABLE OF CONTENTS

1.	Introduction.....	4
1.1.	Interoperability Compliance Testing	4
1.2.	Support.....	5
1.3.	Known Limitations	5
2.	Reference Configuration.....	6
2.1.	Illustrative Configuration Information.....	8
2.2.	Call Flows	9
2.2.1.	Inbound	9
2.2.2.	Outbound.....	10
2.2.3.	Call Forward Re-direction	11
2.2.4.	Coverage to Voicemail	12
3.	Equipment and Software Validated	13
4.	Avaya Aura™ Session Manager.....	15
4.1.	Background.....	15
4.2.	Routing Policies	15
4.3.	SIP Domains	18
4.4.	Locations.....	19
4.5.	Adaptations	20
4.5.1.	Adaptation for calls to AT&T.....	21
4.5.2.	Adaptation for calls to Avaya Aura™ Communication Manager	22
4.6.	SIP Entities.....	24
4.6.1.	Avaya Aura™ Session Manager SIP Entity	24
4.6.2.	Avaya Aura™ Communication Manager SIP Entity.....	26
4.6.3.	Avaya Aura™ Session Border Controller SIP Entity.....	27
4.6.4.	Avaya SIP Endpoints SIP Entity.....	28
4.6.5.	Avaya Modular Messaging SIP Entity	29
4.7.	Entity Links.....	30
4.7.1.	Entity Links to Avaya Aura™ Communication Manager	30
4.7.2.	Entity Link to AT&T IP Flexible Reach Service via Session Border Controller	31
4.7.3.	Entity Link to Avaya Aura™ Communication Manager for SIP Endpoints	31
4.7.4.	Entity Link to Avaya Modular Messaging.....	32
4.8.	SIP Entity Completed Configuration	33
4.9.	Time Ranges	36
4.10.	Routing Policies	37
4.10.1.	Routing to AT&T Flexible Reach Service.....	37
4.10.2.	Routing to Avaya Aura™ Communication Manager	39
4.10.3.	Routing to Avaya Modular Messaging	40
4.11.	Dial Patterns.....	41
4.11.1.	Matching Outbound AT&T IP Flexible Reach Service Calls	41
4.11.2.	Matching Inbound Calls to Avaya Aura™ Communication Manager	44
4.11.3.	Matching Inbound Calls to Avaya Modular Messaging Pilot Number via Avaya Aura™ Communication Manager.....	45
4.12.	Routing Policy Completed Configuration	46
4.13.	Session Manager Administration.....	49

5.	Avaya Aura™ Communication Manager	50
5.1.	System Parameters	50
5.2.	Dial Plan and Feature Access Codes	53
5.3.	IP Network Parameters	54
5.4.	Automatic Route Selection (ARS) Table.....	58
5.5.	Alternate Automated Routing (AAR) Table.....	59
5.6.	SIP Trunks	59
5.6.1.	SIP Trunk for AT&T Access	59
5.6.2.	Local SIP Trunk (Modular Messaging and SIP Telephones)	62
5.7.	Route Pattern for Outbound Calls.....	64
5.7.1.	Calls to AT&T	64
5.7.2.	Local Calls	65
5.8.	Private Numbering.....	66
5.9.	Public Unknown Numbering	67
5.10.	Optional Features	67
5.10.1.	Modular Messaging Coverage Path and Hunt Group	67
5.10.2.	Auto Attendant.....	69
5.10.3.	Meet-me Conference.....	70
6.	Avaya Modular Messaging	70
7.	Avaya Aura™ Session Border Controller	71
7.1.	Avaya Aura™ SBC Installation.....	72
7.2.	Avaya Aura™ Session Border Controller Configuration	80
7.2.1.	Login and License Installation.....	80
7.2.2.	Stripping SIP Headers.....	82
7.2.3.	ICMP Configuration For ATT OPTIONS Message Response.....	84
7.2.4.	Contact Header Update	85
7.2.5.	Saving Configuration	87
7.3.	Avaya Aura™ Session Border Controller Running Configuration	88
8.	General Test Approach and Test Results.....	94
9.	Verification Steps.....	96
9.1.	General.....	96
9.2.	Avaya Aura™ Communication Manager	96
9.3.	Avaya Aura™ Session Manager.....	97
9.4.	Protocol Traces	99
9.5.	Avaya Aura™ Session Border Controller	100
10.	Conclusion	102
11.	References.....	102
12.	Addendum 1 – Provisioning for Ptime in Avaya Aura™ Session Border Controller	103
12.1.	Header Manipulation for Inbound and Outbound Calls	103
12.2.	Running Configuration Changes on Session Border Controller.....	105
12.3.	Sample Trace Reflecting the Addition of the Ptime Header.....	106

1. Introduction

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

Avaya Aura™ Session Manager 6.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura™ Communication Manager 6.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura™ Session Manager. An Avaya Aura™ Session Border Controller (SBC) is the point of connection between Avaya Aura™ Session Manager and the AT&T IP Flexible Reach service and is used not only to 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.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 2.2** for examples) between Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, Avaya Aura™ Session Border Controller, and the AT&T IP Flexible Reach service using AVPN or MIS/PNT transport.

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

- SIP trunking.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- PBX features such as hold, resume, conference and transfer.
- Call redirection with Diversion Header.

¹ AVPN uses compressed RTP (cRTP).

² MIS/PNT does not support cRTP.

1.2. Support

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

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.

1.3. Known Limitations

1. 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.
2. **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 Customer's responsibility to ensure proper operation with its equipment/software vendor.

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

3. Communication Manager 6.0 currently uses a SIP telephone event type 127 for the Extend-Call feature. This may cause connectivity issues with AT&T IP Flexible Reach service. As a result, the Extend-Call feature is not supported until this problem is fixed in Communication Manager (Target release for fix - CM R6.0 SP2).
4. Avaya Modular Messaging 5.2 currently uses a SIP telephone event type 127 for the Find-Me feature. This may cause connectivity issues with AT&T IP Flexible Reach service. As a result , the Find-Me feature is not supported until this problem is fixed in Modular Messaging (Target release for fix MM R5.2 SP5).
5. Avaya Network Call Redirection (NCR) must be disabled (default) on the Communication Manager SIP trunk to the AT&T Flexible Reach service, otherwise connectivity issues may result in call scenarios involving Hold being signaled with “sendonly” (Communication Manager signals Hold with “sendonly” only when NCR is enabled).

6. Shuffling must be disabled on the Communication Manager “local” SIP trunk due to codec negotiation issues with Avaya SIP telephones.
7. Currently Communication Manager 6.0 does not include Ptime in SIP message headers when packet intervals other than the default of 20ms are specified. The AT&T IP Flexible Reach service recommendation is to use 30ms intervals, so while Communication Manager 6.0 can be provisioned to transmit at this interval, the associated SIP Ptime signaling will not be sent to the AT&T IP Flexible Reach service. This may result in asymmetric intervals and increased network bandwidth utilization. The procedure described in **Section 12, Addendum 1** shows how the Session Border Controller used in this reference configuration can be configured to insert the ptime=30 parameter, as requested by the AT&T IP Flexible Reach service.

2. Reference Configuration

The reference configuration used in these Application Notes is shown in the figure below and consists of several components:

- Session Manager provides core SIP routing and integration services that enables communications between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- System Manager provides a common administration interface for centralized management of all Avaya Aura™ Session Manager instances in an enterprise.
- Communication Manager provides the voice communications services for a particular enterprise site. In the reference configuration, Communication Manager runs on an Avaya S8800 Server. 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. This solution is extensible to other Avaya Media Gateways.
- Avaya “desk” phones are represented with Avaya 4600 and 9600 Series IP Telephones running H.323 software, 9600 Series IP Telephones running SIP software, Avaya 6211 series Analog Telephones, and Avaya one-X™ Communicator, a PC based Softphone.
- Session Border Controller provides SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network. UDP transport protocol is used between the Session Border Controller 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 and its provisioning is beyond the scope of this document.
- Outbound calls are originated from a phone or fax provisioned on Communication Manager. Signaling is passed from Communication Manager to Session Manager and on to the Session Border Controller, before being sent to the AT&T network for termination. Media is sent from the calling phone to the Communication Manager Media Processor initially on call setup, but when applicable, the media is redirected directly from the station (“shuffled”) via the Session Border Controller.

- Inbound calls are sent from AT&T, through the Session Border Controller to the Session Manager which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate phone or fax extension. The H.323 phones on the enterprise side registered to the Communication Manager C-LAN controller. The SIP phones on the enterprise side registered to the Session Manager.
- Enterprise sites may have additional or alternate routes to PSTN using analog or digital TDM trunks. However these trunks were not used in the reference configuration.

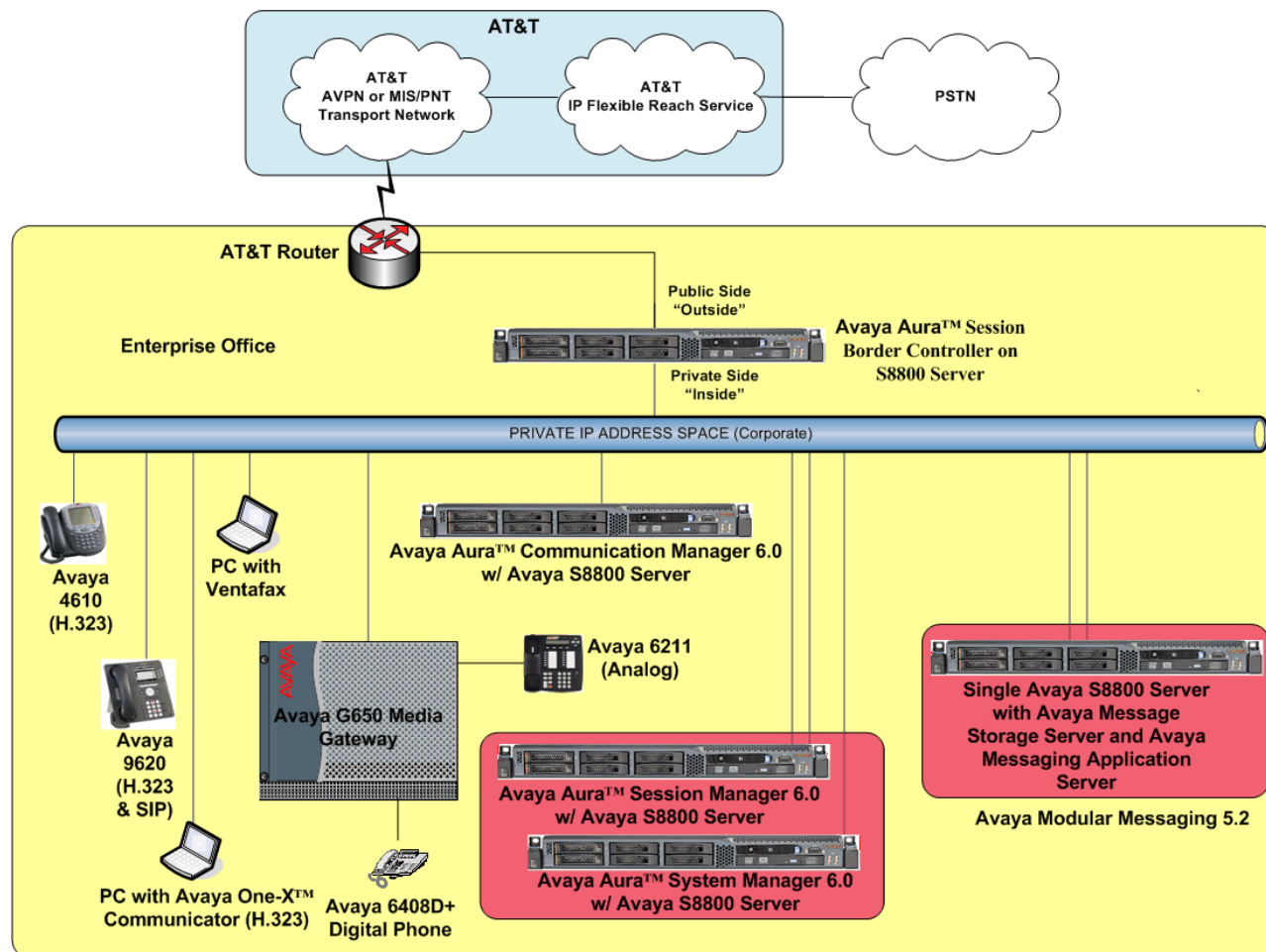


Figure 1: Reference configuration

2.1. Illustrative Configuration Information

The specific values listed in the table 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 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.

Component	Illustrative Value in these Application Notes
Avaya Aura™ System Manager	
Management IP Address	10.80.120.21
Avaya Aura™ Session Manager	
Management IP Address	10.80.120.27
Network IP Address	10.80.120.28
Avaya Aura™ Communication Manager	
C-LAN IP Address	10.80.111.31
Avaya Aura™ Communication Manager extensions	666-50xx = H323 666-51xx=Analog 666-52xx=Digital 666-54xx=SIP
Avaya CPE local dial plan	666-5xxx
Voice Messaging Pilot Extension	666-4999
Avaya Modular Messaging	
Messaging Application Server (MAS) IP Address	10.80.100.30
Messaging Server (MSS) IP Address	10.80.100.29
Avaya Aura™ Session Border Controller	
IP Address of “Outside” (Public) Interface (connected to AT&T Access Router/IP Flexible Reach Service)	192.168.62.55 (active)
IP Address of “Inside” (Private) Interface (connected to Avaya Aura™ Session Manager)	10.80.130.12 (active)
AT&T IP Flexible Reach Service	
Border Element IP Address	135.242.225.210

Table 1: Illustrative Values Used in these Application Notes

2.2. Call Flows

To understand how inbound and outbound AT&T IP Flexible Reach service calls are handled by Session Manager and Communication Manager, four basic call flows are described in this section.

2.2.1. Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IP Flexible Reach service call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a phone, fax, or in some cases, a vector.

1. A PSTN phone originates a call to an AT&T IP Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service routes the call to the Session Border Controller.
4. The Session Border Controller performs any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone, a fax or a vector.

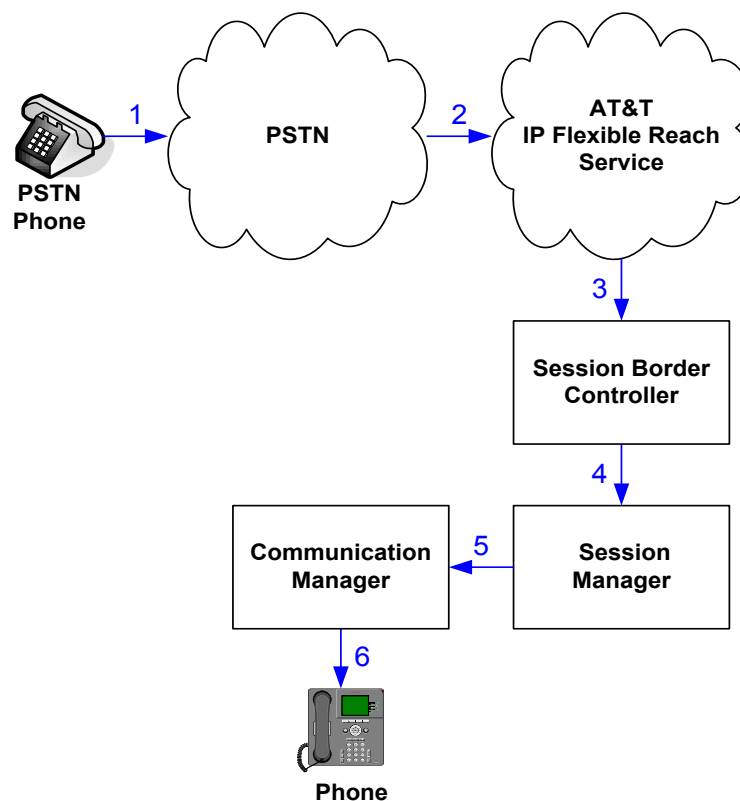


Figure 2: Inbound AT&T IP Flexible Reach Call

2.2.2. Outbound

The second call scenario illustrated in the figure below is an outbound call initiated on Communication Manager, routed to Session Manager and is subsequently sent to the Session Border Controller 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 Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to the Session Border Controller.
4. The Session Border Controller performs any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach service.
5. The AT&T IP Flexible Reach service delivers the call to PSTN.
6. The PSTN delivers the call to the PSTN Phone.

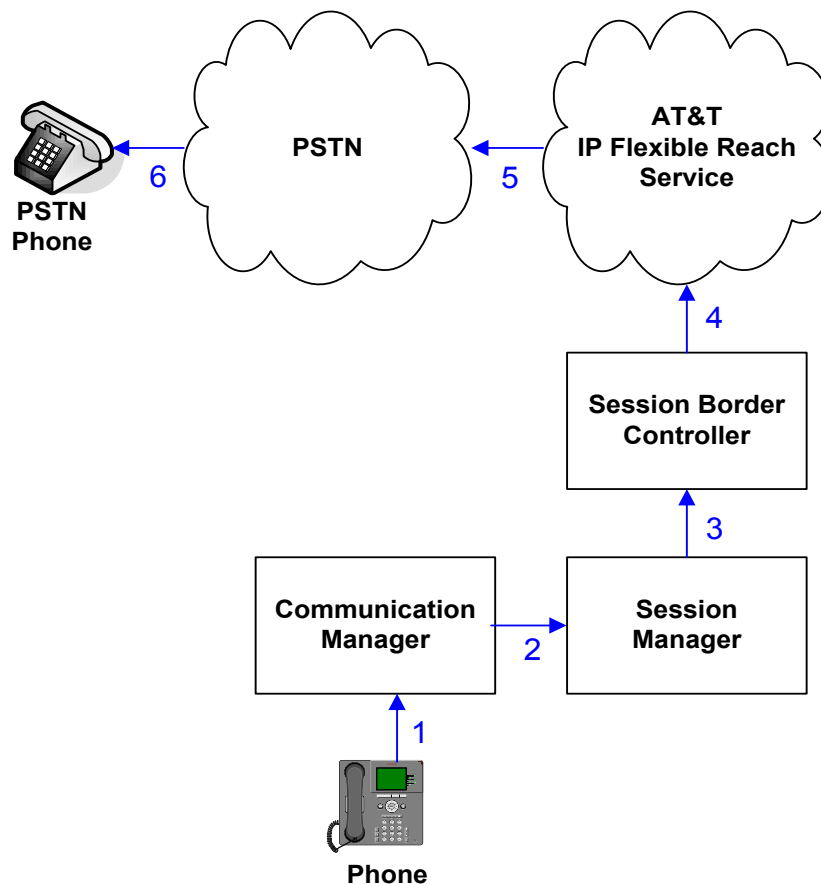


Figure 3: Outbound AT&T IP Flexible Reach Call

2.2.3. Call Forward Re-direction

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

Note –ATT requires the diversion header when a call is redirected to ATT IP Flexible Reach telephone number. (see **Section 5.6.1, Step 5**).

1. Same as the first call scenario in **Section 2.2.1**.
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 Session Manager, the Session Border Controller, and to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service places a call to the alternate destination and upon answer, Communication Manager connects the calling party to the target party.

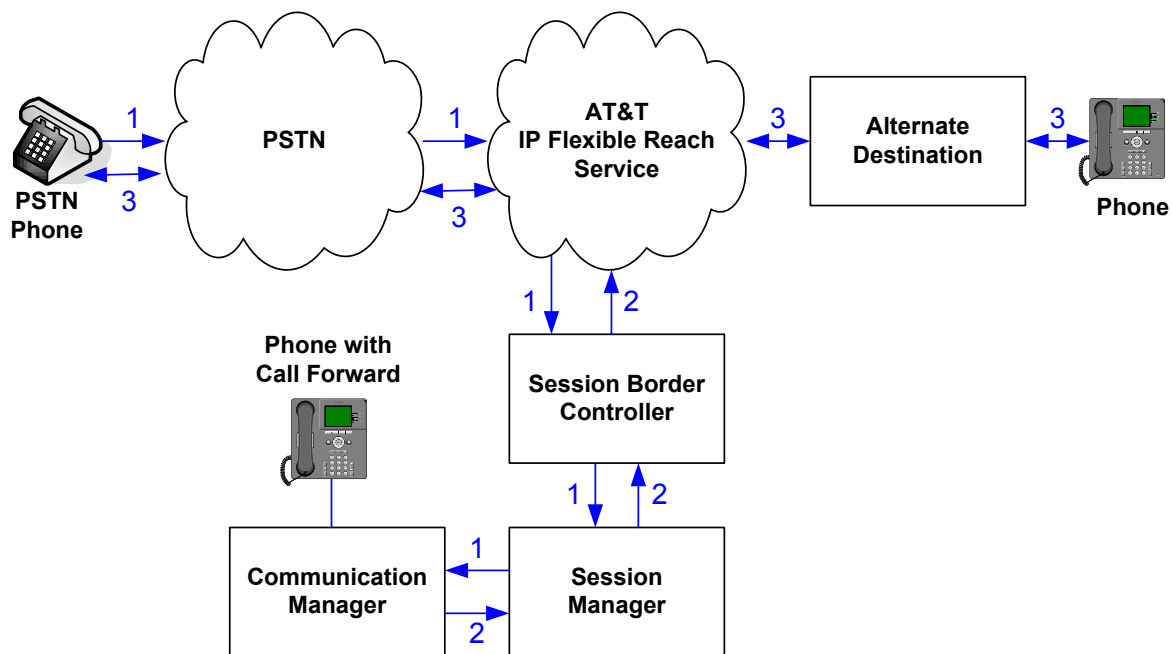


Figure 4: Re-directed (e.g. Call Forward) AT&T IP Flexible Reach Call

2.2.4. Coverage to Voicemail

The call scenario illustrated in the figure below is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Modular Messaging system connected to Session Manager.

