



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager R5.2.1, Avaya Aura® Session Manager R6.1 and Acme Packet Net-Net 6.2.0 with AT&T 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 with SIP Network Call Redirection, Avaya Aura® Session Manager R6.1, and the Acme Packet Net-Net 3800 with the AT&T IP Flexible Reach-Enhanced Features service using **AVPN** or **MIS/PNT** transport connections. 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. Note that these Application Notes are intended to supplement the separate document: *Applications Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.0 and Acme Packet Net-Net 6.2.0 with AT&T IP Flexible Reach SIP Trunk Service*.

Avaya Aura® Session Manager R6.1 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 R6.1 and the AT&T 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.....	3
2.	General Test Approach and Test Results.....	3
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results and Known Limitations	4
2.3.	Support	6
3.	Reference Configuration	7
3.1.	Illustrative Configuration Information	9
3.2.	Call Flows	10
4.	Equipment and Software Validated	11
5.	Configure Avaya Aura® Session Manager Release 6.1	12
5.1.	SIP Domain	13
5.2.	Locations	14
5.3.	Configure Adaptations	16
5.4.	SIP Entities.....	18
5.5.	Entity Links	20
5.6.	Time Ranges.....	20
5.7.	Routing Policies	21
5.8.	Dial Patterns	23
5.9.	Session Manager Administration	24
6.	Configure Avaya Aura® Communication Manager 5.2.1	25
6.1.	Dial Plan.....	25
6.2.	IP Node Names.....	26
6.3.	IP Network Regions	26
6.4.	IP Codec Parameters	26
6.5.	SIP Trunks.....	27
6.5.1.	SIP Trunk for AT&T IP Flexible Reach-Enhanced Features calls.....	27
6.6.	Public Unknown Numbering.....	29
6.7.	Outbound Call Routing From Avaya Aura® Communication Manager	29
6.7.1.	Route Pattern.....	29
6.7.2.	ARS Dialing.....	30
6.8.	Post-Answer Redirection.....	31
6.9.	Saving Translations	31
7.	Configure Acme Packet Session Border Controller (SBC)	32
8.	Verification Steps.....	51
9.	Conclusion	51
10.	References.....	52

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager with SIP Network Call Redirection, Avaya Aura® Session Manager R6.1, and the Acme Packet Net-Net 3800s¹ with the AT&T IP Flexible Reach-Enhanced Features service using **AVPN** or **MIS/PNT** transport connections. 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. Note that these Application Notes are intended to supplement the separate document: *Applications Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.0 and Acme Packet Net-Net 6.2.0 with AT&T IP Flexible Reach SIP Trunk Service*.

Avaya Aura® Session Manager R6.1 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 Aura® Communication Manager R5.2.1 Access Element configuration). Acme Packet Net-Net 3800 is the point of connection between Avaya Aura® Session Manager R6.1 and the AT&T IP Flexible Reach-Enhanced Features (IPFR-EF) service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

Note: For Sequential Ring inbound (Locate Me) calls from PSTN, AT&T IPFR-EF service sends an INVITE with a=inactive in its SDP. When Communication Manager sends a 200 OK, AT&T IPFR-EF service sends a re-INVITE with no SDP and Communication Manager sends a=inactive again. AT&T IPFR-EF service expects a=sendrecv and hence no audio path is established between two endpoints. A hot fix was delivered by Communication Manager development team which will be delivered in Service Pack 13.

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 that no AT&T IPFR-EF test cases involved Avaya Modular Messaging system.**
2. A laboratory version of the AT&T IPFR-EF 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.

¹Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

2.1. Interoperability Compliance Testing

The interoperability compliance testing with AT&T IPFR-EF service verified basic inbound and outbound call flows with focus on IPFR-EF feature test cases. **Section 3.2** provides additional call flow tested for AT&T IPFR-EF service. For call flows related to AT&T IP Flexible Reach service, please refer to [9, **Section 2.2**].

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. Following additional AT&T IPFR-EF were tested along with the AT&T IP Flexible Reach service features [9]:

- 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 Manager²
 - 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 verified³.

1. For inbound calls from AT&T IPFR-EF service, G.729b is offered as a priority codec but for outbound calls from Communication Manager, even if G.729b is the only codec being offered, AT&T IPFR-EF service responds with G.729a and the call is rejected by Communication Manager. The workaround is to offer G.729b followed by G.729a in the codec list so that inbound calls use G.729b and outbound calls use G.729a.
2. When the call is put on hold on Communication Manager, SDP with **a=sendonly** is sent to AT&T IPFR-EF 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.
3. When 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 IPFR-EF service which in turn acknowledges the REFER and a BYE is received by 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.
4. 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.

