



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.3, with AT&T IP Flexible Reach - Enhanced Features Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 6.3, and Avaya Session Border Controller for Enterprise 6.3, with the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Communication Manager 6.3 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. The Avaya Session Border Controller for Enterprise 6.3 is the point of connection between Avaya Aura® Session Manager 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.

The AT&T Flexible Reach is one of the many SIP-based Voice over IP (VoIP) 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.

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

Table of Contents

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	6
2.2.	Test Results	7
2.3.	Support	8
3.	Reference Configuration.....	8
3.1.	Illustrative Configuration Information.....	10
3.2.	AT&T IP Flexible Reach - Enhanced Features Service Call Flows	11
3.2.1.	Inbound.....	11
3.2.2.	Outbound.....	12
3.2.3.	Call Forward Re-direction.....	13
3.3.	AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow	14
4.	Equipment and Software Validated.....	15
5.	Configure Avaya Aura® Session Manager	16
5.1.	SIP Domain	17
5.2.	Locations	17
5.2.1.	Main Location.....	17
5.2.2.	Common Location	19
5.3.	Configure Adaptations	20
5.3.1.	Adaptation for Avaya Aura® Communication Manager Extensions	20
5.3.2.	Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service.....	21
5.3.3.	Adaptation for Meet-Me Conference Calls	22
5.3.4.	Adaptation for calls to Avaya Aura® Messaging.....	23
5.4.	SIP Entities	24
5.4.1.	Avaya Aura® Session Manager SIP Entity.....	25
5.4.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk	26
5.4.3.	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	27
5.4.4.	Avaya Aura® Communication Manager SIP Entity – Meet-Me Trunk.....	27
5.4.5.	Avaya Session Border Controller for Enterprise SIP Entity	28
5.4.6.	Avaya Aura® Messaging SIP Entity	28
5.5.	Entity Links	29
5.5.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	29
5.5.2.	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	30
5.5.3.	Entity Link to Avaya Aura® Communication Manager – Meet-Me Trunk	30
5.5.4.	Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE	31
5.5.5.	Entity Link to Avaya Aura® Messaging.....	31
5.6.	Time Ranges – (Optional)	32
5.7.	Routing Policies	32
5.7.1.	Routing Policy for AT&T Routing to Avaya Aura® Communication Manager	32
5.7.2.	Routing Policy for Inbound Routing to Avaya Aura® Communication Manager Meet-Me Conference.....	34
5.7.3.	Routing Policy for Inbound Routing to Avaya Aura® Messaging	35

5.7.4.	Routing Policy for Outbound Calls to AT&T	36
5.8.	Dial Patterns	37
5.8.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager	37
5.8.2.	Matching Outbound Calls to AT&T	38
5.8.3.	Matching Inbound Calls to Avaya Aura® Communication Manager Meet-Me Conference	40
5.8.4.	Matching Inbound PSTN Calls to Avaya Aura® Messaging	41
6.	Configure Avaya Aura® Communication Manager	42
6.1.	System-Parameters Customer-Options	42
6.2.	System-Parameters Features	44
6.3.	Dial Plan	45
6.4.	IP Node Names	45
6.5.	IP Interface for procr	46
6.6.	IP Network Regions	46
6.6.1.	IP Network Region 1 – Local CPE Region	46
6.6.2.	IP Network Region 2 – AT&T Trunk Region	48
6.7.	IP Codec Parameters	48
6.7.1.	Codecs for IP Network Region 1 (calls within the CPE)	48
6.7.2.	Codecs for IP Network Region 2 (calls to/from AT&T)	49
6.8.	SIP Trunks	49
6.8.1.	SIP Trunk for Inbound/Outbound AT&T calls	49
6.8.2.	Local SIP Trunk (Avaya SIP Telephone and Avaya Messaging Access)	52
6.8.3.	SIP Trunk for Meet-Me Conference Calls	54
6.9.	Private Numbering	55
6.10.	Route Patterns	56
6.10.1.	Route Pattern for Calls to AT&T	56
6.10.2.	Route Pattern for Calls within the CPE	57
6.11.	Automatic Route Selection (ARS) Dialing	57
6.12.	Automatic Alternate Routing (AAR) Dialing	58
6.13.	Avaya G430 Media Gateway Provisioning	58
6.14.	Meet-Me Conference Vector and Vector Directory Number (VDN)	59
6.14.1.	Meet-Me Vector	59
6.14.2.	Meet-Me VDN	60
6.15.	Save Translations	60
7.	Configure Avaya Session Border Controller for Enterprise	61
7.1.	System Management – Status	63
7.2.	Global Profiles	63
7.2.1.	Server Interworking – Avaya	64
7.2.2.	Server Interworking – AT&T	66
7.2.3.	Server Configuration – Session Manager	67
7.2.4.	Server Configuration – AT&T	68
7.2.5.	Routing – To Session Manager	69
7.2.6.	Routing – To AT&T	70
7.2.7.	Topology Hiding – Avaya Side	71
7.2.8.	Topology Hiding – AT&T Side	73

7.2.9.	Signaling Manipulation.....	73
7.3.	Domain Policies.....	74
7.3.1.	Application Rules	74
7.3.2.	Media Rules.....	74
7.3.3.	Signaling Rules.....	75
7.3.4.	Endpoint Policy Groups – Avaya Connection.....	83
7.3.5.	Endpoint Policy Groups – AT&T Connection	83
7.4.	Device Specific Settings.....	84
7.4.1.	Network Management.....	84
7.4.2.	Advanced Options.....	85
7.4.3.	Media Interfaces	86
7.4.4.	Signaling Interface	86
7.4.5.	Endpoint Flows – For Session Manager	87
7.4.6.	Endpoint Flows – For AT&T	88
8.	Verification Steps.....	90
8.1.	AT&T IP Flexible Reach – Enhanced Features	90
8.2.	Avaya Aura® Communication Manager	90
8.3.	Avaya Aura® Session Manager	91
8.4.	Avaya Session Border Controller for Enterprise	93
8.4.1.	System Status.....	93
8.4.2.	Protocol Traces	93
9.	Conclusion	95
10.	References.....	96
11.	Addendum 1 – Redundancy to Multiple AT&T Border Elements	97
11.1.	Secondary AT&T Border Element Server Configuration	97
11.2.	Add Secondary IP Address to Routing.....	98
11.3.	Configure End Point Flows – Server Flow - ATT_Secondary	99

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 6.3 (Communication Manager), Avaya Aura® Session Manager 6.3 (Session Manager), Avaya Aura® System Manager 6.3 (System Manager), and the Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE), with the AT&T IP Flexible Reach - Enhanced Features service (IPFR-EF) using AVPN or MIS/PNT transport connections.

Avaya Aura® Communication Manager 6.3 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® System Manager 6.3 is the provisioning/management application for Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 6.3 is the point of connection between Avaya Aura® Session Manager 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.

The AT&T Flexible Reach service is one of the many SIP-based Voice over IP (VoIP) 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. The AT&T IP Flexible Reach - Enhanced Features service utilizes AT&T's AVPN¹ or MIS/PNT² transport services.

2. General Test Approach and Test Results

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.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPFR-EF and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, and the Avaya SBCE (see **Section 3.2** for call flow examples).

The test environment consisted of:

- A simulated enterprise with, Communication Manager, Session Manager, System Manager (for Session Manager provisioning), Avaya SBCE, Avaya phones, fax machines (Ventafax application), and Avaya Aura® Messaging.
- An IPFR-EF service production circuit, to which the simulated enterprise was connected via AVPN transport.

¹ AVPN supports compressed RTP (cRTP).

² MIS/PNT does not support cRTP.

2.1. Interoperability Compliance Testing

Note – Documents used to provision the test environment are listed in **Section 10**. In the following sections, references to these documents are indicated by the notation [x], where x is the document reference number.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPFR-EF network. Calls were made from the PSTN across the IPFR-EF network, to the CPE.

The following SIP trunking VoIP features were tested with the IPFR-EF service:

- Incoming and outgoing voice calls between PSTN, the IPFR-EF service, the Avaya SBCE, Session Manager, and Communication Manager. Avaya SIP telephones (desk and softphone), and H.323 telephones (desk) were used.
- Inbound/Outbound fax calls using T38.
- Various outbound PSTN destinations were tested including long distance, international, and toll-free.
- Requests for privacy (i.e., caller anonymity) for Communication Manager outbound calls to the PSTN, as well as privacy requests for inbound calls from the PSTN to Communication Manager users.
- SIP OPTIONS messages used to monitor the health of the SIP trunks between the CPE and AT&T.
- Incoming and outgoing calls using the G.729(A & B) and G.711 ULAW codecs.
- Call redirection with Diversion Header.
- Operator assistance and 911 calls.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful PSTN and Communication Manager voice menu navigation.
- Telephony features such as hold, transfer, and conference.
- Basic Communication Manager EC500 “mobility” calls (e.g., extend and return call).
- An Avaya Remote Worker endpoint (an Avaya 9621 SIP telephone) was used in the reference configuration. The Remote Worker endpoint resides on the public side of the Avaya SBCE (via a TLS connection), and registers/communicates with Avaya Session Manager via Avaya SBCE as though it was an endpoint residing in the private CPE space.

Note – The configuration of the Remote Worker environment is beyond the scope of this document. Refer to [10] for information on Remote Worker deployments.

- AT&T IPFR-EF service features such as:
 - Simultaneous Ring
 - Sequential Ring
 - Call Forward – Always
 - Call Forward – Busy
 - Call Forward – Ring No Answer
 - “Blind” and Attended transfers utilizing Refer messaging.

2.2. Test Results

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

- 1) **Communication Manager Meet-Me conference can isolate PSTN parties if the conference takes place via an NCR enabled SIP trunk.**
 - a) This issue may occur if a three party Meet-Me conference is established via an NCR enabled trunk, with two parties on the PSTN and one party on Communication Manager station. Should the Communication Manager station leaves the conference, Communication Manager will issue a Refer, resulting in the two PSTN parties being directly connected by the IPFR-EF service, and Communication Manager ending the Meet-Me conference.
 - b) The workaround for this issue is to create a “Meet-Me Conference” SIP trunk with NCR *disabled*, used exclusively for customers placing Meet-Me conference calls (see **Section 6.8.3**).
 - c) Create a “general access” SIP trunk, with NCR *enabled*, for all other inbound and outbound calls (see **Section 6.8.1**). This supports the use of Refer for IPFR-EF “Blind Transfers” (call redirection) and station initiated call transfers.
- 2) **IPFR-EF Simultaneous Ring and Sequential Ring - Loss of calling display information on Communication Manager stations.** If the Communication Manager station associated with these IPFR-EF “secondary” number answers the call, the phone will not display the calling information. Based on the SIP signaling, Communication Manager expects a display update from the network. However, the subsequent network signaling does not contain new calling information.
 - a) The recommended workaround is described in **Section 6.8.1**, where Communication Manager will retrieve the display information using the *From* header. **Note that this solution is only applicable to Communication Manager 6.x platforms.**
- 3) **The Avaya SBCE issues a Remote-Address header even though the option to do so is disabled** - During testing it was found that the Avaya SBCE was including a Remote-Address header to SIP Invite messages leaving the Avaya SBCE (inbound or outbound, depending on call direction), even though the option was disabled.
 - a) No issues were caused by the inclusion of this header, however the Avaya SBCE was provisioned to remove this header (see **Section 7.3.3**, and **Item 6** below) for calls to AT&T, to reduce overall packet size.
- 4) **G.711 fax is not supported between Communication Manager and the IPFR-EF service.** Communication Manager does not support the protocol negotiation required for G.711 fax to work with the IPFR-EF service. T.38 fax is supported, however connections are limited to 9600 bps. The sender and receiver of a T.38 fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3.
- 5) **IPFR-EF Sequential Ring – Loss of connection if Secondary party is busy.** The following IPFR_EF service limitation was observed during testing. If a PSTN Sequential Ring call is directed to the designated “secondary” destination, and that destination returns a 486 Busy,

PSTN does not hear a busy tone or any other call progress indications (ringing, reorder, etc.). After approximately 30 seconds the call is dropped.

- 6) **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), the Avaya SBCE is provisioned to remove SIP headers not required by the AT&T IPFR-EF service (see **Section 7.3.3**, and **Item 3** above).
- 7) **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) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor. While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at <http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

2.3. Support

For more information on the AT&T IP Flexible Reach service visit:

<http://www.business.att.com/enterprise/Service/voice-services/null/sip-trunking/>

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

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

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

- Communication Manager 6.3, System Manager 6.3, Session Manager 6.3, and the Avaya SBCE 6.3 are used in the reference configuration.
- 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. Avaya SIP endpoints register to Session Manager.
- 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. Avaya H.323 endpoints register to Communication Manager.

- An Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G430 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya desk telephones used are Avaya 96x1 Series IP Telephones (H.323 and SIP), Avaya one-X® Communicator soft phone (SIP), as well as 6424 Digital Telephones.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPFR-EF service and the enterprise internal network.
- The IPFR-EF service Border Element (BE) uses SIP over UDP to communicate with enterprise edge SIP devices, (e.g., the Avaya SBCE in this sample configuration). Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP and TLS to communicate with Communication Manager. UDP transport protocol is used between the Avaya SBCE and the IPFR-EF service.
- Avaya Aura® Messaging was used in the reference configuration to provide voice messaging capabilities. This solution is extensible to other Avaya Messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Testing was performed using an IPFR-EF service production circuit.