1. Same as the first call scenario in **Section 2.2.1**.
2. The called Communication Manager phone does not answer the call, and the call covers to the phone's voicemail. Communication Manager forwards³ the call to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Avaya Modular Messaging. Avaya Modular Messaging answers the call and connects the caller to the called phone's voice mailbox. Note that the call⁴ continues to go through Communication Manager.

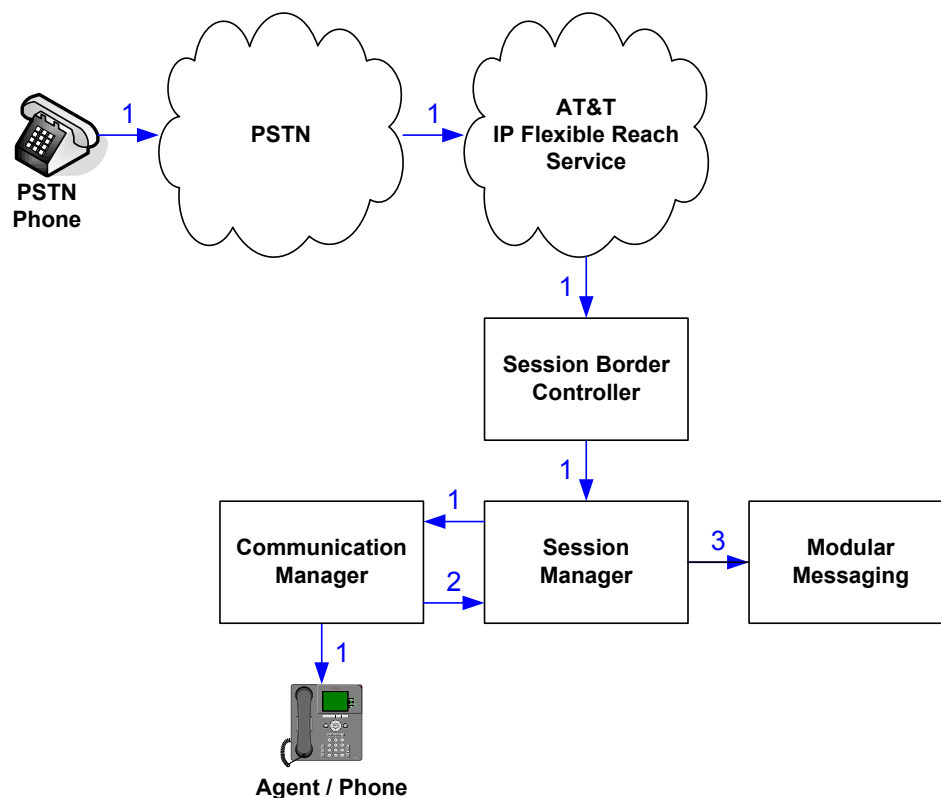


Figure 5: Coverage to Voicemail

³ Communication Manager places a call to Modular Messaging, and then connects the inbound caller to Modular Messaging. SIP redirect methods, e.g., 302, are not used.

⁴ The SIP signaling path still goes through Communication Manager. In addition, since the inbound call and Modular Messaging use different codecs (G.729 and G.711, respectively), Communication Manager performs the transcoding, and thus the RTP media path also goes through Communication Manager.

3. Equipment and Software Validated

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

Component	Version
Avaya S8800 Server	Avaya Aura™ System Manager 6.0 (6.0.0.0.556-3.0.6.1)
Avaya S8800 Server	Avaya Aura™ Session Manager 6.0 (6.0.0.0.600020)
Avaya S8800 Server	Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with patch 18246
Avaya S8800 Server	Avaya Aura™ Session Border Controller 6.0 (R6.0.0.2.4), Product Version 36M2, Build Version 3.6.0, Build 46752
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW15 FW050
TN799DP Control-LAN (C-LAN)	HW01 FW037
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW054
TN2501AP VAL-ANNOUNCEMENT	HW03 FW021
TN2224CP Digital Line	HW08 FW015
TN793CP Analog Line	HW04 FW010
Avaya 9630 IP Telephone	Avaya one-X™ Deskphone Edition H.323 Version S3.1
Avaya 9620C IP Telephone	Avaya one-X™ Deskphone Edition SIP Version 2.6.0
Avaya one-X™ Communicator (H323 Only)	5.2.0.16
Avaya 4625SW IP Telephone	a25d01a2_8.bin
Avaya 6211 Analog phone	-
Avaya S8800 Single Server	Avaya Modular Messaging 5.2
Fax device	Ventafax Home Version 6.2
AT&T IP Flexible Reach Service using AVPN or MIS/PNT transport service connections.	VNI 18

Table 2: Equipment and Software Versions

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1. Avaya agrees to provide service and support for the integration of Avaya

Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1 with the AT&T IP Flexible Reach service offer, in compliance with existing support agreements for Avaya Aura® Communication Manager release 6.0 and Avaya Aura® Session Manager 6.0, and in conformance with the integration guidelines as specified in the body of this document.

4. Avaya Aura™ Session Manager

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

4.1. Background

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

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

4.2. Routing Policies

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

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

- **Locations** – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.
- **Adaptations** – Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities. For example, an AT&T-specific Adaptation is used in these Application Notes to remove SIP History-Info headers from SIP messages sent to the AT&T IP Flexible Reach service network. As another example, basic “Digit Conversion” Adaptations are used in this reference configuration to convert digit strings in “destination” (e.g., Request-URI) and “origination” (e.g. P-Asserted Identity) type headers of SIP messages sent to and received from SIP Entities.
- **Dial Patterns** – A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one⁵ of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed. Note that Dial Patterns are matched after ingress Adaptations have already been applied.
- **Time Ranges** – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Routing Policy may be associated with one or more Time Ranges during which the Routing Policy is in effect. For example, for a Dial Pattern administered with two Routing Policies, one Routing Policy can be in effect on weekday business hours and the other Routing Policy can be in effect on weekday off-hours and weekends. In the reference configuration no restrictions were placed on calling times.

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

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

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

To view the sequenced steps required for configuring network routing policies, click on “**Routing**” in the left pane of the System Manager Common Console (see below).

⁵ The Routing Policy in effect at that time with highest ranking is attempted first. If that Routing Policy fails, then the Routing Policy with the next highest rankings is attempted, and so on.

Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

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

Step 5: Create the "Entity Links"

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

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

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

Step 8: Create "Dial Patterns"

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

Step 9: Create "Regular Expressions"

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

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

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

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

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

Figure 6: Main Routing Page

4.3. SIP Domains

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

1. In the left pane under **Routing**, click on “**Domains**”. In the **Domain Management** page click on “**New**” (not shown) and configure as follows:
 - **Name** –Set to **avaya.com** in this reference configuration
 - **Type** – Set to **sip**
 - **Notes** – Optional Field
2. Click on “**Commit**”
3. Repeat above steps to add additional domains.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top header features the Avaya logo, the product name 'Avaya Aura™ System Manager 6.0', and a welcome message for user 'admin' with a 'Log off' link. A red breadcrumb trail indicates the path 'Home / Routing / Domains'. The left sidebar contains a navigation menu with categories like Elements, Events, Groups & Roles, Licenses, and Routing. Under 'Routing', 'Domains' is selected. The main content area is titled 'Domain Management' and includes 'Commit' and 'Cancel' buttons. Below this is a table with one item, 'avaya.com', which has a type of 'sip' and a default checkbox that is unchecked. A 'Filter: Enable' link is also present. At the bottom, a red asterisk indicates 'Input Required'.

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

Figure 7: Domain Management Page

4.4. Locations

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

1. In the left pane under **Routing**, click on “**Locations**”. In the **Location** page [not shown] click on “**New**”.
2. In the **Location Details** page, configure as follows:
 - **Name** – Enter any descriptive string.
 - **Notes** – (Optional) Enter a description
 - **Managed Bandwidth** and **Average Bandwidth per Call** – (Optional) To limit the number of calls going to and from this location i.e., apply Call Admission Control.
 - **Location Pattern** - (Optional) To identify IP addresses associated with this Location. In the reference configuration, the IP address of Session Border Controller i.e. **10.80.130.12** was used.
3. Click on “**Commit**”.
4. Repeat above steps to add any additional Locations (e.g. **Location 1 Subnet 10.80.100.x**, **Location 1 Subnet 10.80.120.x**, **Loc1 Subnet 10.80.130.x**, **Location 1 Subnet 10.80.111.x**) used in this Reference Configuration.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top navigation bar shows the user is logged in as 'admin' and provides links for Help, About, Change Password, and Log off. The left sidebar contains a tree view with categories like Elements, Events, Groups & Roles, Licenses, and Routing. The 'Routing' category is expanded, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Locations' item is selected. The main content area is titled 'Location Details' and includes a 'General' tab. Under the 'General' tab, there are input fields for 'Name' (filled with 'AuraSBC'), 'Notes' (filled with 'AuraSBC used for ATT Testing'), 'Managed Bandwidth' (with a dropdown for 'Kbit/sec'), and 'Average Bandwidth per Call' (filled with '80' and a dropdown for 'Kbit/sec'). Below this is a 'Location Pattern' section with an 'Add' button and a table. The table has one item with the 'IP Address Pattern' '10.80.130.12' and the 'Notes' 'Inside IP Address of the Aura SBC'. At the bottom of the page, there are 'Commit' and 'Cancel' buttons.

Figure 8: Location Details Page

4.5. Adaptations

Adaptations on Session Manager are always between Session Manager and another entity.

Adaptations could potentially be applied to both calls coming into Session Manager and going out from the Session Manager. In this section, Adaptations are administered for the following purposes:

1. Calls to AT&T (**Section 4.5.1**) - Modification⁶ of SIP messages sent to the AT&T IP Flexible Reach service.
 - The Avaya CPE domain (**avaya.com**) is replaced with the IP address of the AT&T Border Element (**135.242.225.210**) in the Request URI.
 - The “AttAdapter” module removes the History-Info SIP header on egress toward AT&T.
2. Calls from AT&T (**Section 4.5.2**) - Modification of SIP messages sent to Communication Manager.
 - The IP address of Session Manager is replaced with the Avaya CPE SIP domain (**avaya.com**) in the PAI Header.
 - The AT&T DID called number digit strings in the Request URIs are replaced with their associated Communication Manager extensions.

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

4.5.1. Adaptation for calls to AT&T

The Adaptation administered in this section is applied to SIP messages sent to the AT&T IP Flexible Reach service (via the SBC). No Adaptation was applied to the calls coming from AT&T.

1. In the left pane under **Routing**, click on “**Adaptations**”. In the **Adaptations** page, click on “**New**” (not shown).
2. In the **Adaptation Details** page, configure as follows:
 - **Adaptation name** – Set to any descriptive string.
 - **Module name** - Select “**AttAdapter**” from the drop down menu; if no module name is present, select “<click to add module>” and enter “**AttAdapter**”.
 - **Module parameter** - Enter **odstd=135.247.225.210**, which is the IP address of the AT&T Border Element. This will replace the SIP Domain of Session manager (*avaya.com*) in the *outbound* Request URI to AT&T.
3. Click on “**Commit**”.

Note - No digit conversions for incoming or outgoing calls are configured for this Adaptation.

The screenshot shows the Avaya Aura System Manager 6.0 interface. The top header includes the Avaya logo, the title "Avaya Aura™ System Manager 6.0", and a welcome message for user "admin" logged in on August 17, 2010 at 8:14 AM. Navigation links for Help, About, Change Password, and Log off are present. A red breadcrumb trail shows the path: Home / Routing / Adaptations / Adaptation Details. On the left, a sidebar menu lists various system components, with "Routing" expanded and "Adaptations" selected. The main content area is titled "Adaptation Details" and contains a "General" section with the following fields: "Adaptation name" (AT&T Adaptations), "Module name" (AttAdapter), "Module parameter" (odstd=135.247.225.210), "Egress URI Parameters" (empty), and "Notes" (empty). Below this are two sections for "Digit Conversion". The first, "Digit Conversion for Incoming Calls to SM", has an "Add" button and a table with 0 items. The second, "Digit Conversion for Outgoing Calls from SM", also has an "Add" button and a table with 0 items. Both tables have columns for Matching Pattern, Min, Max, Delete Digits, Insert Digits, Address to modify, and Notes. At the bottom, there is a red asterisk indicating "Input Required" and "Commit" and "Cancel" buttons.

Figure 9: Adaptation Details Page – Adaptation for AT&T

4.5.2. Adaptation for calls to Avaya Aura™ Communication Manager

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

1. In the left pane under **Routing**, click on “**Adaptations**”. In the **Adaptations** page, click on “**New**” (not shown).
2. In the **Adaptation Details** page, configure as follows:
 - **Adaptation name** – Set to any descriptive string.
 - **Module name** - Select “**DigitConversionAdapter**” from the drop down menu; if no module name is present, select “<click to add module>” and enter “**DigitConversionAdapter**”.
 - **Module parameter** - Enter **osrcd=avaya.com**, which will replace the IP Address/Domain in the PAI header with the Avaya CPE domain (avaya.com) for egress to Communication Manager.
 - Configure **Digit Conversion for Outgoing Calls from SM** section as follows:
 - a) Click **Add**
 - b) **Matching Pattern** – Add a matching pattern in the Request URI of the call coming into Session Manager
 - c) **Min** and **Max** – Set the minimum and maximum value of the pattern to be matched
 - d) **Delete Digits** – Set the number of digits to be deleted from the pattern
 - e) **Insert Digits** – Set the number of digits to be added to the number in the Request URI
 - f) **Address to modify** – Set the address to modify i.e. origination/destination or both
 - g) **Notes** – [Optional]
 - Repeat the previous step for additional digit conversions to be configured.
 - The figure below lists the digit conversions done for calls coming from ATT Flex Reach service destined for Communication Manager. Note that the ATT DIDs are converted to 7 digit Communication Manager extensions.
3. Click on “Commit”.

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

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 29, 2010 10:31 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Adaptations / Adaptation Details

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

Help

Help for Adaptation Details fields
Help for Committing configuration changes

Adaptation Details

Commit
Cancel

General

* Adaptation name:
ATT CLAN

Module name:
DigitConversionAdapter

Module parameter:
osrcd=avaya.com

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add
Remove

0 Items
Refresh
Filter: Enable

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

Digit Conversion for Outgoing Calls from SM

Add
Remove

8 Items
Refresh
Filter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 3143325084	* 10	* 10	* 10	6665011	destination	
<input type="checkbox"/>	* 3143325085	* 10	* 10	* 10	6665013	destination	
<input type="checkbox"/>	* 3143325100	* 10	* 10	* 10	6665401	destination	
<input type="checkbox"/>	* 3143325101	* 10	* 10	* 10	6665201	destination	
<input type="checkbox"/>	* 4086	* 4	* 4	* 4	6665401	destination	
<input type="checkbox"/>	* 7323204084	* 10	* 10	* 10	6665011	destination	
<input type="checkbox"/>	* 7323204085	* 10	* 10	* 10	6665013	destination	
<input type="checkbox"/>	* 7323204348	* 10	* 10	* 10	6665201	destination	

Select : All, None

* Input Required

Commit
Cancel

Figure 10: Adaptation Details Page – Adaptation for Avaya Aura™ Communication Manager

4.6. SIP Entities

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

- Avaya Aura™ Session Manager
- Avaya Aura™ Communication Manager
- Avaya Aura™ Session Border Controller
- Avaya SIP Endpoints SIP Entity
- Avaya Modular Messaging

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

4.6.1. Avaya Aura™ Session Manager SIP Entity

1. In the left pane under **Routing**, click on “**SIP Entities**”. In the **SIP Entities** page click on “**New**” (not shown).
2. In the **General** section of the **SIP Entity Details** page, configure as follows:
 - **Name** – Enter a descriptive name for Session Manager (e.g. **SM1**).
 - **FQDN or IP Address** – Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation. Set to **10.80.120.28** in this reference configuration.
 - **Type** – Select “**Session Manager**”.
 - **Location** – Select “**Location 1 Subnet 10.80.120.x**” as configured in **Section 4.4**.
 - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
 - **Time Zone** – Select the time zone in which Session Manager resides.
3. In the **SIP Monitoring** section of the **SIP Entity Details** page select “**Use Session Manager Configuration**” for **SIP Link Monitoring** field.
4. In the **Port** section of the **SIP Entity Details** page, click on “**Add**” and provision an entry as follows:
 - **Port** – Enter “**5060**” (see note above).
 - **Protocol** – Select “**TCP**” (see note above).
 - **Default Domain** – (Optional) Select a SIP domain administered in **Section 4.3**.
5. Repeat **Step 4** to provision another entry, except with “**5080**” for **Port** and “**TCP**” for **Protocol**. Since a single C-LAN was used in this reference configuration, a separate port was configured to separate the SIP endpoint traffic from other traffic on C-LAN. This was done because of the known limitation noted in **Section 1.3, Item 6**.
6. Click on “**Commit**”.

These entries enable Session Manager to accept SIP requests on the specified ports/protocols.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 29, 2010 7:20 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

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

Help

Help for SIP Entity Details fields
Help for Committing configuration changes

SIP Entity Details

CommitCancel

General

Name: SM1

FQDN or IP Address: 10.80.120.28

Type: Session Manager

Notes:

Location: Location 1 Subnet 10.80.120.X

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

AddRemove

2 Items Refresh

Filter: Enable

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

Select : All, None

* Input Required

CommitCancel

Figure 11: SIP Entity Details Page – Avaya Aura™ Session Manager SIP Entity

4.6.2. Avaya Aura™ Communication Manager SIP Entity

1. In the **SIP Entities** page, click on “New”.
2. In the **General** section of the **SIP Entity Details** page, configure as follows:
 - **Name** – Enter any descriptive name for the Communication Manager Signaling Interface.
 - **FQDN or IP Address** – Enter the IP address of the Communication Manager C-LAN provisioned in **Section 5.3, Step 5**.
 - **Type** – Select “CM”.
 - **Adaptation** – Select the Adaptation administered in **Section 4.5.2**.
 - **Location** – Select a Location administered in **Section 4.4**.
 - **Time Zone** – Select the time zone in which Communication Manager resides.
 - In the **SIP Monitoring** section of the **SIP Entity Details** page select “Use Session Manager Configuration” for **SIP Link Monitoring** field.
3. Click on “Commit”.

The screenshot displays the Avaya Aura™ System Manager 6.0 interface for configuring a SIP Entity. The top header shows the Avaya logo, the title 'Avaya Aura™ System Manager 6.0', and user information: 'Welcome, admin Last Logged on at July 29, 2010 7:20 PM' with links for 'Help | About | Change Password | Log off'. The breadcrumb trail is 'Home / Routing / SIP Entities / SIP Entity Details'. The left sidebar contains a navigation menu with categories: Elements, Events, Groups & Roles, Licenses, Routing (selected), Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults, Security, System Manager Data, and Users. Below the sidebar is a 'Help' section with links for 'Help for SIP Entity Details fields', 'Help for Committing configuration changes', and 'Help for Committing configuration changes'. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into sections: 'General' (with fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, and Override Port & Transport with DNS SRV), 'SIP Link Monitoring' (with a dropdown for SIP Link Monitoring), and 'Entity Links' (with a note: 'Entity Links can be modified after SIP Entity is committed.'). A red asterisk indicates required fields. The bottom of the page has another set of 'Commit' and 'Cancel' buttons.

Figure 12: SIP Entity Details Page – Avaya Aura™ Communication Manager SIP Entity

4.6.3. Avaya Aura™ Session Border Controller SIP Entity

To configure the Session Border Controller entity, repeat the Steps in **Section 4.6.2**. The **FQDN or IP Address** field is populated with the IP address of the private (inside) interface configured in **Section 7.1** and the **Type** field is set to “**Other**”. See the figure below for the values used in the reference configuration.

The screenshot shows the Avaya Aura System Manager 6.0 interface. The top header includes the Avaya logo, the product name 'Avaya Aura™ System Manager 6.0', and a welcome message for user 'admin' last logged on at July 30, 2010 11:26 AM. A navigation bar shows the path: Home / Routing / SIP Entities / SIP Entity Details. A left sidebar contains a tree view with categories: Elements, Events, Groups & Roles, Licenses, Routing (selected), Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults, Security, System Manager Data, and Users. Below the sidebar is a 'Help' section with links for 'Help for SIP Entity Details fields' and 'Help for Committing configuration changes'. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into sections: 'General' (with a blue header), 'SIP Link Monitoring' (with a blue header), and 'Entity Links' (with a blue header). The 'General' section contains fields for: * Name (AuraSBC), * FQDN or IP Address (10.80.130.12), Type (Other), Notes (Avaya Aura SBC Inside IP), Adaptation (AT&T Adaptations), Location (AuraSBC), Time Zone (America/Denver), Override Port & Transport with DNS SRV (unchecked), * SIP Timer B/F (in seconds) (4), Credential name (empty), and Call Detail Recording (none). The 'SIP Link Monitoring' section has a field for SIP Link Monitoring set to 'Use Session Manager Configuration'. The 'Entity Links' section has a red warning message: 'Entity Links can be modified after SIP Entity is committed.' At the bottom of the main content area, there is a red asterisk and the text '* Input Required', followed by 'Commit' and 'Cancel' buttons.

Figure 13: SIP Entity Details Page – Session Border Controller SIP Entity

4.6.4. Avaya SIP Endpoints SIP Entity

Because of the shuffling limitation noted in **Section 1.3, Item 6**, a separate SIP Entity was created to handle calls to and from SIP Endpoints registered with Session Manager. A single CLAN was used in this reference configuration but a different port number was used as configured in **Section 4.6.1, Step 5**. Configuration for this entity is similar to the Entity configured in **Section 4.6.2**.

Note: For routing the calls from SIP Endpoints to Communication Manager, this entity has to be used in Application Sequence. The configuration of the Application Sequence on Session Manager is beyond the scope of this document.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, admin Last Logged on at July 30, 2010 11:26 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Entity Links can be modified after SIP Entity is committed.

