



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager R5.2.1, Avaya Aura® Session Manager R6.2 and Acme Packet Net-Net 6.2.0 with AT&T IP Flexible Reach and IP Flexible Reach-Enhanced Features SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager R5.2.1, Avaya Aura® Session Manager R6.2, and the Acme Packet Net-Net 3800 with the AT&T IP Flexible Reach and IP Flexible Reach-Enhanced Features service using **AVPN** or **MIS/PNT** transport connections. The AT&T Flexible Reach is one of the many SIP-based Voice over IP services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features which are not part of IP Flexible Reach service.

Avaya Aura® Session Manager R6.2 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. In the reference configuration, Avaya Aura® Communication Manager R5.2.1 is provisioned in an Access Element configuration (note that SIP endpoints are not supported in an Avaya Aura® Communication Manager R5.2.1 Access Element configuration). Acme Packet Net-Net 3800 is the point of connection between Avaya Aura® Session Manager R6.2 and the AT&T IP Flexible Reach and IP Flexible Reach-Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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 at the Avaya Solution and Interoperability Test Lab.

TABLE OF CONTENTS

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results and Known Limitations	5
2.3.	Support	7
3.	Reference Configuration	8
3.1.	Illustrative Configuration Information	10
3.2.	Call Flows	11
3.2.1.	Inbound	11
3.2.2.	Outbound.....	12
3.2.3.	Call Forward Re-direction (Diversion Header)	14
3.2.4.	Coverage to Voicemail	15
3.2.5.	AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow.....	16
4.	Equipment and Software Validated	17
5.	Configure Avaya Aura® Session Manager Release 6.2	19
5.1.	SIP Domain	21
5.2.	Locations	21
5.3.	Configure Adaptations	23
5.4.	SIP Entities	25
5.5.	Entity Links	29
5.6.	Time Ranges.....	30
5.7.	Routing Policies	30
5.8.	Dial Patterns	33
5.9.	Session Manager Administration	35
6.	Configure Avaya Aura® Communication Manager 5.2.1	36
6.1.	System Parameters	36
6.2.	Dial Plan.....	37
6.3.	IP Node Names.....	38
6.4.	IP Codec Parameters	38
6.5.	IP Network Regions	39
6.6.	SIP Trunks.....	40
6.6.1.	SIP Trunk for AT&T IP Flexible Reach.....	40
6.6.2.	SIP Trunk for AT&T IP Flexible Reach – Network Based Blind Transfer calls	42
6.7.	Public Unknown Numbering.....	43
6.8.	Outbound Call Routing From Avaya Aura® Communication Manager	43
6.8.1.	Route Pattern.....	43
6.8.2.	ARS Dialing for AT&T IP Flexible Reach service	44
6.8.3.	ARS Dialing for AT&T IP Flexible Reach-Enhanced Features	44
6.9.	Post-Answer Redirection.....	45
6.10.	Saving Translations	45
7.	Configure Acme Packet Session Border Controller (SBC)	46
8.	Verification Steps.....	65
8.1.	AT&T IP Flexible Reach	65
8.2.	AT&T IP Flexible Reach-Enhanced Features.....	65

8.3.	Avaya Aura® Communication Manager	65
8.4.	Avaya Aura® Session Manager	66
9.	Conclusion	66
10.	References.....	67

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager R5.2.1, Avaya Aura® Session Manager R6.2, and the Acme Packet Net-Net 3800 with the AT&T IP Flexible Reach and IP Flexible Reach-Enhanced Features service using **AVPN** or **MIS/PNT** transport connections. The AT&T Flexible Reach is one of the many SIP-based Voice over IP services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features which are not part of IP Flexible Reach service.

Avaya Aura® Session Manager R6.2 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. In the reference configuration, Avaya Aura® Communication Manager R5.2.1 is provisioned in an Access Element configuration (note that SIP endpoints are not supported in an Avaya Aura® Communication Manager R5.2.1 Access Element configuration). Acme Packet Net-Net 3800 (Acme Packet SBC) is the point of connection between Avaya Aura® Session Manager R6.2 and the AT&T IP Flexible Reach and IP Flexible Reach-Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

Note - References to the AT&T IP Flexible Reach service in the remainder of this document include AT&T IP Flexible Reach-Enhanced Features as well, unless otherwise specified.

Note: For several AT&T IP Flexible Reach – Enhanced Features, Service Pack 13 (SP 13) needs to be applied on Avaya Aura® Communication Manager R5.2.1.

2. General Test Approach and Test Results

The test environment consisted of:

1. A simulated enterprise with System Manager, Session Manager, Communication Manager, Avaya phones, fax machines (Ventafax application), Acme Session Border Controller (SBC), and Avaya Modular Messaging. **Note: No voicemail test cases were executed for Avaya Modular Messaging system.**
2. A laboratory version of the AT&T IP Flexible Reach service, to which the simulated enterprise was connected via AVPN or MIS-PNT transport.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing verified basic inbound and outbound call flows along with Enhanced Features with AT&T IP Flexible Reach service. **Section 3.2** provides call flows tested for AT&T IP Flexible Reach service.

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

- AT&T IP Flexible Reach service
 - SIP trunking.
 - Inbound and outbound dialing including international calls.
 - Voicemail (leave and retrieve messages). **Note that these test cases were not run but are expected to work.**
 - T.38 Fax.
 - Passing of DTMF events and their recognition by navigating automated menus.
 - Basic telephony features such as hold, resume, conference and transfer.
 - Call Forward with Diversion Header.
- AT&T Network IP Flexible Reach-Enhanced Features
 - Network based Simultaneous Ring
 - Network based Sequential Ring (Locate Me)
 - Network based Blind Call Transfer using SIP REFER on Communication Manager¹
 - Network based Call Forwarding Always (CFA/CFU)
 - Network based Call Forwarding Ring No Answer (CF-RNA)
 - Network based Call Forwarding Busy (CF-Busy)
 - Network based Call Forwarding Not Reachable (CF-NR)

2.2. Test Results and Known Limitations

The test objectives stated in **Section 2.1** with limitations noted below were verified.

1. When the call is put on hold on Communication Manager, SDP with **a=sendonly** is sent to AT&T IP Flexible Reach service but it sends **a=inactive** in response which results in no Music-on-Hold being sent to PSTN. A Header Manipulation Rule was provided as shown in **Section 7** to send **a=sendrecv** to resolve this situation.
2. While using Meetme-Conference feature on Communication Manager, when the number of parties on PSTN connected to Communication Manager goes down to two, and if Network Call Redirection (NCR) is enabled, Communication Manager sends a REFER message back to AT&T IP Flexible Reach service which in turn acknowledges the REFER and a BYE is received by the remaining two parties on the conference. As a result, the two parties are directly connected to each other. This does not happen if one of the parties is on the Enterprise side and connected to Communication Manager. As a workaround, the DIDs used for this feature can use a separate trunk with NCR set to disabled as shown in **Section 6.6.1**.

¹ Network based Blind Call Transfer uses Vectors and VDNs on Communication Manager. Phone based transfers (attended or unattended) are not supported.

3. In the case of Simultaneous Ring, while both Communication Manager phones are ringing they display the calling number. If the primary phone answers, it continues to display the calling number. However, if the secondary number answers, the display changes to "Unavailable". The sequential call had similar results for both primary and secondary number.
4. Unattended and Attended off-net transfer from Communication Manager phones is not supported. This may be supported when a two trunk solution is implemented and this call routes over NCR disabled trunk as shown in **Section 6.6.1**.
5. Although Session Manager R6.2 supports the possibility of using SIP phones, SIP phones are not supported by Communication Manager 5.2.1 in an Access Element configuration.
6. 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 bps in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Communication Manager.
7. Calls From/to Customer Trunks via the same AT&T border element (e.g., "looped" calls), which result in Communications Manager sending a **491 Request Pending**, may experience a dropped call. This issue was observed during a **looped** call where Communication Manager phone dials an AT&T IP Flexible Reach number, and the network destination of that call is a second Communication Manager phone behind the same AT&T border element. Sometimes these calls result in Communication Manager issuing a **491 Request Pending** in response to the **looped Invite** from the network. When the network also **loops** the **491** back to Communication Manager, the network inserts a Contact header that contains the IP address of an internal AT&T network node. As a result, Communication Manager attempts to route subsequent **Invites** to this un-routable address. Eventually these **Invites** time out and the call may be dropped. This issue is under investigation by AT&T.
8. Emergency 911/E911 Services Limitations and Restrictions - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with 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.

2.3. Support

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

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

3. Reference Configuration

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

- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager provides the voice communication services for a particular enterprise site. In the reference configuration, Communication Manager 5.2.1 runs on an Avaya S8720 Server in a G650/Control LAN (C-LAN) configuration. This solution is extensible to other Avaya S8xxx Servers.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G650 Media Gateway is used. The G650 contains system boards such as the Control LAN (C-LAN) and Media Processor (MedPro). This solution is extensible to other Avaya Media Gateways.
- Avaya “desk” telephones are represented with Avaya 96x0 and 96x1 Series IP Telephones running H.323, Avaya 6408D Series Digital Telephone, Avaya Analog phone and Avaya one-X® Communicator PC based softphone (configured as H.323 endpoint).
- The Acme Packet SBC provides SIP Session Border Controller functionality, including address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network². UDP transport protocol is used between the Acme Packet SBC and the AT&T Flexible Reach service.
- An existing Avaya Modular Messaging system provides the corporate voice messaging capabilities in the reference configuration. The provisioning of Modular Messaging is beyond the scope of this document and is shown here for illustrative purposes only. **Note: No Modular Messaging test cases were run but it was shown in the configuration for completeness of the solution.**
- Inbound and outbound calls were placed between PSTN and the Customer Premises Equipment (CPE) via the AT&T IP Flexible Reach service, through the Acme Packet SBC, Session Manager, and Communication Manager. Communication Manager originated/terminated the calls using appropriate phone or fax stations. The H.323 phones in the CPE registered to the Avaya Aura® Communication Manager C-LANs.

² The AT&T Enhanced IP Flexible Reach service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Acme Packet SBC in this sample configuration. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Acme Packet SBC and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Acme Packet SBC and Communication Manager.