² Network based Blind Call Transfer uses Vectors and VDNs on Communication Manager. Phone based transfers (attended or unattended) are not supported.

³ Refer to [9] for test objectives, results and known limitation for the AT&T IP Flexible Reach basic service.

5. Unattended and Attended off-net transfer from Communication Manager phones is not supported.
6. 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.
- The Acme Packet SBC provides SIP Session Border Controller functionality, including address translation and SIP header manipulation between the AT&T IPFR-EF service and the enterprise internal network⁴. UDP transport protocol is used between the Acme Packet SBC and the AT&T IPFR-EF 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. AT&T IPFR-EF service does not have any test cases where Modular Messaging was used. Modular Messaging was left 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 IPFR-EF 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.

⁴ 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.

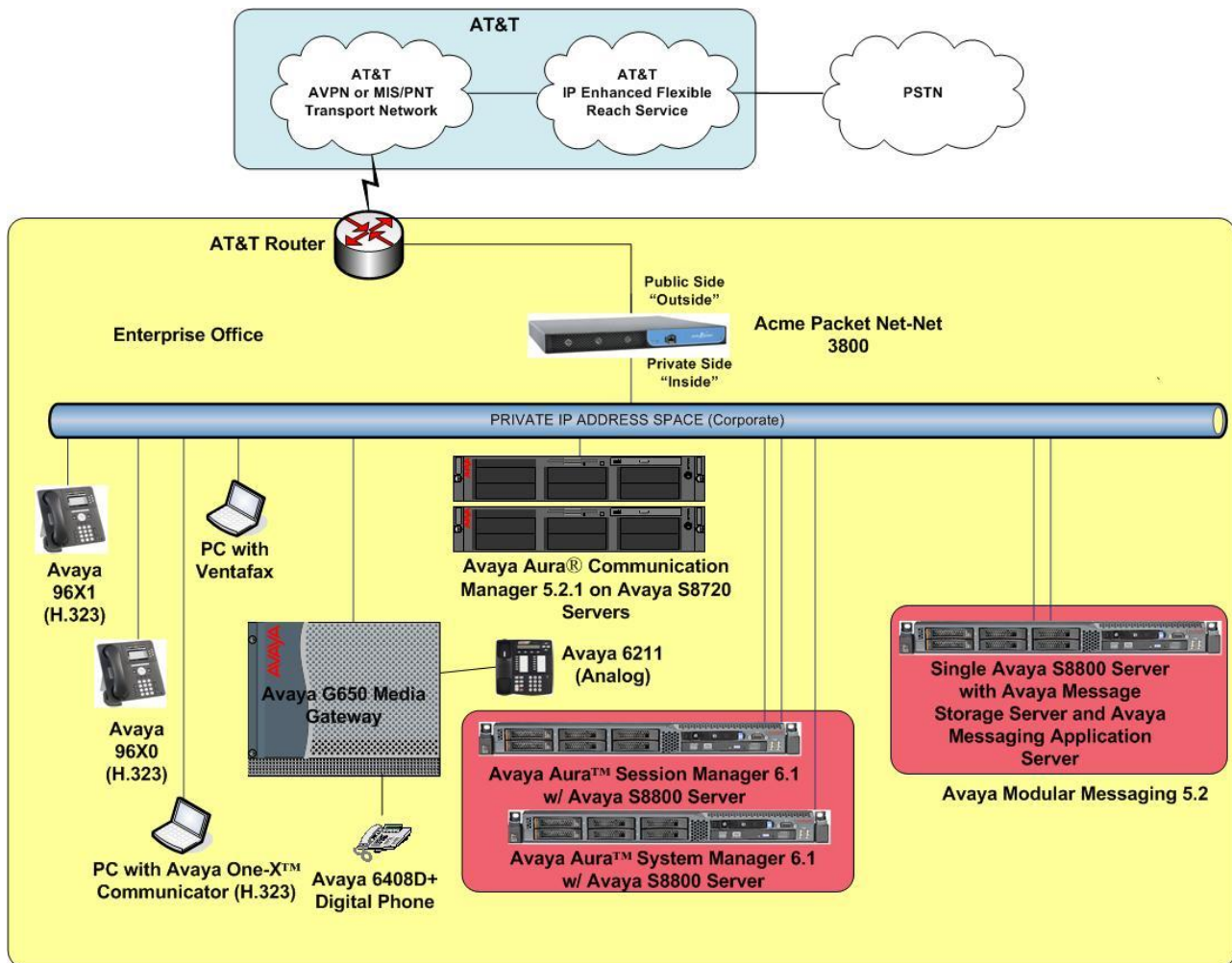


Figure 1: Reference configuration

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	10.80.150.204
Avaya Aura® Session Manager	
Management IP Address	10.80.150.205
Network IP Address	10.80.150.206
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
Avaya Aura® 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