* Input Required Commit Cancel

Help

[Help for SIP Entity Details fields](#)

[Help for Committing configuration changes](#)

Figure 14: SIP Entity Details Page – Avaya SIP Endpoints

4.6.5. Avaya Modular Messaging SIP Entity

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

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top navigation bar shows the Avaya logo, the title 'Avaya Aura™ System Manager 6.0', and a user status 'Welcome, admin Last Logged on at September 1, 2010 5:39 PM'. A secondary navigation bar contains links: 'Home / Routing / SIP Entities / SIP Entity Details', 'Help | About | Change Password | Log off', and buttons for 'Commit' and 'Cancel'.

The left sidebar contains a tree view with categories: Elements, Events, Groups & Roles, Licenses, Routing (expanded), Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults, Security, System Manager Data, and Users. A 'Help' section at the bottom of the sidebar provides links for 'Help for SIP Entity Details fields' and 'Help for Committing configuration changes'.

The main content area is titled 'SIP Entity Details' and features a 'General' tab. The configuration fields are as follows:

- Name:** ModMess5_2
- * FQDN or IP Address:** 10.80.100.30
- Type:** Other
- Notes:** Modular Messaging 5.2 SS MS
- Adaptation:** (dropdown menu)
- Location:** Location 1 Subnet 10.80.100.x
- Time Zone:** America/Denver
- Override Port & Transport with DNS SRV:** ☐
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (text field)
- Call Detail Recording:** none

Below the General tab is the 'SIP Link Monitoring' section with a dropdown menu set to 'Use Session Manager Configuration'. The 'Entity Links' section contains a red warning: 'Entity Links can be modified after SIP Entity is committed.' At the bottom left, a red asterisk indicates '* Input Required'. Buttons for 'Commit' and 'Cancel' are located at the bottom right.

Figure 15: SIP Entity Details Page – Avaya Modular Messaging SIP Entity

4.7. Entity Links

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

- Avaya Aura™ Communication Manager
- Avaya Aura™ Session Border Controller
- Avaya SIP Endpoints
- Avaya Modular Messaging

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

4.7.1. Entity Links to Avaya Aura™ Communication Manager

1. In the left pane under **Routing**, click on “**Entity Links**”. In the **Entity Links** page click on “**New**” (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name for this link to Communication Manager (e.g. **SM1-ATTClan**).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 4.6.1** for Session Manager. SIP Entity 1 must always be an Session Manager instance.
 - **SIP Entity 1 Port** – Enter “**5060**”
 - **SIP Entity 2** – Select the SIP Entity administered in **Section 4.6.2** for Communication Manager.
 - **SIP Entity 2 Port** - Enter “**5060**”.
 - **Trusted** – Check the checkbox.
 - **Protocol** – Select “**TCP**”.
3. Click on “**Commit**”.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, admin Last Logged on at July 29, 2010 7:20 PM
Help | About | Change Password | Log off

Home / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM1-ATTClan	* SM1	TCP	* 5060	* ATT-CLAN	* 5060	<input checked="" type="checkbox"/>	Entity Link to AT

* Input Required

Commit Cancel

Figure 16: Entity Links Page – Entity Link to Avaya Aura™ Communication Manager

4.7.2. Entity Link to AT&T IP Flexible Reach Service via Session Border Controller

To configure the entity link between Session Manager and Session Border Controller entity, repeat the Steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.3**. See the figure below for the values used in the reference configuration.

The screenshot shows the Avaya Aura System Manager 6.0 interface. The left sidebar contains a navigation menu with options: Elements, Events, Groups & Roles, Licenses, and Routing (expanded). Under Routing, there are links for Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, and Routing Policies. The main content area is titled 'Entity Links' and includes a 'Commit' and 'Cancel' button. Below this is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The row shows: Name: SM1_AuraSBC, SIP Entity 1: SM1, Protocol: TCP, Port: 5060, SIP Entity 2: AuraSBC, Port: 5060, Trusted: checked, Notes: empty. A red asterisk indicates required input. At the bottom right are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM1_AuraSBC	* SM1	TCP	* 5060	* AuraSBC	* 5060	<input checked="" type="checkbox"/>	

Figure 17: Entity Links Page – Entity Link to AT&T IP Flexible Reach Service via Session Border Controller

4.7.3. Entity Link to Avaya Aura™ Communication Manager for SIP Endpoints

To configure this entity link, repeat the Steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.4**. See the figure below for the values used in the reference configuration.

The screenshot shows the Avaya Aura System Manager 6.0 interface. The left sidebar contains a navigation menu with options: Elements, Events, Groups & Roles, Licenses, and Routing (expanded). Under Routing, there are links for Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, and Routing Policies. The main content area is titled 'Entity Links' and includes a 'Commit' and 'Cancel' button. Below this is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The row shows: Name: SM1_AvayaSIPEndg, SIP Entity 1: SM1, Protocol: TCP, Port: 5080, SIP Entity 2: AvayaSIPEndpointsTrunk, Port: 5080, Trusted: checked, Notes: empty. A red asterisk indicates required input. At the bottom right are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM1_AvayaSIPEndg	* SM1	TCP	* 5080	* AvayaSIPEndpointsTrunk	* 5080	<input checked="" type="checkbox"/>	

Figure 18: Entity Links Page – Entity Link to SIP Endpoints via Communication Manager

4.7.4. Entity Link to Avaya Modular Messaging

To configure this entity link, repeat the Steps in **Section 4.7.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 4.6.5**. See the figure below for the values used in the reference configuration.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 29, 2010 7:20 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Entity Links

Entity Links

Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM1_ModMess5_2	* SM1	TCP	* 5060	* ModMess5_2	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

Figure 19: Entity Links Page – Entity Link to Avaya Modular Messaging

4.8. SIP Entity Completed Configuration

After the SIP Entity and their corresponding links have been configured, the SIP Entity screens change with the entity link information appended to it. Following figures show all the Entities configured in **Section 4.6** after the entity links have been added in **Section 4.7**.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 4, 2010 11:49 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name: SM1

* FQDN or IP Address: 10.80.120.28

Type: Session Manager

Notes:

Location: Location 1 Subnet 10.80.120.X

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

4 Items Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM1	TCP	* 5060	ATT-CLAN	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	AuraSBC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5080	AvayaSIPEndpointsTrunk	* 5080	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	ModMess5_2	* 5060	<input checked="" type="checkbox"/>

Select : All, None

Port

Add Remove

2 Items Refresh Filter: Enable

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

Select : All, None

* Input Required Commit Cancel

Figure 20: Completed Session Manager Entity configured in Section 4.6.1

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at July 29, 2010 7:20 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name: ATT-CLAN

* FQDN or IP Address: 10.80.111.31

Type: CM

Notes: ATT CLAN

Adaptation: ATT CLAN

Location: Location 1 Subnet 10.80.111.x

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item Refresh Filter: Enable						
	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM1	TCP	* 5060	ATT-CLAN	* 5060	<input checked="" type="checkbox"/>

Select : All, None

* Input Required Commit Cancel

Figure 21: Completed Communication Manager Entity configured in Section 4.6.2

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at July 29, 2010 7:20 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name: AuraSBC

* FQDN or IP Address: 10.80.130.12

Type: Other

Notes: Avaya Aura SBC Inside IP

Adaptation: AT&T Adaptations

Location: AuraSBC

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item Refresh Filter: Enable						
	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM1	TCP	* 5060	AuraSBC	* 5060	<input checked="" type="checkbox"/>

Select : All, None

* Input Required Commit Cancel

Figure 22: Completed Session Border Controller Entity configured in Section 4.6.3

AVAYA Avaya Aura™ System Manager 6.0 Welcome, admin Last Logged on at August 4, 2010 11:49 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name:
 * FQDN or IP Address:
 Type:
 Notes:
 Adaptation:
 Location:
 Time Zone:
 Override Port & Transport with DNS SRV: ☐
 * SIP Timer B/F (in seconds):
 Credential name:
 Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links
 Add Remove

1 Item	Refresh	Filter: Enable				
<input type="checkbox"/>	<input type="text" value="SM1"/>	<input type="text" value="TCP"/>	<input type="text" value="5080"/>	<input type="text" value="AvayaSIPEndpointsTrunk"/>	<input type="text" value="5080"/>	<input checked="" type="checkbox"/>

Select : All, None

* Input Required Commit Cancel

Figure 23: Completed SIP Endpoints Entity configured in Section 4.6.4

AVAYA Avaya Aura™ System Manager 6.0 Welcome, admin Last Logged on at July 29, 2010 7:20 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / SIP Entities / SIP Entity Details

SIP Entity Details Commit Cancel

General

* Name:
 * FQDN or IP Address:
 Type:
 Notes:
 Adaptation:
 Location:
 Time Zone:
 Override Port & Transport with DNS SRV: ☐
 * SIP Timer B/F (in seconds):
 Credential name:
 Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links
 Add Remove

1 Item	Refresh	Filter: Enable				
<input type="checkbox"/>	<input type="text" value="SM1"/>	<input type="text" value="TCP"/>	<input type="text" value="5060"/>	<input type="text" value="ModMess5_2"/>	<input type="text" value="5060"/>	<input checked="" type="checkbox"/>

Select : All, None

* Input Required Commit Cancel

Figure 24: Completed Modular Messaging Entity configured in Section 4.6.5

4.9. Time Ranges

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

Avaya Aura™ System Manager 6.0

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

Home / Routing / Time Ranges

Time Ranges

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

2 Items [Refresh](#) Filter: [Enable](#)

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

Select : All, None

Figure 25: Time Ranges Page

4.10. Routing Policies

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

- To the AT&T Flexible Reach Service (via the Avaya Aura™ Session Border Controller)
- To Avaya Aura™ Communication Manager
- To Avaya Modular Messaging

4.10.1. Routing to AT&T Flexible Reach Service

1. In the left pane under **Routing**, click on “**Routing Policies**”. In the **Routing Policies** page click on “**New**” (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **To_ATT**) for routing calls to AT&T, and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at September 1, 2010 5:39 PM

Help | About | Change Password | Log off

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details

Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

Figure 26: Routing Policy To AT&T

3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on “**Select**”.
4. In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.6.3** for Session Border Controller (**AuraSBC**), and click on “**Select**”.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 30, 2010 5:19 PM

Help | About | Change Password | Log off

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

SIP Entity List

Select Cancel

SIP Entities

23 Items Refresh Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	ATT-CLAN	10.80.111.31	CM	ATT CLAN
<input checked="" type="radio"/>	AuraSBC	10.80.130.12	Other	Avaya Aura SBC Inside IP
<input type="radio"/>	Avaya-CM	135.8.19.121	CM	
<input type="radio"/>	AvayaSIPEndpointsTrunk	10.80.111.31	CM	Endpoints Registered with SM

Figure 27: SIP Entity List Page - Routing to AT&T

5. Returning to the **Routing Policy Details** page, click on “**Add**” in the **Time of Day** section.
6. In the **Time Range List** page [not shown], check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 4.9**, and click on “**Select**”.
7. Returning to the **Routing Policy Details** page, enter a **Ranking** (the lower the number, the higher the ranking) in the **Time of Day** section for each Time Range.
8. Any **Dial Patterns** that were previously defined will be displayed and entries may be added or removed here. Dial patterns for this reference configuration are configured in **Section 4.11**.
9. No **Regular Expressions** were used in this reference configuration.
10. Click **Commit**.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at September 1, 2010 5:39 PM

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

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AuraSBC	10.80.130.12	Other	Avaya Aura SBC Inside IP

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Select : All, None

Dial Patterns

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

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

* Input Required Commit Cancel

Figure 28: Routing Policy Details Page to AT&T

4.10.2. Routing to Avaya Aura™ Communication Manager

To configure this routing policy to Communication Manager, repeat the Steps in **Section 4.10.1**. In the **SIP Entity as Destination** section, select the SIP Entity administered in **Section 4.6.2** for Communication Manager. See the figure below for the values used in the reference configuration.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at July 30, 2010 5:19 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
ATT-CLAN	10.80.111.31	CM	ATT CLAN

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

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

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

Select : All, None

Dial Patterns

[Add](#) [Remove](#)

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

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Regular Expressions

[Add](#) [Remove](#)

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

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

* Input Required [Commit](#) [Cancel](#)

Figure 29: Routing Policy Details Page to Communication Manager

4.10.3. Routing to Avaya Modular Messaging

To configure this routing policy to Modular Messaging, repeat the Steps in **Section 4.10.1**. In the **SIP Entity as Destination** section, select the SIP Entity administered in **Section 4.6.5** for Modular Messaging. See the figure below for the values used in the reference configuration.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 2, 2010 12:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ModMess5_2	10.80.100.30	Other	Modular Messaging 5.2 SS MS

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Select : All, None

Dial Patterns

Add Remove

0 Items Refresh Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--	---------	-----	-----	----------------	------------	----------------------	-------

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

	Pattern	Rank Order	Deny	Notes
--	---------	------------	------	-------

* Input Required Commit Cancel

Figure 30: Routing Policy Details Page to Avaya Modular Messaging

4.11. Dial Patterns

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

- Inbound/outbound PSTN calls via AT&T IP Flexible Reach service.
- Calls to/from 11-digit local dial plan numbers associated with extensions on Communication Manager or the Avaya Modular Messaging pilot number.
- Notifications from Avaya Modular Messaging (MWI) to Communications Manager 7 digit local extensions.

4.11.1. Matching Outbound AT&T IP Flexible Reach Service Calls

In this example outbound calls to any PSTN numbers with the pattern 1303538xxxx are defined.

1. In the left pane under **Routing**, click on “**Dial Patterns**”. In the **Dial Patterns** page click on “**New**” (not shown).
2. In the **General** section of the **Dial Pattern Details** page, configure as follows:
 - **Pattern** – Enter matching patterns for outbound dialed digits. Set to **1303538** in this example.
 - **Min** and **Max** – Enter **11**.
 - **SIP Domain** – Select one of the SIP Domains defined in **Section 4.3** or “**-ALL-**”, to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or any of the administered SIP Domains if “**-ALL-**” is selected) can match this Dial Pattern. Set to **avaya.com** in this example.
 - (Optional) Add any notes if desired.
3. In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on “**Add**”.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at July 30, 2010 11:26 AM
Help | About | Change Password | Log off

Home / Routing / Dial Patterns / Dial Pattern Details

Dial Pattern Details [Commit] [Cancel]

General

* **Pattern:** 1303538

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Calls To ATT Sonus Network

Originating Locations and Routing Policies

[Add] [Remove]

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
--------------------------	---------------------------	----------------------------	---------------------	------	-------------------------	----------------------------	----------------------

Denied Originating Locations

[Add] [Remove]

0 Items | Refresh Filter: Enable

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

* **Input Required** [Commit] [Cancel]

Figure 31: Dial Pattern Details Page - Matching Outbound AT&T IP Flexible Reach Service Calls

4. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, select the locations from where calls can originate to be routed to AT&T Flexible Reach service via Session Border Controller. Note that only those calls that originate from the selected Location(s), or any of the administered Locations if “-ALL-” is selected, can match this Dial Pattern.
5. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, select the Routing Policy administered for routing calls to the AT&T IP Flexible Reach service in **Section 4.10.1**.
6. Click on **Select**.

Avaya Aura™ System Manager 6.0
Welcome, admin Last Logged on at July 30, 2010 11:26 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

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

> Elements

> Events

> Groups & Roles

Licenses

> **Routing**

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

> Security

> System Manager Data

> Users

Help

Originating Location and Routing Policy List

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

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

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	AuraSBC	AuraSBC used for ATT Testing
<input type="checkbox"/>	Branch_Location_1	BSM1
<input checked="" type="checkbox"/>	Loc1 10.80.130.x	10.80.130.x
<input type="checkbox"/>	Location 1 Subnet 10.80.100.x	
<input checked="" type="checkbox"/>	Location 1 Subnet 10.80.111.x	Location 1 Subnet 10.80.111.x
<input type="checkbox"/>	Location 1 Subnet 10.80.120.X	
<input type="checkbox"/>	Location 1 Subnet 10.80.48.x	
<input type="checkbox"/>	Location 1 Subnet 10.80.50.X	CS1000E
<input type="checkbox"/>	Location 1 Subnet 10.80.60.x	Avaya HQ
<input type="checkbox"/>	Location 1 Subnet 135.8.19.X	
<input type="checkbox"/>	Location for BCM	
<input type="checkbox"/>	SRST Branch 1	Remote Branch 1 - 10.80.61.*

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

Routing Policies

☐ Apply The Selected Routing Policies to All Routing Policies

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

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	CS1K via M1k	<input type="checkbox"/>	Mediant1000-West	
<input type="checkbox"/>	silconf-bridge	<input type="checkbox"/>	silconf-bridge	
<input type="checkbox"/>	SIPEndpointsRouting	<input type="checkbox"/>	AvayaSIPEndpointsTrunk	Calls for ATT testing
<input checked="" type="checkbox"/>	To_AT&T	<input type="checkbox"/>	AuraSBC	Route to ATT via Avaya SBC
<input type="checkbox"/>	To ATT CLAN	<input type="checkbox"/>	ATT-CLAN	Calls for ATT testing

Figure 32: Originating Location and Routing Policy List Page - Matching Outbound AT&T IP Flexible Reach Service Calls

7. Returning to the **Dial Pattern Details** page below, click on “**Commit**”.
8. Repeat **Steps 2-7** for each outbound matching dial pattern required (e.g. 1314346xxxx, 1800346xxxx, 1914222xxxx, and international 011 calls)

AVAYA
Avaya Aura™ System Manager 6.0
Welcome, **admin** Last Logged on at July 30, 2010 11:26 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details

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

Help

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

Dial Pattern Details
Commit Cancel

General

* Pattern: 1303538
* Min: 11
* Max: 11
Emergency Call: ☐
SIP Domain: avaya.com
Notes: Call To ATT Sonus Network

Originating Locations and Routing Policies
Add Remove

3 Items Refresh
Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AuraSBC	AuraSBC used for ATT Testing	To AT&T	0	<input type="checkbox"/>	AuraSBC	Route to ATT via Avaya SBC
<input type="checkbox"/>	Loc1 10.80.130.x	10.80.130.x	To AT&T	0	<input type="checkbox"/>	AuraSBC	Route to ATT via Avaya SBC
<input type="checkbox"/>	Location 1 Subnet 10.80.111.x	Location 1 Subnet 10.80.111.x	To AT&T	0	<input type="checkbox"/>	AuraSBC	Route to ATT via Avaya SBC

Select : All, None

Denied Originating Locations
Add Remove

0 Items Refresh
Filter: Enable

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

* Input Required
Commit Cancel

Figure 33: Dial Pattern Details – After adding Originating Locations and Routing Policies

4.11.2. Matching Inbound Calls to Avaya Aura™ Communication Manager

To match dial pattern for the calls coming in from AT&T Flex Reach service via Session Border Controller, repeat the Steps in **Section 4.11.1**. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, select the locations from where calls can originate to be routed to Communication Manager. Note that only those calls that originate from the selected Location(s), or any of the administered Locations if “-ALL-” is selected, can match this Dial Pattern. See the figure below for the values used in the reference configuration. In this example inbound calls from AT&T with the called digit pattern 7323xxxxxxx are shown below. See Section 4.12 for all the Dial Patterns used in this reference configuration.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at August 2, 2010 12:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AuraSBC	AuraSBC used for ATT Testing	To ACM	0	<input type="checkbox"/>	ATT-CLAN	Calls for ATT Network To ACM

Select : All, None

Denied Originating Locations

Add Remove

0 Items [Refresh](#) Filter: Enable

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

* Input Required Commit Cancel

Figure 34: Dial Pattern Details - Matching Inbound AT&T IP Flexible Reach Service Calls

4.11.3. Matching Inbound Calls to Avaya Modular Messaging Pilot Number via Avaya Aura™ Communication Manager

Communication Manager stations cover to Modular Messaging using a pilot extension (6664999 in this reference configuration). Also, stations on Communication Manager may dial this number to retrieve messages or modify mailbox settings. To match dial pattern for the calls covered to Modular Messaging, repeat the Steps in **Section 4.11.1**. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, select the locations from where calls can originate to be routed to Modular Messaging. Note that only those calls that originate from the selected Location(s), or any of the administered Locations if “-ALL-” is selected, can match this Dial Pattern. See the figure below for the values used in the reference configuration.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at August 2, 2010 12:06 PM [Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Dial Patterns / Dial Pattern Details

Dial Pattern Details Commit Cancel

General

* Pattern: 6664999

* Min: 7

* Max: 7

Emergency Call: ☐

SIP Domain: avaya.com

Notes: to MM 5.2: Single Server

Originating Locations and Routing Policies

Add Remove

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input checked="" type="checkbox"/>	-ALL-	Any Locations	ToMMS_2	0	<input type="checkbox"/>	ModMess5_2	Coverage to MM 5.2

Select : All, None

Denied Originating Locations

Add Remove

0 Items [Refresh](#) Filter: Enable

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

* Input Required Commit Cancel

Help

[Help for Dial Pattern Details fields](#)

[Help for Location and Routing Policy Lists](#)

[Help for Denied Location fields](#)

[Help for Committing configuration changes](#)

Figure 35: Dial Pattern Details - Coverage to Modular Messaging

4.12. Routing Policy Completed Configuration

After the Routing Policy and various Dial Patterns have been configured, the Routing Policy screens change to reflect all the Dial Patterns used to determine where the call needs to be routed. Following figures show all the Routing Policies configured in **Section 4.10** after the Dial Patterns have been added in **Section 4.11**.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The left sidebar shows a navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. The 'General' tab is active, showing the policy name 'To_AT&T', a 'Disabled' checkbox, and a note 'Calls to ATT Network via SBC'. Below this is the 'SIP Entity as Destination' section with a 'Select' button and a table listing SIP entities. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, followed by a table showing a single time range for 24/7. The 'Dial Patterns' section has 'Add' and 'Remove' buttons, followed by a table listing 17 dial patterns. The 'Regular Expressions' section includes 'Add' and 'Remove' buttons and a table with 0 items. At the bottom, there is a 'Commit' button and a 'Cancel' button.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 4, 2010 11:49 AM
Help | About | Change Password | Log off