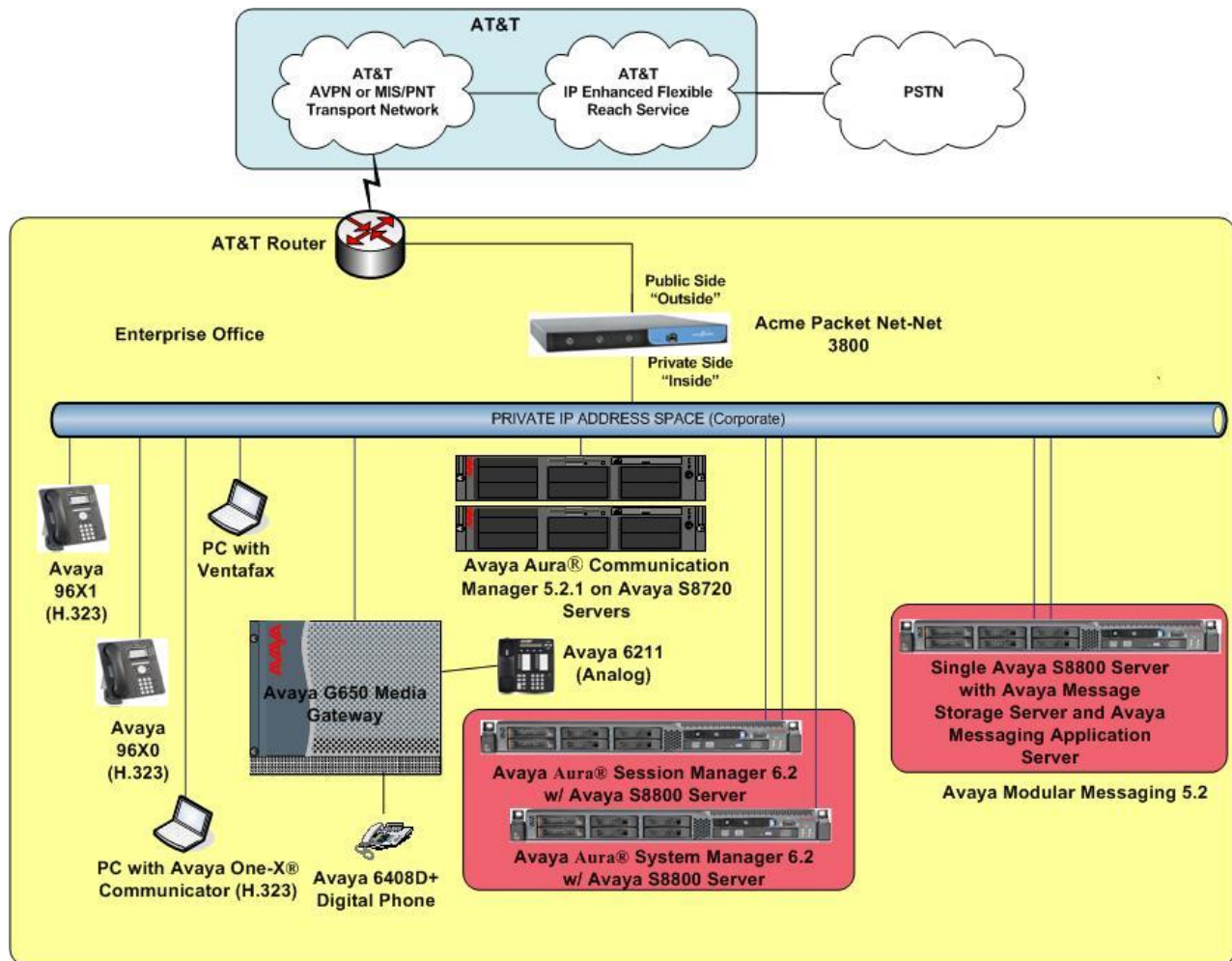


Figure 1: Reference Configuration

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their configurations. For security purposes, real IP addresses and DID numbers were not included.

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

Component	Illustrative Value in these Application Notes
Avaya Aura® System Manager	
Management IP Address	10.80.150.209
Avaya Aura® Session Manager	
Management IP Address	10.80.150.210
Network IP Address	10.64.19.210
Avaya Aura® Communication Manager	
Control LAN (C-LAN) IP Address	10.80.130.206
Media Processor (MedPro) IP Address	10.80.130.207
Avaya Aura® Communication Manager extensions	50xxx
Acme Packet Session Border Controller	
IP Address of “Outside” (Public) Interface (connected to AT&T Access Router/IP Flexible Reach-Enhanced Features service)	192.168.62.51
IP Address of “Inside” (Private) Interface (connected to Avaya Aura® Session Manager)	10.80.130.250
AT&T IP Flexible Reach-Enhanced Features service	
Border Element IP Address	192.242.225.210

Table 1: Illustrative Values Used in this Compliance Test

3.2. Call Flows

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

3.2.1. Inbound

The first call scenario illustrated in **Figure 2** 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 Acme Packet SBC.
4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines 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.

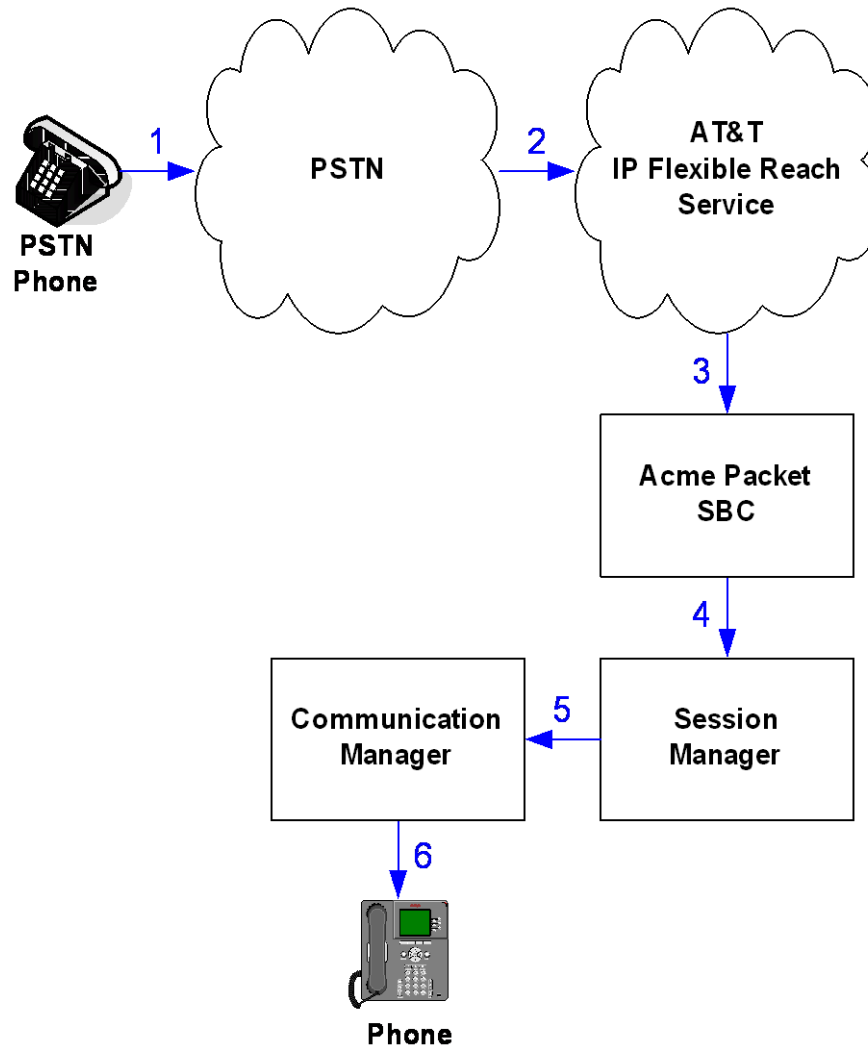


Figure 2: Inbound AT&T IP Flexible Reach Call

3.2.2. Outbound

The second call scenario illustrated in **Figure 3** is an outbound call initiated on Communication Manager, routed to Session Manager and is subsequently sent to the Acme SBC for delivery to AT&T IP Flexible Reach service.

1. 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 Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to the Acme Packet SBC.
4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach service.
5. The AT&T IP Flexible Reach service delivers the call to PSTN.

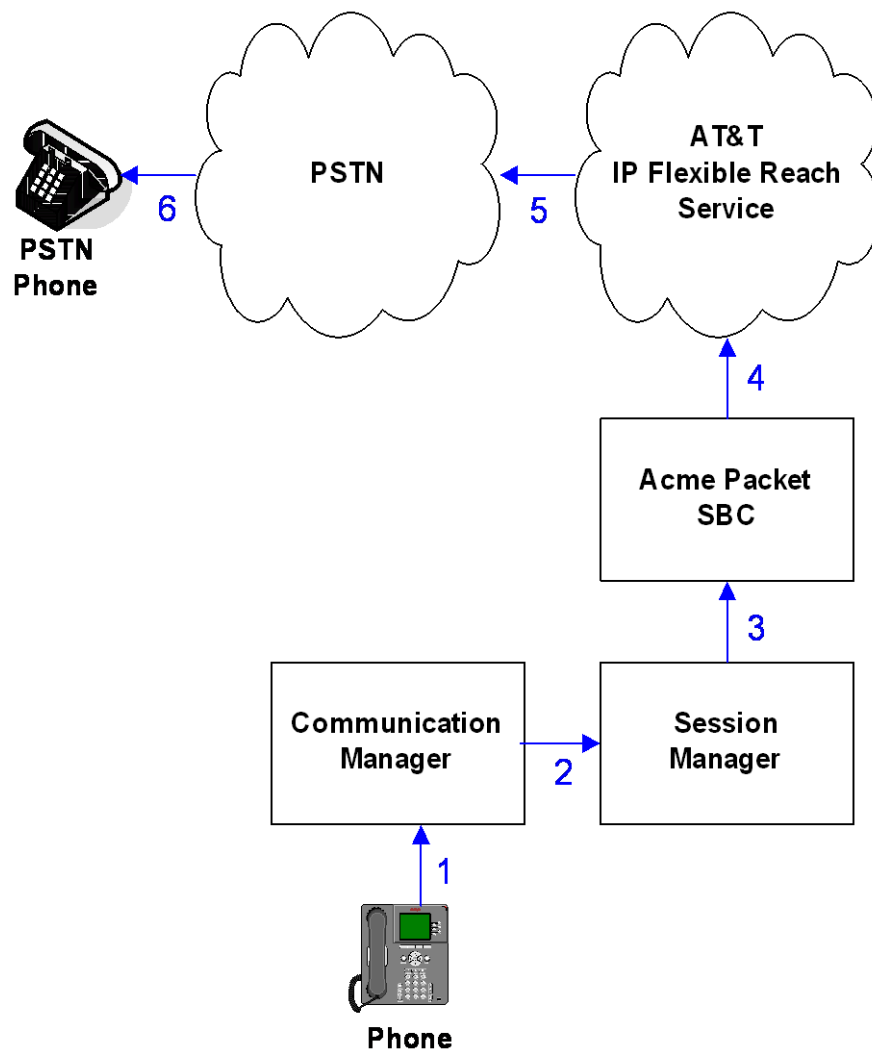


Figure 3: Outbound AT&T IP Flexible Reach Call

3.2.3. Call Forward Re-direction (Diversion Header)

The third call scenario illustrated in **Figure 4** 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.