This section describes the call flow used for AT&T IPFR-EF service which uses SIP-Refer method to off-net blind transfers. For other call flows tested, refer to [9, Section 2.2].

The call scenario illustrated in figure below is an inbound AT&T IPFR-EF 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 IPFR-EF service for routing to an alternate destination.

1. A PSTN phone originates a call to an AT&T IPFR-EF service number.
2. The PSTN routes the call to the AT&T IPFR-EF service network.
3. The AT&T IPFR-EF 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 IPFR-EF service.
7. The AT&T IPFR-EF 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 Transfer Connect service clears the call on the redirecting/referring party (Communication Manager).

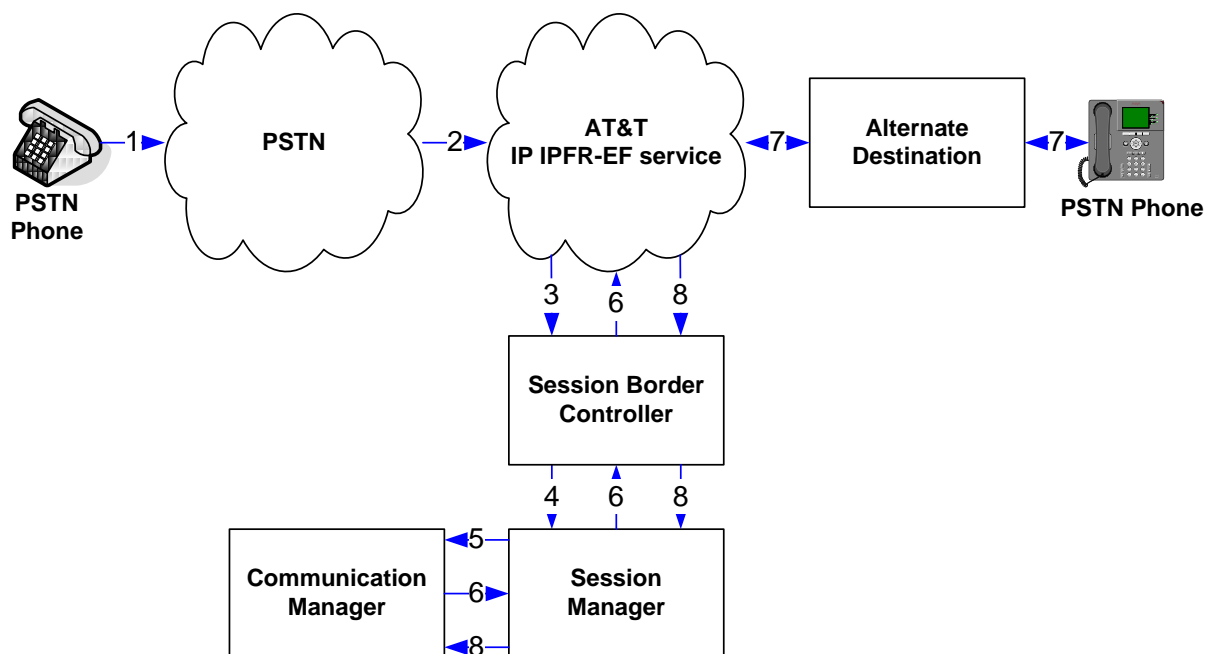


Figure 2: Inbound AT&T IPFR-EF – Post-Answer SIP REFER Redirection Call

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 6.1 SP5 (6.1.0.0.7345-6.1.5.502) System Platform 6.0.3.3.3
Avaya S8800 Server	Avaya Aura® Session Manager 6.1 SP5 (6.1.5.0.615006)
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 9641G IP Telephone	H.323 Version S6.0.0
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. A hot fix was delivered by Communication Manager development team which will be delivered in Service Pack 13.