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AuraSBC	10.80.130.12	Other	Avaya Aura SBC Inside IP

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Select : All, None

Dial Patterns

Add Remove

17 Items Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
011	3	36	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.111.x	International Calls for ATT Testing
011	3	36	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	International Calls for ATT Testing
1303538	11	11	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	Call To ATT Sonus Network
1303538	11	11	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.111.x	Call To ATT Sonus Network
1303538	11	11	<input type="checkbox"/>	avaya.com	AuraSBC	Call To ATT Sonus Network
1314346	11	11	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.111.x	Call to ATT NSN Network
1314346	11	11	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	Call to ATT NSN Network
1314346	11	11	<input type="checkbox"/>	avaya.com	AuraSBC	Call to ATT NSN Network
1732	11	11	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	Loopback Call to ATT and back to CM
1732	11	11	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.111.x	Loopback Call to ATT and back to CM
1800	11	11	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	Call to ATT Network
1800	11	11	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.111.x	Call to ATT Network
1800	11	11	<input type="checkbox"/>	avaya.com	AuraSBC	Call to ATT Network
1914222	11	11	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.111.x	Call to ATT TDM Network
1914222	11	11	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	Call to ATT TDM Network

Select : All, None < Previous Page 1 of 2 Next >

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

Pattern	Rank Order	Deny	Notes
---------	------------	------	-------

* Input Required [Commit] [Cancel]

Figure 36: Completed Routing Policy Details to AT&T (Section 4.10.1)

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 4, 2010 11:49 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

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

Help

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

Routing Policy Details
Commit Cancel

General

Name:
To ACM

Disabled:
☐

Notes:
Calls for ATT Network To ACM

SIP Entity as Destination

Select:

Name	FQDN or IP Address	Type	Notes
ATT-CLAN	10.80.111.31	CM	ATT CLAN

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Select : All, None

Dial Patterns

Add Remove

5 Items Refresh Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	314332	10	10	<input type="checkbox"/>	avaya.com	AuraSBC	Inbound Calls from NSN Network
<input type="checkbox"/>	4086	4	4	<input type="checkbox"/>	avaya.com	AuraSBC	
<input type="checkbox"/>	6665	7	7	<input type="checkbox"/>	avaya.com	Loc1 10.80.130.x	Endpoints on ES
<input type="checkbox"/>	6665	7	7	<input type="checkbox"/>	avaya.com	Location 1 Subnet 10.80.100.x	Endpoints on ES
<input type="checkbox"/>	7323	10	10	<input type="checkbox"/>	avaya.com	AuraSBC	Inbound Call from ATT

Select : All, None

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

	Pattern	Rank Order	Deny	Notes
--	---------	------------	------	-------

* Input Required

Commit Cancel

Figure 37: Completed Routing Policy Details to Communication Manager (Section 4.10.2)

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 4, 2010 11:49 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

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

Help

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

Routing Policy Details
Commit Cancel

General

Name:
ToMM5.2

Disabled:
☐

Notes:
Coverage to MM 5.2

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ModMess5.2	10.80.100.30	Other	Modular Messaging 5.2 SS MS

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Select : All, None

Dial Patterns

Add Remove

1 Item Refresh Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	6664999	7	7	<input type="checkbox"/>	avaya.com	-ALL-	to MM 5.2. Single Server

Select : All, None

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

	Pattern	Rank Order	Deny	Notes
--	---------	------------	------	-------

Input Required
Commit Cancel

Figure 38: Completed Routing Policy Details to Modular Messaging (Section 4.10.3)

AT:Reviewed
SPOC 2/18/2011

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

48 of 107
CMSMAASBC60IPFR

4.13. Session Manager Administration

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

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at August 4, 2010 11:49 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Session Manager / Session Manager Administration / New Session Manager

Elements

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

Add Session Manager Commit Cancel

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

General

*SIP Entity Name
Description
*Management Access Point Host Name/IP
*Direct Routing to Endpoints

Security Module

SIP Entity IP Address
*Network Mask
*Default Gateway
*Call Control PHB
*QOS Priority
*Speed & Duplex
VLAN ID

Figure 39: Add Session Manager Page

5. Avaya Aura™ Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. For any values not configured, defaults are used in this reference configuration. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [3] and [4] for further details if necessary.

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

5.1. System Parameters

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

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

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		8000	0
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		0	0
Maximum Concurrently Registered Remote Office Stations:		0	0
Maximum Concurrently Registered IP eCons:		0	0
Max Concur Registered Unauthenticated H.323 Stations:		0	0
Maximum Video Capable H.323 Stations:		0	0
Maximum Video Capable IP Softphones:		0	0
Maximum Administered SIP Trunks:		24000	85
Maximum Administered Ad-hoc Video Conferencing Ports:		0	0
Maximum Number of DS1 Boards with Echo Cancellation:		0	0
Maximum TN2501 VAL Boards:		10	1
Maximum Media Gateway VAL Sources:		0	0
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	2
Maximum Number of Expanded Meet-me Conference Ports:		0	0
(NOTE: You must logoff & login to effect the permission changes.)			

Figure 40: System Parameters Customer Options Form – Page 2

2. On **Page 3** of the **system-parameters customer-options** form, verify that the **ARS** feature is enabled.

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

Figure 41: System Parameters Customer Options Form – Page 3

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

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

Figure 42: System Parameters Customer Options Form – Page 4

4. On **Page 5** of the **system-parameters customer-options** form, verify that the **Private Networking** and **Processor Ethernet** fields are set to “y”.

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

Figure 43: System Parameters Customer Options Form – Page 5

5.2. Dial Plan and Feature Access Codes

This section briefly describes the dial plan requirements and feature access codes for the reference configuration described in these Application Notes.

1. Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings administered in figure below:
 - 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.
 - 7-digit extensions with a **Call Type** of “**ext**” beginning with the digits “**6665**”, e.g., Local extensions for Communication Manager stations, agents, and Vector Directory Numbers (VDNs) in this reference configuration conform to this format.
 - 1-digit facilities access code (indicated with a **Call Type** of “**fac**”), e.g., “**9**” access code for outbound ARS dialing and “**8**” for AAR local dialing.
 - 3-digit facilities access codes, e.g., codes starting with “*****” and “**#**” for Agent logon/logoff).

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	3	dac						
6665	7	ext						
3	5	ext						
8	1	fac						
9	1	fac						
*	3	fac						
#	3	fac						

Figure 44: Dialplan Analysis Form

2. Enter the **change feature-access-codes** command. On Page 1 of the **feature-access-codes** form, set **Auto Alternate Routing (AAR) Access Code** to “**8**” and **Auto Route Selection (ARS) – Access Code 1** to “**9**” that is valid under the administered dial plan in **Step 1**.

change feature-access-codes		Page	1 of	8
FEATURE ACCESS CODE (FAC)				
Abbreviated Dialing List1 Access Code:				
Abbreviated Dialing List2 Access Code:				
Abbreviated Dialing List3 Access Code:				
Abbreviated Dial - Prgm Group List Access Code:				
Announcement Access Code:				
Answer Back Access Code:				
Attendant Access Code:				
Auto Alternate Routing (AAR) Access Code: 8				
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:	
Automatic Callback Activation:			Deactivation:	

Figure 45: Feature-Access-Codes Form

5.3. IP Network Parameters

These Application Notes assume that the appropriate IP network regions and IP codec sets have already been administered to support internal calls, i.e., calls within the Avaya site. For simplicity in this reference configuration, all Communication Manager elements, e.g., stations, C-LAN and MedPro boards, etc., within the Avaya site are assigned to a single IP network region and all internal calls use a single IP codec set. This section describes the steps for administering additional IP network regions to represent the PSTN and the TDM gateway sites, and another IP codec set for external calls, i.e., calls between the Avaya site and the PSTN and the TDM gateway sites.

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

Note - The **Frames Per Pkt** and **Packet Size (ms)** values for **G.729B** and **G.729A** are set according to the requirements of the AT&T IP Flexible Reach service.

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

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

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

change ip-codec-set 2		Page 2 of 2	
IP Codec Set			
Allow Direct-IP Multimedia? n			
FAX	Mode	Redundancy	
	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

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

- Repeat this step as necessary for each IP codec set used only for internal calls.

2. Enter the **change ip-codec-set *ce*** command, where *ce* is the number of an unused IP codec set. This IP codec set will be used for external calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown in figure below.

Note - The **Frames Per Pkt** and **Packet Size (ms)** values for **G.729B** and **G.729A** are set according to the requirements of the AT&T IP Flexible Reach service.

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

Figure 48: IP-Codec-Set Form for External Calls – Page 1

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

change ip-codec-set 3		Page 2 of 2	
IP Codec Set			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	
FAX	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

Figure 49: IP-Codec-Set Form for External Calls – Page 2

- Enter the **change ip-network-region nrl**, where **nrl** is the number of an unused IP network region for local Communication Manager Elements within the Avaya site. On **Page 1** of the **ip-network-region** form, set the **UDP Port Min** and **UDP Port Max** to “**16384**” and “**32767**” (this port range is an AT&T IP Flexible Reach service requirement).

change ip-network-region 2		Page 1 of 19
IP NETWORK REGION		
Region: 2		
Location:	Authoritative Domain: avaya.com	
Name: Local		
MEDIA PARAMETERS		
Codec Set: 2	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 16384	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 32767	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46	RTCP Reporting Enabled? y	
Audio PHB Value: 46	RTCP MONITOR SERVER PARAMETERS	
Video PHB Value: 26	Use Default Server Parameters? y	
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS		
H.323 Link Bounce Recovery? y	RSVP Enabled? n	
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Figure 50: IP-Network-Region Form for the Network Region Representing the Local Communication Manager Elements

- On **Page 4** of the **ip-network-region** form, enter codec set “**3**” for dst rgn **3** so that source network region **2** can talk to destination network region **3** using codec set **3**. The settings shown in figure below were used in this reference configuration.

change ip-network-region 2		Page 4 of 20
Source Region: 2	Inter Network Region Connection Management	
	I	M
	G	A
dst codec direct	WAN-BW-limits	Video
rgn set	WAN Units	Intervening
	Total Norm	Prio Shr Regions
		CAC
2	2	
3	3	
y	NoLimit	
		all
		n

Figure 51: IP-Network-Region Form for an IP Network Region Administered for Local Communication Manager Elements – Page 4

4. Enter the **change ip-network-region nrp**, where **nrp** is the number of an IP network region administered for the ATT calls. On **Page 1** of the **ip-network-region** form, set the **UDP Port Min** and **UDP Port Max** to “**16384**” and “**32767**” (this port range is an AT&T IP Flexible Reach service requirement)

change ip-network-region 3		Page 1 of 19
IP NETWORK REGION		
Region: 3		
Location: Authoritative Domain: avaya.com		
Name: ATT PSTN		
MEDIA PARAMETERS		
Codec Set: 3	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 16384	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 32767	IP Audio Hairpinning? y	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Figure 52: IP-Network-Region Form for a Network Region Administered for ATT – Page 1

- On **Page 4** of the **ip-network-region** form, enter codec set “**3**” for dst rgn **2** so that source network region **3** can talk to destination network region **2** using codec set **3**. The settings shown in figure below were used in this reference configuration.

change ip-network-region 3		Page 4 of 20	
Source Region: 3		Inter Network Region Connection Management	
dst codec direct		I	M
WAN-BW-limits		G	A
Video		Dyn	A
Intervening		CAC	R
Regions		n	all
rqn	set	WAN	Units
2	3	y	NoLimit
3	3		

Figure 53: IP-Network-Region Form for an IP Network Region Administered for ATT – Page 4

- Enter the **list node-names** command, and note the node names and IP addresses of the Session Manager server used in **Section 5.6.1** and **Section 5.6.2** as well as of the C-LAN board used in **Section 5.6.1** and **Section 5.6.2**.

list node-names		
NODE NAMES		
Type	Name	IP Address
IP	CLAN-1A03	10.80.111.31
IP	Gateway	10.80.111.1
IP	MEDPRO-1A11	10.80.111.32
IP	ASM1	10.80.120.28
IP	procr	10.80.111.73
IP	default	0.0.0.0

Figure 54: List Node-Names Form

5.4. Automatic Route Selection (ARS) Table

The ARS table is selected based on the caller dialing the ARS access code (e.g. “9”) as defined in **Section 5.2**. The access code is removed and the ARS table is used to associate calls that match the remaining dialed digits to the designated route-pattern. Configure as follows:

- Dialed String** – Set to **1303** for outbound calls.
- Min** and **Max** – Set to **11**, the minimum and maximum size the dialed string will assume.
- Route Pattern** – Set to **20** as configured in **Section 5.7**.
- Call Type** – Set to **natl**.
- Repeat above steps for other dialed strings to be configured.

In figure below, entries are shown for outbound calls to **1-303-xxx-xxxx**, and **1-800-xxx-xxxx**. Typical deployments generally require additional entries, or the use of less exact or wildcard matching strings, to cover all permitted local, long distance, international, operator, N11 service, and other PSTN destination numbers, but that is beyond the scope of these Application Notes. Ensure that there are entries to cover all permitted PSTN destination numbers. Refer to [3] and [4] for further information on ARS administration.

list ars analysis							Page	1 of	2
ARS DIGIT ANALYSIS TABLE							Percent Full: 1		
Location: all									
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd			
1303	11	11	20	natl		n			
1800	11	11	20	natl		n			
011	10	18	20	natl		n			

Figure 55: ARS Analysis Form

5.5. Alternate Automated Routing (AAR) Table

The AAR table is selected based on the caller dialing the AAR access code (e.g. “8”) as defined in **Section 5.2**. The access code is removed and the AAR table matches the remaining dialed digits and sends the matched call to the designated route pattern (see **Section 5.7**). Configure as follows:

- **Dialed String** – Set to “6665” for calls to SIP endpoints registered with Session Manager.
- **Min** and **Max** - Set to 7, the minimum and maximum size the dialed string will assume.
- **Route Pattern** – Set to 21 as configured in **Section 5.7**.
- **Call Type** – Set to **aar**.
- Repeat the above steps for calls to Modular Messaging pilot number “6664999”.

change aar analysis 0						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 1			
Dialed		Total		Route	Call	Node	ANI
String		Min	Max	Pattern	Type	Num	Reqd
6665		7	7	21	aar		n
6664999		7	7	21	unku		n

Figure 56: AAR Analysis Form

5.6. SIP Trunks

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

- Inbound/Outbound for AT&T access – SIP Trunk 1
- Local for Modular Messaging and Avaya SIP telephone access – SIP Trunk 2

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

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

5.6.1. SIP Trunk for AT&T Access

This section describes the steps for administering the SIP trunk connecting to Session Manager used for AT&T access. This trunk corresponds to the **SM1** Entity defined in **Section 4.6.1**.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. 20), 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 Session Border Controller and the AT&T IP Flexible Reach service is UDP.
- Verify that **Peer Detection Enabled** is “**y**” and that **Peer Server** is **SM**.
- **Near-end Node Name** – Set to the node name of the C-LAN i.e. **CLAN-1A03** noted in **Section 5.3, Step 5**.
- **Far-end Node Name** – Set to the node name of Session Manager i.e. **ASM1** noted in **Section 5.3, Step 5**.
- **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 **3**, as defined in **Section 5.3, Step 4**.
- **Far-end Domain** – Enter “**avaya.com**”. This is the domain inserted by Session Manager in **Section 4.5.2**.
- **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 Communication Manager audio resources when possible.
- **Enable Layer 3 Test** – Set to “**y**”. This allows Communication Manager to send SIP OPTIONS “pings” to Session Manager to monitor link status.

add signaling-group 20		Page 1 of 1
SIGNALING GROUP		
Group Number: 20	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: CLAN-1A03	Far-end Node Name: ASM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 3	
Far-end Domain: avaya.com	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Figure 57: Signaling-Group Form for AT&T IP Flexible Reach Calls

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. **20**). On **Page 1** of the **trunk-group** form, provision the following:
 - **Group Type** – Set to “**sip**”.
 - **Group Name** – Enter any descriptive name.
 - **TAC** – Enter a trunk access code that is consistent with the dial plan.
 - **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 .
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g. **20**).

add trunk-group 20		Page 1 of 21	
TRUNK GROUP			
Group Number: 20	Group Type: sip	CDR Reports: y	
Group Name: ATT Testing	COR: 1	TN: 1	TAC: 120
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? N		
	Member Assignment Method: auto		
	Signaling Group: 20		
	Number of Members: 20		

Figure 58: Trunk-Group Form for AT&T IP Flexible Reach Calls – Page 1

3. On **Page 2** of the **trunk-group** form, set the **Preferred Minimum Session Refresh Interval(sec)** field to “**900**”. This entry will actually cause a value of 1800 to be generated in the SIP header which is the value required by AT&T IP Flexible Reach service.

add trunk-group 20		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
SCCAN? n	Redirect On OPTIM Failure: 5000		
	Digital Loss Group: 18		
	Preferred Minimum Session Refresh Interval(sec): 900		
	Delay Call Setup When Accessed Via IGAR? n		

Figure 59: Trunk Group Form for AT&T IP Flexible Reach Calls – Page 2

4. On **Page 3** of the **trunk-group** form, set **Numbering Format** field to **private**

add trunk-group 20		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private		UI Treatment: service-provider	
		Replace Restricted Numbers? y	
		Replace Unavailable Numbers? y	
	Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y			

Figure 60: Trunk-Group Form for AT&T IP Flexible Reach Calls – Page 3

5. On **Page 4** of the **Trunk Group** form set **Send Diversion Header** to “y” (see note in **Section 2.2.3**) and set **Telephone Event Payload Type** to the RTP payload type required by the AT&T IP Flexible Reach service (e.g. **100**). Contact AT&T or examine a SIP trace of an inbound call from the AT&T IP Flexible Reach service to determine this value.

Note – The AT&T IP Flexible Reach service does not support History Info headers, however Communication Manager enables History Info Headers by default (*Support Request History?* y). Although these headers could be disabled by changing this setting to “n”, in the reference configuration this default value is used and Session Manager is configured to remove any History Info Headers sent by Communication Manager (see **Section 4.5**).

add trunk-group 20	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? y Support Request History? y Telephone Event Payload Type: 100 Convert 180 to 183 for Early Media? y Always Use re-INVITE for Display Updates? n Enable Q-SIP? n	

Figure 61: Trunk Group Form for AT&T IP Flexible Reach Calls – Page 4

5.6.2. Local SIP Trunk (Modular Messaging and SIP Telephones)

This section describes the steps for administering the local SIP trunk for Avaya Modular Messaging and SIP Telephone traffic.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **21**), and follow the same procedures described in **Section 5.6.1, Step 1**, except:
 - **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 5.3**.
 - **Near-end Listen Port** and **Far-end Listen Port** – set to “**5080**” (see **Section 4.6.1, Step 5** for using a different port number).
 - **Direct IP-IP Audio Connections** – Set to “n”. In an AT&T Flexible Reach environment, shuffling needs to be disabled for Avaya SIP telephones as noted in **Section 1.3, Item 6**.
 - **Enable Layer 3 Test** – Set to “n”.

add signaling-group 21		Page 1 of 1
SIGNALING GROUP		
Group Number: 21	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: CLAN-1A03	Far-end Node Name: ASM1	
Near-end Listen Port: 5080	Far-end Listen Port: 5080	
	Far-end Network Region: 2	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? n	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
	Alternate Route Timer(sec): 6	

Figure 62: Signaling Group Form for Local Calls

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group. On **Page 1** of the **trunk-group** form, provision the following:
 - **Group Type** – Set to “sip”.
 - **Group Name** – Enter any descriptive name.
 - **TAC** – Enter a trunk access code that is consistent with the dial plan.
 - **Direction** – Set to “two-way”.
 - **Service Type** – Set to “tie”.
 - **Signaling Group** – Set to the number of the signaling group administered in **Step 1**.
 - **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group.

change trunk-group 21		Page 1 of 21
TRUNK GROUP		
Group Number: 2	Group Type: sip	CDR Reports: y
Group Name: MM_and_SIP_Phones	COR: 1	TN: 1 TAC: 121
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 21	
	Number of Members: 20	

Figure 63: Trunk Group Form for Local Calls – Page 1

3. Repeat **Section 5.6.1, Steps 3 and 4** for pages 2 and 3 of the form.

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

Figure 64: Trunk Group Form for Local Calls – Page 2

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

Figure 65: Trunk Group Form for Local Calls – Page 3

4. On **Page 4** of the **trunk-group** form set **Send Diversion Header** to “n” and 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		
Convert 180 to 183 for Early Media? y		
Always Use re-INVITE for Display Updates? n		
Enable Q-SIP? n		

Figure 66: Trunk Group Form for Local Calls – Page 4

5.7. Route Pattern for Outbound Calls

5.7.1. Calls to AT&T

This form defines the SIP trunk to be used based on the route-pattern selected by the ARS table for outbound calls (see **Sections 5.4 and 5.6.1**). Configure as follows:

- **Grp No** – Set to **20** i.e. the trunk group configured for AT&T Access.
- **FRL** – Set to **0** (zero).
- **Pfx Mrk** – Set to **1**

- **LAR** - Enter **next** in the row corresponding to **1:**.

change route-pattern 20															Page 1 of 3	
Pattern Number: 1 Pattern Name: To_AT&T																
SCCAN? n Secure SIP? n																
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/	IXC
No			Mrk	Lmt	List	Del	Digits								QSIG	
															Intw	
1:	20	0	1												n	user
2:															n	user
3:															n	user
4:															n	user
5:															n	user
6:															n	user
		BCC VALUE		TSC	CA-TSC			ITC	BCIE	Service/Feature		PARM	No.	Numbering	LAR	
		0	1	2	M	4	W			Request				Dgts	Format	
														Subaddress		
1:	y	y	y	y	y	n	n			rest					next	
2:	y	y	y	y	y	n	n			rest					none	
3:	y	y	y	y	y	n	n			rest					none	
4:	y	y	y	y	y	n	n			rest					none	
5:	y	y	y	y	y	n	n			rest					none	
6:	y	y	y	y	y	n	n			rest					none	

Figure 67: Route Pattern Form for AT&T IP Flexible Reach Calls

5.7.2. Local Calls

This form defines the SIP trunk to be used based on the route-pattern selected by the AAR table for outbound calls (see **Sections 5.5** and **5.6.2**).