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

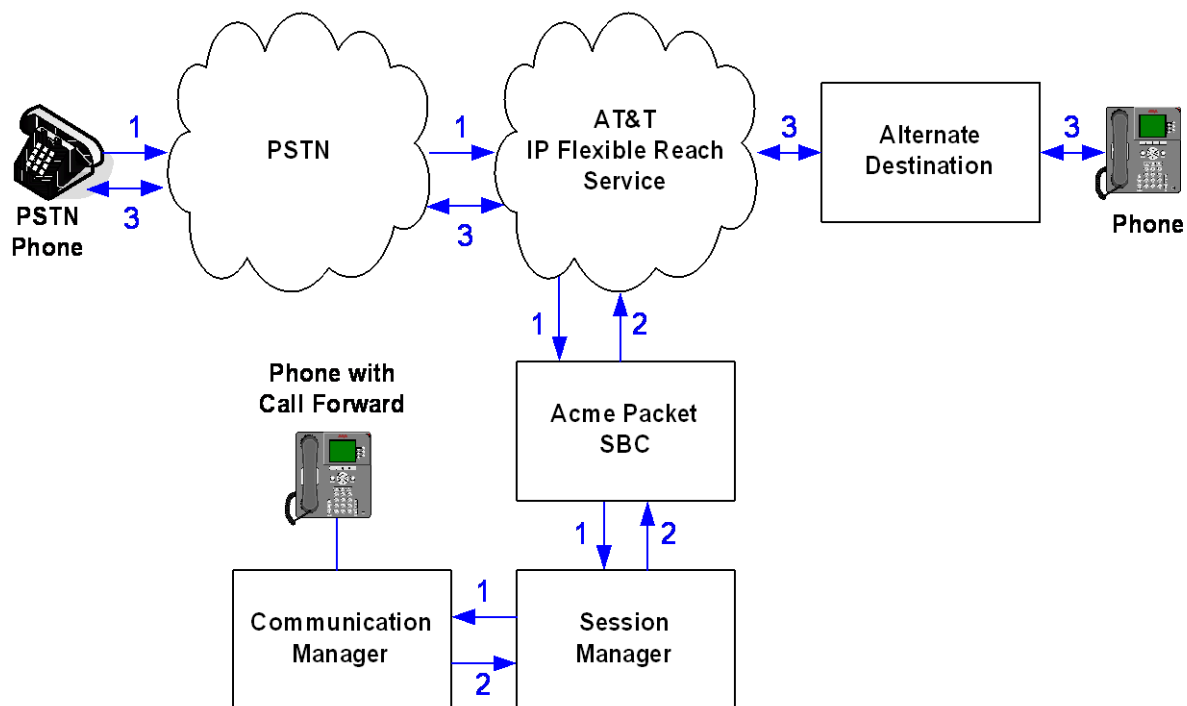


Figure 4: Re-directed (e.g., Call Forward) AT&T IP Flexible Reach Call

3.2.4. Coverage to Voicemail

The call scenario illustrated in **Figure 5** 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. Note that this call scenario was not executed but is expected to work.

1. Same as the first call scenario in **Section 3.2.1**.
2. The called Communication Manager phone does not answer the call, and the call covers to the phone's voicemail. Communication Manager forwards³ the call to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines 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.

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

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

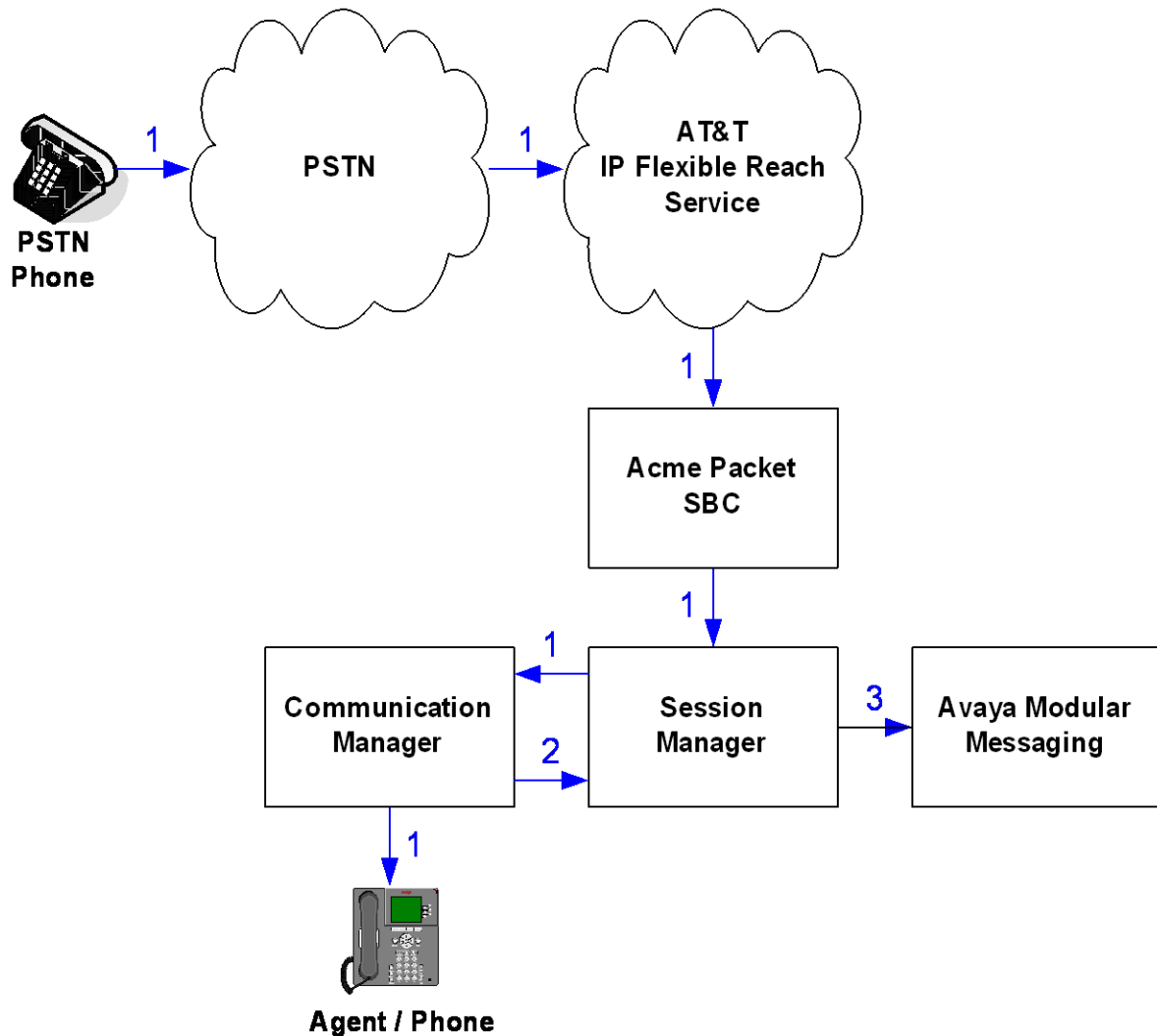


Figure 5: Coverage to Voicemail

3.2.5. AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow

This section describes the call flow used for AT&T IP Flexible Reach-Enhanced Features service which uses SIP-Refer method for off-net blind transfers. The call scenario illustrated in 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 vector. The vector answers the call and then redirects the call back to the AT&T IP Flexible Reach service for routing to an alternate destination.

1. A PSTN phone originates a call to an AT&T IP Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service routes the call to the Acme Packet SBC.

4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Communication Manager routes the call to a vector, which answers the call and plays an announcement, and attempts to redirect the call by sending a SIP REFER message back out on the SIP trunk on which the inbound call arrived. The SIP REFER message specifies the alternate destination, and is routed back through Session Manager and then the Acme Packet SBC to the AT&T IP Flexible Reach service.
7. The AT&T IP Flexible Reach service places a call to the target party (alternate destination) and upon answer, connects the calling party to the target party.
8. The AT&T IP Flexible Reach service clears the call on the referring party (Communication Manager).

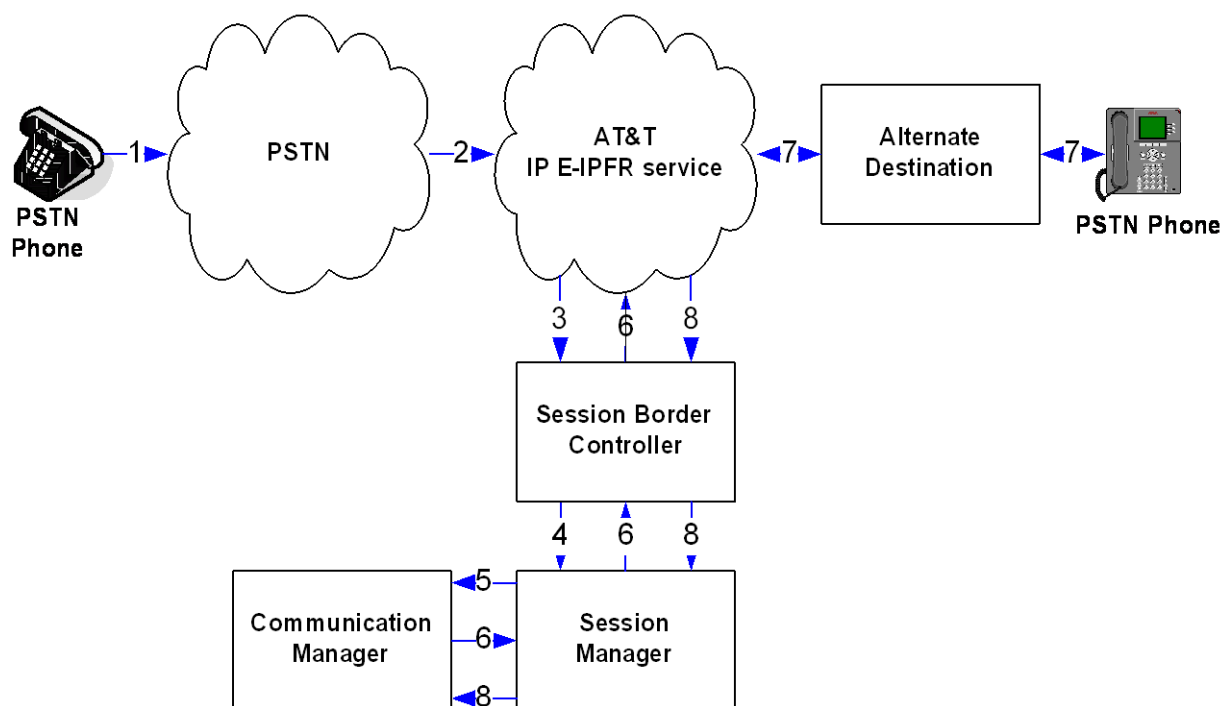


Figure 6: Inbound AT&T IP Flexible Reach – Post-Answer SIP REFER Redirection Call