5. Configure Avaya Aura® Session Manager Release 6.1

This section illustrates relevant aspects of the Session Manager configuration used in the verification of this compliance test. These application notes only cover the additional configuration required for supporting AT&T IPFR-EF service features. For AT&T IP Flexible reach service Session Manager configuration, please refer [9, Section 4].

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

The following administration activities are described:

- Define SIP Domain
- Define Locations for routing purpose
- 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**.

Users	Elements	Services
Administrators Manage Administrative Users	Application Management Manage applications and application certificates	Backup and Restore Backup and restore System Manager database
Groups & Roles Manage groups, roles and assign roles to users	Communication Manager Manage Communication Manager objects	Configurations Manage system wide configurations
Subscribers Manage users and shared resources associated with CS1000, including LDAP/file import and export	Conferencing Conferencing	Events Manage alarms, view and harvest logs
Synchronize and Import Synchronize users with the enterprise directory, import users from file	Inventory Manage, discover, and navigate to elements, update element software	Licenses View and configure licenses
UCM Roles Manage UCM Roles, assign roles to users	Messaging Manage Messaging System objects	Replication Track data replication nodes, repair replication nodes
User Management Manage users, shared user resources and provision users	Presence Presence	Scheduler Schedule, track, cancel, update and delete jobs
	Routing Network Routing Policy	Security Manage Security Certificates
	Session Manager Session Manager Element Manager	Templates Manage Templates for Communication Manager and Messaging System objects
	SIP AS 8.1 SIP AS 8.1	UCM Services Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

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

▼ Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

5.1. SIP Domain

The following screen shows the domain used for AT&T IPFR-EF service testing. Please refer to [9] for SIP Domain configuration.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) × [Home](#)

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

Home / Elements / Routing / Domains- Domain Management

Domain Management [Help ?](#)