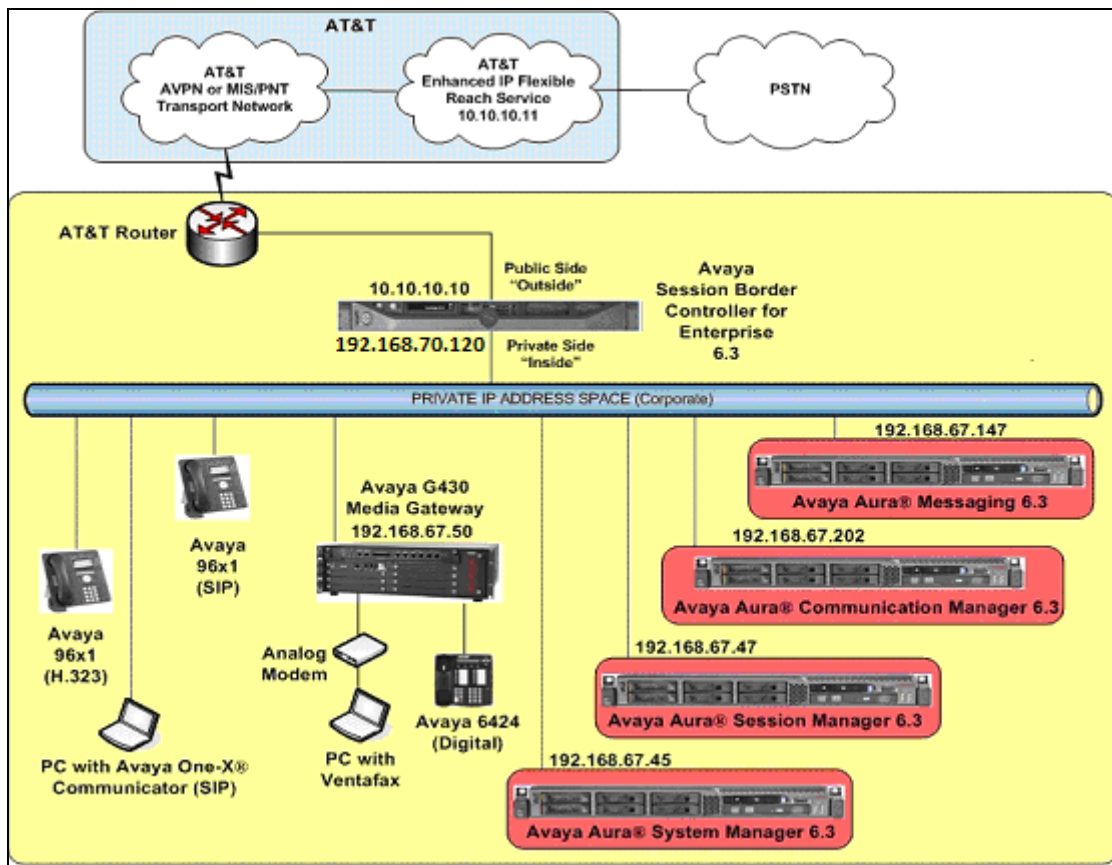


Figure 1: Reference configuration

3.1. Illustrative Configuration Information

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

Note – The IPFR-EF service Border Element IP address and DID/DNIS digits are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DID/DNIS digits as part of the IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura® Session Manager	
Management IP Address	192.168.67.46
Network IP Address	192.168.67.47
Avaya Aura® Communication Manager	
IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	19xxx
Avaya Aura® System Manager	
IP Address	192.168.67.45
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Outside (Public) Interface	10.10.10.10 (see note below)
IP Address of Inside (Private) Interface	192.168.70.120

Table 1: Illustrative Values Used in these Application Notes

NOTE – The Avaya SBCE Outside interface communicates with AT&T Border Elements (BEs) located in the AT&T IP Flexible Reach network. For security reasons, the IP addresses of the AT&T BEs are not included in this document. However as placeholders in the following configuration sections, the IP address of **10.10.10.10** (Avaya SBCE public interface), and **10.10.10.11** (AT&T BE IP addresses), are specified.

3.2. AT&T IP Flexible Reach - Enhanced Features Service Call Flows

To understand how IPFR-EF service calls are handled by the Avaya CPE environment, three basic call flows are described in this section. However, for brevity, not all possible call flows are described.

3.2.1. Inbound

The first call scenario illustrated is an inbound IPFR-EF service call that arrives at the Avaya SBCE, to Session Manager, and is subsequently routed to Communication Manager, which in turn routes the call to a phone or fax endpoint.

1. A PSTN phone originates a call to an IPFR-EF service number.
2. The PSTN routes the call to the IPFR-EF service network.
3. The IPFR-EF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs IP address translations 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 Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone or fax endpoint.

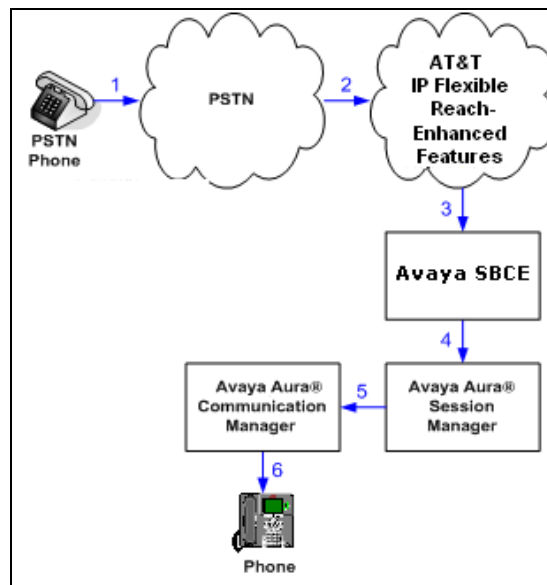


Figure 2: Inbound IPFR-EF Call

3.2.2. Outbound

The second call scenario illustrated is an outbound call initiated on Communication Manager, routed to Session Manager, and is subsequently sent to the Avaya SBCE for delivery to the IPFR-EF service.

1. A Communication Manager phone or fax endpoint originates a call to an IPFR-EF service number for delivery to the 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 Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to the Avaya SBCE.
4. The Avaya SBCE performs IP address translations and any necessary SIP header modifications, and routes the call to the IPFR-EF service.
5. The IPFR-EF service delivers the call to the PSTN.

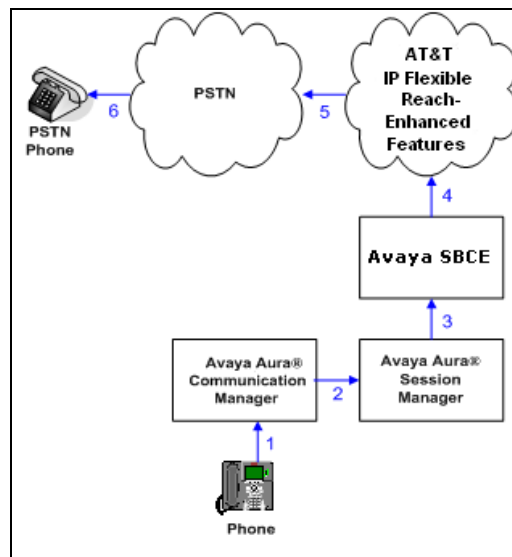


Figure 3: Outbound IPFR-EF Call

3.2.3. Call Forward Re-direction

The third call scenario illustrated is an inbound IPFR-EF service call that arrives at the Avaya SBCE, to Session Manager, and subsequently Communication Manager. Communication Manager routes the call to a destination station, however the station has set Call Forward to an alternate destination. Without answering the call, Communication Manager redirects the call back to the IPFR-EF service for routing to the alternate destination.

Note – In cases where calls are forwarded to an alternate destination such as an 8xx numbers, the IPFR-EF service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 6.8**).

1. Same as the first call scenario in **Section 3.2.1**.
2. Because the Communication Manager phone has set Call Forward to another IPFR-EF service number, Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network.
3. The IPFR-EF service places a call to the alternate destination, and upon answering Communication Manager connects the calling party to the target party.

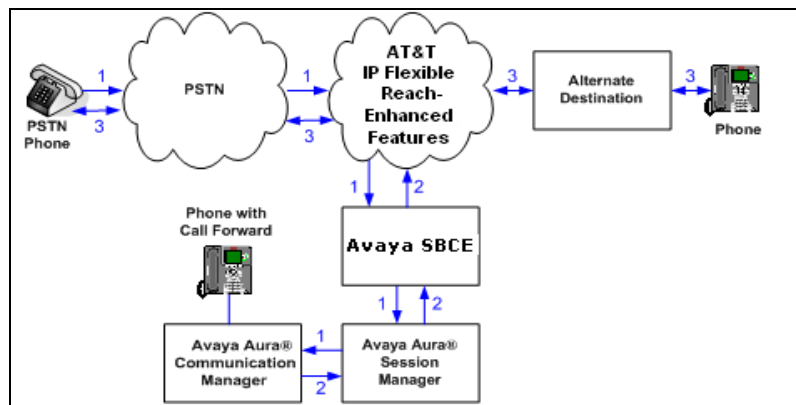


Figure 4: Station Re-directed (e.g. Call Forward) IPFR-EF Call

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

This section describes the call flow for IPFR-EF using SIP Refer to perform Network Based Blind Transfer. The Refer is generated by an inbound call to a Communication Manager Vector. The call scenario illustrated in figure below is an inbound IPFR-EF 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, using Refer (without the *replaces* parameter), redirects the call back to the IP E-IPFR service for routing to an alternate destination.

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE 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 VDN/Vector, which answers the call and plays an announcement, and attempts to redirect the call using a SIP Refer message. The SIP Refer message specifies the alternate destination, and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the IPFR-EF service.
7. IPFR-EF places a call to the alternate destination specified in the Refer, and upon answer, connects the calling party to the alternate party.
8. IPFR-EF clears the call on the redirecting/referring party (Communication Manager).

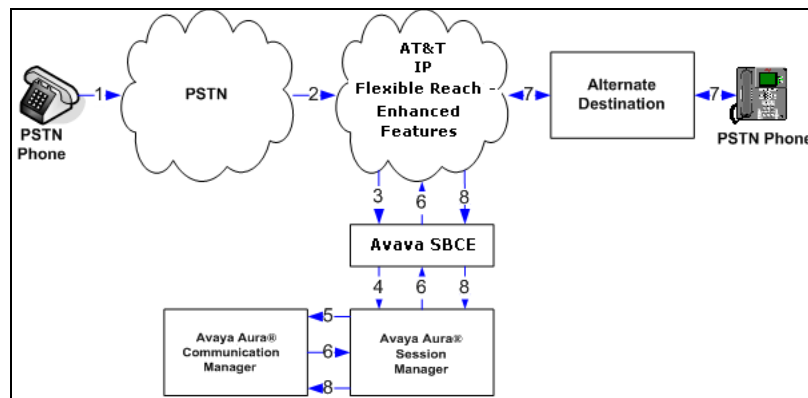


Figure 5: Network Based Blind Transfer Using Refer (Communication Manager Vector)

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
HP Proliant DL360 G7 server <ul style="list-style-type: none">System PlatformAvaya Aura® System Manager	<ul style="list-style-type: none">6.3.5.01003.06.3 SP 11 (6.3.11_r4802871)
Avaya 8800 server <ul style="list-style-type: none">Avaya Aura® Session Manager	<ul style="list-style-type: none">6.3 SP11 (6.3.11.0.631103)
Avaya 8800 server <ul style="list-style-type: none">System PlatformAvaya Aura® Communication Manager	<ul style="list-style-type: none">6.3.5.01003.06.3 SP8 (03.0.124.0-21588)
Avaya G430 Media Gateway	<ul style="list-style-type: none">g430_sw_36_9_0HW7 FW15
Dell R610 <ul style="list-style-type: none">System PlatformAvaya Aura® Messaging	<ul style="list-style-type: none">6.3.4.08011.06.3.1 (MSG-03.0.124.0-321_0104.tar)
Dell R210 <ul style="list-style-type: none">Avaya Session Border Controller for Enterprise	<ul style="list-style-type: none">6.3.1-22-4653
Avaya 96x1 IP Telephone	<ul style="list-style-type: none">H.323 Version 6.4014SIP Version 6.4.125
Avaya one-X® Communicator (SIP)	<ul style="list-style-type: none">6.2.4.07-FP4
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none">7.0.202.494

Table 2: Equipment and Software Versions

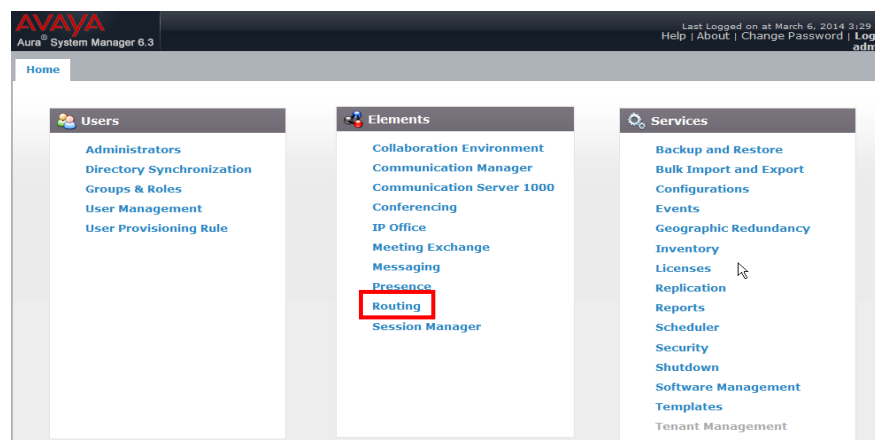
5. Configure Avaya Aura® Session Manager

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

This section provides the procedures for configuring Session Manager to process inbound and outbound calls between Communication Manager and the Avaya SBCE. In the Reference configuration, all Session Manager provisioning is performed via System Manager.

- Define a SIP Domain
- Define Locations for Customer Premises Equipment (CPE), including the Main and Common sites.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Avaya SBCE, and Avaya Messaging.
- Define SIP Entities corresponding to Session Manager, Communication Manager, the Avaya SBCE, and Avaya Messaging.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, and Avaya Messaging, as well as the SIP trunks between the Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, Session Manager, Avaya Messaging, and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for inbound and outbound call routing.