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya S8800 Server	Avaya Aura® System Manager 6.2 SP5 (6.1.0.0.7345-6.1.5.502) System Platform 6.0.3.3.3
Avaya S8800 Server	Avaya Aura® Session Manager 6.2 SP5 (6.2.2.0.62205)

Avaya S8720 Server	Avaya Aura® Communication Manager 5.2.1 SP13 ⁵ (02.1.016.4-19880)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW15 FW054
TN799DP Control-LAN (C-LAN)	HW01 FW040
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW062
TN2501AP VAL-ANNOUNCEMENT	HW03 FW018
TN2224CP Digital Line	HW08 FW015
TN793B Analog Line	HW05 FW011
Avaya 9650 IP Telephone	H.323 Version S3.11b
Avaya 9620C IP Telephone	H.323 version S3.11b
Avaya 9611G IP Telephone	H.323 Version S6.2009 ⁶
Avaya one-X® Communicator	6.1.1.02-SP1-32858
Avaya Digital Telephone 6408D+	
Avaya Analog phone	-
Fax device	Ventafax Home Version 6.1.59.144
Acme Packet Net-Net 3800	SCX6.2.0 MR-6 Patch 5 (Build 916)
AT&T IP Flexible Reach-Enhanced Features service using AVPN/MIS-PNT transport service connection	VNI 23

Table 2: Equipment and Software Versions

⁵ For sequential ring inbound calls from PSTN, AT&T E-IPFR service sends an INVITE with a=inactive in its SDP. When Communication Manager sends a 200 OK, AT&T E-IPFR service sends a re-INVITE with no SDP and Communication Manager sends a=inactive again. AT&T E-IPFR service expects a=sendrecv and hence no audio path is established between two endpoints. Service Pack 13 is required to resolve this issue.

⁶ This is the minimum firmware version required for all 96x1 IP telephones to resolve the negative Round Trip Delay in RTCP calculations.

5. Configure Avaya Aura® Session Manager Release 6.2

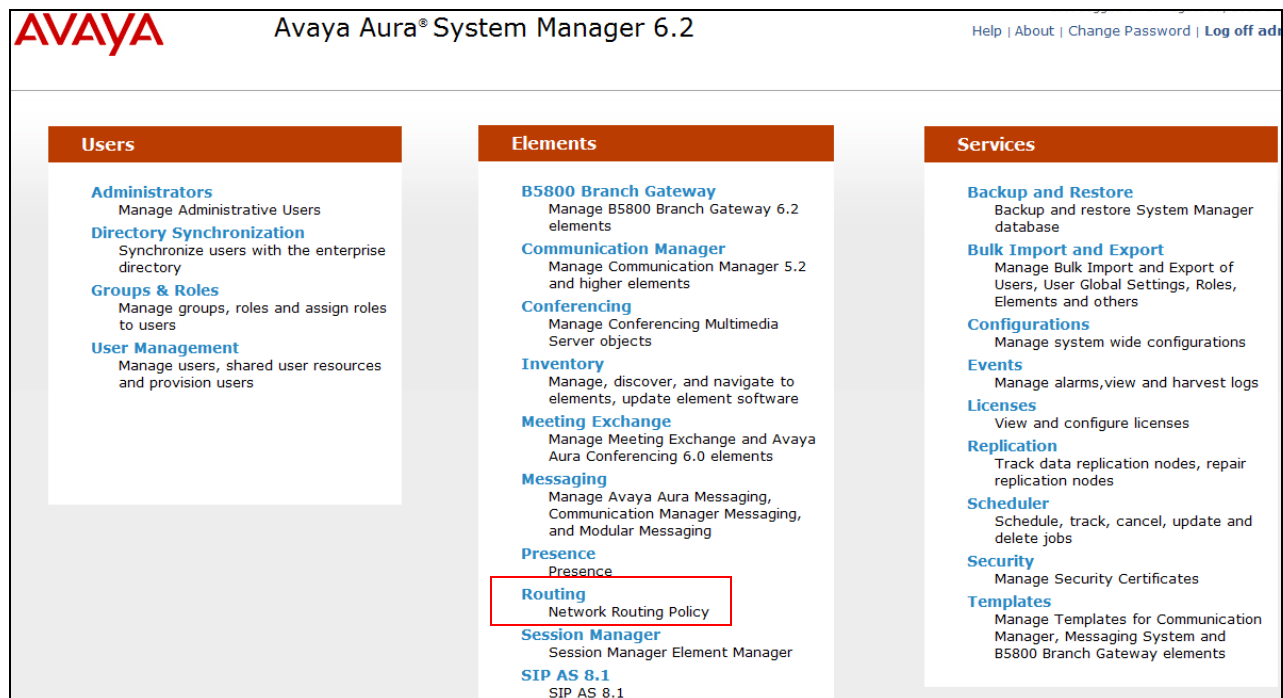
This section illustrates relevant aspects of the Session Manager configuration used in the verification of this compliance test solution for supporting AT&T IP Flexible Reach service.

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Refer to [1] to [4] for further details if necessary.

The following administration activities are described:


- Define SIP Domain
- Define Locations for routing purposes
- Configure the Adaptation Modules that are associated with various SIP Entities
- Define SIP Entities for Session Manager, Communication Manager, Acme Packet SBC, etc
- Define Entity Links between various SIP entities
- Define Routing Policies associated with Communication Manager, Acme Packet SBC, etc
- Define Dial Patterns which in conjunction with Routing Policies determine to which entity a call is routed to

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “<http://<ip-address>>”, where <ip-address> is the IP address of System Manager and logging in with the appropriate credentials. Once logged in, navigate to **Elements**→**Routing**.



System Manager Home Page

The screen below shows the various sub-headings with explanation of the left navigation menu that are referenced in this section.



Avaya Aura® System Manager 6.2

Last Logged on at August 29, 2012 3:35 PM

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

Routing

[Domains](#)
[Locations](#)
[Adaptations](#)
[SIP Entities](#)
[Entity Links](#)
[Time Ranges](#)
[Routing Policies](#)
[Dial Patterns](#)
[Regular Expressions](#)
[Defaults](#)

Home / Elements / Routing

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)

Network Routing Policy Page

AT:Reviewed
SPOC 10/1/2012

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

20 of 68
CM521SM62APEFR

5.1. SIP Domain

Navigate to **Routing→Domains** and click **New** (not shown). The following screen shows the domain used in this reference configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', and 'Dial Patterns'. The main content area is titled 'Domain Management' and shows a table with one item: 'attavaya.com'. The table has columns for Name, Type (sip), Default, and Notes (SIP Domain for ATT Testing). Buttons for 'Commit' and 'Cancel' are visible.

Name	Type	Default	Notes
* attavaya.com	sip	<input type="checkbox"/>	SIP Domain for ATT Testing

SIP Domains

5.2. Locations

Navigate to **Routing→Locations** and click **New** (not shown). The following screens show Location Details for various locations used in this AT&T IP Flexible Reach service testing.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left sidebar contains a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', and 'Time Ranges'. The main content area is titled 'Location Details' and shows the 'General' tab. The 'Name' field is set to 'SessionManager' and the 'Notes' field is set to 'Session Manager'. Buttons for 'Commit' and 'Cancel' are visible.

* Name: SessionManager
Notes: Session Manager

Session Manager Location Details

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Location Details' and shows the 'General' tab. The 'Name' field is set to 'Acme_SBC_130' and the 'Notes' field is set to 'SBC to ATT'. Below the 'General' tab, there are sections for 'Overall Managed Bandwidth' and 'Per-Call Bandwidth Parameters'. The 'Default Audio Bandwidth' is set to 80 Kbit/sec. At the bottom, there is a 'Location Pattern' section with a table showing one item: '10.80.130.250'. Buttons for 'Add', 'Remove', 'Commit', and 'Cancel' are visible.