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

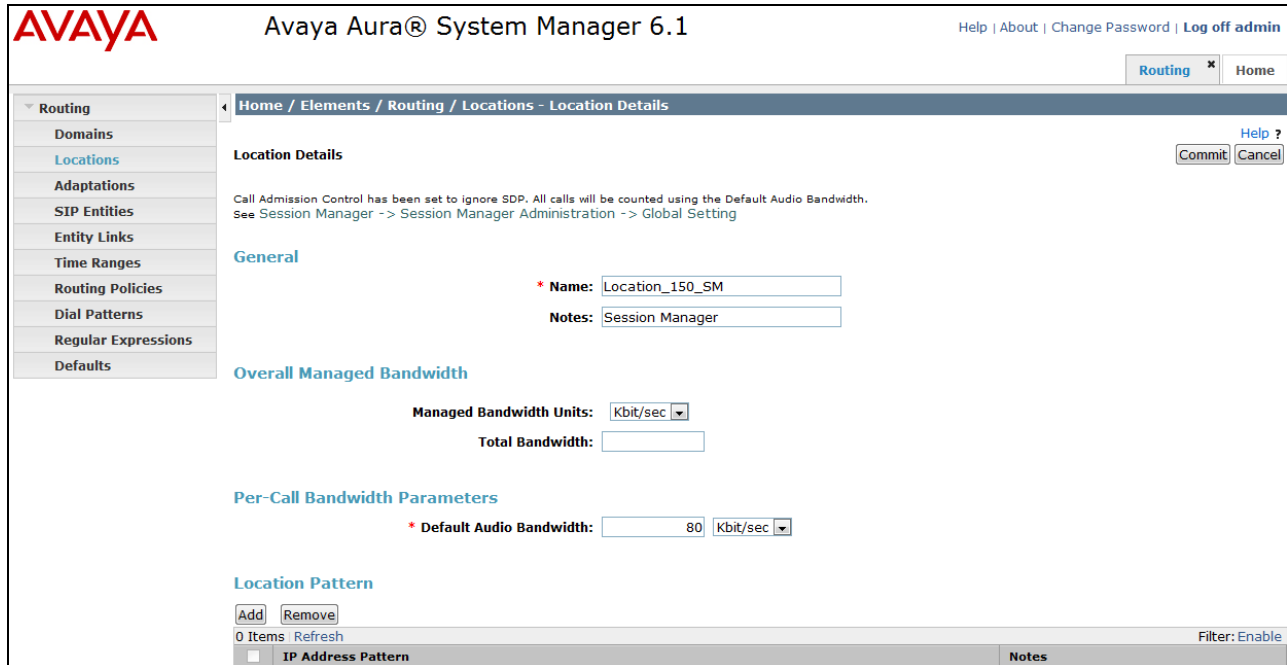
1 Item [Refresh](#) Filter: Enable

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

SIP Domain

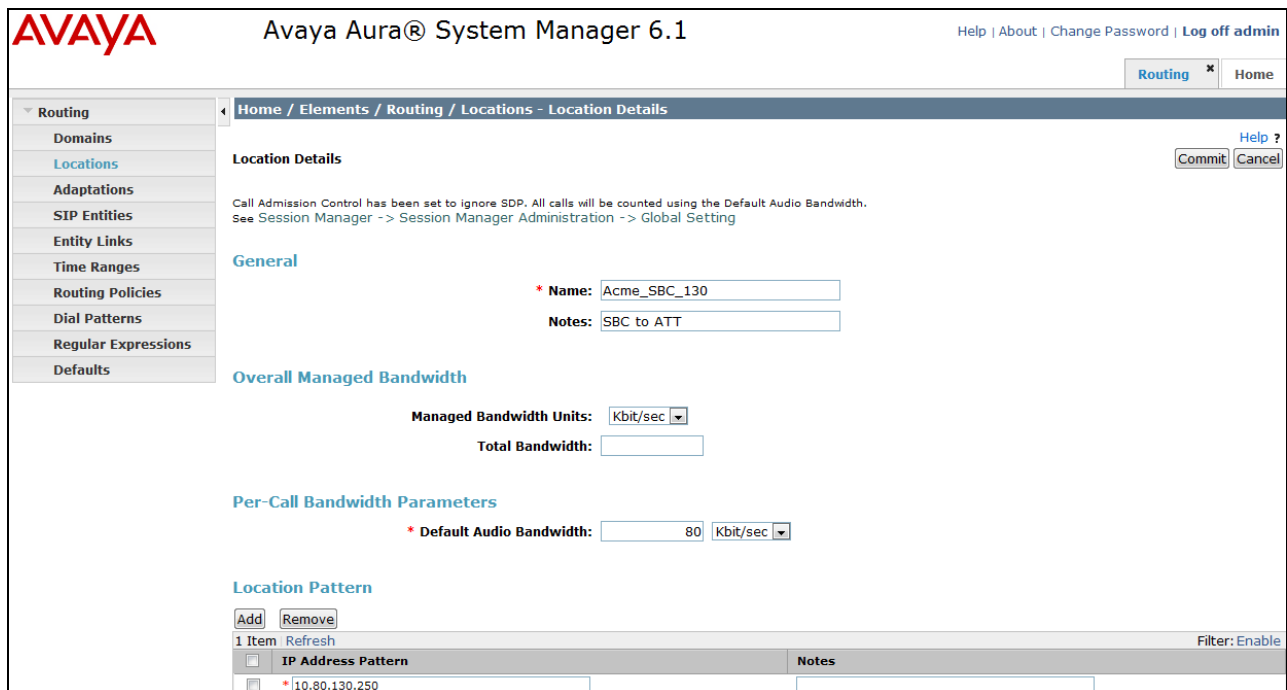
5.2. Locations

The following screens show Location Details for various locations used in this AT&T IPFR-EF service testing. Please refer to [9] for additional configuration details.



The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations (selected), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Locations - Location Details'. It includes a 'Location Details' section with a 'Help ?' link, 'Commit', and 'Cancel' buttons. Below this is a 'General' section with fields for '* Name' (Location_150_SM) and 'Notes' (Session Manager). The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Kbit/sec' and 'Total Bandwidth' as an empty field. The 'Per-Call Bandwidth Parameters' section shows '* Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section has 'Add' and 'Remove' buttons, '0 Items', and a 'Refresh' button. At the bottom, there is a table with columns 'IP Address Pattern' and 'Notes', and a 'Filter: Enable' button.

Session Manager Location Details



The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations (selected), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Locations - Location Details'. It includes a 'Location Details' section with a 'Help ?' link, 'Commit', and 'Cancel' buttons. Below this is a 'General' section with fields for '* Name' (Acme_SBC_130) and 'Notes' (SBC to ATT). The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Kbit/sec' and 'Total Bandwidth' as an empty field. The 'Per-Call Bandwidth Parameters' section shows '* Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section has 'Add' and 'Remove' buttons, '1 Item', and a 'Refresh' button. At the bottom, there is a table with columns 'IP Address Pattern' and 'Notes', and a 'Filter: Enable' button. The table contains one row with the IP address pattern '10.80.130.250'.