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



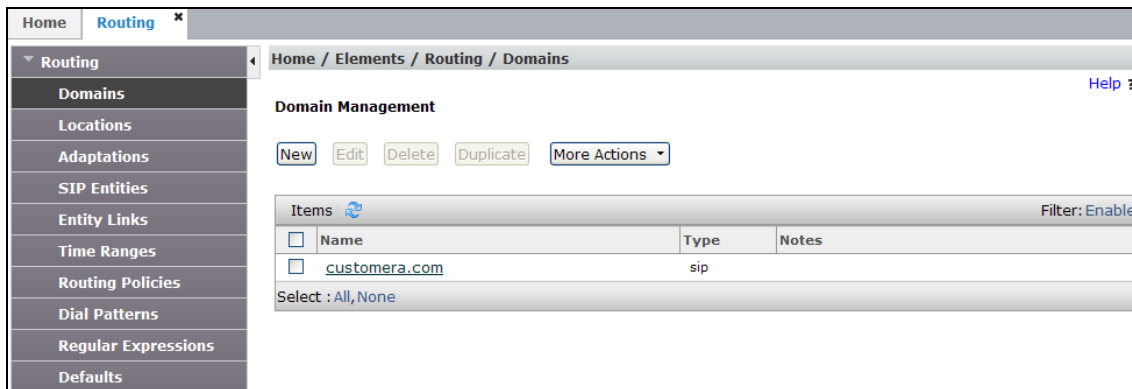
5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain **customera.com** was defined.

Step 2 - Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **customera.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description.

Step 3 - Click **Commit** to save.



The screenshot shows a web interface for 'Domain Management'. On the left is a navigation menu with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table titled 'Items' with a refresh icon and a 'Filter: Enable' link contains one row with columns 'Name', 'Type', and 'Notes'. The row shows 'customera.com' under 'Name' and 'sip' under 'Type'. Below the table is a 'Select : All, None' option.

Name	Type	Notes
customera.com	sip	

5.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, two Locations are specified:

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager, the G430 Media Gateway, and telephones.
- **Common** – This site contains the Avaya SBCE as well as the IPFR-EF access router.

5.2.1. Main Location

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the Location (e.g., **Main**).
- **Notes:** Add a brief description.

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern:** Leave blank.
- **Notes:** Add a brief description.

Step 3 - Click **Commit** to save.

Home
Routing

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

Home / Elements / Routing / Locations

Location Details
Commit Cancel

General
Name: Main
Notes:

Dial Plan Transparency in Survivable Mode
Enabled:
Listed Directory Number:
Associated CM SIP Entity:

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
IP Address Pattern
Notes
Select : All, None
Commit Cancel

5.2.2. Common Location

Follow the steps from **Section 5.2.1** with the following changes:

- **Name:** Enter a descriptive name for the Location (e.g., **Common**).

Home / Elements / Routing / Locations

Location Details

General

Name: Common

Notes: A-SBCE & ATT router

Dial Plan Transparency in Survivable Mode

Enabled: ☒

Listed Directory Number:

Associated CM SIP Entity:

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): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 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

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

Select: All, None

Location

New Edit Delete Duplicate More Actions

Items Filter: Enable

Name	Notes
Common	A-SBCE & ATT router
Main	

Select: All, None

5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T, and for converting SIP headers sent between Communication Manager and Avaya Messaging. In the reference configuration the following Adaptations were used.

- Calls from AT&T (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager extensions.
 - The IP address of Session Manager (**192.168.67.47**) is replaced with the Avaya CPE SIP domain (**customera.com**) for destination domain.
 - The AT&T called number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDNs.
- Calls to AT&T (**Section 5.3.2**) - Modification of SIP messages sent by Communication Manager extensions.
 - The domain of Session Manager (**customera.com**) is replaced with the AT&T BE IP address (**10.10.10.11**) in the destination headers.
 - The History-Info header is removed automatically by the **ATTAdapter**.
- Meet-Me Conference calls to Communication Manager (**Section 5.3.3**)
 - The dedicated Meet-Me conference DNIS number is converted to the Meet-Me conference VDN extension.
- Calls to Avaya Messaging (**Section 5.3.4**).

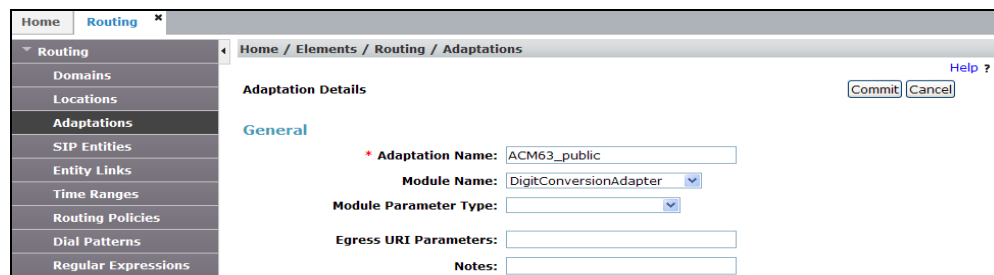
5.3.1. Adaptation for Avaya Aura® Communication Manager Extensions

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager extensions from AT&T.

Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

Step 2 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **ACM63_public**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).



Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager).

1. **Example 1 – destination extension:** 5553161 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension 19001.

- Enter **5553161** in the **Matching Pattern** column.
- Enter **7** in the **Min/Max** columns.
- Enter **7** in the **Delete Digits** column.
- Enter **19001** in the **Insert Digits** column.
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 – Repeat **Step 3** for all additional AT&T DNIS numbers.

Step 5 - Click on **Commit**.

Note – As shown in the screen below, no **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

Note – In the reference configuration, the AT&T IPFR-EF service delivered 7 digit DNIS numbers. The numbers defined here are those sent by AT&T in the R-URI, *not* the number that was dialed.

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 5553161	* 7	* 7		* 7	19001	destination	
<input type="checkbox"/>	* 5553162	* 7	* 7		* 7	19002	destination	
<input type="checkbox"/>	* 5553163	* 7	* 7		* 7	19003	destination	

5.3.2. Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service

The Adaptation administered in this section is used for modification of SIP messages from Communication Manager to AT&T. Repeat the steps in **Section 5.3.1** with the following changes.

Step 1 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **ATT**).
2. Select **AttAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **AttAdapter**). The AttAdapter will automatically remove History-Info headers, (which the IPFR-EF service does not support), sent by Communication Manager (see **Section 6.8.1**).

Note – As shown in the screen below, no Incoming or Outgoing Digit Conversion was required in the reference configuration.

5.3.3. Adaptation for Meet-Me Conference Calls

The dedicated Meet-Me conference DNIS number is converted to the Meet-Me conference VDN extension (see **Section 2.2, Item 1**). Repeat the steps in **Section 5.3.1** with the following changes.

Step 1 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **Main_Meet-Me**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).

Step 2 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section.

3. 5553180 is the DNIS string for the Meet-Me conference. It is associated with Communication Manager VDN extension 19000.
 - Enter **5553180** in the **Matching Pattern** column.
 - Enter **7** in the **Min/Max** columns.
 - Enter **7** in the **Delete Digits** column.
 - Enter **19000** in the **Insert Digits** column.
 - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
 - Enter any desired notes.

Note – As shown in the screen below, no Incoming Digit Conversion was required in the reference configuration.

5.3.4. Adaptation for calls to Avaya Aura® Messaging

This adaptation is for call to Avaya Messaging (e.g., message retrieval). Repeat the steps in **Section 5.3.1** with the following changes.

Step 1 - In the **Adaptation Details** page, enter:

4. A descriptive **Name**, (e.g., **AAM_Digits**).
5. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section.

6. 5553170 is the DNIS string for Avaya messaging access.
 - Enter **5553170** in the **Matching Pattern** column.
 - Enter **7** in the **Min/Max** columns.
 - Enter **7** in the **Delete Digits** column.
 - Enter **36000** in the **Insert Digits** column.
 - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
 - Enter any desired notes.

Step 4 – Click on **Commit**.

Note – As shown in the screen below, no Incoming Digit Conversion was required in the reference configuration.

Adaptation Details Commit Cancel

General

* Adaptation Name:

Module Name:

Module Parameter Type:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Filter: Enable

<input type="checkbox"/> 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

1 Item Filter: Enable

<input type="checkbox"/> Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input checked="" type="checkbox"/> *5553170	*10	*10		*10	36000	destination		

Select : All, None

5.4. SIP Entities

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

- Session Manager (**Section 5.4.1**).
- Communication Manager for AT&T trunk access (**Section 5.4.2**) – This entity, and its associated Entity Link (using TCP with port 5062), is for calls to/from AT&T and Communication Manager via the Avaya SBCE. Note that this connection will be associated with the NCR *enabled* trunk on Communication Manager (see **Section 2.2**, Item 1).
- Communication Manager for local trunk access (**Section 5.4.3**) – This entity, and its associated Entity Link (using TCP with port 5060), is primarily for traffic between Avaya SIP telephones and Communication Manager, as well as calls to Avaya Messaging.
- Communication Manager for Meet-Me conference trunk access (**Section 5.4.4**) – If support for Meet-Me conferences is required, then this Entity, and its associated Entity Link must be added. Note that this connection will be associated with the NCR *disabled* trunk on Communication Manager (see **Section 2.2**, Item 1).
- Avaya SBCE (**Section 5.4.5**) - This entity, and its associated Entity Link (using TCP and port 5060), is for calls to/from the IPFR-EF service via the Avaya SBCE.
- Avaya Messaging (**Section 5.4.6**) - This entity, and its associated Entity Link (using TCP and port 5060), is for calls to/from Avaya Messaging.

Note – In the reference configuration, TCP is used as the transport protocol between Session Manager and Communication Manager (ports 5060, 5062, and 5080), and to the Avaya SBCE (port 5060). This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS to be used as the transport protocol whenever possible. The connection between the Avaya SBCE and the AT&T IPFR-EF service uses UDP/5060 per AT&T requirements.

5.4.1. Avaya Aura® Session Manager SIP Entity

Step 1 - In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name (e.g., **sm63**).
- **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **192.168.67.47**).
- **Type** – Verify **Session Manager** is selected.
- **Location** – Select location **Main** (Section 5.2.1).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.

Step 3 - In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:

- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.

The screenshot shows the 'SIP Entity Details' page with the 'General' tab selected. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the following fields: Name (sm63), FQDN or IP Address (192.168.67.47), Type (Session Manager), Notes (blank), Location (Main), Outbound Proxy (blank), Time Zone (America/New_York), and Credential name (blank). At the bottom, the 'SIP Link Monitoring' section is set to 'Use Session Manager Configuration'. Buttons for 'Commit' and 'Cancel' are in the top right corner.

Step 4 – Scrolling down to the **Port** section of the **SIP Entity Details** page, click on **Add** and provision entries as follow:

- **Port** – Enter **5060**.
- **Protocol** – Select **TCP**.
- **Default Domain** – Select a SIP domain administered in **Section 5.1** (e.g., **customer.com**).

Step 5 - Repeat **Step 4** to provision entries for:

- **5062** for **Port** and **TCP** for **Protocol**.
- **5080** for **Port** and **TCP** for **Protocol**.
- **5061** for **Port** and **TLS** for **Protocol**. While TLS is not used in the reference configuration, it is included here for completeness.

Step 6 – Enter any notes as desired and leave all other fields on the page blank/default.

Step 7 - Click on **Commit**.

Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

The screenshot shows a configuration form for a SIP Entity. At the top, there are fields for 'TCP Failover port' and 'TLS Failover port', each with an 'Add' and 'Remove' button. Below this is a table with 4 items, showing a list of ports (5060, 5061, 5062, 5080) with checkboxes, protocols (TCP, TLS), and default domains (customera.com). A 'Filter: Enable' button is on the right. Below the table is a 'Select: All, None' dropdown. The next section is 'SIP Responses to an OPTIONS Request', which has an 'Add' and 'Remove' button and a table with 0 items. The table has columns for 'Response Code & Reason Phrase', 'Mark Entity Up/Down', and 'Notes'. A 'Filter: Enable' button is also present on the right.

5.4.2. Avaya Aura® Communication Manager SIP Entity – Public Trunk

Step 1 - In the **SIP Entities** page, click on **New** (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name (e.g. **ACM63_public**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 6.5** (e.g. **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **ACM63_public** administered in **Section 5.3.1**.
- **Location** – Select a Location **Main** administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

The screenshot shows the 'SIP Entity Details' form for a new entity. The left sidebar has a menu with 'Routing' selected. The main area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. The 'General' section contains fields for 'Name' (ACM63_public), 'FQDN or IP Address' (192.168.67.202), 'Type' (CM), 'Notes', 'Adaptation' (ACM63_public), 'Location' (Main), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Credential name', and 'Call Detail Recording' (none). The 'Loop Detection' section has a 'Loop Detection Mode' (Off). The 'SIP Link Monitoring' section has 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. At the bottom, there are checkboxes for 'Supports Call Admission Control' and 'Shared Bandwidth Manager', and dropdowns for 'Primary Session Manager Bandwidth Association' and 'Backup Session Manager Bandwidth Association'.

5.4.3. Avaya Aura® Communication Manager SIP Entity – Local Trunk

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 5.4.2** with the following changes:

- **Name** – Enter a descriptive name (e.g. **ACM63_local**).
- Note that this Entity has no Adaptation defined.

The screenshot shows the 'SIP Entity Details' window with the 'General' tab selected. The configuration is as follows:

- Name:** ACM63_local
- FQDN or IP Address:** 192.168.67.202
- Type:** CM
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** Main
- Time Zone:** America/New_York
- SIP Timer B/F (In seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty)
- Backup Session Manager Bandwidth Association:** (empty)

5.4.4. Avaya Aura® Communication Manager SIP Entity – Meet-Me Trunk

Repeat the steps in **Section 5.4.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **ACM63_Meet-Me**).
- **Adaptations** – Select Adaptation **Main_Meet-Me** (Section 5.3.3).

The screenshot shows the 'SIP Entity Details' window with the 'General' tab selected. The configuration is as follows:

- Name:** ACM63_Meet-Me
- FQDN or IP Address:** 192.168.67.202
- Type:** CM
- Notes:** Meet-Me Conference without NCR
- Adaptation:** Main_Meet-Me
- Location:** Main
- Time Zone:** America/New_York
- SIP Timer B/F (In seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty)
- Backup Session Manager Bandwidth Association:** (empty)

5.4.5. Avaya Session Border Controller for Enterprise SIP Entity

Repeat the steps in **Section 5.4.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **A-SBCE**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **192.168.70.120**, see **Section 7.4.1**).
- **Type** – Verify **Other** is selected.
- **Adaptations** – Select Adaptation **ATT** (**Section 5.3.2**).
- **Location** – Select location **Common** (**Section 5.2.2**).