* Name: Acme_SBC_130
Notes: SBC to ATT

Overall Managed Bandwidth
Managed Bandwidth Units: Kbit/sec
Total Bandwidth:

Per-Call Bandwidth Parameters
* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern
Add Remove
1 Item Refresh
Filter: Enable

IP Address Pattern	Notes
* 10.80.130.250	

Acme Packet SBC Location Details

AVAYA

Avaya Aura® System Manager 6.2

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

Routing

Home / Elements / Routing / Locations

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Location Details

Commit

Cancel

General

* Name:

Location_130

Notes:

Subnet 130

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

* Latency before Overall Alarm Trigger:

5

Minutes

* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.80.130.*	

Subnet 130 Location Details

AT:Reviewed
SPOC 10/1/2012

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

22 of 68
CM521SM62APEFR

5.3. Configure Adaptations

The following screen displays the adaptations used for inbound calls to support AT&T IP Flexible Reach service along with Enhanced Features like simultaneous and sequential ring. In this reference configuration, DID **7323680195** was used for simultaneous ring feature where an INVITE is sent to both extensions **50002** and **50004** and DID **732368096** was used for sequential ring feature where extension **50004** rings first and if not answered extension **50002** will ring. Additionally, this adaptation was used for calls which do not require NCR to be enabled as shown in **Section 6.6.1**.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Adaptations'. It displays 'Adaptation Details' for 'ATT-CLAN05'. The 'General' tab is active, showing fields for 'Adaptation name', 'Module name' (DigitConversionAdapter), 'Module parameter' (fromto=true osrcd=attavaya.com), 'Egress URI Parameters', and 'Notes' (Adaptation used for CM CLAN). Below this, there are two sections: 'Digit Conversion for Incoming Calls to SM' (0 items) and 'Digit Conversion for Outgoing Calls from SM' (4 items). The outgoing calls section contains a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 7323680193	* 10	* 10		* 10	50001	destination		
* 7323680195	* 10	* 10		* 10	50002	destination		Simul Ring first, Sequential Rin
* 7323680196	* 10	* 10		* 10	50004	destination		Sequential Ring first, Simul Rin

Communication Manager Adaptations NCR disabled calls

The following screen shows the adaptation used for calls routed to Communication Manager trunk with NCR enabled. See **Section 2.2** and **Section 6.6.2** for further details.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation name: ATT_CLAN02

Module name: DigitConversionAdapter

Module parameter: fromto=true osrcd=attavaya.com

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*7323680194	*10	*20		*10	2018	destination		Test Blind Transfer

Communication Manager Adaptations NCR enabled calls

The following screen shows the adaptation used for outbound calls to AT&T IP Flexible Reach service. The **Module parameter** field is set to **fromto=true iodstd=attavaya.com osrcd=192.168.62.51** (IP Address of the external interface of Acme Packet SBC) **odstd=135.242.225.210** (IP Address of AT&T IP Flexible Reach Border Element)

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation name: AT&T Adaptations

Module name: AttAdapter

Module parameter: fromto=true iodstd=attavaya.com

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM

Add Remove

Acme Packet SBC Adaptation

5.4. SIP Entities

The following screens show the entities along with Entity links configured for AT&T IP Flexible Reach service. See **Section 5.5** for Entity link configuration.

Note – In this reference configuration TCP is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS to be used as transport protocol when possible.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The left sidebar shows a navigation menu with options like Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration fields for the 'DenverSM' entity are as follows:

- Name:** DenverSM
- FQDN or IP Address:** 10.64.19.210
- Type:** Session Manager
- Notes:** Session Manager
- Location:** SessionManager
- Outbound Proxy:** (empty)
- Time Zone:** America/Denver
- Credential name:** (empty)

Below the general settings is the 'SIP Link Monitoring' section, which is set to 'Use Session Manager Configuration'. The 'Entity Links' section shows a table with 4 items, each representing a link between the 'DenverSM' entity and another entity (Loc19-CM Messaging, AcmeSBCATT-5060, CM5.2CLAN1A02, and CM5.2CLAN1A05) using either TLS or TCP protocols. The 'Port' section shows two items: TCP Failover port (5060) and TLS Failover port (5061), both for the domain attavaya.com. The 'SIP Responses to an OPTIONS Request' section is currently empty.

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
DenverSM	TLS	5071	Loc19-CM Messaging	5071	Trusted
DenverSM	TCP	5060	AcmeSBCATT-5060	5060	Trusted
DenverSM	TCP	5060	CM5.2CLAN1A02	5060	Trusted
DenverSM	TCP	5060	CM5.2CLAN1A05	5060	Trusted

Port	Protocol	Default Domain	Notes
5060	TCP	attavaya.com	TCP port for ATT test domain
5061	TLS	attavaya.com	TLS port for ATT test domain

Session Manager Entity

AVAYA

Avaya Aura® System Manager 6.2

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

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit

Cancel

General

* Name:

AcmeSBCATT-5060

* FQDN or IP Address:

10.80.130.250

Type:

Other

Notes:

Acme SBC to ATT

Adaptation:

AT&T Adaptations

Location:

Acme_SBC_130

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

Supports Call Admission Control:

☐

Shared Bandwidth Manager:

☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Add

Remove

1 Item

Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	DenverSM	TCP	* 5060	AcmeSBCATT-5060	* 5060	Trusted

Acme Packet SBC Entity

The following screen shows SIP Entity configured for the Communication Manager trunk group with NCR disabled. See **Section 2.2** and **Section 6.6.1** for further details.

AVAYA

Avaya Aura® System Manager 6.2

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

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit

Cancel

Help ?

General

* Name:

CM5.2CLAN1A05

* FQDN or IP Address:

10.80.130.206

Type:

CM

Notes:

CLAN on CM5.2 at 1A05

Adaptation:

ATT-CLAN05

Location:

Location_130

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

Supports Call Admission Control:

☐

Shared Bandwidth Manager:

☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

Add

Remove

1 Item

Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	DenverSM	TCP	* 5060	CM5.2CLAN1A05	* 5060	Trusted

Communication Manager Entity (CLAN1A05)

The following screen shows SIP Entity configured for the Communication Manager trunk group with NCR enabled. See **Section 2.2** and **Section 6.6.2** for further details.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The left sidebar shows a navigation menu with options like Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and 'General'. It contains various configuration fields: Name (CM5.2CLAN1A02), FQDN or IP Address (10.80.130.204), Type (CM), Notes (Entity to CM Trunk with NCR enable), Adaptation (ATT_CLAN02), Location (Location_130), Time Zone (America/Denver), Override Port & Transport with DNS SRV (unchecked), SIP Timer B/F (4 seconds), Credential name, Call Detail Recording (none), SIP Link Monitoring (Use Session Manager Configuration), Supports Call Admission Control (unchecked), Shared Bandwidth Manager (unchecked), Primary Session Manager Bandwidth Association, and Backup Session Manager Bandwidth Association. Below these is the 'Entity Links' section with 'Add' and 'Remove' buttons. At the bottom, there is a table with 1 item, showing a link between 'DenverSM' and 'CM5.2CLAN1A02' on port 5060 with a 'Trusted' connection policy.

AVAYA Avaya Aura® System Manager 6.2 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

[Commit](#) [Cancel](#)

General

* Name: CM5.2CLAN1A02

* FQDN or IP Address: 10.80.130.204

Type: CM

Notes: Entity to CM Trunk with NCR enable

Adaptation: ATT_CLAN02

Location: Location_130

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

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

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

1 Item [Refresh](#) Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	DenverSM	TCP	* 5060	CM5.2CLAN1A02	* 5060	Trusted

Communication Manager Entity (CLAN1A02)

5.5. Entity Links

The following screens show the entity links configured for this reference configuration.

The screen below shows an Entity link configured for the Communication Manager trunk group with NCR disabled.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left sidebar contains a menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, and Dial Patterns. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row shows: Name: SM-CM5.2CLAN1A05, SIP Entity 1: DenverSM, Protocol: TCP, Port: 5060, SIP Entity 2: CM5.2CLAN1A05, Port: 5060, Connection Policy: Trusted, Notes: To CM5.2.1 CLAN 1A05.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM-CM5.2CLAN1A05	* DenverSM	TCP	* 5060	* CM5.2CLAN1A05	* 5060	Trusted	To CM5.2.1 CLAN 1A05

Entity link between Session Manager and Communication Manager (CLAN1A05)

The screen below shows an Entity link configured for the Communication Manager trunk group with NCR enabled.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left sidebar contains a menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, and Dial Patterns. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row shows: Name: SM-CM5.2CLAN1A02, SIP Entity 1: DenverSM, Protocol: TCP, Port: 5060, SIP Entity 2: CM5.2CLAN1A02, Port: 5060, Connection Policy: Trusted, Notes: To CLAN1A02 with NCR.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM-CM5.2CLAN1A02	* DenverSM	TCP	* 5060	* CM5.2CLAN1A02	* 5060	Trusted	To CLAN1A02 with NCR

Entity link between Session Manager and Communication Manager (CLAN1A02)

The screenshot shows the Avaya Aura System Manager 6.2 interface. The left sidebar contains a menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, and Dial Patterns. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row shows: Name: SM-AcmeSBCATT-TCI, SIP Entity 1: DenverSM, Protocol: TCP, Port: 5060, SIP Entity 2: AcmeSBCATT-5060, Port: 5060, Connection Policy: Trusted, Notes: To ATT Acme SBC.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM-AcmeSBCATT-TCI	* DenverSM	TCP	* 5060	* AcmeSBCATT-5060	* 5060	Trusted	To ATT Acme SBC

Entity link between Session Manager and Acme Packet SBC

5.6. Time Ranges

The following screen shows the time range used for AT&T IP Flexible Reach service testing.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions

1 Item Refresh Filter: Enable

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
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

Time Range

5.7. Routing Policies

The following screens show routing policies along with dial patterns defined for AT&T IP Flexible Reach service. See **Section 5.8** for dial pattern configuration.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: ToCM5.2CLAN1A05

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM5.2CLAN1A05	10.80.130.206	CM	CLAN on CM5.2 at 1A05

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

1 Item Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
732368019	10	10	<input type="checkbox"/>	attavaya.com	Acme_SBC_130	

Routing Policy for Communication Manager (CLAN1A05)

Avaya Aura® System Manager 6.2

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

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit

Cancel

General

Name

ToCM5.2CLAN1A02

Disabled

☐

Retries

0

Notes

To trunk_group with NCR enabled

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM5.2CLAN1A02	10.80.130.204	CM	Entity to CM Trunk with NCR enabled

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"/>	7323680194	10	10	<input type="checkbox"/>	attavaya.com	Acme_SBC_130	

Routing Policy for Communication Manager (CLAN1A02)

Avaya Aura® System Manager 6.2

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

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit

Cancel

Help ?