- **Grp No** – Set to **21** i.e. the trunk group configured for Local Access.
- **FRL** – Set to **0** (zero).
- **Pfx Mrk** – Set to **1**

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

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

Figure 68: Route Pattern Form for Local Calls

5.8. Private Numbering

For AT&T Flexible Reach service call admission control purposes, calling number origination SIP header contents (e.g. From, Contact, and PAI) are converted to public numbers (previously identified by AT&T) from Communication Manager local extensions. Enter **change private - numbering 0** command, and configure as follows:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. 7).
- **Ext Code** – Enter the leading digits of Communication Manager extensions (e.g. 6665).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g. 20).
- **Private Prefix** – Enter the corresponding AT&T DID (e.g 732) used for the specified extensions (e.g. 6665xxx).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g. 10).

In the example below any 7 digit extension starting with **6665** calls out to Session Manager for delivery to AT&T using trunk group **20** with “**732**” pre-pended to the 7 digit extension. The CPN delivered for call made from 6665011 to PSTN will be 7326665011.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp (s)	Prefix	Len		
7	6665	20	732	10	Total Administered: 4	
					Maximum Entries: 540	

Figure 69: Private-Numbering Form

5.9. Public Unknown Numbering

Communication Manager Diversion Header processing (see **Section 2.2.3**) uses the contents of the public-unknown-numbering form to populate the calling party number field. Therefore any extension to AT&T DID conversions specified in the private-numbering form should be specified in the public-unknown-numbering table as well. Enter **change public-unknown-numbering 0** command, and configure as follows:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. 7).
- **Ext Code** – Enter the Communication Manager extension (e.g. 6665011).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g. 20).
- **CPN Prefix** – Enter the corresponding AT&T DID (e.g. 7323204084) used for the specified extension (e.g. 6665011).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g. 10).
- Repeat above steps to configure additional extensions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
7	6665011	20	7323204084	10	Total Administered: 3
7	6665013	20	7323204085	10	Maximum Entries: 9999
7	6665401	20	7323204086	10	

Figure 70: Public Numbering Form

5.10. Optional Features

The reference configuration uses hunt groups, vectors, and Vector Directory Numbers (VDNs), to provide additional functionality during testing:

- Hunt Group 1 – Modular Messaging coverage for Communication Manager extensions.
- VDN 6665301/Vector 31 – Auto-attendant.
- VDN 6665300/Vector 30 – Meet-me Conference

Note - The administration of Communication Manager Call Center elements – hunt groups, vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Additional licensing may be required for some of these features. Consult[3], [4], [5], and [6] for further details if necessary. The samples that follow are provided for reference purposes only.

5.10.1. Modular Messaging Coverage Path and Hunt Group

Hunt group 1 is used in the reference configuration to verify Modular Messaging coverage functionality. The hunt group (e.g. 1) is defined with the 7 digit Modular Messaging pilot number (e.g. 6664999). The hunt group is associated with a coverage path (e.g. h1) and the coverage path is assigned to a station (e.g. 6665011 in **Figure 74**). Communication Manager will use the AAR access code “8” (defined in **Section 5.5**) to dial Modular Messaging (e.g. 86664999) as shown in **Figure 73**.

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

Figure 71: Coverage Path 1 Form

display hunt-group 1		Page 1 of 60
HUNT GROUP		
Group Number: 1	ACD? n	
Group Name: MM	Queue? n	
Group Extension: 6664999	Vector? n	
Group Type: ucd-mia	Coverage Path:	
TN: 1	Night Service Destination:	
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display: mbr-name		

Figure 72: Hunt Group 1Form – Page 1

display hunt-group 1		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
6664999	6664999	8

Figure 73: Hunt Group 1 Form – Page 2

display station 6665011		Page 1 of 5
STATION		
Extension: 6665011	Lock Messages? n	BCC: 0
Type: 9620	Security Code: 123456	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: H323-96XX-5011	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 6665011	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Figure 74: Station Form

5.10.2. Auto Attendant

A basic auto-attendant functionality is defined in the reference configuration for DTMF testing. The auto-attendant is defined by a VDN (e.g. **6665301**) and a Vector (e.g. **31**)..

display vdn 6665301		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 666-5301		
Name*: Auto-Attendant		
Destination: Vector Number	31	
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		
VDN of Origin Annc. Extension*:		
1st Skill*:		

Figure 75: Auto Attendant VDN

display vector 31		Page 1 of 6
CALL VECTOR		
Number: 24	Name: Auto-Attendant	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
		BSR? y
		Holidays? y
01 wait-time	4 secs hearing ringback	
02 collect	5 digits after announcement	33017 for none
03 route-to	digits with coverage n	
04 wait-time	5 secs hearing silence	

Figure 76: Auto Attendant Vector

5.10.3. Meet-me Conference

A basic meet-me conference functionality is defined in the reference configuration for DTMF testing. The meet-me conference is defined by a VDN (e.g. **6665300**) and a Vector (e.g. **30**).

display vdn 6665300	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 666-5300	
Name: MeetMeConf	
Destination: Vector Number	30
Meet-me Conferencing? y	
COR: 1	
TN: 1	

Figure 77: Meet-me Conference VDN – Page 1

display vdn 6665300	Page 2 of 3
VECTOR DIRECTORY NUMBER	
MEET-ME CONFERENCE PARAMETERS:	
Conference Access Code: 123456	
Conference Controller: 6665011	
Conference Type: 6-party	

Figure 78: Meet-me Conference VDN – Page 2

display vector 30	Page 1 of 6
CALL VECTOR	
Number: 6 Name: MeetMeConf	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? y Lock? y
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 wait-time	2 secs hearing ringback
02 collect	6 digits after announcement 33011 for none
03 goto step	5 if digits = meet-me-access
04 goto step	2 if unconditionally
05 announcement	33014
06 route-to	meetme
07 stop	

Figure 79: Meet-me Conference Vector

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 which allows Avaya Modular Messaging subscribers to be in multiple locations. The administration for Modular Messaging is beyond the scope of these Application Notes. Consult [7 - 11] for further details.

7. Avaya Aura™ Session Border Controller

This section illustrates an example of installation and configuration of the Session Border Controller. Similar to Communication Manager Release 6.0, the Session Border Controller runs on its own S8800 Server as an application template using Avaya Aura™ System Platform. The installation of the System Platform is assumed to have been previously completed.

The Session Border Controller includes a configuration wizard that can be used as part of the installation of the Session Border Controller template on System Platform. As such, screens from the installation of the SBC template are presented in **Section 7.1**. The wizard pre-configures the underlying Session Border Controller for much of the required provisioning. After the installation wizard is completed, subsequent configuration can be performed through the GUI as shown in **Section 7.2**.

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. The port labeled “4” (virtual “eth2”) is used for the public (outside) network interface of the SBC.

Note: If using an Acme Packet Net-Net OS-E / Net-Net 2600 rather than an Avaya Aura™ Session Border Controller (SBC), the configuration can be obtained from the following Acme Packet website: <https://support.acmepacket.com>. Please note that an Acme Packet ID and Password are required.

7.1. Avaya Aura™ SBC Installation

To begin the SBC Template installation, 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 **10.80.130.11**, and the system domain uses the IP Address **10.80.130.10**. Enter an appropriate **User Id** and click **Continue**.



Figure 80: System Platform - Console Domain Login Screen

On the subsequent screen [not shown], enter the appropriate **Password** and click the **Log On** button.

Select **Virtual Machine Management** → **Solution Template**. In the **Install Template From** area, choose where the template files are located. In the sample configuration, the template was copied to the USB drive. Click **Search**.

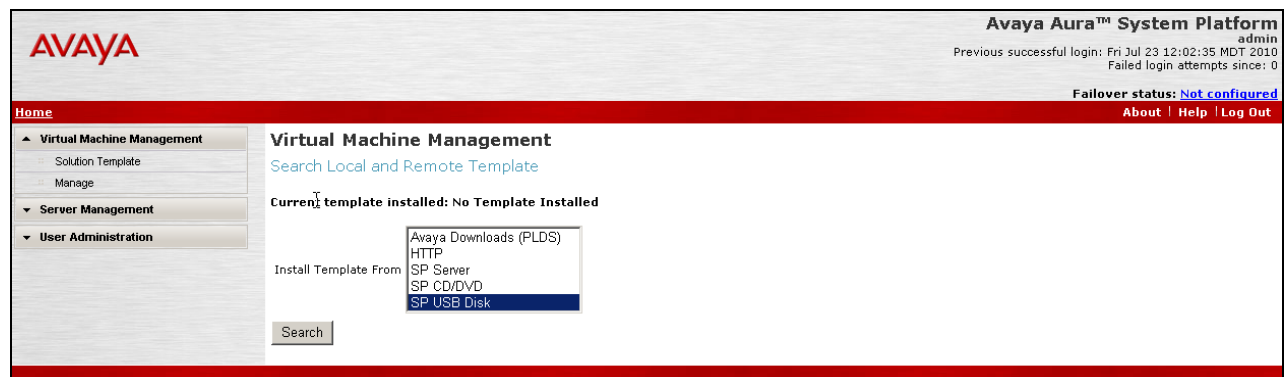


Figure 81: SBC Installation - Template Search screen

Select the appropriate file, such as “SBCT.ovf”. Click the **Select** button.

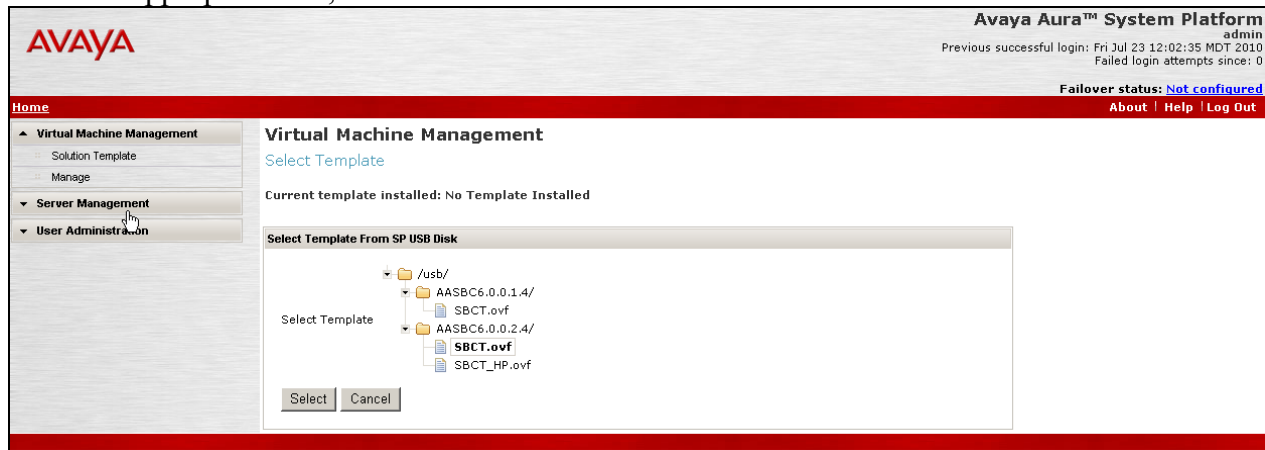


Figure 82: SBC Installation - Template Selection screen

In the resultant screen shown below, the **Selected Template** can be observed. If an EPW file is available, it may be uploaded and used. In the sample configuration, the **Continue without EPW file** button was used.

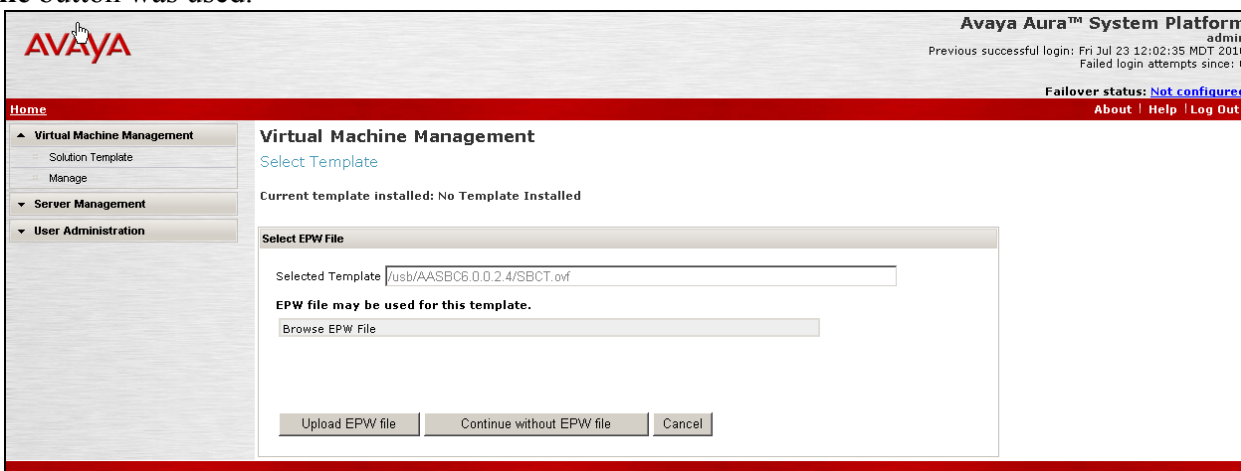


Figure 83: SBC Installation - EPW screen

The **Template Details** screen is presented. If satisfied that the information is correct, click the **Install** button.

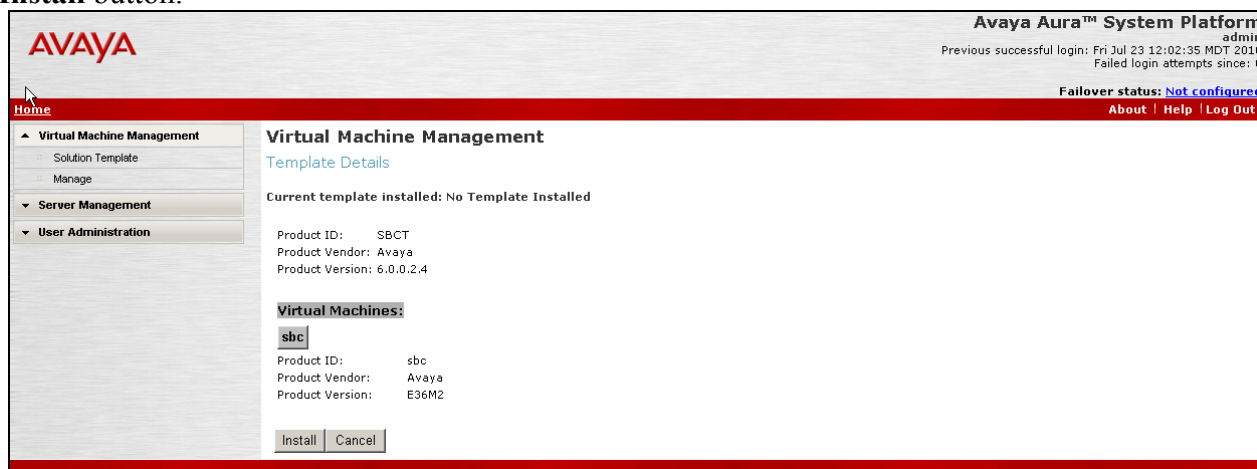


Figure 84: SBC Installation Template - Details screen

The installation will proceed until user input is expected, as shown below. The following shows the first screen in a series, beginning with **Network Settings**. The SystemDomain Domain-0 IP Address, Console Domain CDom IP Address, Gateway IP Address, a Network Mask and Primary DNS and Secondary DNS (if configured) are pre-populated. This information was supplied during the System Platform installation. Enter the **IP Address** to be assigned to the SBC (e.g. **10.80.130.12**) and **Hostname** and click on **Next Step**. This IP Address becomes the private, inside IP Address as well as the management address for the Session Border Controller.

AVAYA

Home

Configuration

Installation

Network Settings

VPN Access

SBC

Summary

Finish

Network Settings

Enter network settings

Domain-0 IP Address: 10.80.130.10

CDom IP Address: 10.80.130.11

Gateway IP Address: 10.80.130.1

Network Mask: 255.255.255.0

Primary DNS: 135.9.1.2

Secondary DNS:

HTTPS Proxy (if required) [IP Address:Port Number]:

Virtual Machine	IP Address	Hostname	Domain
SBC	10.80.130.12	AvayaSBC	

[Next Step](#)

Figure 85: SBC Installation - Network Settings screen

The resulting screen [not shown] allows VPN Access parameters to be configured. Configure as appropriate, or skip, and click **Next Step**. In this reference configuration, this step was skipped.

The following screen shows the Session Border Controller Data entry screen. Note that the Private (Management) Interface information has already been completed with the IP Address (10.80.130.12) provided as the **Virtual Machine IP Address** on the first screen of the series.

Configure the **SIP Service Provider Data** section as follows:

- **Service Provider** – Set to **AT&T**
- **IP Address** – Set to the AT&T Border Element IP Address (e.g. **135.242.225.210**)
- **Port** – Port number for the SIP Signaling port
- **Media Network** – Set to the AT&T Media Network
- **Media Netmask** – Set to the AT&T Media Netmask

Configure the **SBC Network Data** (Public section) as follows:

- **IP Address** – IP Address of the public interface of the Session Border Controller
- **NetMask** – Netmask for the public IP interface of the Session Border Controller
- **Gateway** – IP Address of the Gateway for the public side of the Session Border Controller

Configure the **Enterprise SIP Server** section as follows:

- **IP Address** – Set to IP Address of the Session Manager network Interface configured in Section 4.6.1.
- **Transport** – Set to **TCP** in Reference Configuration; **TLS** may be used in production environment.
- **SIP Domain** – Set to **avaya.com**
- Click **Next Step**

AVAYA

Home

Configuration

Installation

- Network Settings
- VPN Access
- SBC
- Summary
- Finish

SBC

Session Border Controller Data

SIP Service Provider Data

Service Provider	IP Address	Port	Media Network	Media Netmask
AT&T	135.242.225.210	5060	135.242.225.0	255.255.255.0

SBC Network Data

Interface	IP Address	Net Mask	Gateway
Private (Management)	10.80.130.12	255.255.255.0	10.80.130.1
Public	192.168.62.55	255.255.255.0	192.168.62.1

Enterprise SIP Server

IP Address	Transport	SIP Domain
10.80.120.28	TCP	avaya.com

Previous Step Next Step

Figure 86: SBC Installation - Session Border Controller Data

A summary screen will be presented. The sample configuration is shown in the lower portion of the summary screen.

AVAYA

Home

Configuration

Installation

- Network Settings
- VPN Access
- SBC
- Summary
- Finish

Summary

Network Settings	
Domain-0 Address	10.80.130.10
CDom Address	10.80.130.11
Gateway Address	10.80.130.1
Network Mask	255.255.255.0
Primary DNS	135.9.1.2
Secondary DNS	Not set
HTTPS Proxy	Not set

Virtual Machine	IP Address	Hostname
SBC	10.80.130.12	AvayaSBC

VPN Access	
VPN Access	Not Configured

SBC	
Service Provider	att
Service Provider IP Address	135.242.225.210
Service Provider Port	5060
Service Provider Media Network	135.242.225.0
Service Provider Media Netmask	255.255.255.0
Public IP Address	192.168.62.55
Public Netmask	255.255.255.0
Public Gateway	192.168.62.1
Enterprise SIP Server IP	10.80.120.28
Enterprise SIP Server Domain	avaya.com
Enterprise SIP Server Transport	TCP

[Previous Step](#) [Next Step](#)

Figure 87: SBC Installation - Summary

Click **Next Step** and a **Confirm Installation** [not shown] screen is presented. After reading and heeding the Warning, click the **Accept** button if satisfied. Click **Install** button to proceed at the screen shown below.

AVAYA

Home

Configuration

Installation

Network Settings

VPN Access

SBC

Summary

Finish

Confirm Installation

The following optional fields have not been set

[Secondary DNS](#)

[HTTPS Proxy](#)

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook*, 555-025-600.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

[Previous Step](#)

Figure 88: SBC Installation - Confirm Installation

The Virtual Machine Management window, which had previously been at the “Wait for User to Complete Data Entry” step, is now proceeding with other aspects of the installation, as shown below.