The screenshot shows the 'SIP Entity Details' configuration window with the 'General' tab selected. The window has 'Commit' and 'Cancel' buttons in the top right corner. The configuration fields are as follows:

- Name:** A-SBCE
- FQDN or IP Address:** 192.168.70.120
- Type:** Other
- Notes:** (empty text box)
- Adaptation:** ATT
- Location:** Common
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text box)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty dropdown)
- Loop Detection:** Loop Detection Mode: Off
- SIP Link Monitoring:** SIP Link Monitoring: Use Session Manager Configuration
- Supports Call Admission Control:** (unchecked checkbox)
- Shared Bandwidth Manager:** (unchecked checkbox)
- Primary Session Manager Bandwidth Association:** (empty dropdown)
- Backup Session Manager Bandwidth Association:** (empty dropdown)

5.4.6. Avaya Aura® Messaging SIP Entity

Repeat the steps in **Section 5.4.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **AA-M**).
- **FQDN or IP Address** – Enter the IP address of Avaya Messaging (e.g., **192.168.67.147**, see **Section 3.1**).
- **Type** – Verify **Other** is selected.
- **Adaptations** – Select Adaptation **AAM_Digits** (**Section 5.3.4**).
- **Location** – Select location **Main** (**Section 5.2.1**).

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

Loop Detection

Loop Detection Mode:

SIP Link Monitoring

SIP Link Monitoring:

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

5.5. Entity Links

In this section, Entity Links are administered for the following connections:

- Session Manager to Communication Manager Public trunk (**Section 5.5.1**).
- Session Manager to Communication Manager Local trunk (**Section 5.5.2**).
- Session Manager to Communication Manager Meet-Me trunk (**Section 5.5.3**).
- Session Manager to Avaya SBCE (**Section 5.5.4**).
- Session Manager to Avaya Messaging (**Section 5.5.5**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 5.4**.

Note – See the information in **Section 5.4** regarding the transport protocols and ports used in the reference configuration.

5.5.1. Entity Link to Avaya Aura® Communication Manager – Public Trunk

Step 1 - In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).

Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g., **sm63**).
- **SIP Entity 1 Port** – Enter **5062**.
- **Protocol** – Select **TCP** (see **Section 6.8.1**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **ACM63_public**).

- **SIP Entity 2 Port** - Enter **5062** (see Section 6.8.1).
- **Connection Policy** – Select **Trusted**.

Step 3 - Click on **Commit**.

5.5.2. Entity Link to Avaya Aura® Communication Manager – Local Trunk

To configure this Entity Link, repeat the steps in Section 5.5.1, with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_local**).
- **SIP Entity 1 Port** – Enter **5060**.
- **SIP Entity 2** –Select the SIP Entity administered in Section 5.4.3 for the Communication Manager local entity (e.g., **ACM63_local**).
- **SIP Entity 2 Port** - Enter **5060** (see Section 6.8.2).

5.5.3. Entity Link to Avaya Aura® Communication Manager – Meet-Me Trunk

To configure this Entity Link, repeat the steps in Section 5.5.1, with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_Meet-Me**).
- **SIP Entity 1 Port** – Enter **5080**.
- **SIP Entity 2** –Select the SIP Entity administered in Section 5.4.4 for the Communication Manager Meet-Me trunk entity (e.g., **ACM63_Meet-Me**).
- **SIP Entity 2 Port** - Enter **5080** (see Section 6.8.3).

5.5.4. Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sm63_A-SBCE**).
- **SIP Entity 1 Port** – Enter **5060**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.5** for the Avaya SBCE entity (e.g., **A-SBCE**).
- **SIP Entity 2 Port** - Enter **5060**

5.5.5. Entity Link to Avaya Aura® Messaging

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to Avaya Messaging (e.g., **sm63_AAM**).
- **SIP Entity 1 Port** – Enter **5060**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.6** for the Avaya Messaging entity (e.g., **AA-M**).
- **SIP Entity 2 Port** - Enter **5060** (see **Section 6.8.2**).

5.6. Time Ranges – (Optional)

Step 1 - In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New** (not shown).

Step 2 - Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkbox(s) for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on **Commit**. Repeat these steps to provision additional time ranges as required.

The screenshot shows the 'Time Ranges' configuration page. The left sidebar has 'Time Ranges' selected under the 'Routing' section. The main area shows a table with one item, '24/7', which is checked for all days of the week (Mo, Tu, We, Th, Fr, Sa, Su). The start time is 00:00 and the end time is 23:59. The notes field contains 'Time Range 24/7'. There are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' at the top. A 'Filter: Enable' link is on the right.

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

5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (**Section 5.7.1**).
- Inbound calls to Communication Manager Meet-Me Conference (**Section 5.7.2**).
- Inbound calls to Avaya Messaging (**Section 5.7.3**).
- Outbound calls to AT&T/PSTN (**Section 5.7.4**).

5.7.1. Routing Policy for AT&T Routing to Avaya Aura® Communication Manager

This Routing Policy is used for inbound calls from AT&T.

Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **ACM63_Public**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the **SIP Entities** list page will open.

The screenshot shows the 'Routing Policy Details' page. The left sidebar has 'Routing Policies' selected under the 'Routing' section. The main area shows the 'General' section with fields for 'Name' (ACM63_Public), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (from AT&T). There are 'Commit' and 'Cancel' buttons. Below is the 'SIP Entity as Destination' section with a 'Select' button and a table with columns 'Name', 'FQDN or IP Address', 'Type', and 'Notes'.

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

Step 4 - In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**ACM63_Public**), and click on **Select**.

Name	FQDN or IP Address	Type	Notes
ACM63_local	192.168.67.202	CN	
ACM63_Meet-Me	192.168.67.202	CN	Meet-Me Conference without NCR
ACM63_public	192.168.67.202	CN	
A-SBC	192.168.75.120	Other	
sm63	192.168.67.47	Session Manager	

Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**.

Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, enter a **Ranking** of 2, and click on **Commit**.

Step 8 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

Step 9 - No **Regular Expressions** were used in the reference configuration.

Step 10 - Click on **Commit**.

Routing Policy Details

General

* Name: ACM63_Public

Disabled: ☐

* Retries: 0

Notes: from AT&T

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM63_public	192.168.67.202	CN	

Time of Day

Add Remove View Gaps/Overlaps

1 Item

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

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Select: All, None

Regular Expressions

Add Remove

0 Items

Pattern	Rank Order	Deny	Notes

5.7.2. Routing Policy for Inbound Routing to Avaya Aura® Communication Manager Meet-Me Conference

As described in **Section 2.2, Item 1**, an issue was found with Meet-Me conference calls when Network Call Redirection (NCR) is enabled on Communication Manager. This requires Meet-Me conference calls to use a separate SIP trunk with NCR disabled. As a result separate routing is required to deliver Meet-Me conference calls to this trunk. Repeat the steps in **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **ACM63_Meet-Me**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.4** for Communication Manager Meet-Me conference (e.g. **ACM63_Meet-Me**).
- In the **Time of Day** section, change the ranking number to **1**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Home / Elements / Routing / Routing Policies

Routing Policy Details [Commit] [Cancel] [Help ?]

General

* Name: ACM63_Meet-Me

Disabled: ☐

* Retries: 0

Notes: IPFR Meet-Me

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM63_Meet-Me	192.168.67.202	CM	Meet-Me Conference without NCR

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
1	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

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

Select : All, None

Regular Expressions

Add Remove

0 Items Filter: Enable

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

5.7.3. Routing Policy for Inbound Routing to Avaya Aura® Messaging

This routing policy is for inbound calls to Avaya Messaging for message retrieval.

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **To_AAM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.6** for Avaya Messaging (e.g. **AA-M**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details

Commit

Cancel

General

* Name:

To_AAM

Disabled:

☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AA-M	192.168.67.147	Modular Messaging	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

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

Filter: Enable

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

Select : All, None

Regular Expressions

Add

Remove

0 Items

Filter: Enable

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

5.7.4. Routing Policy for Outbound Calls to AT&T

This Routing Policy is used for Outbound calls to AT&T. Repeat the steps in **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to the AT&T IPFR-EF service via the Avaya SBCE (e.g. **A-SCBE_to_ATT**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.5** for the Avaya SBCE SIP Entity (e.g. **A-SBCE**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

The screenshot shows the 'Routing Policy Details' page for a policy named 'A-SCBE_to_ATT'. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is divided into several sections:

- General**: Includes fields for Name (A-SCBE_to_ATT), Disabled (unchecked), Retries (0), and Notes.
- SIP Entity as Destination**: A 'Select' button and a table listing SIP entities.
- Time of Day**: Includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. It shows 1 item with a table of time ranges.
- Dial Patterns**: Includes 'Add' and 'Remove' buttons and a table for dial patterns.
- Regular Expressions**: Includes 'Add' and 'Remove' buttons and a table for regular expressions.

SIP Entity as Destination Table:

Name	FQDN or IP Address	Type	Notes
A-SBCE	192.168.70.120	Other	

Time of Day Table:

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7

Dial Patterns Table:

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

Regular Expressions Table:

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

5.8. Dial Patterns

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

- Inbound PSTN calls via the IPFR-EF service to Communication Manager (**Section 5.8.1**).
- Outbound calls to AT&T (**Section 5.8.2**).
- Inbound calls to Communication Manager Meet-Me conference (**Section 5.8.3**).
- Inbound calls to Avaya Messaging (**Section 5.8.4**).

5.8.1. Matching Inbound PSTN Calls to Avaya Aura® Communication Manager

In the reference configuration inbound calls from the IPFR-EF service sent 7 digits in the SIP Request URI. This pattern must be matched for further call processing.

Note – Be sure to match on the digit string specified in the AT&T Request URI, not the digit string that is dialed. They may be different.

Step 1 - In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** (not shown).

Step 2 - In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – In the reference configuration, AT&T sends a 7 digit number in the Request URI with the format 555xxxx. Enter **555**. Note - The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 555xxxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **7**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.

The screenshot displays the 'Dial Pattern Details' configuration page in the Avaya Aura web interface. The left-hand navigation pane is expanded to 'Routing', and 'Dial Patterns' is the active selection. The breadcrumb trail at the top reads 'Home / Elements / Routing / Dial Patterns'. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are populated: 'Pattern' is '555', 'Min' is '7', 'Max' is '7', 'Emergency Call' is unchecked, 'Emergency Priority' is '1', 'Emergency Type' is empty, 'SIP Domain' is set to '-ALL-' via a dropdown menu, and 'Notes' contains the text 'ATT Production inbound 7 digits'.

Step 3 – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.

Step 4 - In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to all Locations).

Step 5 - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7.1** (e.g., **ACM63_Public**). Click on **Select**.

Originating Location Select Cancel

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

4 Items Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Common	A-SBCE & ATT router
<input type="checkbox"/>	Main	

Select : All, None

Routing Policies

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ACM63_Local	<input type="checkbox"/>	ACM63_local	
<input type="checkbox"/>	ACM63_Meet-Me	<input type="checkbox"/>	ACM63_Meet-Me	IPFR Meet-Me
<input checked="" type="checkbox"/>	ACM63_Public	<input type="checkbox"/>	ACM63_public	from AT&T
<input type="checkbox"/>	A-SBCE_to_ATT	<input type="checkbox"/>	A-SBCE	

Select : All, None

Step 6 - Returning to the Dial Pattern Details page click on **Commit**.

Originating Locations and Routing Policies

Add Remove

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		ACM63_Public		<input type="checkbox"/>	ACM63_public	from AT&T

Select : All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

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

Commit Cancel

Step 7 - Repeat **Steps 1-7** for any additional inbound dial patterns from AT&T.

5.8.2. Matching Outbound Calls to AT&T

In this section, Dial Patterns are administered for all outbound calls to AT&T. In the reference configuration 1xxxxyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes *7 and *9 (e.g., *71yyyzzzzxxxx & *91yyyzzzzxxxx) were verified.

Step 1 - Repeat the steps shown in **Section 5.8.1**, with the following changes:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to AT&T/PSTN (e.g. **1732**).
- Enter a **Min** and **Max** pattern of **11**.

- In the **Routing Policies** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to the Routing Policy administered for routing calls to AT&T in **Section 5.7.4** (e.g., **A-SBCE_to_ATT**).

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

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

Select : All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

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

Step 2 - Repeat **Step 1** to add patterns for IPFR-EF Call Forward access codes with patterns ***7** and ***9**, and **Min/Max=13**.

Step 3 - Repeat **Step 1** to add patterns for international calls with pattern **011** with **Min=11** and **Max=16**.

Step 4 - Repeat **Step 1** to add any additional outbound patterns as required.

Dial Patterns New Edit Delete Duplicate More Actions

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	0	1	1	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	011	12	16	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1303	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1513	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1720	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1732	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1800	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1877	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1888	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1908	11	11	<input type="checkbox"/>			-ALL-	

Select : All, None Page 1 of 2

5.8.3. Matching Inbound Calls to Avaya Aura® Communication Manager Meet-Me Conference

As described in **Section 2.2, Item 1**, an issue was found with Meet-Me conference calls when Network Call Redirection (NCR) is enabled on Communication Manager. This requires Meet-Me conference calls to use a separate SIP trunk with NCR disabled. As a result a specific IPFR-EF access number(s) must be selected for user to generate inbound Meet-Me conference calls. This unique Dial Pattern is required to deliver Meet-Me conference calls to this dedicated trunk.

In the reference configuration, the designated Meet-Me conference IPFR-EF access number generates a R-URI with the digits 5553180. The call is then directed to the Communication Manager VDN extension 19000, used for the Meet-Me conference (see **Sections 5.3.3** and **6.14.2**).