General

* Name:

To_ATTAcme5060

Disabled:

☐

* Retries:

0

Notes:

Routing Policy to Acme connected

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AcmeSBCATT-5060	10.80.130.250	Other	Acme SBC to ATT

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

9 Items

Refresh

Filter: Enable

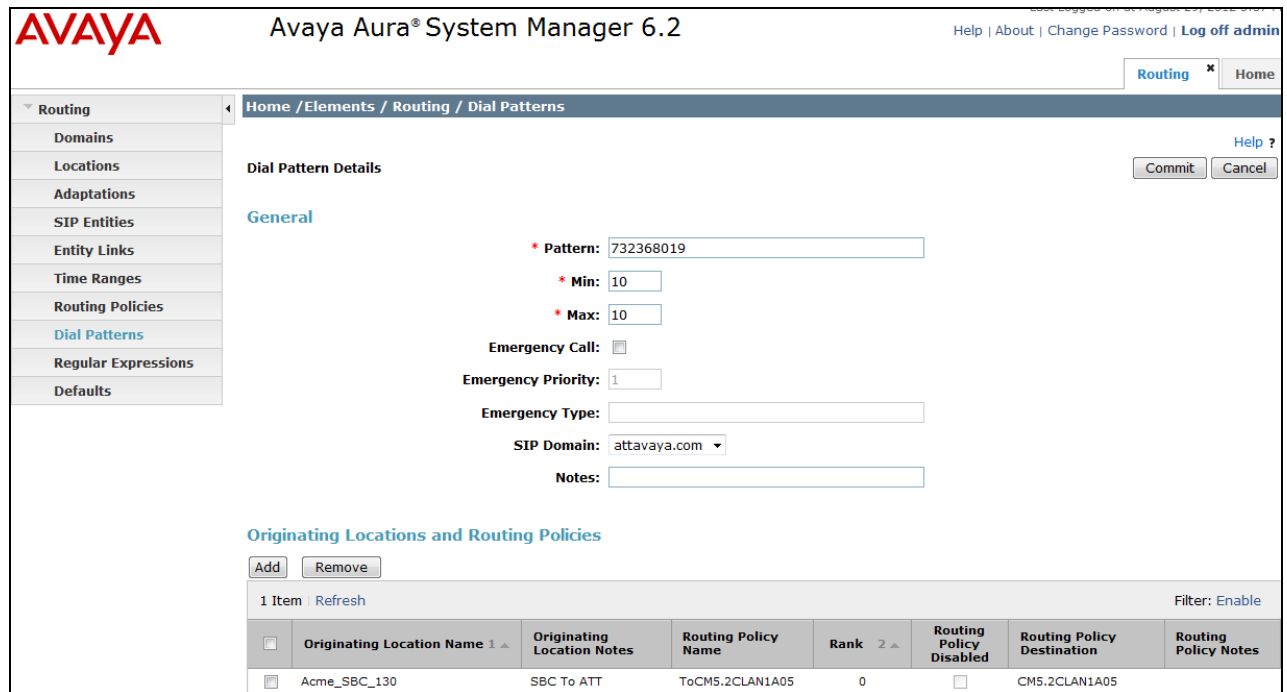
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	*	3	13	<input type="checkbox"/>	attavaya.com	Location_130	To handle Call Forwarding Scenarios
<input type="checkbox"/>	0	1	1	<input type="checkbox"/>	attavaya.com	Location_130	Operator Assisted calls
<input type="checkbox"/>	01141	5	36	<input type="checkbox"/>	attavaya.com	Location_130	International calls
<input type="checkbox"/>	173236801	11	11	<input type="checkbox"/>	attavaya.com	Location_130	Loopback calls via ATT network to CM
<input type="checkbox"/>	1800	11	11	<input type="checkbox"/>	attavaya.com	Location_130	
<input type="checkbox"/>	1800	11	11	<input type="checkbox"/>	attavaya.com	Acme_SBC_130	
<input type="checkbox"/>	303538	10	10	<input type="checkbox"/>	attavaya.com	Location_130	
<input type="checkbox"/>	732	10	10	<input type="checkbox"/>	attavaya.com	Location_130	
<input type="checkbox"/>	8	10	10	<input type="checkbox"/>	attavaya.com	Location_130	

Select : All, None

Routing Policy for Acme Packet SBC

5.8. Dial Patterns

The following screens show dial patterns configured in this reference configuration.



Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 732368019

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: attavaya.com

Notes:

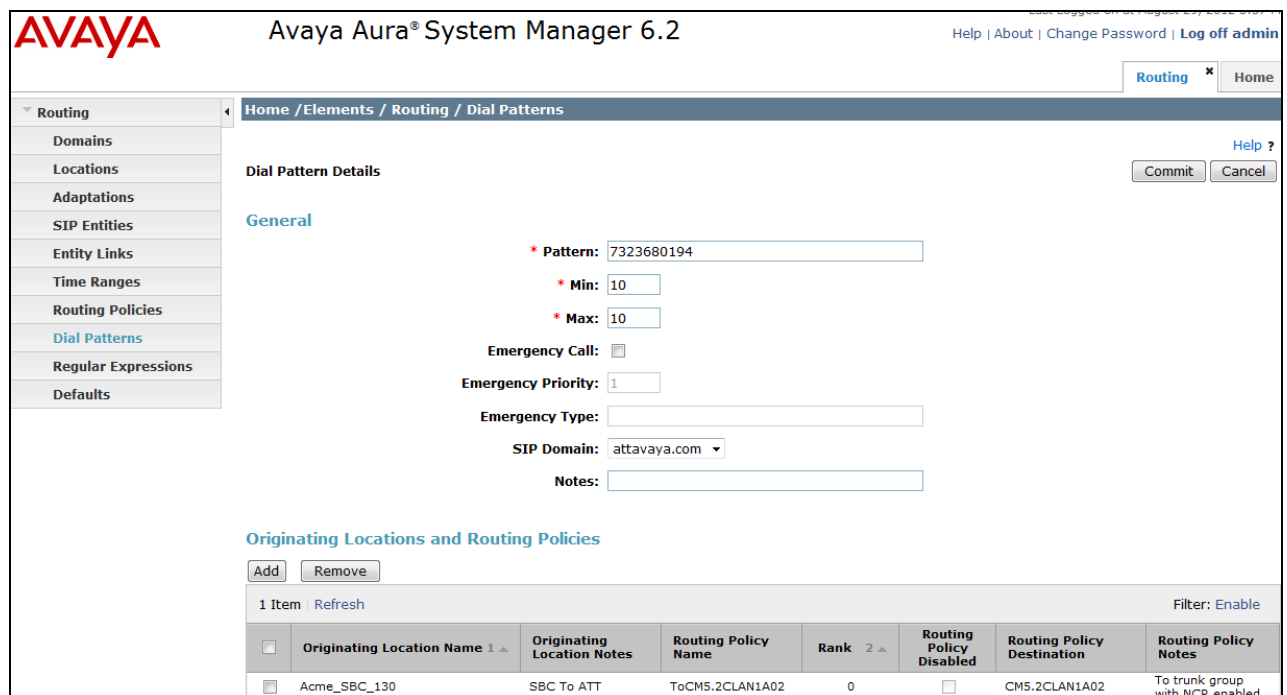
Originating Locations and Routing Policies

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"/>	Acme_SBC_130	SBC To ATT	ToCMS.2CLAN1A05	0	<input type="checkbox"/>	CMS.2CLAN1A05	

Dial Pattern for Inbound Calls to Communication Manager (CLAN1A05)



Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 7323680194

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: attavaya.com

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"/>	Acme_SBC_130	SBC To ATT	ToCMS.2CLAN1A02	0	<input type="checkbox"/>	CMS.2CLAN1A02	To trunk group with NCR enabled

Dial Pattern for Inbound Calls to Communication Manager (CLAN1A02)

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 303538

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: attavaya.com

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"/>	Location_130	Subnet 130	To_ATTAcme5060	0	<input type="checkbox"/>	AcmeSBCATT-5060	Routing Policy to Acme connected to ATTBE

Dial Pattern for Outbound Calls

The following screen show the dial pattern configured to support network based call forwarding features setup listed in **Section 2.1** under AT&T IP Flexible Reach-Enhanced Features. See corresponding configuration for Communication Manager in **Section 6.8.3**.

Avaya Aura® System Manager 6.2

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: *

* Min: 3

* Max: 13

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: attavaya.com

Notes: To handle Call Forwarding Scenarios

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"/>	Location_130	Subnet 130	To_ATTAcme5060	0	<input type="checkbox"/>	AcmeSBCATT-5060	Routing Policy to Acme connected to ATTBE

Dial Pattern for additional Network Features

5.9. Avaya Aura® Session Manager Administration

Navigate to **Home**→**Elements**→**Session Manager**→**Session Manager Administration** and in **Session Manager Instances** select the appropriate Session Manager already configured. The following screen shows the Session Manager instance **DenverSM** used in this reference configuration.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top header includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and navigation links: "Help | About | Change Password | Log off admin". Below the header is a breadcrumb trail: "Home / Elements / Session Manager / Session Manager Administration". A left sidebar contains a menu with options: "Session Manager", "Dashboard", "Session Manager Administration", "Communication Profile Editor", "Network Configuration", "Device and Location Configuration", "Application Configuration", "System Status", "System Tools", and "Performance". The main content area is titled "View Session Manager" and includes a "Return" button. It features a tabbed interface with "General" and "Security Module" tabs. The "General" tab is active, showing configuration details for the "DenverSM" instance. The "Security Module" tab is also visible, showing IP address and network settings.

Field	Value
SIP Entity Name	DenverSM
Description	Session Manager
Management Access Point Host Name/IP	10.80.150.210
Direct Routing to Endpoints	Enable
SIP Entity IP Address	10.64.19.210
Network Mask	255.255.255.0
Default Gateway	10.64.19.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

View Session Manager (DenverSM)

6. Configure Avaya Aura® Communication Manager 5.2.1

In this reference configuration Communication Manager 5.2.1 is provisioned in an Access Element configuration, supporting H.323 and Digital endpoints (SIP endpoints are not supported in this configuration). This section describes the administration steps for Communication Manager in support of the AT&T IP Flexible Reach service features listed in **Section 2**. These steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration, including stations, C-LAN, Media Processor, and announcement boards, etc., has already been performed. Consult [5] and [6] for further details if necessary.

Note – In the following sections, only the parameters that are highlighted in **bold** text are specifically applicable to these Application Notes. Other parameter values may or may not match based on local configurations. Also **NCR** feature may require additional licensing.

6.1. System Parameters

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

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

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

2. On **Page 4** of the **system-parameters customer-options**, verify that the **IP Trunks** field is set to **y**.

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

6.2. Dial Plan

The dial plan defines how the digit string will be used locally by Communication Manager. Note that the values shown below are examples used in the reference configuration. Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings:

- 3-digit Dial Access Codes (indicated with a **Call Type** of **dac**) beginning with the digit **1** (e.g. Trunk Access Codes, TACs, defined for trunk groups in this reference configuration conform to this format).
- 5-digit Extensions with a **Call Type** of **ext** beginning with the digits **5xxxxx** (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). Note – ARS is typically used for public trunk calls. In the reference configuration ARS is used for calls to PSTN via the AT&T IP Flexible Reach service (see **Section 6.8**).