AVAYA

Avaya Aura™ System Platform

admin

Previous successful login: Fri Jul 23 12:02:35 MDT 2010

Failed login attempts since: 0

Template Installation in progress

Log Out

Virtual Machine Management

Server Management

User Administration

Virtual Machine Management

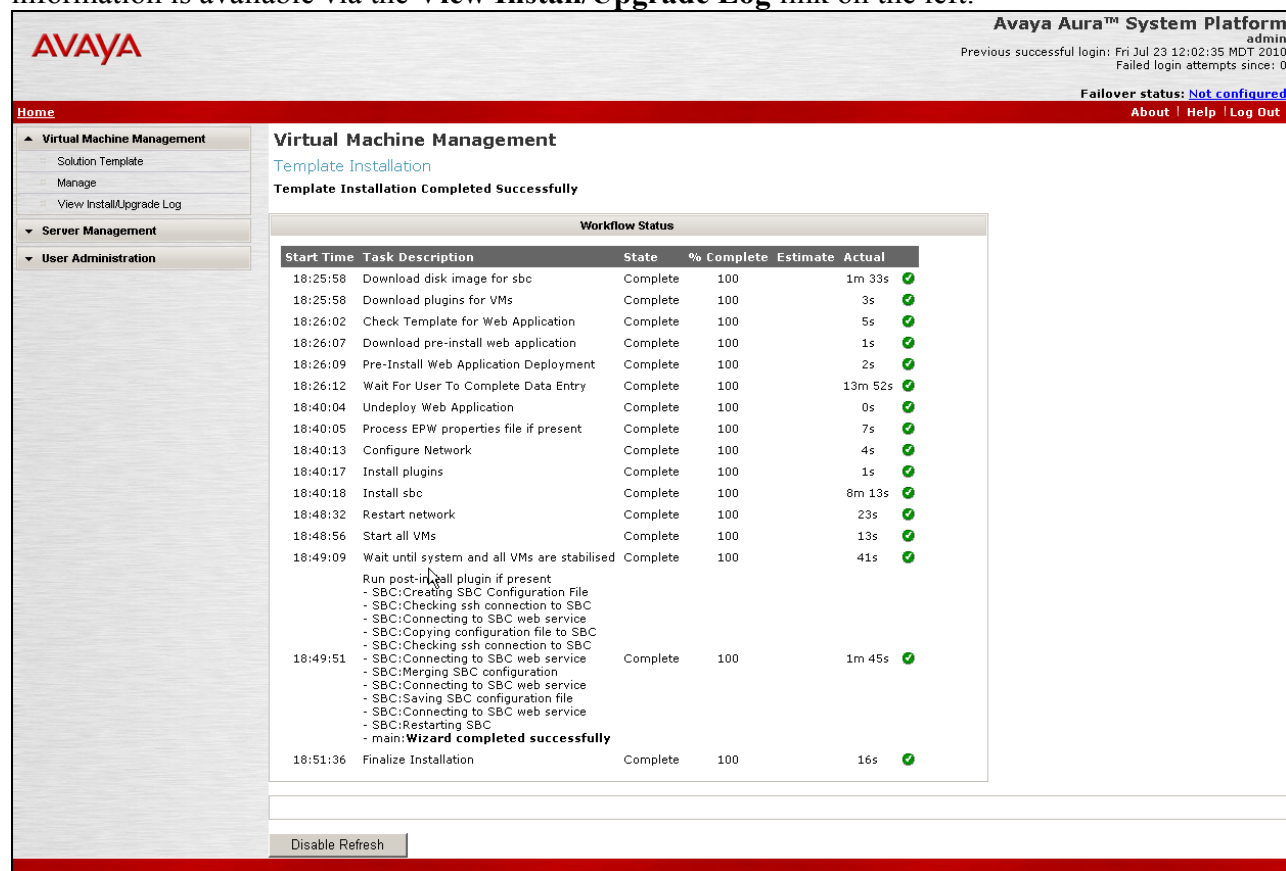
Template Installation

Template Installation In Progress

Start Time	Task Description	State	% Complete	Estimate	Actual
18:25:58	Download disk image for sbc	Complete	100	1m 33s	✓
18:25:58	Download plugins for VMs	Complete	100	3s	✓
18:26:02	Check Template for Web Application	Complete	100	5s	✓
18:26:07	Download pre-install web application	Complete	100	1s	✓
18:26:09	Pre-Install Web Application Deployment	Complete	100	2s	✓
18:26:12	Wait For User To Complete Data Entry	Complete	100	13m 52s	✓
18:40:04	Undeploy Web Application	Complete	100	0s	✓
18:40:05	Process EPW properties file if present	Complete	100	7s	✓
18:40:13	Configure Network	Complete	100	4s	✓
18:40:17	Install plugins	Complete	100	1s	✓
18:40:18	Install sbc	Complete	100	8m 13s	✓
18:48:32	Restart network	Complete	100	23s	✓
18:48:56	Start all VMs	Complete	100	13s	✓
18:49:09	Wait until system and all VMs are stabilised	Complete	100	41s	✓

Figure 89: SBC Installation - Template Installation Progress

Wait for the “Finalize Installation” task to reach the Complete State, as shown below. This same information is available via the **View Install/Upgrade Log** link on the left.



Avaya Aura™ System Platform
admin
Previous successful login: Fri Jul 23 12:02:35 MDT 2010
Failed login attempts since: 0
Failover status: **Not configured**
About | Help | Log Out

Home

Virtual Machine Management

Solution Template
Manage
View Install/Upgrade Log

Server Management

User Administration

Virtual Machine Management

Template Installation

Template Installation Completed Successfully

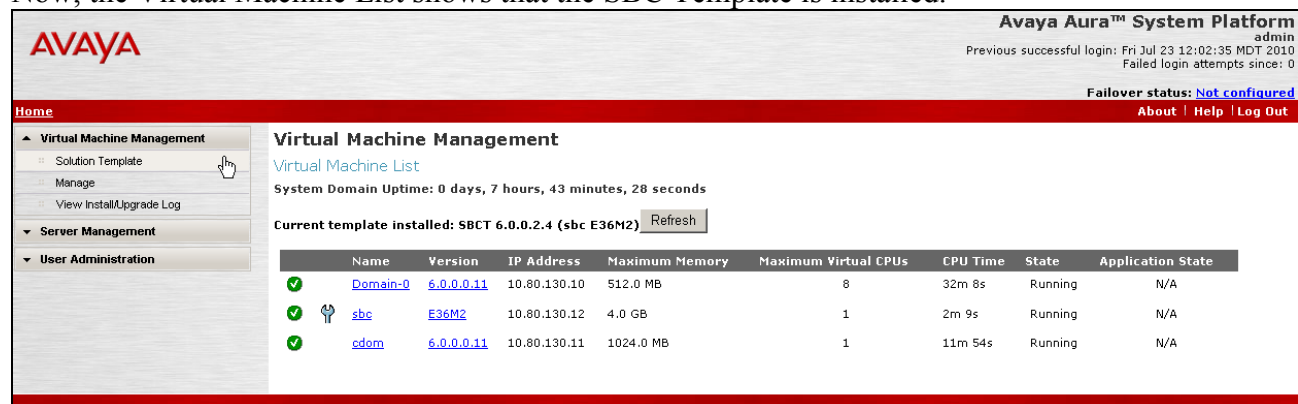
Workflow Status

Start Time	Task Description	State	% Complete	Estimate	Actual
18:25:58	Download disk image for sbc	Complete	100	1m 33s	✓
18:25:58	Download plugins for VMs	Complete	100	3s	✓
18:26:02	Check Template for Web Application	Complete	100	5s	✓
18:26:07	Download pre-install web application	Complete	100	1s	✓
18:26:09	Pre-Install Web Application Deployment	Complete	100	2s	✓
18:26:12	Wait For User To Complete Data Entry	Complete	100	13m 52s	✓
18:40:04	Undeploy Web Application	Complete	100	0s	✓
18:40:05	Process EPW properties file if present	Complete	100	7s	✓
18:40:13	Configure Network	Complete	100	4s	✓
18:40:17	Install plugins	Complete	100	1s	✓
18:40:18	Install sbc	Complete	100	8m 13s	✓
18:48:32	Restart network	Complete	100	23s	✓
18:48:56	Start all VMs	Complete	100	13s	✓
18:49:09	Wait until system and all VMs are stabilised	Complete	100	41s	✓
18:49:51	Run post-install plugin if present - SBC:Creating SBC Configuration File - SBC:Checking ssh connection to SBC - SBC:Connecting to SBC web service - SBC:Copying configuration file to SBC - SBC:Checking ssh connection to SBC - SBC:Connecting to SBC web service - SBC:Merging SBC configuration - SBC:Connecting to SBC web service - SBC:Saving SBC configuration file - SBC:Connecting to SBC web service - SBC:Restarting SBC	Complete	100	1m 45s	✓
18:51:36	Finalize Installation	Complete	100	16s	✓

Disable Refresh

Figure 90: SBC Installation - Template Installation Completed

Once the SBC template install has completed, select **Virtual Machine Management** on the left. Now, the Virtual Machine List shows that the SBC Template is installed.



Avaya Aura™ System Platform
admin
Previous successful login: Fri Jul 23 12:02:35 MDT 2010
Failed login attempts since: 0
Failover status: **Not configured**
About | Help | Log Out

Home

Virtual Machine Management

Solution Template
Manage
View Install/Upgrade Log

Server Management

User Administration

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 0 days, 7 hours, 43 minutes, 28 seconds

Current template installed: SBCT 6.0.0.2.4 (sbc E36M2) Refresh


	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	10.80.130.10	512.0 MB	8	32m 8s	Running	N/A
✓	sbc	E36M2	10.80.130.12	4.0 GB	1	2m 9s	Running	N/A
✓	cdom	6.0.0.0.11	10.80.130.11	1024.0 MB	1	11m 54s	Running	N/A

Figure 91: System Platform - Virtual Management Screen with SBC installed

7.2. Avaya Aura™ Session Border Controller Configuration

After the installation wizard is completed, and proper template (i.e. AT&T) is selected, there would be no need to do any further configuration in future releases. However, in the current release of the Session Border Controller, some additional configuration needs to be performed through the GUI on the SBC. The configuration screens will be familiar to the reader experienced with the Acme Packet Net-Net OS-E.

7.2.1. Login and License Installation

To log in, either select the wrench  [sbc](#) icon shown in the prior screen, or enter the `https://<ip-addr>` where <ip-addr> is the management IP Address of the SBC. Enter appropriate **Username** and **Password** and click **Login**.

Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

Username:

Password:

Login

Figure 92: SBC Configuration Login Screen

Following **Home** screen appears. Note the box-identifier field. This is required for obtaining the license. **Please acquire licenses prior to proceeding with other configuration steps.**

AVAYA
aura

acme packet
powered

Logout admin

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Get summary for: Box 1 Refresh Help

box-identifier

0126-5384-c725-6213

box-status

IPAddress

LocalBox (10.80.130.12)

State

Connected 

build-version

3.6.0

build-number

46572

master-services

accounting, database

up-time

time

18:57:45 Mon 2010-08-02

timezone

MDT

uptime

0 days 00:06:07

system-info

cpu-usage-one-second

0%

call-info

active-calls

location-info

total-cache-entries

location-bindings

registration-info

total-nonlocal-registrations

total-terminated

total-declined

Figure 93: SBC Configuration Home screen

- Click on the **Tools** tab and select **Upload license file** from the left pane.
- Select the location on your local desktop where the license file is located.
- Check the **Apply License** box.
- Click **Upload**.
- If the license install is successful, a message is displayed.
- Click on the **Configuration** tab.
- On the Configuration screen [not shown], click on **Configuration** in the left pane and select **Update and save configuration**.
- Click on the **Actions** tab and select **restart** from the left pane to reboot SBC.
- After the reboot the SBC, the license is enabled.

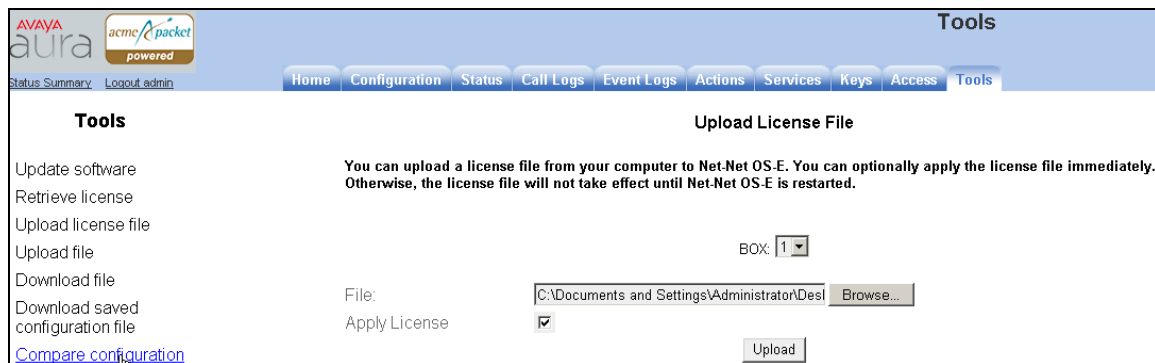


Figure 94: SBC Upload license File screen

7.2.2. Stripping SIP Headers

Session Border Controller can be used to strip SIP headers. For headers that have relevance only within the enterprise, it may be desirable to prevent these headers from being sent to the public SIP Service Provider. For example, Session Manager Release 6 inserts the P-Site header. The following procedures may be used to strip the P-Site header.

- Select the **Configuration** tab. Using the menu on the left hand side, select **vsp** → **default-session-config**, then locate **header-settings** under the **header:** section as shown in the screen below. Select the **Configure** link on the right.

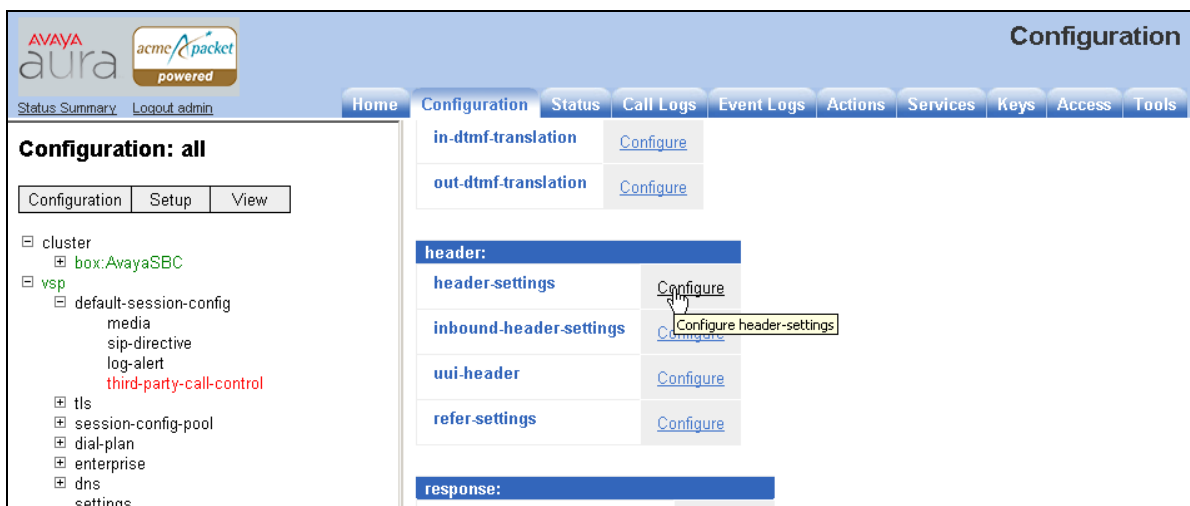


Figure 95: SBC Configuration header-settings

- In the subsequent screen [not shown] click **Edit blocked-header** and the following screen is displayed. Enter the header **P-Site** to be blocked and click **OK**.

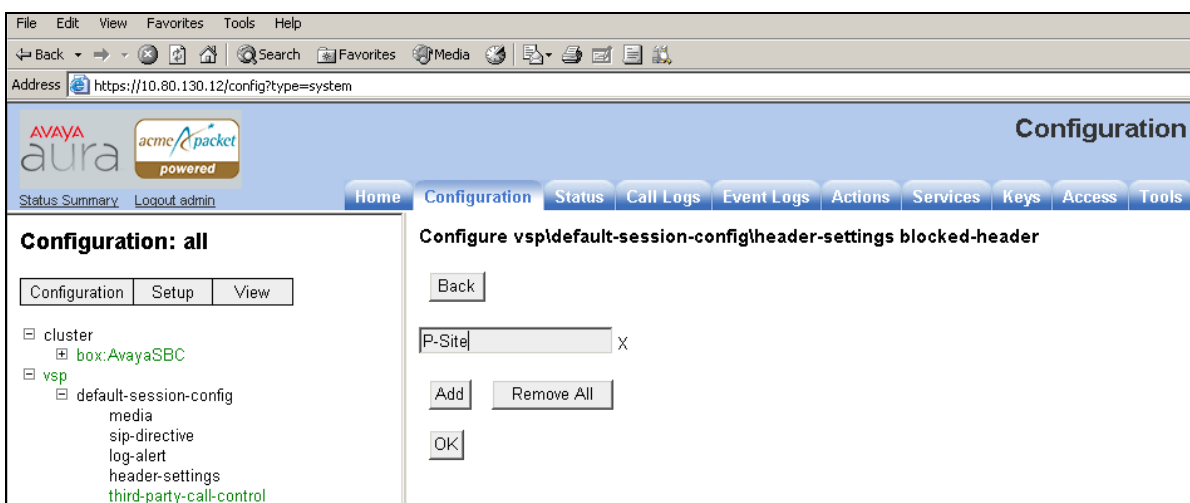


Figure 96: SBC Configuration blocked-header Entry

- The following screen is displayed indicating that P-Site header is configured to be blocked. Click **Set**.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main content area is titled 'Configure vsp\default-session-config\header-settings'. On the left, a tree view shows the configuration hierarchy: cluster > box:AvayaSBC > vsp > default-session-config > header-settings. The main panel contains a table with header settings:

Header Setting	Value / Action
allowed-header	Edit allowed-header
blocked-header	P-Site Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization
altered-body	Add altered-body
reg-ex-collector	Add reg-ex-collector
apply-allow-block-to	requests-and-responses (apply to requests and responses)
apply-to-allow-block-to-dialog	both (Apply to both inbound and outbound dialogs.)

Buttons for Set, Reset, Back, and Delete are available at the top and bottom of the configuration area.

Figure 97: SBC Configuration blocked-header

7.2.3. ICMP Configuration For ATT OPTIONS Message Response

Navigate to **cluster** → **box:AvayaSBC** → **interface eth2** → **ip outside** and click on **Configure** for **icmp** to allow Session Border Controller to respond to OPTIONS messages from the AT&T Border Element.



Figure 98: SBC Configuration ICMP

- Select **enabled** in the **admin** field and click **Set**.

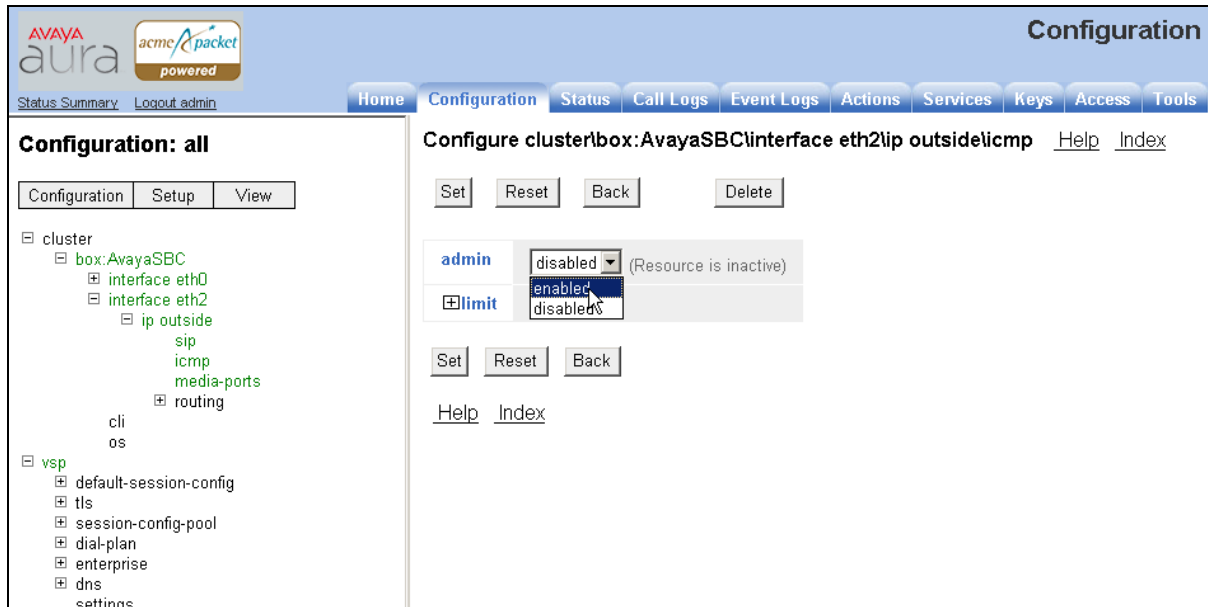


Figure 99: SBC Configuration Enable ICMP Admin

7.2.4. Contact Header Update

To enable the contact header to be updated after calls are transferred for both inbound and outbound calls, following configuration needs to be done:

1. Disable Third Party Call Control

- To disable third party call control, navigate to **vsp** → **default-session-config** → **third-party-call-control** and select **disabled** in the **admin** field. Click **Set**.

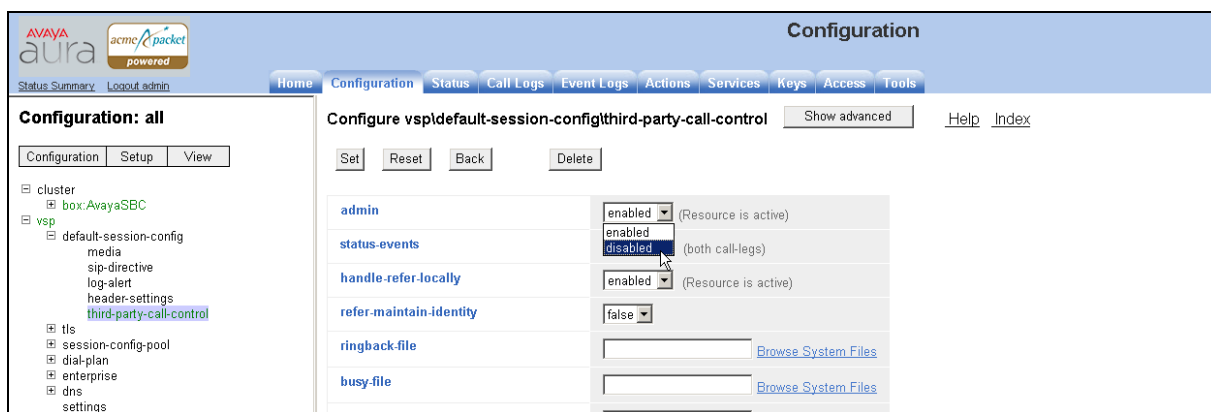


Figure 100: SBC Configuration Disabling Third Party Call Control

2. Enable **use-incoming-contact** for both inside and outside leg for calls coming into PBX and going out to ATT
 - Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway PBX** → **vsp\session-config-pool\entry ToPBX** and click **Configure** for **contact-uri-setting-in-leg**.