Step 1 – Repeat the steps in **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern matching the IPFR-EF access number selected for inbound Meet-Me conference calls (e.g., **5553180**).
- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to Location **Common** (**Section 5.2.2**).
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy **ACM63_Meet-Me** (**Section 5.7.2**).

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: 5553180

* Min: 7

* Max: 7

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: To Meet-Me Conf

Originating Locations and Routing Policies

[Add] [Remove]

2 Items [Filter: Enable]

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Common	A-SBCE & ATT router	ACM63_Meet-Me	1	<input type="checkbox"/>	ACM63_Meet-Me	IPFR Meet-Me

Select : All, None

Denied Originating Locations

[Add] [Remove]

0 Items [Filter: Enable]

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

5.8.4. Matching Inbound PSTN Calls to Avaya Aura® Messaging

In order for PSTN to check and retrieve messages, the following Dial Pattern is defined. In the reference configuration, Communication Manager extension 36000 is used for Avaya Messaging access (see [Section 5.3.4](#)).

Step 1 – Repeat the steps in [Section 5.8.1](#) with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern matching the IPFR-EF access number selected for calls to Avaya Messaging (e.g., **5553170**).
- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to **All** Locations.
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy **To_AAM** ([Section 5.7.3](#)).

Dial Pattern Details

Commit

Cancel

General

* Pattern: 5553170

* Min: 7

* Max: 7

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: To AAM

Originating Locations and Routing Policies

Add

Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To_AAM	0	<input type="checkbox"/>	AA-M	

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Filter: Enable

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

6. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration have already been performed. Consult [5 - 7] for more information.

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

6.1. System-Parameters Customer-Options

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

NOTE - For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.

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

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	12000	0	
Maximum Concurrently Registered IP Stations:	18000	4	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	41000	0	
Maximum Video Capable IP Softphones:	18000	5	
Maximum Administered SIP Trunks:	24000	30	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	522	0	
Maximum TN2501 VAL Boards:	128	0	
Maximum Media Gateway VAL Sources:	250	1	
Maximum TN2602 Boards with 80 VoIP Channels:	128	0	
Maximum TN2602 Boards with 320 VoIP Channels:	128	0	
Maximum Number of Expanded Meet-me Conference Ports:	300	0	
(NOTE: You must logoff & login to effect the permission changes.)			

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

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

Step 3 - On Page 4 of the form, verify that the Enhanced EC500?, IP Stations?, IP Trunks?, and ISDN/SIP Network Call Redirection? fields are set to y.

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

Step 5 - On **Page 5** of the form, verify that the **Private Networking** and **Processor Ethernet** fields are set to **y**.

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

6.2. System-Parameters Features

Step 1 - Enter the **change system-parameters features** command. On **Page 1** of the form, verify that the **Trunk-to-Trunk Transfer** is set to **all**.

change system-parameters features		Page 1 of 20
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled? y		
Trunk-to-Trunk Transfer: all		
Automatic Callback with Called Party Queuing? n		
Automatic Callback - No Answer Timeout Interval (rings): 3		
Call Park Timeout Interval (minutes): 10		
Off-Premises Tone Detect Timeout Interval (seconds): 20		
AAR/ARS Dial Tone Required? y		
Music (or Silence) on Transferred Trunk Calls? no		
DID/Tie/ISDN/SIP Intercept Treatment: attendant		
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred		
Automatic Circuit Assurance (ACA) Enabled? n		
Abbreviated Dial Programming by Assigned Lists? n		
Auto Abbreviated/Delayed Transition Interval (rings): 2		
Protocol for Caller ID Analog Terminals: Bellcore		
Display Calling Number for Room to Room Caller ID Calls? n		

6.3. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager.

Step 1 - Enter the **change dialplan analysis** command to provision the following dial plan.

- 3-digit facilities access codes (indicated with a **Call Type** of **fac**) beginning with ***** and **#** for Feature Access Code (FAC) access.
- 5-digit extensions with a **Call Type** of **ext** beginning with:
 - The digit **1** for Communication Manager extensions.
 - The digit **3** for the Avaya Messaging access extension.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code **6xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 6.8**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**), e.g., access code **8** for Automatic Alternate Routing dialing, see **Section 6.12**; code **9** for outbound Automatic Route Selection dialing, see **Section 6.11**.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	5	ext							
3	5	ext							
6	3	dac							
8	1	fac							
9	1	fac							
*	3	fac							
#	3	fac							

6.4. IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. Note that a Processor Ethernet (procr) based Communication Manager platform is used in the reference configuration for Communication Manager. Note that the Communication Manager procr name and IP address are entered during installation. The procr IP address was used to define the Communication Manager SIP Entities in **Section 5.4**.

Step 1 - Enter the **change node-names ip** command, and add a node name and IP address for the following:

- Avaya SBCE private network interface (e.g., **A-SBCE** and **192.168.70.120**).
- Session Manager SIP signaling interface (e.g., **SM63** and **192.168.67.47**).

change node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
A-SBCE	192.168.70.120		
SM63	192.168.67.47		
default	0.0.0.0		
procr	192.168.67.202		

6.5. IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters defined during installation.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to **y**.
- In the reference configuration the procr is assigned to **Network Region: 1**.
- The default values are used for the remaining parameters.

display ip-interface procr		Page 1 of 2	
IP INTERFACES			
Type: PROCR		Target socket load: 1700	
Enable Interface? y		Allow H.323 Endpoints? y	
Network Region: 1		Allow H.248 Gateways? y	
		Gatekeeper Priority: 5	
IPV4 PARAMETERS			
Node Name: procr		IP Address: 192.168.67.202	
Subnet Mask: /24			

6.6. IP Network Regions

Network Regions are used to group various Communication Manager resources such as codecs, UDP port ranges, and inter-region communication. In the reference configuration, two network regions are used, one for the Main site (region 1), and one for AT&T SIP trunk access (region 2).

6.6.1. IP Network Region 1 – Local CPE Region

Step 1 – Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region **1**). This IP network region will be used to represent the local CPE. Populate the form with the following values:

- Enter a descriptive name (e.g., **Main**).
- Enter the enterprise domain (e.g., **customera.com**) in the **Authoritative Domain** field (see **Section 5.1**).
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min:** – Set to **16384** (**AT&T requirement**).
- **UDP Port Max:** – Set to **32767** (**AT&T requirement**).

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

Step 2 - On page 2 of the form:

- Verify that RTCP Reporting Enabled is set to **y**.

change ip-network-region 1	Page 2 of 20
IP NETWORK REGION	
RTCP Reporting Enabled? y	
RTCP MONITOR SERVER PARAMETERS	
Use Default Server Parameters? y	

Step 3 - On page 4 of the form:

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **2** in the **dst rgn** column, enter **2** for the codec set (this means region 1 is permitted to talk to region 2 and it will use codec set 2 to do so). The **direct WAN** and **Units** columns will self populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

change ip-network-region 1										Page 4 of 20		
Source Region: 1 Inter Network Region Connection Management										I	M	
										G	A t	
dst	codec	direct	WAN-BW-limits	Video	Intervening					Dyn	A G c	
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions					CAC	R L e
1	1											all
2	2	y	NoLimit								n	t

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

Note that this region is used for general inbound/outbound calls with AT&T, as well as for calls to the Meet-Me conference, and Avaya Messaging access. Repeat the steps in **Section 6.6.1** with the following changes:

Step 1 – On **Page 1** of the form (not shown):

- Enter a descriptive name (e.g., **AT&T**).
- Enter **2** for the **Codec Set** parameter.

Step 2 – On **Page 4** of the form:

- Set codec set **2** for **dst rgn 1**.
- Note that **dst rgn 2** is pre-populated with codec set **2** (from page 1 provisioning).

change ip-network-region 2										Page	4	of	20
Source Region: 2 Inter Network Region Connection Management										I			M
										G	A		t
dst	codec	direct	WAN-BW-limits	Video	Intervening					Dyn	A	G	c
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions				CAC	R	L	e
1	2	y	NoLimit								n		t
2	2												all

6.7. IP Codec Parameters

6.7.1. Codecs for IP Network Region 1 (calls within the CPE)

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

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

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

change ip-codec-set 1		IP Codec Set	Page	2 of 2
Allow Direct-IP Multimedia? y				
Maximum Call Rate for Direct-IP Multimedia:		2048:Kbits		
Maximum Call Rate for Priority Direct-IP Multimedia:		2048:Kbits		
Mode		Redundancy		
FAX	t.38-standard	0		
Modem	off	0		
TDD/TTY	off	0		
Clear-channel	n	0		

6.7.2. Codecs for IP Network Region 2 (calls to/from AT&T)

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g., **2**). This IP codec set will be used for IPFR-EF calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown, however the order of G.729B and G.729A may be reversed as required. Set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms).

change ip-codec-set 2		IP Codec Set		Page	1 of 2
Codec Set: 2					
Audio	Silence	Frames	Packet		
Codec	Suppression	Per Pkt	Size (ms)		
1: G.729B	n	3	30		
2: G.729A	n	3	30		
3: G.711MU	n	2	30		

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

change ip-codec-set 2		IP Codec Set		Page	2 of 2
		Allow Direct-IP Multimedia? y			
		Maximum Call Rate for Direct-IP Multimedia: 2048:Kbits			
		Maximum Call Rate for Priority Direct-IP Multimedia: 2048:Kbits			
	Mode	Redundancy			
FAX	t.38-standard	0			
Modem	off	0			
TDD/TTY	off	0			
Clear-channel	n	0			

6.8. SIP Trunks

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group. Three SIP trunks are defined on Communication Manager in the reference configuration:

- Inbound/outbound AT&T access – SIP Trunk 2
 - Note that this trunk will use TCP port 5062 as described in **Section 5.5.1**.
- Internal CPE access (e.g., Avaya SIP telephones, Avaya Messaging, etc) – SIP Trunk 1
 - Note that this trunk will use TCP port 5060 as described in **Section 5.5.2**.
- Avaya Meet-Me conference access – SIP Trunk 3
 - Note that this trunk will use TCP port 5080 as described in **Section 5.5.3**.

Note – Although TCP is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the IPFR-EF service. See the note in **Section 5.4** regarding the use of TCP and TLS transport protocols in the CPE.

6.8.1. SIP Trunk for Inbound/Outbound AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for IPFR-EF calls. This trunk corresponds to the **ACM63_Public** SIP Entity defined in **Section 5.4.2**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **2**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp** (see the note at the beginning of this section).
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.4** (e.g., **SM63**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5062**.
- **Far-end Network Region** – Set the IP network region to **2**, as set in **Section 6.6.2**.
- **Far-end Domain** – Enter **customerera.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **OPTIONAL**: If desired, set **Initial IP-IP Direct Media** is set to **y**. Otherwise leave it disable (default).

Note - Enabling the **Initial IP-IP Direct Media** parameter allows Communication Manager to signal the IP address of Avaya SIP telephones during the initial setup of a call. This permits the Avaya SIP telephone and the AT&T caller to exchange Media directly, without allocating Communication Manager media resources. However, unless network routing permits direct IP access between the Avaya SIP telephone and AT&T, a loss of audio can occur when this option is enabled.

- Use the default parameters on **page 2** of the form (not shown).

add signaling-group 2		SIGNALING GROUP		Page 1 of 1	
Group Number: 2		Group Type: sip			
IMS Enabled? n		Transport Method: tcp			
Q-SIP? n					
IP Video? n				Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y		Peer Server: SM			
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n					
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n					
Near-end Node Name: procr		Far-end Node Name: SM63			
Near-end Listen Port: 5062		Far-end Listen Port: 5062			
Far-end Domain: customerera.com		Far-end Network Region: 2			
		Bypass If IP Threshold Exceeded? n			
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n			
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y			
Session Establishment Timer(min): 3		IP Audio Hairpinning? n			
Enable Layer 3 Test? y		Initial IP-IP Direct Media? n			
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6			

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

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **ATT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **602**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Step 1** (e.g., **2**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **20**).

add trunk-group 2		TRUNK GROUP	Page 1 of 21
Group Number: 2	Group Type: sip	COR: 1	CDR Reports: y
Group Name: ATT	TN: 1	TAC: 602	
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 2	
		Number of Members: 20	

Step 3 - On **Page 2** of the **Trunk Group** form:

- Set the **Preferred Minimum Session Refresh Interval(sec)**: to **900**. This entry will actually cause a value of 1800 to be generated in the SIP Session-Expires header pertaining to active call session refresh.

add trunk-group 2		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
	Redirect On OPTIM Failure: 6000	
SCCAN? n	Digital Loss Group: 18	
	Preferred Minimum Session Refresh Interval(sec): 900	
Disconnect Supervision - In? y Out? y		
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n	

Step 4 - On **Page 3** of the **Trunk Group** form:

- Set **Numbering Format**: to **private**.

Note – Typically a trunk defined as **public-ntwrk** (see **Step 2** above), will use a public numbering format. However, when a public numbering format is selected, Communication Manager will insert a plus sign (+) prefix. When a private numbering format is specified, Communication Manager does not insert the plus prefix. The IPFR-EF service does not require number formats with plus, so private numbering was used for the public trunk (see **Section 6.9**).

add trunk-group 2	TRUNK FEATURES	Page 3 of 21
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
	UI Treatment: service-provider	
	Replace Restricted Numbers? y	
	Replace Unavailable Numbers? y	
	Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y		

Step 5 - On Page 4 of the Trunk Group form:

- Verify **Network Call Redirection** is set to **y**. See **Section 2.2, Item 1** regarding the use of Network Call Redirection (NCR) with Meet-Me conference.
- Set **Send Diversion Header** to **y**. This is required for Communication Manager station Call Forward scenarios to IPFR-EF service.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPFR-EF service (e.g., **100**).
- Set **Identity for Calling Party Display** to **From**. Note that the display issue described in **Section 2.2, Item 2** may be resolved by setting the *Identity for Calling Party Display*: parameter to *From*. However this parameter is only available on Communication Manager 6.x platforms.