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						
5	5	ext						
9	1	fac						

6.3. IP Node Names

Following screen shows the node names used for AT&T IP Flexible Reach service provisioning.

change node-names ip		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
Gateway001	10.80.130.1			
CLAN-1A02	10.80.130.204			
CLAN-1A05	10.80.130.206			
SM62	10.64.19.210			

6.4. IP Codec Parameters

Following screen shows the codec set used in this reference configuration.

change ip-codec-set 2

Page1 of 2

IP Codec Set

Codec Set: 2

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

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

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

6.5. IP Network Regions

Network Regions are used to group various Communication Manager Resources such as codecs, UDP port ranges, and inter-region communication. In this reference configuration only one network region was configured for all elements. Additional network regions can be defined if required. Enter **ip-network-region x**, where **x** is the number of an unused IP network region and configure as follows:

- **Name** - Enter any descriptive string.
- **Codec Set** – Set to Codec set configure in **Section 6.4**.
- **Intra and Inter IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible within the same region.
- **UDP Port Min:** - Set to **16384** (Required for AT&T IP Flexible Reach service)
- **UDP Port Max:** - Set to **32767** (Required for AT&T IP Flexible Reach service)

change ip-network-region 2		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain: attavaya.com		
Name: ATT Calls		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 2		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 16384		IP Audio Hairpinning? y
UDP Port Max: 32767		
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? y
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
AUDIO RESOURCE RESERVATION PARAMETERS		

On **Page 3** of the form, verify that region 2 is using codec set 2 as specified on **Page 1** (this field is automatically populated). If additional regions are configured, this form can dictate what codec set to be used for communication with elements belonging to different network regions.

change ip-network-region 2		Page 3 of 19
Source Region: 2		Inter Network Region Connection Management
		I M
		G A e
dst codec direct	WAN-BW-limits	Video Intervening Dyn A G a
rgn set WAN Units	Total Norm Prio Shr Regions	CAC R L s
1 2		
2		
3		

6.6. SIP Trunks

Two trunks are configured for testing in this reference configuration. All the parameters are same except on **Page 4** of the **trunk-group** form, NCR is enabled for one trunk group and disabled for the 2nd trunk group. See **Section 2** for further details.

6.6.1. SIP Trunk for AT&T IP Flexible Reach

This SIP trunk is used in this reference configuration for all features listed in **Section 2** except for Network-based Blind Transfer.

1. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group as shown in the following screen.

add signaling-group 5		Page 1 of 1
SIGNALING GROUP		
Group Number: 5	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
Near-end Node Name: CLAN_1A05	Far-end Node Name: SM62	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
Far-end Domain: attavaya.com	Far-end Network Region: 2	
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

2. Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. 5).

add trunk-group 5		Page 1 of 21
TRUNK GROUP		
Group Number: 5	Group Type: sip	CDR Reports: y
Group Name: ATT	COR: 1	TN: 1 TAC: 105
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Signaling Group: 5	
	Number of Members: 10	

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.

add trunk-group 5	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	
Disconnect Supervision - In? y Out? y	

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

add trunk-group 5	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: public	
	UII Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
Show ANSWERED BY on Display? y	

5. On **Page 4** of the **trunk-group** form:
- Set **Network Call Redirection?** to **n**. (Note: NCR feature may require additional licensing)
 - Set **Send Diversion Header?** field to **y**
 - Set **Support Request History?** field to **n**.
 - Set **Telephone Event Payload Type** field to the RTP payload type required by the AT&T IPFR-EF service (e.g. **100**).

add trunk-group 5	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? n	
Telephone Event Payload Type: 100	

6.6.2. SIP Trunk for AT&T IP Flexible Reach – Network Based Blind Transfer calls

This SIP trunk is used for network based blind transfer using vectors and only for inbound calls. See **Section 6.9** for vector configuration. Configuration for this trunk is similar to the trunk group configured in **Section 6.6.1** with the differences shown in the screens below:

add signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
Near-end Node Name: CLAN_1A02	Far-end Node Name: SM62	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 2	
Far-end Domain: attavaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

add trunk-group 2		Page 1 of 21
TRUNK GROUP		
Group Number: 2	Group Type: sip	CDR Reports: y
Group Name: ATT	COR: 1	TN: 1
Direction: incoming	Outgoing Display? n	TAC: 102
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Signaling Group: 2	
	Number of Members: 10	

On **Page 4** of the **trunk-group** form, set **Network Call Redirection?** to **y**.

add trunk-group 2		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? y		
Send Diversion Header? n		
Support Request History? n		
Telephone Event Payload Type: 100		

6.7. Public Unknown Numbering

In the public unknown numbering form, Communication Manager local extensions are converted to AT&T Flexible Reach numbers (previously assigned by AT&T) and directed to the “public” trunks defined in **Section 6.6**. Use the **change public-unknown-numbering 0** command to add entries for AT&T IP Flexible Reach service DIDs. Additionally, this form is used for inbound calls to populate the user part in **Contact** and **PAI** headers.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
5	5			5	
5	50001	5	7323680193	10	Total Administered: 3
5	50002	5	7323680194	10	Maximum Entries: 9999
5	50003	5	7323680195	10	

6.8. Outbound Call Routing From Avaya Aura® Communication Manager

Route pattern and ARS analysis table forms are configured for outbound calls to PSTN using AT&T IP Flexible Reach service.

6.8.1. Route Pattern

Route patterns are used to direct calls to the appropriate SIP trunk using either the Automatic Route Selection (ARS) or Automatic Alternate Routing (AAR) dialing tables. Use the **change route-pattern x** command, where **x** is an available route to define new route pattern. The following screen shows the route pattern (**3**) used to support AT&T IP Flexible Reach features.

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

6.8.2. ARS Dialing for AT&T IP Flexible Reach service

Automatic Route Selection (ARS) is used to direct calls to AT&T Flexible Reach service via the route pattern defined in **Section 6.8.1**. Following screen shows the entries made for ARS dialing to support outbound AT&T IP Flexible Reach service calls.

change ars analysis 1							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 15
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	1732	11	11	3	natl		n
	1303	11	11	3	natl		n

6.8.3. ARS Dialing for AT&T IP Flexible Reach-Enhanced Features

Following screen shows the entries made for ARS dialing to support additional AT&T IP Flexible Reach-Enhanced Features service calls.

- *72 – To enable Call Forwarding Unconditional
- *73 – To disable Call Forwarding Unconditional
- *90 – To enable Call Forwarding Busy
- *91 – To disable Call Forwarding Busy
- *92 – To enable Call Forwarding – Ring No Answer
- *93 – To disable Call Forwarding – Ring No Answer
- *94 – To enable Call Forwarding – Not Reachable
- *95 – To disable Call Forwarding – Not Reachable

Note: All these features are enabled on a particular line and multiple features can be enabled at the same time. Refer to AT&T feature documentation for priority order for these features.

change ars analysis *							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 15
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	*72	13	13	3	natl		n
	*73	3	3	3	natl		n
	*90	13	13	3	natl		n
	*91	3	3	3	natl		n
	*92	13	13	3	natl		n
	*93	3	3	3	natl		n
	*94	13	13	3	natl		n
	*95	3	3	3	natl		n

6.9. Post-Answer Redirection

This section provides an example of Post-Answer Redirection. In this example, the inbound call is routed to the VDN shown in screen below, which invokes the vector shown in the next screen.

```
display vdn 2018                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 2018
      Name*: NCR Ringback REFER
      Destination: Vector Number 18
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none

      VDN of Origin Annc. Extension*:
      1st Skill*:
      2nd Skill*:
      3rd Skill*:
* Follows VDN Override Rules
```

Sample VDN for Post-Answer Redirection

```
display vector 18                                     Page 1 of 6
                                         CALL VECTOR

      Number: 18      Name: NcrRefer_wUui
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock?
n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing?
y
      Prompting? y      LAI? n      G3V4 Adv Route? y      CINFO? n      BSR? y      Holidays? n
      Variables? y      3.0 Enhanced? y
01 #      NCR Refer with ringback
02 wait-time 2 secs hearing ringback
03 # Answer call with announcement
04 announcement 33007
05 # Refer
06 route-to number ~r3035381761 with cov n if unconditionally
10 #      Play this announcement only on redirect failure
11 disconnect after announcement 33008
12
```

Sample Vector for Post-Answer Redirection

6.10. Saving Translations

To save all Communication Manager provisioning changes, enter the command **save translations**.

7. Configure Acme Packet Session Border Controller (SBC)

These Application Notes assume that basic Acme Packet SBC administration has already been performed. The Acme Packet SBC configuration used in the reference configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Use **putty** or similar tool to access Acme Packet SBC for configuration. Consult with Acme Packet Support [7] for further details and explanations on the configuration below.

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

local-policy

from-address

*

to-address

*

source-realm

Enterprise

description

activate-time

N/A

deactivate-time

N/A

state

enabled

policy-priority

none

policy-attribute

next-hop

sag:SP_PROXY

realm

ATT

action

none

terminate-recursion

disabled

carrier

start-time

0000

end-time

2400

days-of-week

U-S

cost

0

app-protocol

state

enabled

methods

media-profiles

lookup

single

next-key

eloc-str-lookup

disabled

eloc-str-match

ANNOTATION: The local policy below governs the routing of SIP messages from the AT&T IPFR-EF service to Session Manager.

local-policy

from-address	*
to-address	*
source-realm	ATT
description	
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
policy-attribute	
next-hop	10.64.19.210
realm	Enterprise
action	none
terminate-recursion	disabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	

network-interface

name	wancom0
sub-port-id	0
description	
hostname	
ip-address	192.9.230.221
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	192.9.230.254
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0

retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	
ftp-address	
icmp-address	
snmp-address	
telnet-address	
ssh-address	

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

```

network-interface
  name s0p0
  sub-port-id 0
  description
  hostname
  ip-address 10.80.130.250
  pri-utility-addr
  sec-utility-addr
  netmask 255.255.255.0
  gateway 10.80.130.1
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain attavaya.com
  dns-timeout 11
  hip-ip-list 10.80.130.250
  ftp-address
  icmp-address 10.80.130.250
  snmp-address
  telnet-address
  ssh-address

```


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

```
network-interface
  name          s1p0
  sub-port-id    0
  description
  hostname
  ip-address     192.168.62.51
  pri-utility-addr
  sec-utility-addr
  netmask        255.255.255.128
  gateway        192.168.62.1
  sec-gateway
  gw-heartbeat
    state        disabled
    heartbeat     0
    retry-count   0
    retry-timeout 1
    health-score  0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout     11
  hip-ip-list     192.168.62.51
  ftp-address
  icmp-address    192.168.62.51
  snmp-address
  telnet-address
  ssh-address
```