Acme Packet SBC Location Details

AVAYA

Avaya Aura® System Manager 6.1

[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 / Locations- Location Details

Location Details

Commit

Cancel

Help ?

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

Location_130

Notes:

Subnet 130

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
<input type="checkbox"/>	* 10.80.130.*	

Subnet 130 Location Details

5.3. Configure Adaptations

The following screen displays the additional adaptations used for inbound calls to support AT&T IPFR-EF service simultaneous and sequential ring DID. In this reference configuration, DID **7324110194** was used for simultaneous ring feature where an INVITE is sent to both extensions **50002** and **50001** and DID **732411096** was used for sequential ring feature where extension **50007** rings first and if not answered extension **50001** will ring. Please refer to [9] for additional configuration details.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations (highlighted), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Adaptations- Adaptation Details'. It includes a 'Commit' button and a 'Cancel' button. The 'General' section shows the following fields: * Adaptation name: ATT CLAN, Module name: DigitConversionAdapter (dropdown), Module parameter: fromto=true osrcd=attavaya.com, Egress URI Parameters: (empty), and Notes: (empty). Below this, there are two sections: 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM'. Each section has an 'Add' button and a 'Remove' button. The 'Digit Conversion for Incoming Calls to SM' section shows 0 items. The 'Digit Conversion for Outgoing Calls from SM' section shows 4 items. The table for outgoing calls has columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, and Notes. The data rows are as follows:

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
* 7324110193	* 10	* 10		* 10	50001	destination	
* 7324110194	* 10	* 10		* 10	50002	destination	
* 7324110195	* 10	* 10		* 10	50001	destination	
* 7324110196	* 10	* 10		* 10	50007	destination	

Communication Manager Adaptations

Avaya Aura® System Manager 6.1

[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 / Adaptations- Adaptation Details

Adaptation Details

Commit

Cancel

Help ?

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	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 IPFR-EF service. Please refer to [9] for SIP Entity configuration.

Note – In the 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 6.1 web interface. The left sidebar shows a navigation menu with options like Routing, 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 breadcrumb trail: 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. The 'General' tab is active, showing fields for Name (ASM), FQDN or IP Address (10.80.150.206), Type (Session Manager), Notes (Session Manager), Location (Location_150_SM), Outbound Proxy, Time Zone (America/Denver), and Credential name. Below this is the 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. The 'Entity Links' section shows a table with two items, each linking the 'ASM' entity to 'AcmeSBCATT-5060' and 'CM5.2CLAN1A05' via TCP on port 5060 with a 'Trusted' connection policy. At the bottom, the 'Port' section shows two items: port 5060 and 5090, both using TCP and the default domain 'attavaya.com'.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details [Help ?](#)
[Commit](#) [Cancel](#)

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links
[Add](#) [Remove](#)

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

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

Select : All, None

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

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

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	attavaya.com	
<input type="checkbox"/>	5090	TCP	attavaya.com	

Session Manager Entity

AVAYA

Avaya Aura® System Manager 6.1

[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

SIP Entity Details

Commit

Cancel

Help ?

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

SIP Link Monitoring

SIP Link Monitoring:

Link Monitoring Disabled

* Proactive Monitoring Interval (in seconds):

900

* Reactive Monitoring Interval (in seconds):

120

* Number of Retries:

1

Entity Links

Add

Remove

1 Item

Refresh

Filter: Enable

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

Acme Packet SBC Entity

AVAYA

Avaya Aura® System Manager 6.1

[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

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 for ATT te

Adaptation:

ATT CLAN

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

Entity Links

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	ASM	TCP	*5060	CM5.2CLAN1A05	*5090	Trusted

Communication Manager Entity

5.5. Entity Links

The following screens show the entity links configured for AT&T IPFR-EF service testing. Please refer to [9] for Entity link configuration.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM_CM5.2CLAN1A05	* ASM	TCP	* 5060	* CM5.2CLAN1A05	* 5060	Trusted	

Entity link between Session Manager and Communication Manager

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM_AcmeSBCATT-5	* ASM	TCP	* 5060	* AcmeSBCATT-5060	* 5060	Trusted	SM to SBC to ATT

Entity link between Session Manager and Acme Packet SBC

5.6. Time Ranges

The following screen shows the time range used for AT&T IPFR-EF service testing. Please refer to [9] for further configuration.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Time Ranges - Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions

2 Items 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 Ranges

5.7. Routing Policies

The following screens show routing policies along with dial patterns defined for AT&T IPFR-EF service testing. Please refer to [9] for further configuration steps.