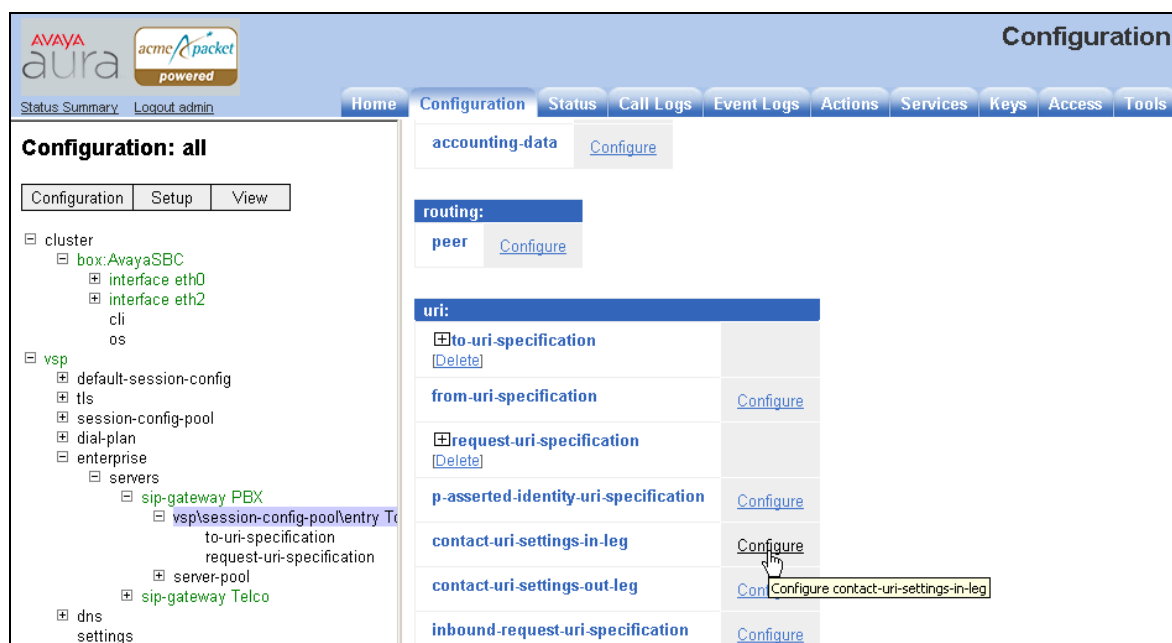


Figure 101: SBC Configuration Contact URI Settings

- Set **add-maddr** field to **disabled** and **use-incoming-contact** to **enabled**. Click **Set**.

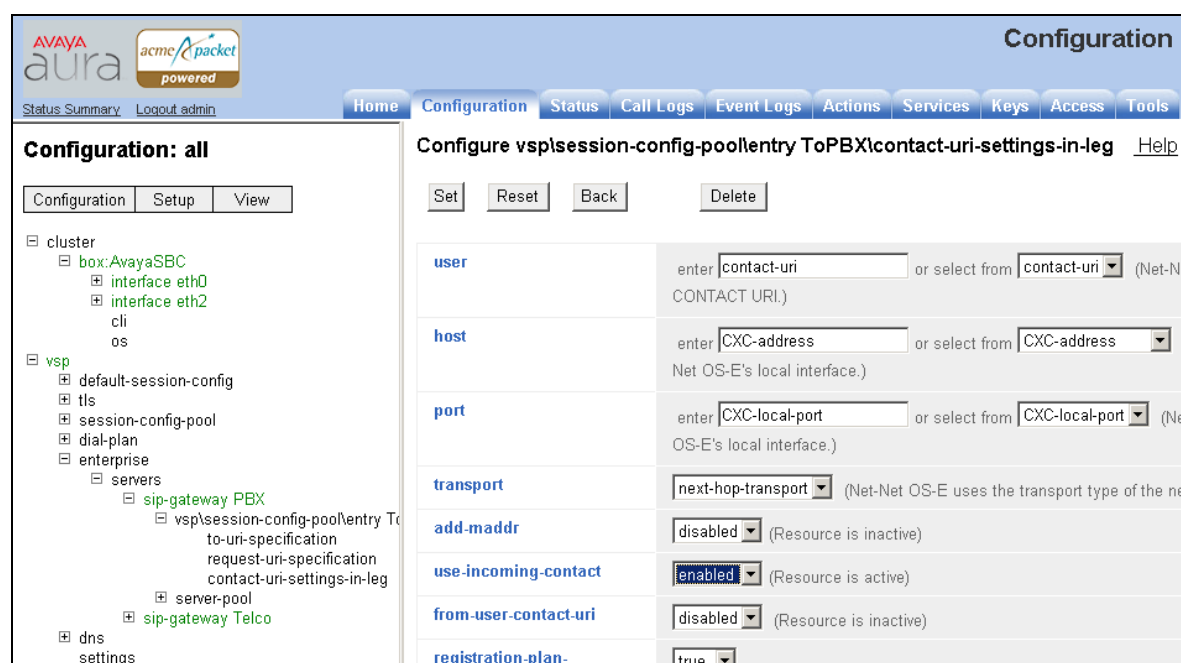


Figure 102: SBC Configuration Enabling Use Incoming Contact

- Repeat above steps to configure **contact-uri-setting-out-leg** by navigating to **vsp → enterprise → servers → sip-gateway PBX → vsp\session-config-pool\entry ToPBX**. Screen displays are similar to the above two figures.
- Similarly, **contact-uri-setting-in-leg** and **contact-uri-setting-out-leg** can be configured by navigating to **vsp → enterprise → servers → sip-gateway PBX → vsp\session-config-pool\entry ToTelco**.

7.2.5. Saving Configuration

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



Figure 103: SBC Configuration Update and Save Configuration

The following screen indicates that the configuration was updated and saved.

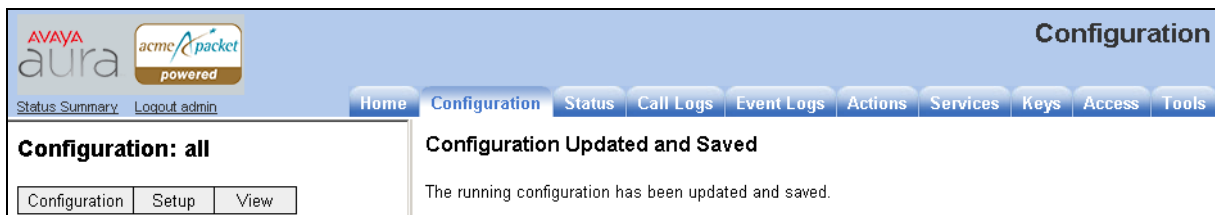


Figure 104: SBC Configuration Saved Confirmation

7.3. Avaya Aura™ Session Border Controller Running Configuration

The notable settings are highlighted in bold on the pertinent settings done during installation in **Section 7.1** and further configuration in **Section 7.2**.

```
cat cxc.cfg
#
# Copyright (c) 2004-2010 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
#
config cluster
config box 1
  set hostname AvayaSBC
  set timezone America/Denver
  set name AvayaSBC
  set identifier 00:ca:fe:07:98:42
  config interface eth0
  config ip inside
    set ip-address static 10.80.130.12/24
  config ssh
  return
  config snmp
    set trap-target 10.80.130.11 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" any 0
  return
  config icmp
  return
  config media-ports
  return
```



```

config routing
config route Default
  set gateway 10.80.130.1
return
config route Static0
  set destination network 192.11.13.4/30
  set gateway 10.80.130.10
return
config route Static1
  set admin disabled
return
config route Static2
  set admin disabled
return
config route Static3
  set admin disabled
return
config route Static4
  set admin disabled
return
config route Static5
  set admin disabled
return
config route Static6
  set admin disabled
return
config route Static7
  set admin disabled
return
config route internal-sip-media
  set destination host 10.80.120.28
  set gateway 10.80.130.1
return
return
return
return
config interface eth2
config ip outside
set ip-address static 192.168.62.55/25
config sip
  set udp-port 5060 "" "" any 0
  set tcp-port 5060 "" "" any 0
  set tls-port 5061 "" "" any 0
return
config icmp

```

```

return
config media-ports
return
config routing
config route Default
    set admin disabled
return
config route external-sip-media
    set destination network 135.242.225.0/24
    set gateway 192.168.62.1
return
return
return
return
config cli
    set prompt AvayaSBC
return
config os

return
return
return
config services
config event-log
config file access
    set filter access info
return
config file system
    set filter general info
    set filter system info
return
config file errorlog
    set filter all error
return
config file db
    set filter db debug
    set filter dosDatabase info
return
config file management
    set filter management info
return
config file peer
    set filter sipSvr info
return
config file cac

```

```
    set filter sipCAC warning
return
config file dos
    set filter dos alert
    set filter dosSip alert
    set filter dosTransport alert
    set filter dosUrl alert
return
config file krnlsys
    set filter krnlsys debug
return
config file acct
    set filter acct debug
return
return
config master-services
config accounting
return
config database
    set media enabled
return
return
config vsp
    set admin enabled
config default-session-config
config media
    set anchor enabled
    set rtp-stats enabled
return
config sip-directive
    set directive allow
return
config log-alert
    set apply-to-methods-for-filtered-logs
return
config header-settings
set blocked-header P-Site
return
config third-party-call-control
return
return
config tls
config certificate ws-cert
    set certificate-file /cxc/certs/ws.cert
```

```
return
return
config session-config-pool
config entry ToTelco
  config to-uri-specification
    set host next-hop
  return
  config from-uri-specification
    set host local-ip
  return
  config request-uri-specification
    set host next-hop
  return
  config p-asserted-identity-uri-specification
    set host local-ip
  return
  config contact-uri-settings-in-leg
    set add-maddr disabled
    set use-incoming-contact enabled
  return
  config contact-uri-settings-out-leg
  set add-maddr disabled
  set use-incoming-contact enabled
  return
return
config entry ToPBX
  config to-uri-specification
    set host next-hop-domain
  return
  config request-uri-specification
    set host next-hop-domain
  return
  config contact-uri-settings-in-leg
  set add-maddr disabled
  set use-incoming-contact enabled
  return
  config contact-uri-settings-out-leg
  set add-maddr disabled
  set use-incoming-contact enabled
  return
return
config entry Discard
  config sip-directive
  return
return
```

```

return
config dial-plan
config route Default
    set priority 500
    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
return
config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
return
config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
return
return
config enterprise
config servers
config sip-gateway PBX
    set peer-identity ""
set domain avaya.com
    set outbound-session-config-pool-entry vsp\session-config-pool\entry ToPBX
config server-pool
config server PBX1
    set host 10.80.120.28
    set transport TCP
return
return
return
config sip-gateway Telco
    set peer-identity ""
    set outbound-session-config-pool-entry vsp\session-config-pool\entry ToTelco
config server-pool
config server Telco1
    set host 135.242.225.210
return
return
return
return
return
config dns
config resolver
    config server 135.9.1.2
return
return

```

```

return
config settings
  set stack-socket-threads-max 2
return
return
config external-services
return
config preferences
  config gui-preferences
return
return
config access
  config permissions superuser
  set cli advanced
return
  config permissions read-only
  set config view
  set actions disabled
return
  config users
  config user admin
  set password 0x002bdd5d9fea2fefeb97b0115854a47db2c8b27a2fe0187e0274977f4b
  set permissions access\permissions superuser
return
  config user cust
  set password 0x004803cd9fae4ee1b2462598359d6c5e179008f9083caa7b30b9b19b43
  set permissions access\permissions read-only
return
return
return
config features
return

```

8. General Test Approach and Test Results

The test environment consisted of:

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

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

- Inbound AT&T IP Flexible Reach service calls to Communication Manager telephones and VDNs/Vectors.

- Call and two-way talk path establishment between PSTN and Communication Manager phones via the AT&T 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 8** with limitations as noted in **Section 1.3**, were verified.

9. Verification Steps

The following steps may be used to verify the configuration:

9.1. General

- 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.
- Place an inbound call to an agent or phone, but do not answer the call. Verify that the call covers to Modular Messaging voicemail. Retrieve the message from Modular Messaging.

9.2. Avaya Aura™ Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See [3] for more information.

1. From the Communication Manager console connection enter the command *list trace tac xxx*, where **xxx** is a trunk access code defined for the SIP trunk to AT&T (e.g. 120).

```
list trace tac 120
```

```
LIST TRACE
time      data
14:16:25  TRACE STARTED 07/14/2010 CM Release String cold-00.0.345.0-18246
14:16:27  SIP>INVITE sip:13035381760@avaya.com SIP/2.0
14:16:29      dial 913035381760 route:ARS
14:16:29      route-pattern 20 preference 1 cid 0x1b7
14:16:29      seize trunk-group 20 member 11 cid 0x1b7
14:16:29      Setup digits 13035381760
14:16:29      Calling Number & Name 7326665012 H323-46XX-5012
14:16:29  SIP<SIP/2.0 100 Trying
14:16:29      Proceed trunk-group 20 member 11 cid 0x1b7
14:16:31  SIP<SIP/2.0 180 Ringing
14:16:31  SIP>PRACK sip:13035381760@10.80.130.12:5060;transport=tcp
14:16:31  SIP>cp SIP/2.0
14:16:31      Alert trunk-group 20 member 11 cid 0x1b7
14:16:31      G729B ss:off ps:20
14:16:31      rgn:3 [10.80.130.12]:16718
14:16:31      rgn:3 [10.80.111.32]:16388
14:16:31      xoip options: fax:T38 modem:off tty:US uid:0x50003
14:16:31      xoip ip: [10.80.111.32]:16388
14:16:33  SIP<SIP/2.0 200 OK
14:16:33  SIP>ACK sip:13035381760@10.80.130.12:5060;transport=tcp
14:16:33  SIP>cp SIP/2.0
14:16:33      active trunk-group 20 member 11 cid 0x1b7
14:16:33  SIP>INVITE sip:13035381760@10.80.130.12:5060;transport=tcp
14:16:33  SIP>tcp SIP/2.0
14:16:33  SIP<SIP/2.0 100 Trying
14:16:33  SIP<SIP/2.0 200 OK
14:16:33      G729B ss:off ps:20
14:16:33      rgn:3 [10.80.130.43]:17382
14:16:33      rgn:3 [10.80.130.12]:16718
14:16:34  SIP>ACK sip:13035381760@10.80.130.12:5060;transport=tcp
14:16:50  SIP<BYE sip:7326665012@10.80.111.31;transport=tcp SIP/2.0
14:16:50  SIP</2.0
14:16:50  SIP>SIP/2.0 200 OK
14:16:50      idle trunk-group 20 member 11 cid 0x1b7
```


Figure 105: Communication Manager *list trace tac 120* – Outbound call.

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

9.3. Avaya Aura™ Session Manager

The following commands are issued from the System Manager console.

1. Verify the call routing administration on Session Manager.
 - In the left pane of the Avaya Aura™ System Manager Common Console, under **Elements/Session Manager/System Tools**, click on “**Call Routing Test**”. The **Call Routing Test** page shown figure below will open.
 - In the **Call Routing Test** page, enter the appropriate parameters of the test call. The figure below shows a routing test for an inbound call from PSTN to AT&T DID **7323204085**. The call arrives from the Session Border Controller (note that the source address of the call, **10.80.130.12**, is the “Inside” IP address of the Session Border Controller) and the calling number **+17323204084**.
 - Click on “**Execute Test**”.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, admin Last Logged on at August 6, 2010 10:04 AM Help | About | Change Password | Log off

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

Call Routing Test

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

SIP INVITE Parameters

Called Party URI	7323204085@avaya.com	Calling Party Address	10.80.130.12
Calling Party URI	+17323204084@avaya.com	Session Manager Listen Port	5060
Day Of Week	Friday	Time (UTC)	20:48
Called Session Manager Instance	SM1	Transport Protocol	TCP

Execute Test

Figure 106: Session Manager Call Routing Test Page

- The results of the test are displayed as shown in figure below. The ultimate routing decision is displayed under the heading **Routing Decisions**. The example test shows that the PSTN call to **7323204085** is sent by Session Manager to the Communication Manager extension **6665012**. Under that section the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated). Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 4**.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at August 6, 2010 10:04 AM
Help | About | Change Password | Log off

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

Call Routing Test

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

SIP INVITE Parameters

Called Party URI: 7323204085@avaya.com
 Calling Party URI: +17323204084@avaya.com
 Day Of Week: Friday
 Time (UTC): 20:48
 Called Session Manager Instance: SMI

Calling Party Address: 10.80.130.12
 Session Manager Listen Port: 5060
 Transport Protocol: TCP

Execute Test

Routing Decisions

Route < sip:6665013@avaya.com > to SIP Entity ATT-CLAN (10.80.111.31). Terminating Location is Location 1 Subnet 10.80.111.x.

Routing Decision Process

NRP Adaptations: AT&T Adaptations applied.
 NRP Adaptations: Request URI set to sip:7323204085@avaya.com
 NRP Adaptations: P-Asserted-Identity set to sip:+17323204084@avaya.com
 BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.
 Originating Location is AuraSBC. Using digits < 7323204085 > and host < avaya.com > for routing.
 NRP Dial Patterns: Found a Dial Pattern match for pattern < 7323 > Min/Max length 10/10 and domain < avaya.com >.
 NRP Routing Policies: Ranked destination NRP Sip Entities: ATT-CLAN.
 NRP Routing Policies: Removing disabled routes.
 NRP Routing Policies: Ranked destination NRP Sip Entities: ATT-CLAN.
 END EMERGENCY CALL CHECK: This is not an emergency call.
 Adapting and proxying for SIP Entity ATT-CLAN.
 NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.
 NRP Adaptations: ATT CLAN applied.
 NRP Adaptations: P-Asserted-Identity set to sip:+17323204084@avaya.com
 NRP Adaptations: Request-URI set to sip:6665013@avaya.com

Figure 107: Call Routing Test Page -Completed

9.4. Protocol Traces

Using a SIP protocol analyzer (e.g. Wireshark), monitor the SIP traffic at the Session Border Controller “inside” interface connection to the AT&T IP Flexible Reach service.