ANNOTATION: The realm configuration **ATT** below represents the external network on which the AT&T IP Flexible Reach service resides, and applies the SIP manipulation **modSendRecv**.

```
realm-config
  identifier      ATT
  description
  addr-prefix     0.0.0.0
  network-interface s1p0:0
  mm-in-realm     enabled
  mm-in-network   enabled
  mm-same-ip      enabled
  mm-in-system    enabled
  bw-cac-non-mm   disabled
```

msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	modSendRecv
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled

delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled

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

realm-config

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

in-translationid
 out-translationid
 in-manipulationid
 out-manipulationid
 manipulation-string
 manipulation-pattern
 class-profile
 average-rate-limit 0
 access-control-trust-level none
 invalid-signal-threshold 0
 maximum-signal-threshold 0
 untrusted-signal-threshold 0
 nat-trust-threshold 0
 deny-period 30
 ext-policy-svr
 diam-e2-address-realm
 symmetric-latching disabled
 pai-strip disabled
 trunk-context
 early-media-allow
 enforcement-profile
 additional-prefixes
 restricted-latching none
 restriction-mask 32
 accounting-enable enabled
 user-cac-mode none
 user-cac-bandwidth 0
 user-cac-sessions 0
 icmp-detect-multiplier0
 icmp-advertisement-interval 0
 icmp-target-ip
 monthly-minutes 0
 net-management-control disabled
 delay-media-update disabled
 refer-call-transfer enabled
 dyn-refer-term disabled
 codec-policy
 codec-manip-in-realm disabled
 constraint-name
 call-recording-server-id
 xnq-state xnq-unknown
 hairpin-id 0
 stun-enable disabled
 stun-server-ip 0.0.0.0
 stun-server-port 3478
 stun-changed-ip 0.0.0.0

stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled

<p>ANNOTATION: The session agent below represents the Session Manager used in this reference configuration.</p>
--

session-agent	
hostname	SM61
ip-address	10.64.19.210
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP+TCP
realm-id	Enterprise
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	Proxy
loose-routing	enabled
send-media-session	enabled
response-map	

ping-method **OPTIONS;hops=1**
ping-interval **180**
ping-send-mode **keep-alive**
ping-all-addresses disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me enabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate 0
early-media-allow
invalidate-registrations disabled
rfc2833-mode none
rfc2833-payload 0
codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections TCP
tcp-keepalive enabled
tcp-reconn-interval 10
max-register-burst-rate 0
register-burst-window 0
sip-profile
sip-isup-profile

ANNOTATION: The session agent below represents the AT&T IPFR-EF service border element. The Acme Packet SBC will attempt to send calls to the border element based on successful responses to the OPTIONS **ping-method**. The AT&T IP Flexible Reach service border element is also specified in the **session-group** section below.

session-agent

hostname	135.242.225.210
ip-address	135.242.225.210
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	ATT
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled

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

ANNOTATION: The session agent below is used for failover testing to ATT IPFR-EF service. The state is changed to enabled when the testing is performed.

session-agent
 hostname **1.1.1.1**
 ip-address **1.1.1.1**
 port **5060**
 state **disabled**
 app-protocol **SIP**
 app-type
 transport-method **UDP**
 realm-id **ATT**
 egress-realm-id

description	ATT-Failover
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	

p-asserted-id
 trunk-group
 max-register-sustain-rate 0
 early-media-allow
 invalidate-registrations disabled
 rfc2833-mode none
 rfc2833-payload 0
 codec-policy
 enforcement-profile
 refer-call-transfer disabled
 reuse-connections NONE
 tcp-keepalive none
 tcp-reconn-interval 0
 max-register-burst-rate 0
 register-burst-window 0
 sip-profile
 sip-isup-profile

ANNOTATION: The **session group** below specifies the AT&T IPFR-EF service border element.

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

session-group
group-name SP_PROXY
description
state enabled
app-protocol SIP
strategy RoundRobin
dest
 1.1.1.1
 135.242.225.210
 trunk-group
 sag-recursion enabled
 stop-sag-recurse 401,407

ANNOTATION: The SIP interface below is used to communicate with the AT&T IPFR-EF service.

sip-interface
state enabled
realm-id ATT
description
sip-port
address 192.168.62.51

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

ccf-address
ecf-address
term-tgrp-mode none
implicit-service-route disabled
rfc2833-payload 101
rfc2833-mode transparent
constraint-name
response-map
local-response-map
ims-aka-feature disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive none
add-sdp-invite disabled
add-sdp-profiles
sip-profile
sip-isup-profile

ANNOTATION: The SIP interface below is used to communicate with the Avaya elements.

sip-interface

state enabled
realm-id Enterprise
description
sip-port
 address 10.80.130.250
 port 5060
 transport-protocol TCP
 tls-profile
 allow-anonymous all
 ims-aka-profile
carriers
trans-expire 0
invite-expire 0
max-redirect-contacts 0
proxy-mode
redirect-action
contact-mode none
nat-traversal none
nat-interval 30
tcp-nat-interval 90
registration-caching disabled
min-reg-expire 300
registration-interval 3600
route-to-registrar disabled
secured-network disabled

teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	rejectOptions
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	

ANNOTATION: The SIP manipulation shown below are used for modifying the **sendonly** value in SDP to **sendrecv**. See **Section 2.2**, bullet **1** for further details.

sip-manipulation

name	modSendRecv
description	Modify sendonly to sendrecv
split-headers	
join-headers	
header-rule	
name	modsendonly
header-name	Content-type
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	INVITE
match-value	
new-value	
element-rule	
name	modmline
parameter-name	application/sdp
type	mime
action	find-replace-all
match-val-type	any
comparison-type	case-sensitive
match-value	sendonly
new-value	sendrecv

ANNOTATION: The SIP manipulation shown below intercepts the SIP OPTIONS message from AT&T Border Element and respond with Acme Packet alive message.

sip-manipulation

name	rejectOptions
description	
split-headers	
join-headers	
header-rule	
name	RejectOpts
header-name	From
action	reject
comparison-type	case-sensitive
msg-type	request
methods	OPTIONS
match-value	
new-value	405:"Acme Packet is alive, check back later"

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

steering-pool

ip-address **192.168.62.51**
start-port **16384**
end-port **32767**
realm-id **ATT**

steering-pool

ip-address **10.80.130.250**
start-port **16384**
end-port **32767**
realm-id **Enterprise**

system-config

hostname **Enterprise-Acme**
description
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled enabled
enable-snmp-auth-traps disabled
enable-snmp-syslog-notify disabled
enable-snmp-monitor-traps disabled
enable-env-monitor-traps disabled
snmp-syslog-his-table-length 1
snmp-syslog-level WARNING
system-log-level WARNING
process-log-level NOTICE
process-log-ip-address 0.0.0.0
process-log-port 0
collect
 sample-interval 5
 push-interval 15
 boot-state disabled
 start-time now
 end-time never
 red-collect-state disabled
 red-max-trans 1000
 red-sync-start-time 5000
 red-sync-comp-time 1000
 push-success-trap-state disabled

call-trace	disabled
internal-trace	disabled
log-filter	all
default-gateway	192.168.62.1
restart	enabled
exceptions	
telnet-timeout	0
console-timeout	0
remote-control	enabled
cli-audit-trail	enabled
link-redundancy-state	disabled
source-routing	disabled
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
default-v6-gateway	::
ipv6-support	disabled
cleanup-time-of-day	00:00

8. Verification Steps

The following steps may be used to verify this reference configuration:

8.1. AT&T IP Flexible Reach

1. Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly. Repeat the above step for an outbound call.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

8.2. AT&T IP Flexible Reach-Enhanced Features

1. Based upon the DIDs provided for Network based Simultaneous Ring, verify that the primary and secondary endpoints ring at the same time and calls can be answered on either phone.
2. Based upon the DIDs provided for Network based Sequential Ring (Locate Me), verify that the primary endpoint rings for a designated time determined by the network and if not answered the secondary endpoint rings and call with talkpath can be verified at each endpoint.
3. Based upon the DIDs provided for Network based Blind Transfer (using Communication Manager vector generated REFER), the call can be referred/transferred off-net to another PSTN endpoint using AT&T IP Flexible reach network.
4. Verify that all network based call forwarding features listed in **Section 2.1** can be enabled and calls can be successfully re-directed and answered at the forwarded PSTN number.

8.3. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See [5] and [6] for more information.

- From the Communication Manager console connection, enter the command ***list trace tac xxx***, (not shown) where ***xxx*** is a trunk access code to verify that the inbound or outbound calls are using the right trunk groups. Similarly, ***list trace station***, ***list trace vdn***, and ***list trace vector***, ***status trunk*** and ***status station*** commands can be used on Communication Manager.

8.4. Avaya Aura® Session Manager

Navigate to **Home**→ **Elements**→ **Session Manager**→ **System Status** → **SIP Entity Monitoring** and click on the SIP Entity for which the status is required. Following screen shows status for the entity link between Session Manager and Acme Packet SBC.

Note: The Reason Code column indicates that Session Manager has received a **SIP 405 Method Not Allowed** response (normal for this reference configuration) to the **SIP OPTIONS** it generated. This response is sufficient for SIP Link Monitoring to consider the link up.

The screenshot displays the Avaya Aura® System Manager 6.2 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and links for Help, About, Change Password, and Log off admin. Below the navigation bar, a breadcrumb trail shows the path: Home / Elements / Session Manager / System Status / SIP Entity Monitoring. The left sidebar contains a menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a sub-header 'All Entity Links to SIP Entity: AcmeSBCATT-5060'. A 'Summary View' button is present. Below this, a table shows the connection status for one item, 'DenverSM'. The table has columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The data row shows 'DenverSM' with IP 10.80.130.250, Port 5060, Proto. TCP, Conn. Status Up, Reason Code 405 Method Not Allowed, and Link Status Up.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	DenverSM	10.80.130.250	5060	TCP	Up	405 Method Not Allowed	Up

9. Conclusion

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

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

10. References

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

Avaya Aura® Session Manager/System Manager

- [1] Administering Avaya Aura® Session Manager, Doc ID 03-603324, Issue 4, Feb 2011
- [2] Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Issue 2, November 2010
- [3] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, Issue 3.1, March 2011
- [4] Administering Avaya Aura® System Manager, Document Number 03-603324, June 2010

Avaya Aura® Communication Manager

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

Acme Packet Support (login required):

- [7] <http://www.acmepacket.com/support.htm>

AT&T IP Flexible Reach-Enhanced Features Service Descriptions:

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

©2012 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.