Note – The IPFR-EF service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, the History Info header is automatically removed from SIP signaling by Session Manager, as part of the AttAdapter (see **Section 5.3.2**). Alternatively, History Info may be disabled here.

add trunk-group 2	PROTOCOL VARIATIONS	Page 4 of 21
	Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
	Send Transferring Party Information? n	
	Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n		
	Send Diversion Header? y	
	Support Request History? y	
	Telephone Event Payload Type: 100	
	Convert 180 to 183 for Early Media? n	
	Always Use re-INVITE for Display Updates? n	
	Identity for Calling Party Display: From	
	Block Sending Calling Party Location in INVITE? n	
	Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n	

6.8.2. Local SIP Trunk (Avaya SIP Telephone and Avaya Messaging Access)

This trunk corresponds to the **ACM63_Local** SIP Entity defined in **Section 5.4.3**.

Step 1 – Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **1**), and repeat the steps in **Section 6.8.1** with the following changes:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.6.1**.

add signaling-group 1		SIGNALING GROUP	Page 1 of 1
Group Number: 1	Group Type: sip		
IMS Enabled? n	Transport Method: tcp		
Q-SIP? n			
IP Video? n	Priority Video? y	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y Peer Server: SM			
Near-end Node Name: procr	Far-end Node Name: SM63		
Near-end Listen Port: 5060	Far-end Listen Port: 5060		
	Far-end Network Region: 1		
Far-end Domain: customera.com	Far-end Secondary Node Name:		
	Bypass If IP Threshold Exceeded? n		
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n		
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y		
Session Establishment Timer(min): 3	IP Audio Hairpinning? n		
Enable Layer 3 Test? y	Initial IP-IP Direct Media? y		
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6		

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 1). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.8.1** with the following changes:

- **Group Name** – Enter a descriptive name (e.g., **Local**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **601**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., 1).

add trunk-group 1		TRUNK GROUP	Page 1 of 21
Group Number: 1	Group Type: sip		CDR Reports: y
Group Name: Local	COR: 1	TN: 1	TAC: 601
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 20	

Step 3 - On **Page 2** of the **Trunk Group** form:

- Same as **Section 6.8.1**.

Step 4 - On **Page 3** of the **Trunk Group** form:

- Same as **Section 6.8.1**.

Step 5 - On **Page 4** of the **Trunk Group** form:

- Set **Network Call Redirection** to **n**.
- Set **Diversion header** to **n**.
- Verify **Identity for Calling Party Display** is set to **P-Asserted-Identity** (default).
- Use default values for all other settings.

add trunk-group 1	PROTOCOL VARIATIONS	Page 4 of 21
	Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	Send Transferring Party Information? n	
	Network Call Redirection? n	
	Send Diversion Header? n	
	Support Request History? y	
	Telephone Event Payload Type: 100	
	Convert 180 to 183 for Early Media? n	
	Always Use re-INVITE for Display Updates? n	
	Identity for Calling Party Display: P-Asserted-Identity	
	Block Sending Calling Party Location in INVITE? n	
	Accept Redirect to Blank User Destination? n	
	Enable Q-SIP? n	

6.8.3. SIP Trunk for Meet-Me Conference Calls

This trunk corresponds to the **ACM63_Meet-Me** SIP Entity defined in **Section 5.4.4**.

Step 1 – Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **5**), and repeat the steps in **Section 6.8.1** with the following changes:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5080**
- **Far-end Network Region** – Set to the IP network region **2**, as defined in **Section 6.6.2**.

add signaling-group 5	SIGNALING GROUP	Page 1 of 1
Group Number: 5	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM63	
Near-end Listen Port: 5080	Far-end Listen Port: 5080	
	Far-end Network Region: 2	
Far-end Domain: customera.com	Far-end Secondary Node Name:	
	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **5**). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.8.1** with the following changes:

- **Group Name** – Enter a descriptive name (e.g., **Meet-Me_Conf**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **605**).
- **Service Type** – Set to **public-ntwrk**
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **5**).

add trunk-group 5	TRUNK GROUP	Page 1 of 21
Group Number: 5	Group Type: sip	CDR Reports: y
Group Name: Meet-Me_Conf	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: 605
Dial Access? n		Night Service:
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 5	
	Number of Members: 10	

Step 3 - On **Page 2** of the **Trunk Group** form:

- Same as **Section 6.8.1**.

Step 4 - On **Page 3** of the **Trunk Group** form:

- Same as **Section 6.8.1**.

Step 5 - On **Page 4** of the **Trunk Group** form:

- Verify **Network Call Redirection** to **n**.
- Verify **Diversion header** to **n**.
- Set **Identity for Calling Party Display** to **From** (see **Section 2.2, Item 2**).
- Use default values for all other settings.

add trunk-group 5	PROTOCOL VARIATIONS	Page 4 of 21
	Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type: 100		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? n		
Identity for Calling Party Display: From		
Block Sending Calling Party Location in INVITE? n		
Accept Redirect to Blank User Destination? n		
Enable Q-SIP? n		

6.9. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 6.8.1**), is used to convert Communication Manager local extensions to IPFR-EF DNIS numbers, for inclusion in any SIP headers directed to the IPFR-EF service via the public trunk.

Step 1 – Add the Communication Manager local extension patterns (for the local trunk).

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager station extension pattern 19xxx defined in the Dial Plan in **Section 6.3** (e.g., **19**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 2 – Add each Communication Manager station extension and their corresponding IPFR-EF DNIS numbers (for the public trunk to AT&T). Communication Manager will insert these AT&T DNIS numbers into the From, Contact, and PAI headers as appropriate:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter a Communication Manager extension (e.g., **19001**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **Private Prefix** – Enter the corresponding IPFR-EF DNIS number (e.g., **7325553160**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 3 – Repeat **Step 1** and enter the Avaya Messaging access extension (e.g., **36000**).

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
0	attd		0	1	
5	19	1		5	
5	19001	2	7325553160	10	
5	19002	2	7325553171	10	
5	19003	2	7325553165	10	
5	36000	1		5	

6.10. Route Patterns

Route Patterns are used to direct outbound calls via the public or local CPE SIP trunks.

6.10.1. Route Pattern for Calls to AT&T

This form defines the public SIP trunk, based on the route-pattern selected by the ARS table in **Section 6.11**. In the reference configuration, route pattern 2 is used.

Step 1 – Enter the **change route-pattern 2** command and enter the following:

- In the **Grp No** column enter **2** for SIP trunk 2 (public trunk).
- In the **FRL** column enter **0** (zero).
- In the **Numbering Format** column, across from line **1**: enter **unk-unk** (corresponding to the **private** numbering specified in **Section 6.8.1**).

change route-pattern 2														Page 1 of 3				
Pattern Number: 2														Pattern Name: ATT Trunk				
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: 2	0											n	user					
2:											n	user						
3:											n	user						
		BCC VALUE			TSC CA-TSC		ITC BCIE			Service/Feature			PARM	No.	Numbering	LAR		
0	1	2	M	4	W	Request											Dgts	Format
														Subaddress				
1:	y	y	y	y	y	n	n	rest						unk-unk	none			
2:	y	y	y	y	y	n	n	rest							none			

6.10.2. Route Pattern for Calls within the CPE

This form defines the local SIP trunk, based on the route-pattern selected by the AAR table in **Section 6.12** (e.g., calls to Avaya SIP telephone extensions or Avaya Messaging).

Step 1 – Enter the **change route-pattern 1** command and enter the following:

- In the **Grp No** column enter **1** for SIP trunk 1 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the Numbering Format column, across from line **1**: enter **unk-unk**.

change route-pattern 1															Page 1 of 3		
Pattern Number: 1										Pattern Name: Local Trunk							
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: 1		0												n user			
2:												n user					
3:												n user					
		BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature		PARM	No. Numbering		LAR			
0 1 2 M 4 W					Request							Dgts Format					
										Subaddress							
1: y y y y y n		n												rest		unk-unk none	
2: y y y y y n		n												rest		none	

6.12. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

Step 1 – Enter the following to define Communication Manager extensions:

- **Dialed String** – Enter **19**
- **Min & Max** – Enter **5**.
- **Route Pattern** – Enter **1**.
- **Call Type** – Enter **aar**.

Step 2 – Repeat **Step 1**, and create an entry for Avaya Messaging access extension **36000**.

change aar analysis 0			AAR DIGIT ANALYSIS TABLE				Page 1 of 2	
			Location: all				Percent Full: 1	
Dialed String			Total Min Max	Route Pattern	Call Type	Node Num	ANI	Reqd
19			5 5	1	aar		n	
36000			5 5	1	aar		n	

6.13. Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateways is provisioned. The G430 is located in the Main site and is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. For additional information on G430 provisioning, see [7].

Step 1 – Use SSH to connect to the G430 (not shown). Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., **G430-???(super)#**).

Step 2 - Enter the **show system** command and copy down the G430 serial number (e.g., **10ISO123456**).

Step 3 – Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **192.168.67.202**, see **Section 6.4**).

Step 4 – Enter the **copy run copy start** command to save the G430 configuration.

Step 5 – On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown). Enter the following parameters:

- Set **Type** = **g430**
- Set **Name** = a descriptive name (e.g., **G430**)
- Set **Serial Number** = the serial number copied from **Step 2** (e.g., **10ISO123456**).
- Set the **Encrypt Link** parameter as desired (**n** was used in the reference configuration).
- Set **Network Region** = **1**

Wait a few minutes for the G430 to register to Communication Manager. When the Media Gateway registers, the G430 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., **G430-001(super)#**).

Step 6 – Enter the **display media-gateway 1** command, and verify that the G430 has registered.

```

display media-gateway 1
                                MEDIA GATEWAY 1
                                Type: g430
                                Name: g430
                                Serial No: 10IS0123456
                                Encrypt Link? n
                                Network Region: 1
                                Enable CF? n
                                Location: 1
                                Site Data:

                                Recovery Rule: none
                                Registered? y
                                FW Version/HW Vintage: 34 .5 .1 /1
                                MGP IPV4 Address: 192.168.67.50
                                MGP IPV6 Address:
                                Controller IP Address: 192.168.67.202
                                MAC Address: 00:1b:4f:3c:52:59

```

6.14. Meet-Me Conference Vector and Vector Directory Number (VDN)

Note – The Meet-Me Conference Vector and VDN programming is beyond the scope of this document. The Vectors and VDN shown below are examples and are included for completeness. In addition, the creation of the announcements specified in the vectors is beyond the scope of this document.

In the reference configuration, a separate VDN, and associated Vector, are provisioned to provide the Meet-Me conference functionality in Communication Manager.

6.14.1. Meet-Me Vector

This vector greets the caller and asks for the meeting access code.

```

change vector 6
                                CALL VECTOR
                                Number: 6
                                Name: MeetMeConf
                                Multimedia? n
                                Attendant Vectoring? n
                                Meet-me Conf? y
                                Lock? y
                                Basic? y
                                EAS? y
                                G3V4 Enhanced? y
                                ANI/II-Digits? y
                                ASAI Routing? y
                                Prompting? y
                                LAI? y
                                G3V4 Adv Route? y
                                CINFO? y
                                BSR? y
                                Holidays? y
                                Variables? y
                                3.0 Enhanced? y
                                01 wait-time 5 secs hearing ringback
                                02 collect 6 digits after announcement 12013
                                03 goto step 5 if digits = meet-me-access
                                04 goto step 2 if unconditionally
                                05 route-to meetme
                                06 stop

```

6.14.2. Meet-Me VDN

Note that this VDN extension is specified in the Dial Pattern in **Section 5.8**.

change vdn 19000	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 19000	
Name: MeetMeConf	
Destination: Vector Number	6
Meet-me Conferencing? y	
COR: 1	
TN: 1	

change vdn 19000	Page 2 of 3
VECTOR DIRECTORY NUMBER	
MEET-ME CONFERENCE PARAMETERS:	
Conference Access Code: *	
Conference Controller: 19099	
Conference Type: 6-party	

change vdn 19000	Page 3 of 3
VECTOR DIRECTORY NUMBER	
VDN VARIABLES	
Var	Description Assignment
V1	
V2	
V3	
V4	
V5	
V6	
V7	
V8	
V9	
VDN Time-Zone Offset + 00:00	
Daylight Saving Rule: system	
Use VDN Time Zone For Holiday Vectoring*? n	
Apply Ringback for Auto Answer calls*? y	

6.15. Save Translations

After the Communication Manager provisioning is completed, it must be saved.

Step 1 – Enter the command **save translation**.

7. Configure Avaya Session Border Controller for Enterprise

Note: Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes.

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [8 & 9] for additional information.

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

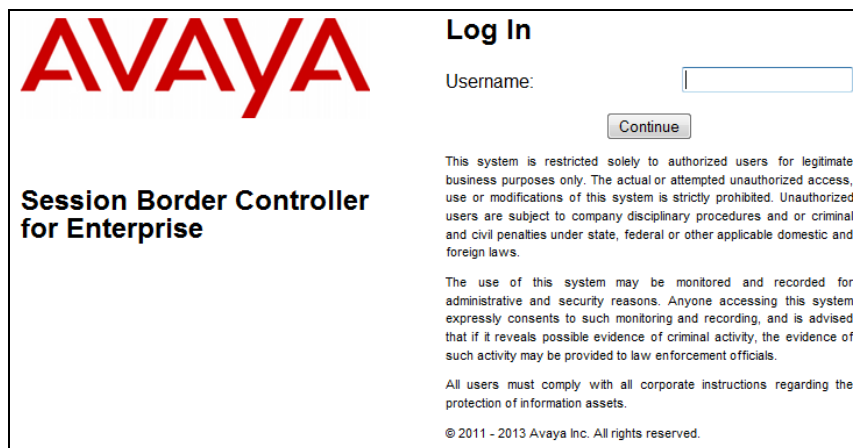
Note – The Avaya SBCE supports a Remote Worker configuration whereby Communications Manager SIP endpoints residing on the public side of the Avaya SBCE, can securely register/operate as a “local” Communication Manager station in the private CPE. While Remote Worker functionality was tested in the reference configuration, Remote Worker provisioning is beyond the scope of this document. See [10] for more information on provisioning Remote Worker.

As described in **Section 3**, the reference configuration places the private interface A1 (IP address 192.168.70.120) of the Avaya SBCE in the Common site with access to the Main site. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 10.10.10.10).