AVAYA

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Help ?

Commit Cancel

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

General

* Name: ToCM5.2CLAN1A05

Disabled: ☐

Notes: To CM5.2 Location 130

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 for ATT testing

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
2	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

3 Items Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
20	4	10	<input type="checkbox"/>	attavaya.com	Acme_SBC_130	
5	5	5	<input type="checkbox"/>	attavaya.com	Acme_SBC_130	
73236801	10	10	<input type="checkbox"/>	attavaya.com	Acme_SBC_130	Inbound Calls from ATT

Routing Policy for Communication Manager

Routing Policy Details

[Help ?](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

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

Time of Day

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

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

Select : All, None

Dial Patterns

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

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	20	4	10	<input type="checkbox"/>	attavaya.com	Location_100	
<input type="checkbox"/>	20	4	10	<input type="checkbox"/>	attavaya.com	Location_130	
<input type="checkbox"/>	*7	3	13	<input type="checkbox"/>	attavaya.com	Location_130	ATT Network Based Call Forwarding Always Activation
<input type="checkbox"/>	13035381	11	11	<input type="checkbox"/>	attavaya.com	Location_130	
<input type="checkbox"/>	*9	3	13	<input type="checkbox"/>	attavaya.com	Location_130	

Routing Policy for Acme Packet SBC

5.8. Dial Patterns

The following screens shot show dial patterns configured to support AT&T IPFR-EF service testing. Please refer to [9] for additional configuration details.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes a breadcrumb trail: Home / Elements / Routing / Dial Patterns - Dial Pattern Details. The 'General' tab is active, displaying the following fields: Pattern (*7), Min (3), Max (13), Emergency Call (unchecked), SIP Domain (attavaya.com), and Notes (ATT Network Based Call Forwarding Always A). Below the 'General' tab is the 'Originating Locations and Routing Policies' section, which includes an 'Add' button, a 'Remove' button, and a table with 1 item. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The table contains one row: Location_130, Subnet 130, To_ATTAcme5060, 0, unchecked, AcmeSBCATT-5060. The bottom right of the interface has 'Commit' and 'Cancel' buttons.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Location_130	Subnet 130	To_ATTAcme5060	0	<input type="checkbox"/>	AcmeSBCATT-5060	

Dial Pattern for Call Forwarding Always Feature

The screenshot shows the Avaya Aura System Manager 6.1 interface, similar to the previous one. The left sidebar is the same. The main content area is titled 'Dial Pattern Details' with the same breadcrumb trail. The 'General' tab is active, displaying the following fields: Pattern (*9), Min (3), Max (13), Emergency Call (unchecked), SIP Domain (attavaya.com), and Notes (empty). Below the 'General' tab is the 'Originating Locations and Routing Policies' section, which includes an 'Add' button, a 'Remove' button, and a table with 1 item. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The table contains one row: Location_130, Subnet 130, To_ATTAcme5060, 0, unchecked, AcmeSBCATT-5060. The bottom right of the interface has 'Commit' and 'Cancel' buttons.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Location_130	Subnet 130	To_ATTAcme5060	0	<input type="checkbox"/>	AcmeSBCATT-5060	

Dial Pattern for other Call Forwarding Features

5.9. Session Manager Administration

The following screen shows the Session Manager configuration used for AT&T IPFR-EF service testing. Please refer to [9] for additional configuration details.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header shows the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and user links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the header is a navigation bar with tabs for 'Session Manager', 'Routing', and 'Home'. A left-hand sidebar contains a tree view of the application's structure, including 'Session Manager', 'Dashboard', 'Session Manager Administration', 'Communication Profile Editor', 'Network Configuration', 'Device and Location Configuration', 'Application Configuration', 'System Status', 'SIP Entity Monitoring', 'Managed Bandwidth Usage', 'Security Module Status', 'Registration Summary', 'User Registrations', 'SIP Performance', 'System Performance', and 'System Tools'. The main content area is titled 'View Session Manager' and includes a breadcrumb trail: 'Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration'. A 'Return' button is located in the top right of the main area. The configuration is organized into two sections: 'General' and 'Security Module'. The 'General' section includes fields for 'SIP Entity Name' (ASM), 'Description', 'Management Access Point Host Name/IP' (10.80.150.205), and 'Direct Routing to Endpoints' (Enable). The 'Security Module' section includes fields for 'SIP Entity IP Address' (10.80.150.206), 'Network Mask' (255.255.255.0), 'Default Gateway' (10.80.150.1), 'Call Control PHB' (46), 'QOS Priority' (6), 'Speed & Duplex' (Auto), and 'VLAN ID'.