1. The following are examples of outbound and inbound calls filtered for the SIP protocol.

No. .	Time	Source	Destination	Protocol	Info
431	2010-07-03 16:38:35	10.80.130.40	10.80.120.28	SIP	Request: SUBSCRIBE sip:6665401@avaya.com
432	2010-07-03 16:38:36	10.80.120.28	10.80.130.40	SIP	Status: 401 Unauthorized
433	2010-07-03 16:38:36	10.80.130.40	10.80.120.28	SIP	Request: SUBSCRIBE sip:6665401@avaya.com
434	2010-07-03 16:38:36	10.80.120.28	10.80.130.40	SIP	Status: 202 Accepted
437	2010-07-03 16:38:36	10.80.120.28	10.80.130.40	SIP	Request: NOTIFY sip:6665401@10.80.130.40;transport=tcp
440	2010-07-03 16:38:36	10.80.130.40	10.80.120.28	SIP	Status: 200 OK
468	2010-07-03 16:38:38	10.80.120.28	10.80.130.12	SIP/SDP	Request: INVITE sip:13035381760@207.242.225.210, with sess
470	2010-07-03 16:38:38	10.80.130.12	10.80.120.28	SIP	Status: 100 Trying
570	2010-07-03 16:38:40	10.80.130.12	10.80.120.28	SIP/SDP	Status: 180 Ringing, with session description
576	2010-07-03 16:38:40	10.80.120.28	10.80.130.12	SIP	Request: PRACK sip:13035381760@207.242.225.210:5060;transp
577	2010-07-03 16:38:40	10.80.130.12	10.80.120.28	SIP	Status: 200 OK
984	2010-07-03 16:38:43	10.80.130.12	10.80.120.28	SIP/SDP	Status: 200 OK, with session description
994	2010-07-03 16:38:43	10.80.120.28	10.80.130.12	SIP	Request: ACK sip:13035381760@207.242.225.210:5060;transpor
1018	2010-07-03 16:38:43	10.80.120.28	10.80.130.12	SIP	Request: INVITE sip:13035381760@207.242.225.210:5060;trans
1021	2010-07-03 16:38:43	10.80.130.12	10.80.120.28	SIP	Status: 100 Trying

Figure 108: –SIP Protocol trace – Outbound call to AT&T

No. .	Time	Source	Destination	Protocol	Info
11	2010-07-03 20:00:03	10.80.130.12	10.80.120.28	SIP/SDP	Request: INVITE sip:7323204084@avaya.com:5060, with sessio
13	2010-07-03 20:00:03	10.80.120.28	10.80.130.12	SIP	Status: 100 Trying
28	2010-07-03 20:00:03	10.80.120.28	10.80.130.12	SIP/SDP	Status: 180 Ringing, with session description
126	2010-07-03 20:00:05	10.80.120.28	10.80.130.12	SIP/SDP	Status: 200 OK, with session description
141	2010-07-03 20:00:06	10.80.130.12	10.80.120.28	SIP	Request: ACK sip:7323204084@avaya.com:5060
150	2010-07-03 20:00:06	10.80.120.28	10.80.130.12	SIP	Request: INVITE sip:+13035381760@207.242.225.210:5060;tran
152	2010-07-03 20:00:06	10.80.130.12	10.80.120.28	SIP	Status: 100 Trying
182	2010-07-03 20:00:06	10.80.130.12	10.80.120.28	SIP/SDP	Status: 200 OK, with session description
195	2010-07-03 20:00:06	10.80.120.28	10.80.130.12	SIP/SDP	Request: ACK sip:+13035381760@207.242.225.210:5060;transpo
205	2010-07-03 20:00:10	10.80.130.40	10.80.120.28	SIP	Request: SUBSCRIBE sip:6665401@avaya.com
209	2010-07-03 20:00:10	10.80.120.28	10.80.130.40	SIP	Status: 202 Accepted
248	2010-07-03 20:00:10	10.80.120.28	10.80.130.40	SIP	Request: NOTIFY sip:6665401@10.80.130.40;transport=tcp
249	2010-07-03 20:00:10	10.80.130.40	10.80.120.28	SIP	Status: 200 OK
289	2010-07-03 20:00:22	10.80.120.28	10.80.130.12	SIP	Request: BYE sip:+13035381760@207.242.225.210:5060;transpo
291	2010-07-03 20:00:22	10.80.130.12	10.80.120.28	SIP	Status: 200 OK

Figure 109: –SIP Protocol trace – Inbound call from AT&T

2. The following is an example of an outbound call filtered for DTMF.

No. .	Time	Source	Destination	Protocol	Info
2039	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2042	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2044	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2046	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2048	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2050	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound # (end)
2051	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound # (end)
2052	2010-07-03 18:25:55	10.80.111.32	10.80.130.12	RTP EVEN	Payload type=RTP Event, DTMF Pound # (end)
2319	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1
2320	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1
2324	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1
2326	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1
2327	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1
2329	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1
2331	2010-07-03 18:25:57	10.80.130.12	10.80.111.32	RTP EVEN	Payload type=RTP Event, DTMF One 1

Figure 110: – RTPEvent (DTMF) trace – Outbound call to AT&T

3. The following is an example of an outbound call filtered for RTP.

Filter: rtp		Expression... <input type="button" value="Clear"/> <input type="button" value="Apply"/>			
No. .	Time	Source	Destination	Protocol	Info
39	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=5, Time=1200
40	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=6, Time=1360
42	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=7, Time=1520
43	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=8, Time=1680
44	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=9, Time=1840
46	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=10, Time=2000
47	2010-07-03 20:00:03	10.80.130.12	10.80.111.32	RTP	PT=ITU-T G.729, SSRC=0xA9590A, Seq=1, Time=1040
48	2010-07-03 20:00:03	10.80.130.12	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=11, Time=2160
49	2010-07-03 20:00:03	10.80.130.12	10.80.111.32	RTP	PT=ITU-T G.729, SSRC=0xA9590A, Seq=2, Time=1280
50	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=12, Time=2320
52	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=13, Time=2480
53	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=14, Time=2640
54	2010-07-03 20:00:03	10.80.130.12	10.80.111.32	RTP	PT=ITU-T G.729, SSRC=0xA9590A, Seq=3, Time=1760
55	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=15, Time=2800
57	2010-07-03 20:00:03	10.80.111.32	10.80.130.12	RTP	PT=ITU-T G.729, SSRC=0x304E60E8, Seq=16, Time=2960

Figure 111: – RTP trace (showing codec used) – Outbound call to AT&T

9.5. Avaya Aura™ Session Border Controller

The Session Border Controller provisioning can be checked by entering the command “**show -v**” at the SBC command line interface. Additionally, call logs can be verified by clicking on the **Call Logs** button [not shown] on the Session Border Controller GUI and then clicking on the **Session Diagram** for the call in question. A split screen showing the call diagram and the actual call flow will be displayed. For convenience, two separate screens are shown here.

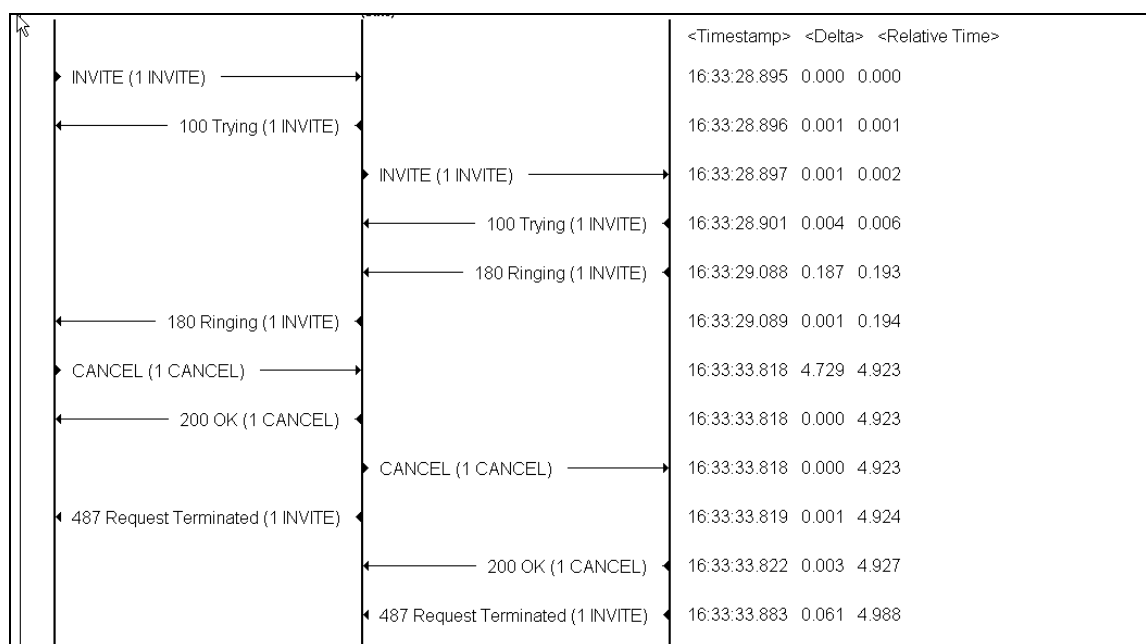


Figure 112: – Call Flow Diagram on Session Border Controller

Call IDs: ASE_1281134548067_2857_null_135.25.250.88 CXC-63-5c37a970-c82500a-13c4-4c5c8db8-15c1e4e9-24c1ed44@207.242.225.210

Expand All

Timestamp	Direction	Remote IP/Port	Local IP/Port	Transport
16:33:28.895 2010-08-06	RX	207.242.225.210:5060	205.168.62.55(eth2):5060	UDP
Message: Less INVITE sip:7323204085@205.168.62.55:5060 SIP/2.0 Via: SIP/2.0/UDP 207.242.225.210:5060;branch=z9hG4bK44so2k00ao3lifcm3201.1 From: "Unavailable" <sip:+13035381760@207.242.225.210:5060;user=phone>;tag=ds9741f1f To: <sip:7323204085@205.168.62.55;user=phone> Call-ID: ASE_1281134548067_2857_null_135.25.250.88 CSeq: 1 INVITE				
16:33:28.896 2010-08-06	TX	207.242.225.210:5060	205.168.62.55(eth2):5060	UDP
Message: More See changes SIP/2.0 100 Trying				
16:33:28.897 2010-08-06	TX	10.80.120.28:5060	10.80.130.12(eth0):1426	TCP
Message: More See changes INVITE sip:7323204085@avaya.com:5060 SIP/2.0				
16:33:28.901 2010-08-06	RX	10.80.120.28:5060	10.80.130.12(eth0):1426	TCP
Message: More SIP/2.0 100 Trying				
16:33:29.088 2010-08-06	RX	10.80.120.28:5060	10.80.130.12(eth0):1426	TCP
Message: More SIP/2.0 180 Ringing				
16:33:29.089 2010-08-06	TX	207.242.225.210:5060	205.168.62.55(eth2):5060	UDP
Message: More See changes SIP/2.0 180 Ringing				
16:33:33.818 2010-08-06	RX	207.242.225.210:5060	205.168.62.55(eth2):5060	UDP
Message: More CANCEL sip:7323204085@205.168.62.55:5060 SIP/2.0				
16:33:33.818 2010-08-06	TX	207.242.225.210:5060	205.168.62.55(eth2):5060	UDP
Message: More See changes SIP/2.0 200 OK				
16:33:33.818 2010-08-06	TX	10.80.120.28:5060	10.80.130.12(eth0):1426	TCP
Message: More See changes CANCEL sip:7323204085@avaya.com:5060 SIP/2.0				
16:33:33.819 2010-08-06	TX	207.242.225.210:5060	205.168.62.55(eth2):5060	UDP

Figure 113: – Call Flow Diagram on Session Border Controller

10. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Session Manager, 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. 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 via AVPN or MIS/PNT transport. These Application Notes further demonstrated that the AT&T Adaptation Module on the Avaya Aura™ Session Manager could be utilized to remove History-Info header information on egress SIP messages to the AT&T IP Flexible Reach service. The DigitConversionAdapter could be utilized to provide required digit manipulation for inbound and outbound calls. Additionally the ability of Avaya Aura™ Communication Manager to provide SIP Diversion Header to the AT&T IP Flexible Reach service for certain out bound call scenarios (see **Section 2.2.3**) was demonstrated.

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

11. References

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

- [1] *Installing and Configuring Avaya Aura™ Session Manager*, Doc ID 03-603473 Release 6.
- [2] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Release 6.0, June 2010
- [3] *Installing and Configuring Avaya Aura™ Communication Manager*, Doc ID 03-603558, Release 6.0 June, 2010
- [4] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 6.0, 555-245-205, Issue 8.0, June 2010
- [5] *Administering Avaya Aura™ Call Center Features*, Release 6.0, June 2010
- [6] *Programming Call Vectors in Avaya Aura™ Call Center*, 6.0, June 2010
- [7] *Modular Messaging 5.2 Single Server Known Issues – Administration and Installers*, November, 2009
- [8] *Modular Messaging Multi-Site Guide Release 5.2*, November 2009
- [9] *Modular Messaging for Microsoft Exchange Release 5.2 Installation and Upgrades*, November 2009
- [10] *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.2 Installation and Upgrades*, November 2009
- [11] *Modular Messaging for IBM Lotus Domino 5.2 Installation and Upgrades*, November 2009

AT&T IP Flexible Reach Service Descriptions:

- [12] *AT&T IP Flexible Reach*

<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>

12. Addendum 1 – Provisioning for Ptime in Avaya Aura™ Session Border Controller

Due to the limitation noted in **Section 1.3, Item 7**, following configuration steps on the Session Border Controller are proposed as a workaround. This workaround is applied to calls from and to the Session Border Controller.

12.1. Header Manipulation for Inbound and Outbound Calls

1. To provide a header manipulation for the outbound calls from Session Border Controller, navigate to **vsp→session-config-pool→entry ToTelco→header-settings→altered-body** and enter any number and click **Create**.

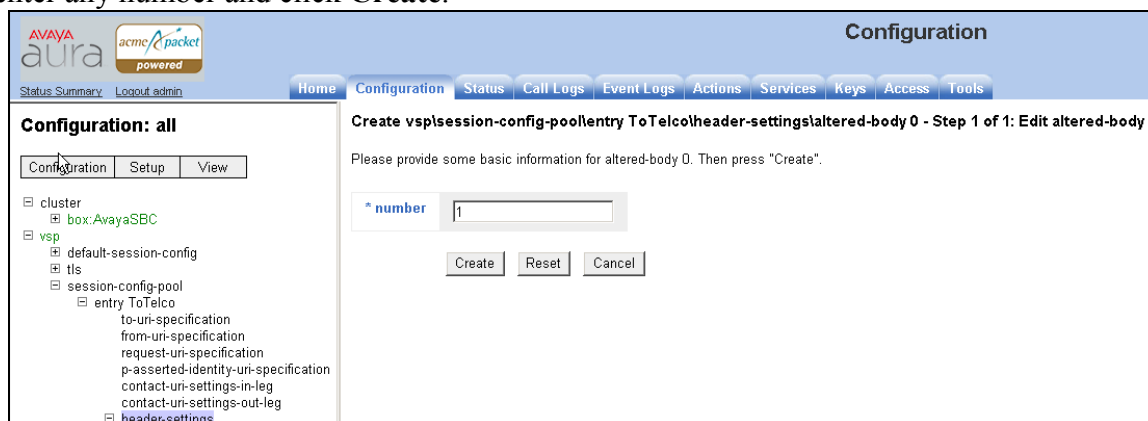


Figure 114: – Creating a Header Manipulation rule on Session Border Controller

2. On the subsequent screen [not shown], select **Configure** for **altered-body** tag. The following screen is displayed. Configure as follows:
 - **expression** – Enter a valid regular expression to look for in the SDP portion of the SIP header. In this reference configuration, "(?ms)(.*)a=rtpmap:100 telephone-event/8000(*)" was used to look for a line in the SDP which contained **a=rtpmap:100 telephone-event/8000** string.
 - **replacement** – Enter a replacement string in the SIP header. In this reference configuration, "\1a=rtpmap:100 telephone-event/8000\ba=ptime:30\2" was used.

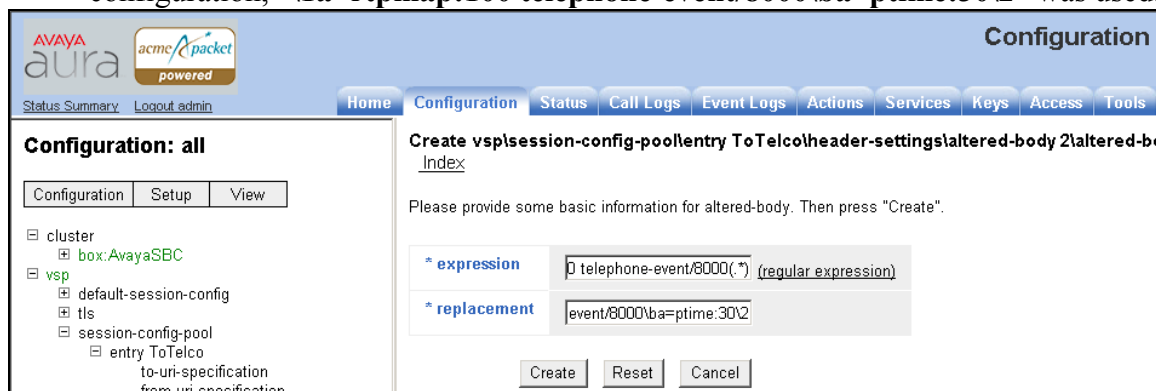


Figure 115: – Altered Body screen on Session Border Controller

- On the subsequent screen make sure that **admin** field is enabled and select **INVITE** and **ACK** in **apply-to-methods** field by pressing the **CTRL** key and clicking to select the methods to alter when an expression is matched in the SDP of the SIP Header.

The screenshot shows the Avaya Aura Configuration interface. On the left, a tree view shows the configuration hierarchy: cluster > vsp > session-config-pool > entry ToTelco > header-settings > altered-body 1. The main panel is titled 'Configure vsplsession-config-poolentry ToTelcoheader-settingsaltered-body 1'. It contains several fields: 'admin' is set to 'enabled' (Resource is active); '* number' is '1'; '* expression' is '(?ms)(.*)a=rtmpmap:1[0,2]0 (regular expression)'; '* replacement' is '\1a=rtmpmap:100 telephone'; 'apply-to-methods' is a list box containing 'INVITE', 'REFER', 'MESSAGE', and 'INFO', with 'Select All' and 'Unselect All' buttons; 'apply-to-responses' is 'no' (Do not apply to responses (requests only)); 'apply-to-dialog' is 'both' (Apply to both inbound and outbound dialogs.); and 'remove-body' is 'false'.

Figure 116: – Selecting the methods for the manipulation on Session Border Controller

- Following screen confirms that the header manipulation rule was applied to both INVITE and ACK methods in this reference configuration to manipulate the ptime header.

The screenshot shows the Avaya Aura Configuration interface. On the left, the same configuration hierarchy is shown. The main panel is titled 'Configure vsplsession-config-poolentry ToTelcoheader-settings'. It contains a table with the following data:

	altered-body	admin	altered-body	apply-to-methods	apply-to-responses	apply-to-dialog	remove-body
Edit Delete	altered-body 1	enabled	(?ms)(.*)a=rtmpmap:1[0,2]0 telephone-event/8000(*)\1a=rtmpmap:100 telephone-event/8000ba=ptime:30/2	INVITE, ACK	no	both	false

Figure 117: – Confirmation screen for the manipulation rule for Outgoing calls from Session Border Controller

- Repeat the above steps by navigating to **vsp**→**session-config-pool**→**entry ToPBX**→**header-settings**→**altered-body** to provide the same manipulation rule for the calls coming to the

Session Border Controller. Following screens show the final manipulations for calls coming into Session Border Controller. Note that the calls coming into Session Border Controller apply the manipulation rule to the 200 OK response too in this reference configuration.



Figure 118: – Confirmation screen for the manipulation rule for Incoming Calls to Session Border Controller

12.2. Running Configuration Changes on Session Border Controller

As a result of configuration done in Section 12.1, following changes were made to the running configuration file on the Session Border Controller:

```

config session-config-pool
config entry ToTelco
.....
config header-settings
config altered-body 1
set altered-body "(?ms)(.*)a=rtpmap:1[0,2]0 telephone-event/8000(.*)"
"\1a=rtpmap:100 telephone-event/8000\ba=ptime:30\2"
set apply-to-methods INVITE+ACK
return
return
return
config entry ToPBX
.....
config header-settings
config altered-body 1
set altered-body "(?ms)(.*)a=rtpmap:100 telephone-event/8000(.*)"
"\1a=rtpmap:100 telephone-event/8000\ba=ptime:30\2"
set apply-to-methods INVITE+ACK
set apply-to-responses both 200
return
return
return

```

12.3. Sample Trace Reflecting the Addition of the Ptime Header

No. .	Time	Source	Destination	Protocol	Info
325	2010-08-12 11:20:59	205.168.62.55	207.242.225.210	SIP/SDP	Request: INVITE sip:13035381760@207.242.225.210, with sess
328	2010-08-12 11:20:59	207.242.225.210	205.168.62.55	SIP	Status: 100 Trying
346	2010-08-12 11:21:01	207.242.225.210	205.168.62.55	SIP/SDP	Status: 180 Ringing, with session description
347	2010-08-12 11:21:01	205.168.62.55	207.242.225.210	SIP	Request: PRACK sip:13035381760@207.242.225.210:5060;transp
356	2010-08-12 11:21:01	207.242.225.210	205.168.62.55	SIP	Status: 200 OK
514	2010-08-12 11:21:03	207.242.225.210	205.168.62.55	SIP/SDP	Status: 200 OK, with session description
523	2010-08-12 11:21:03	205.168.62.55	207.242.225.210	SIP	Request: ACK sip:13035381760@207.242.225.210:5060;transport=
527	2010-08-12 11:21:03	205.168.62.55	207.242.225.210	SIP	Request: INVITE sip:13035381760@207.242.225.210:5060;transp
537	2010-08-12 11:21:03	207.242.225.210	205.168.62.55	SIP	Status: 100 Trying
540	2010-08-12 11:21:03	207.242.225.210	205.168.62.55	SIP/SDP	Status: 200 OK, with session description

Media Format: ITU-T G.711 PCMU
Media Format: 100
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute Fieldname: rtpmap
Media Format: 18
MIME Type: G729
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute Fieldname: rtpmap
Media Format: 0
MIME Type: PCMU
Media Attribute (a): rtpmap:100 telephone-event/8000
Media Attribute Fieldname: rtpmap
Media Format: 100
MIME Type: telephone-event
Media Attribute (a): ptime:30
Media Attribute Fieldname: ptime
Media Attribute Value: 30

Figure 119: – Trace for a call originating from PBX

No. .	Time	Source	Destination	Protocol	Info
321	2010-08-12 12:45:30	207.242.225.210	205.168.62.55	SIP/SDP	Request: INVITE sip:7323204084@205.168.62.55:5060, with se
322	2010-08-12 12:45:30	205.168.62.55	207.242.225.210	SIP	Status: 100 Trying
324	2010-08-12 12:45:30	205.168.62.55	207.242.225.210	SIP/SDP	Status: 180 Ringing, with session description
498	2010-08-12 12:45:32	205.168.62.55	207.242.225.210	SIP/SDP	Status: 200 OK, with session description
513	2010-08-12 12:45:32	207.242.225.210	205.168.62.55	SIP	Request: ACK sip:7326665011@205.168.62.55:5060;transport=u
518	2010-08-12 12:45:32	205.168.62.55	207.242.225.210	SIP	Request: INVITE sip:3035381760@207.242.225.210:5060;transp
522	2010-08-12 12:45:33	207.242.225.210	205.168.62.55	SIP	Status: 100 Trying
529	2010-08-12 12:45:33	207.242.225.210	205.168.62.55	SIP/SDP	Status: 200 OK, with session description
538	2010-08-12 12:45:33	205.168.62.55	207.242.225.210	SIP/SDP	Request: ACK sip:3035381760@207.242.225.210:5060;transport
1424	2010-08-12 12:45:46	205.168.62.55	207.242.225.210	SIP	Request: INVITE sip:3035381760@207.242.225.210:5060;transp

Media Description, name and address (m): audio 24376 RTP/AVP 18 100
Media Type: audio
Media Port: 24376
Media Proto: RTP/AVP
Media Format: ITU-T G.729
Media Format: 100
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute Fieldname: rtpmap
Media Format: 18
MIME Type: G729
Media Attribute (a): rtpmap:100 telephone-event/8000
Media Attribute Fieldname: rtpmap
Media Format: 100
MIME Type: telephone-event
Media Attribute (a): ptime:30
Media Attribute Fieldname: ptime
Media Attribute Value: 30

Figure 120: – Trace for a call originating from ATT

©2011 Avaya Inc. All Rights Reserved.

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

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