The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.


Step 1 - Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).

Step 2 - Enter the **Username** and click on **Continue**.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Below this is another disclaimer: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." At the bottom, it states: "All users must comply with all corporate instructions regarding the protection of information assets." and "© 2011 - 2013 Avaya Inc. All rights reserved."

Step 3 - Enter the password and click on **Log In**.



Session Border Controller for Enterprise

Log In

Username:

Password:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.


Step 4 - The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

Note – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.

AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsers

Settings ▾Help ▾Log Out

Session Border Controller for Enterprise



Dashboard
Administration
Backup/Restore
System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings

Dashboard

Information	
System Time	09:41:13 AM EST Refresh
Version	6.3.000-19-4338
Build Date	Fri Sep 26 09:14:23 EDT 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
A-SBCE: Max forwards Exceeded
A-SBCE: Max forwards Exceeded
A-SBCE: Max forwards Exceeded
A-SBCE: Max forwards Exceeded
A-SBCE: Max forwards Exceeded

Notes

No notes found.

Installed Devices

EMS

A-SBCE

Add

7.1. System Management – Status

Step 1 - Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.

Note – Certain Avaya SBCE configuration changes require that the underlying application be restarted. To do so, click on **Restart Application** shown below.

The screenshot shows the 'System Management' section of a web interface. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management (highlighted), Global Parameters, Global Profiles, PPM Services, and Domain Policies. The main area has tabs for 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is active, displaying a table with columns: Device Name, Management IP, Version, Status, and a row of action buttons. The table contains one entry for 'A-SBCE' with Management IP '192.168.1.20' and Version '6.3.000-19-4338'. The 'Status' column for this device is 'Commissioned'. The action buttons for this device are 'Reboot', 'Shutdown', 'Restart Application' (highlighted with a red box), 'View' (highlighted with a red box), 'Edit', and 'Uninstall'.

Device Name	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
A-SBCE	192.168.1.20	6.3.000-19-4338	Commissioned						

Step 2 - Click on **View** (shown above) to display the **System Information** screen.

The screenshot shows the 'System Information: SBCE' screen. It is divided into several sections: General Configuration, Device Configuration, License Allocation, Network Configuration, DNS Configuration, and Management IP(s). The General Configuration section shows Appliance Name: SBCE, Box Type: SIP, and Deployment Mode: Proxy. The Device Configuration section shows HA Mode: No and Two Bypass Mode: No. The License Allocation section shows Standard Sessions: 0, Advanced Sessions: 0, and Scopia Video Sessions: 0, with an Encryption checkbox checked. The Network Configuration section shows a table with columns: IP, Public IP, Netmask, Gateway, and Interface. The DNS Configuration section shows Primary DNS: 192.168.67.5, Secondary DNS, DNS Location: DMZ, and DNS Client IP: 192.168.70.120. The Management IP(s) section shows IP: 192.168.63.64.

IP	Public IP	Netmask	Gateway	Interface
192.168.70.120	192.168.70.120	255.255.255.0	192.168.70.1	A1
10.10.10.10	10.10.10.10	255.255.255.0	10.10.10.1	B1

7.2. Global Profiles

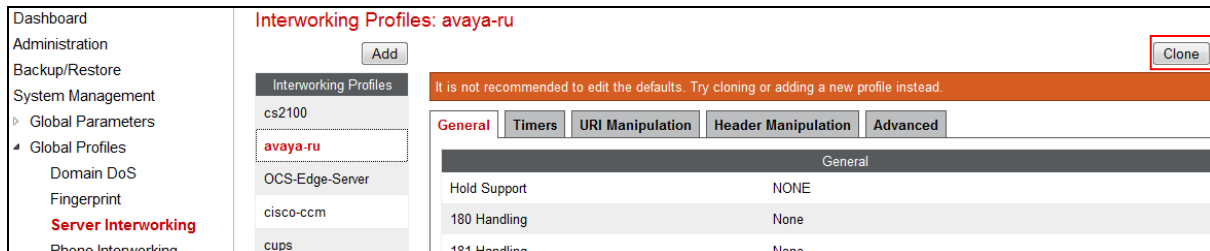
Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

7.2.1. Server Interworking – Avaya

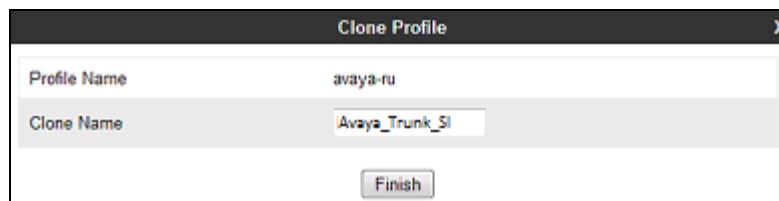
Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Session Manager.

Step 1 - Select **Global Profiles → Server Interworking** from the left-hand menu.

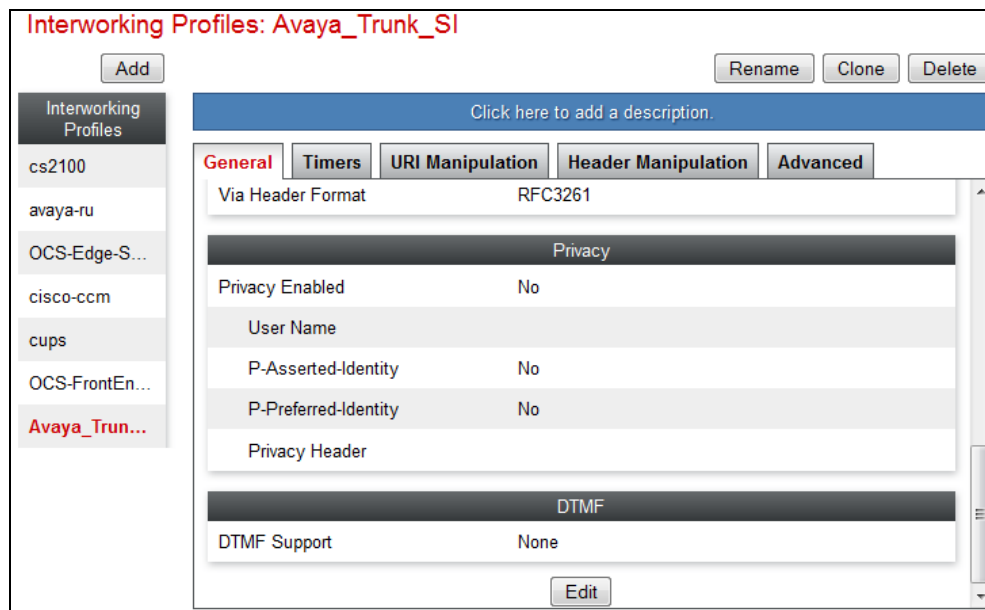
Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.



Step 3 - Enter profile name: (e.g., **Avaya_Trunk_SI**), and click **Finish**.



Step 4 - The new **Avaya_Trunk_SI** profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.



Step 5 - The **General** screen will open.

- Check **T38 Support**.
- All other options can be left with default values.
- Click **Next**.

The screenshot shows the 'Editing Profile: Avaya_Trunk_SI' window with the 'General' tab selected. The window contains various configuration options for SIP settings. The 'T.38 Support' checkbox is checked. The 'Next' button is visible at the bottom right.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Step 6 - On the **Privacy/DTMF** window, select **Finish** to accept default values.

The screenshot shows the 'Editing Profile: IPO_SI' window with the 'Privacy' and 'DTMF' tabs. The 'Privacy' section has checkboxes for 'Privacy Enabled', 'P-Asserted-Identity', and 'P-Preferred-Identity', and a text field for 'Privacy Header'. The 'DTMF' section has radio buttons for 'DTMF Support' (None, SIP NOTIFY, SIP INFO). The 'Finish' button is visible at the bottom right.

Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Step 7 - Returning to the Interworking Profile screen, select the **Advanced** tab, accept the default values, and click **Finish**.

The screenshot shows a web interface titled "Editing Profile: IPO_SI". It contains a list of configuration options, each with a checkbox or radio button. The options are:

- Record Routes: Radio buttons for None (selected), Single Side, and Both Sides.
- Topology Hiding: Change Call-ID: Checkbox (unchecked).
- Call-Info NAT: Checkbox (unchecked).
- Change Max Forwards: Checkbox (checked).
- Include End Point IP for Context Lookup: Checkbox (unchecked).
- OCS Extensions: Checkbox (unchecked).
- AVAYA Extensions: Checkbox (checked).
- NORTEL Extensions: Checkbox (unchecked).
- Diversion Manipulation: Checkbox (unchecked).
- Diversion Header URI: Text input field.
- Metaswitch Extensions: Checkbox (unchecked).
- Reset on Talk Spurt: Checkbox (unchecked).
- Reset SRTP Context on Session Refresh: Checkbox (unchecked).
- Has Remote SBC: Checkbox (checked).
- Route Response on Via Port: Checkbox (unchecked).
- Cisco Extensions: Checkbox (unchecked).

At the bottom right, there is a "Finish" button.

7.2.2. Server Interworking – AT&T

Repeat the steps shown in **Section 7.2.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

Step 1 - Select **Add Profile** (not shown) and enter a profile name: (e.g., **ATT_Trunk_SI**) and click **Next** (not shown).

Step 2 - The **General** screen will open (not shown):

- Check **T38 Support**.
- All other options can be left as default.
- Click **Next**.

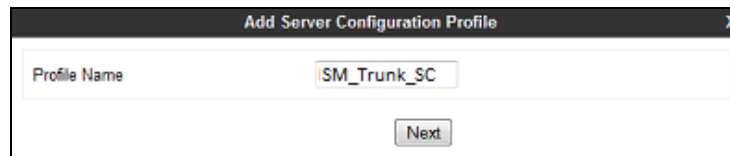
Step 3 - The **Privacy/DTMF**, **SIP Timers/Transport Timers**, and **Advanced** screens will open (not shown), accept default values for all the screens by clicking **Next**, then clicking on **Finish** when completed.

7.2.3. Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

Step 1 - Select **Global Profiles → Server Configuration** from the left-hand menu.

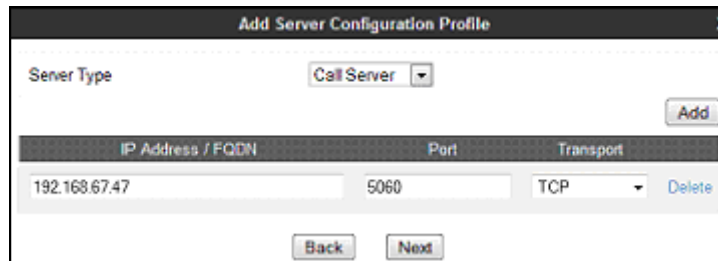
Step 2 - Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM_Trunk_SC**) and click **Next**.



The screenshot shows a window titled "Add Server Configuration Profile". Inside, there is a text field labeled "Profile Name" with the value "SM_Trunk_SC" entered. Below the text field is a "Next" button.

Step 3 - The **Add Server Configuration Profile** window will open.

- Select **Server Type: Call Server**.
- **IP Address: 192.168.67.47** (Session Manager network IP Address)
- **Transports: Select TCP**.
- **Port: 5060**.
- Select **Next**.



The screenshot shows the "Add Server Configuration Profile" window. The "Server Type" is set to "Call Server". Below this is a table with the following data:

IP Address / FQDN	Port	Transport
192.168.67.47	5060	TCP

Buttons for "Add", "Back", "Next", and "Delete" are visible.

Step 4 - The **Authentication** and **Heartbeat** windows will open (not shown).

- Select **Next** to accept default values.

Step 5 - The **Advanced** window will open.

- Select **Avaya_Trunk_SI** (created in **Section 7.2.1**), for **Interworking Profile**.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.

Note – Since TCP transport is specified in **Step 3**, then the **Enable Grooming** option should be enabled.

7.2.4. Server Configuration – AT&T

Note – The AT&T IPFR-EF service may provide a Primary and Secondary Border Element. This section describes the connection to a single (Primary) Border Element. See **Addendum 1** for information on configuring two IPFR-EF Border Elements (Primary & Secondary).

Repeat the steps in **Section 7.2.3**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

Step 1 - Select **Add Profile** and enter a Profile Name (e.g., **ATT_SC**) and select **Next**.

Step 2 - On the **General** window (not shown), enter the following.

- **Server Type:** Select **Trunk Server**.
- **IP Address:** **10.10.10.11** (AT&T Border Element IP address)
- **Transports:** Select **UDP**.
- **Port:** **5060**.
- Select **Next**.

Step 3 - On the **Advanced** window, enter the following.

- Select **ATT_Trunk_SI** (created in **Section 7.2.2**), for **Interworking Profile**.
- Select **Finish**.

IP Address / FQDN	Port	Transport
10.10.10.11	5060	UDP

General	Authentication	Heartbeat	Advanced
Enable DoS Protection		<input type="checkbox"/>	
Enable Grooming		<input type="checkbox"/>	
Interworking Profile		ATT_Trunk_SI	
Signaling Manipulation Script		None	
Connection Type		SUBID	
<input type="button" value="Edit"/>			

7.2.5. Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

Step 1 - Select **Global Profiles** → **Routing** from the left-hand menu, and select **Add** (not shown)

Step 2 - Enter a **Profile Name**: (e.g., **SM_RP**) and click **Next**.

Routing Profile	
Profile Name	SM_RP
<input type="button" value="Next"/>	

Step 3 - The Routing Profile window will open. Using the default values shown, click on **Add**.

Routing Profile	
URI Group	* <input type="button" value="v"/>
Time of Day	default <input type="button" value="v"/>
Load Balancing	Priority <input type="button" value="v"/>
NAPTR	<input type="checkbox"/>
Transport	None <input type="button" value="v"/>
Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>
<input type="button" value="Add"/>	
Click the Add button to add a Next-Hop Address.	
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

Step 4 - The **Next-Hop Address** window will open. Populate the following fields:

- **Priority/Weight** = **1**
- **Server Configuration** = **SM_Trunk_SC** (from **Section 7.2.3**).
- **Next Hop Address** = Select **192.168.67.47:5060 (TCP)** from the drop down menu (Session Manager IP address).
- Click on **Finish**.