Section	Field	Value
General	SIP Entity Name	ASM
	Description	
	Management Access Point Host Name/IP	10.80.150.205
	Direct Routing to Endpoints	Enable
Security Module	SIP Entity IP Address	10.80.150.206
	Network Mask	255.255.255.0
	Default Gateway	10.80.150.1
	Call Control PHB	46
	QOS Priority	6
	Speed & Duplex	Auto
	VLAN ID	

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 IPFR-EF service features listed in **Section 2**. For configuration steps related to AT&T Flexible Reach service, please refer to [**9, Section 5**]. 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 this Application Notes. Other parameter values may or may not match based on local configurations. Also **NCR** feature may require additional licensing.

6.1. 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 IPFR-EF service (see **Section 6.7.1**).

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

6.2. IP Node Names

Following screen shows the node names used for AT&T IPFR-EF service provisioning. Please refer to [9] for additional configuration details.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
Gateway001	10.80.130.1	
CLAN-1A05	10.80.130.206	
SM61	10.80.150.206	

6.3. IP Network Regions

Network Regions are used to group various Communication Manager Resources such as codecs, UDP port ranges, and inter-region communication. No additional IP Network Regions were defined for AT&T IPFR-EF service provisioning. Please refer to [9] for configuring IP Network Regions.

6.4. IP Codec Parameters

Following screen shows the codec set used for AT&T IPFR-EF service. Please refer to [9] for additional configuration details

change ip-codec-set 2

Page1 of 2

IP Codec Set

Codec Set: 2

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

6.5. SIP Trunks

Although SIP trunk configured in [9] with minor modifications, can be used for AT&T IPFR-EF service too but a separate trunk is created to handle additional features provided by this enhanced service.

6.5.1. SIP Trunk for AT&T IP Flexible Reach-Enhanced Features calls

This section describes the steps for administering the SIP trunk used for AT&T IPFR-EF calls.

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: SM61	
Near-end Listen Port: 5090	Far-end Listen Port: 5060	
	Far-end Network Region: 2	
Far-end Domain: attavya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Direct IP-IP Early Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

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
Direction: two-way	Outgoing Display? n	TAC: 105
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	
	UUI 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?** is set to **y**. (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? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 100	

6.6. 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” trunk defined in **Section 6.5.1**. Use the **change public-unknown-numbering 0** command to add entries for AT&T IPFR-EF service DIDs.

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

6.7. Outbound Call Routing From Avaya Aura® Communication Manager

Route Pattern and ARS dialing needs to be configured for Outbound call Routing required for AT&T IPFR-EF service.

6.7.1. 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. The following screen shows the route pattern (3) used to support AT&T IPFR-EF 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:	3	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		

6.7.2. ARS Dialing

Automatic Route Selection (ARS) is used to direct calls to AT&T via the route pattern defined in previous section. Following screen shows the entries made for ARS dialing to support additional AT&T IPFR-EF service features.

- *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						Percent Full: 15			
Location: all									
	Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Reqd		
		Min	Max						
	*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		

6.8. 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 refer failure
11 disconnect after announcement 33008
12
```

Sample Vector for Post-Answer Redirection

6.9. 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 [10] 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	10.80.150.206
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

ANNOTATION: The session agent below represents the Session Manager used in this reference configuration.

```

session-agent
  hostname          SM61
  ip-address        10.80.150.206
  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 **2** 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 the AT&T IPFR-EF service test configuration:

1. Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly.
2. Enter **9*723035551212** to enable Call Forwarding Always feature on AT&T network. Then make in inbound call from PSTN on the DID where this feature is enabled to make sure that the call is forwarded to **3035551212**. Other Call Forwarding features can be enabled similarly.

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 – Enhanced Features service using either AVPN or MIS-PNT transport.

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

Avaya Modular Messaging

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

Other References

- [9] Applications Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.0 and Acme Packet Net-Net 6.2.0 with AT&T IP Flexible Reach SIP Trunk Service (<https://devconnect.avaya.com/public/download/dyn/ACM521SM60SBC.pdf>)

Acme Packet Support (login required):

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

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

- [11] 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.