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
Add			
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	SM_Trunk_SC	192.168.67.47:5060 (TCP)	None
			Delete
Finish			

7.2.6. Routing – To AT&T

Repeat the steps in **Section 7.2.5**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

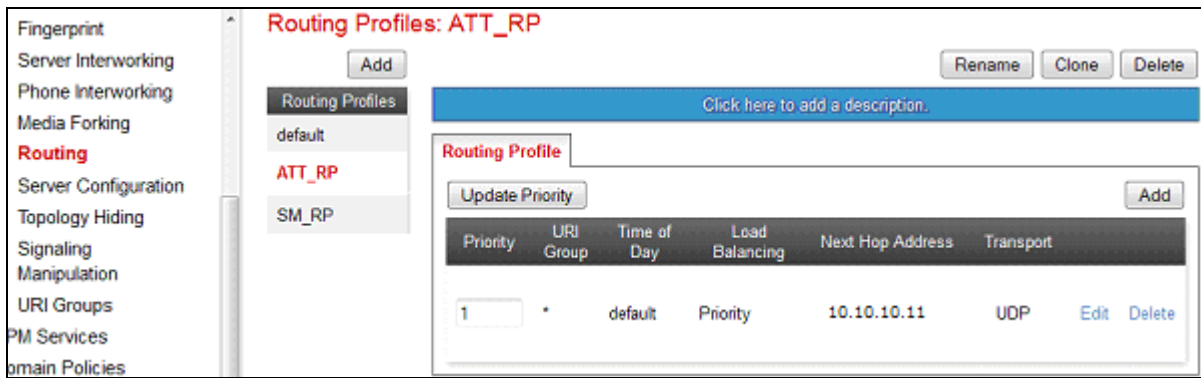
Step 1 - On the **Global Profiles → Routing Profile** window (not shown), enter a Profile Name: (e.g., **ATT_RP**).

Step 2 - On the **Next-Hop Address** window (not shown), populate the following fields:

- **Priority/Weight** = **1**
- **Server Configuration** = **ATT_SC** (from **Section 7.2.4**).
- **Next Hop Address**: select **10.10.10.11:5060**.
- **Transport**: select **UDP**.
- Use default values for the rest of the parameters.

Step 4 - Click **Finish**.

Profile : ATT_RP			
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
Add			
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT_SC	10.10.10.11:5060	UDP
			Delete
Finish			



7.2.7. Topology Hiding – Avaya Side

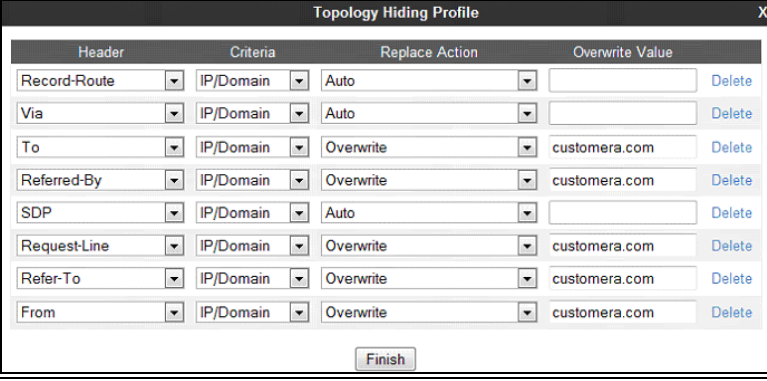
The **Topology Hiding** configuration allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

Step 1 - Select **Global Profiles** → **Topology Hiding** from the left-hand side menu.

Step 2 - Select the **Add** button, enter Profile Name: (e.g., **Avaya_TH**), and click **Next**.

Step 3 - The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until no new headers are added to the list, and the **Add Header** button is no longer displayed.

Step 4 - Populate the fields as shown below, and click **Finish**. Note that **customera.com** is the domain used by the CPE (see **Sections 5.1, 6.6, and 6.8**).



Header	Criteria	Replace Action	Overwrite Value	
Record-Route	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	customera.com	Delete
Referred-By	IP/Domain	Overwrite	customera.com	Delete
SDP	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	customera.com	Delete
Refer-To	IP/Domain	Overwrite	customera.com	Delete
From	IP/Domain	Overwrite	customera.com	Delete

Finish

7.2.8. Topology Hiding – AT&T Side

Repeat the steps in **Section 7.2.7**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

- Enter a **Profile Name**: (e.g., **ATT_TH**).
- Use the default values for all fields and click **Finish**.

Header	Criteria	Replace Action	Overwrite Value	
Record-Route	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
From	IP/Domain	Auto		Delete

Finish

The following screen shows the completed **Topology Hiding Profile** form.

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration
Topology Hiding
Signaling Manipulation
URI Groups

Topology Hiding Profiles: ATT_TH

Add

Rename Clone Delete

Click here to add a description.

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

7.2.9. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. However, no Signaling Manipulations were used in the reference configuration.

Note – The use of Signaling Manipulation scripts demands higher processing requirements for the Avaya SBCE. Therefore, the use of Signaling Rules (**Section 7.3.3**) is the preferred method for header/message manipulation. Signaling Manipulations should only be used in cases where the use of Signaling Rules does not meet the desired result. Refer to [8] for information on the Avaya SBCE scripting language.

7.3. Domain Policies

The Domain Policies feature allows users to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.3.1. Application Rules

Step 1 - Select **Domain Policies** → **Application Rules** from the left-hand side menu (not shown).

Step 2 - Select the **default-trunk** rule (not shown).

Step 3 - Select the **Clone** button (not shown), and the **Clone Rule** window will open (not shown).

- In the **Clone Name** field enter **SIP-Trunk_AR**
- Click **Finish** (not shown). The completed **Application Rule** is shown below.

The screenshot shows the 'Application Rules: SIP_Trunk_AR' configuration window. On the left is a sidebar menu with 'Application Rules' selected, listing various rules including 'default', 'default-trunk', and 'SIP_Trunk_AR' (which is highlighted in red). The main area has a header with 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' buttons. Below the header is a blue bar with the text 'Click here to add a description.' The main content area is titled 'Application Rule' and contains a table with columns: 'Application Type', 'In', 'Out', 'Maximum Concurrent Sessions', and 'Maximum Sessions Per Endpoint'. The table has three rows: 'Audio' (checked in both In and Out columns, with 2000 sessions), 'Video' (unchecked), and 'IM' (unchecked). Below the table is a 'Miscellaneous' section with 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is at the bottom right.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

7.3.2. Media Rules

Media Rules are used to define QoS parameters. The Media Rule described below will be applied to both directions, and therefore, only one rule is needed.

Step 1 - Select **Domain Policies** → **Media Rules** from the left-hand side menu (not shown).

Step 2 - From the Media Rules menu, select the **default-low-med** rule.

Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **Trunk-low-med_MR**
- Click **Finish**. The newly created rule will be displayed.

Step 4 - Highlight the **Trunk-low-med_MR** rule just created (not shown):

- Select the **Media QoS** tab (not shown).
- Click the **Edit** button and the **Media QoS** window will open.
- In the **Media QoS Marking** section, check **Enabled**.
- Select the **DSCP** box.
- **Audio**: Select **EF** from the drop-down.
- **Video**: Select **EF** from the drop-down.

Step 5 - Click **Finish**.

The completed **Media Rule** screen is shown below.

7.3.3. Signaling Rules

In the reference configuration, Signaling Rules are used to filter various SIP headers.

7.3.3.1 Avaya – Signaling Rules

- Step 1** - Select **Domain Policies** → **Signaling Rules** from the left-hand side menu (not shown).
- Step 2** - The **Signaling Rules** window will open (not shown). From the Signaling Rules menu, select the **default** rule.
- Step 3** - Select the **Clone** button and the **Clone Rule** window will open (not shown).
- In the **Rule Name** field enter **Avaya_SR**
 - Click **Finish**. The newly created rule will be displayed (not shown).

7.3.3.1.1 Avaya – Signaling Rule Request Headers Tab

The following Signaling Rules remove SIP headers sent by Communication Manager SIP requests that are either not supported or required by AT&T.

Step 1 - Select the **Avaya_SR** rule created in **Section 7.3.3.1**, select the **Request Headers** tab, and enter the following:

- Select the **Add In Header Control** button (not shown). The **Add Header Control** window will open.

- Select the **Request Headers** tab (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **P-Location**.
- From the **Method Name** menu select **INVITE**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

Step 2 - Click **Finish**

Step 3 - Repeat **Steps 1 & 2** with the following changes, to create a rule to remove the **P-Location** header from ACKs.

- From the **Method Name** menu select **ACK**.

Step 4 - Click **Finish**.

Step 5 - Repeat **Steps 1 & 2** to create a rule to remove the **Alert-Info** header.

- Verify the **Proprietary Request Header** box is *unchecked*.
- From the **Header Name** menu select **Alert-Info**.
- From the **Method Name** menu select **INVITE**.

Step 6 - Click **Finish**.

Edit Header Control

Proprietary Request Header ☐

Header Name

Method Name

Header Criteria ☒ Forbidden
☐ Mandatory
☐ Optional

Presence Action

Step 7 - Repeat **Steps Steps 1 & 2** to create a rule to remove the **Endpoint-View** header.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Method Name** menu select **INVITE**.

Step 8 - Click **Finish**.

Edit Header Control

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria ☒ Forbidden
☐ Mandatory
☐ Optional

Presence Action

Step 9 - Repeat **Steps Steps 1 & 2** to create a rule to remove the **AV-Correlation-ID** header.

- In the **Header Name** field enter **AV-Correlation-ID**.
- From the **Method Name** menu select **INVITE**.

Step 10 - Click **Finish**.

Edit Header Control

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria ☒ Forbidden
☐ Mandatory
☐ Optional

Presence Action

Step 11 - Repeat **Steps 1 & 2** to create a rule to remove the **AV-Global-Session-ID** header.

- In the **Header Name** field enter **AV-Global-Session-ID**.
- From the **Method Name** menu select **ALL**.

Step 12 - Click **Finish**.

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action

486

Step 13 - Repeat **Steps 1 & 2** to create a rule to remove the **P-AV-Message-ID** header.

- In the **Header Name** field enter **P-AV-Message-ID**.
- From the **Method Name** menu select **ALL**.

Step 14 - Click **Finish**.

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action

486

The completed Request Headers form is shown below. Note that the Direction column shows “IN”.

Signaling Rules: Avaya_SR

Filter By Device... [Rename] [Clone] [Delete]

Click here to add a description.

General Requests Responses **Request Headers** Response Headers Signaling

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	INVITE	Forbidden	Remove Header	No	IN	Edit	Delete
4	Endpoint-View	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Location	ACK	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.3.3.1.2 Avaya – Signaling Rule Response Headers Tab

The following Signaling Rules remove headers sent by Communication Manager SIP responses (e.g., 1XX and/or 200OK) that are either not supported or required by AT&T.

Step 1 - Highlight the **Avaya_SR** rule created in **Section 7.3.3.1**, and using the same procedures shown in **Section 7.3.3.1.1**, remove the following headers:

- **P-Location header from 1XX responses to INVITE:**
 - Select the **Response Headers** tab (not shown).
 - Click the **Add In Header Control** button and the **Add Header Control** window will open.
 - Check the **Proprietary Request Header** box.
 - In the **Header Name** field, enter **P-Location**.
 - From the **Response Code** menu select **1XX**.
 - From the **Method Name** menu select **INVITE**.
 - For **Header Criteria** select **Forbidden**.
 - From the **Presence Action** menu select **Remove Header**.
 - Click **Finish**.
- **P-Location header from 2XX responses to INVITE:**
 - From the **Response Code** menu select **2XX**.
 - Click **Finish**.
- **Endpoint-View header from 1XX responses to INVITE:**
 - In the **Header Name** field, enter **Endpoint-View**.

- From the **Response Code** menu select **1XX**.
- From the **Method Name** menu select **INVITE**.
- Click **Finish**.
- **Endpoint-View headers from 2XX responses to INVITE:**
 - From the **Response Code** menu select **2XX**.
 - Click **Finish**.
- **P-AV-Message-ID header from 1xx responses to ALL messages:**
 - In the **Header Name** field, enter **Endpoint-View**.
 - From the **Response Code** menu select **1XX**.
 - From the **Method Name** menu select **ALL**.
 - Click **Finish**.
- **P-AV-Message-ID headers from 2XX responses to ALL messages:**
 - From the **Response Code** menu select **2XX**.
 - Click **Finish**.
- **AV-Global-Session-ID header from 1XX responses to ALL messages:**
 - In the **Header Name** field, enter **AV-Global-Session-ID**.
 - From the **Response Code** menu select **1XX**.
 - From the **Method Name** menu select **ALL**.
 - Click **Finish**.
- **AV-Global-Session-ID headers from 2XX responses to ALL messages:**
 - From the **Response Code** menu select **2XX**.
 - Click **Finish**.
- **Remote-Party-ID header from 1XX responses to ALL messages:**
 - In the **Header Name** field, enter **Remote-Party-ID**.
 - From the **Response Code** menu select **1XX**.
 - Verify the **Proprietary Request Header** box is *unchecked*.
 - From the **Method Name** menu select **ALL**.
 - Click **Finish**.
- **Remote-Party-ID headers from 2XX responses to ALL messages:**
 - From the **Response Code** menu select **2XX**.
 - Click **Finish**.

The completed Response Headers form is shown below. Note that the Direction column shows “IN”.

Signaling Rules: Avaya_SR

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	Remote-Party-ID	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
10	Remote-Party-ID	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

Step 2 - Highlight the **Avaya_SR** rule, select the **Signaling QoS** tab and enter the following:

- Click the **Edit** button and the **Signaling QOS** window will open.
- Verify that **Enabled** is selected.
- Select **DCSP**.
- Select **Value = EF**.

Step 3 - Click **Finish**.

Signaling QoS

Enabled ☒

☐ ToS

Precedence

ToS

☒ DSCP

Value

7.3.3.2 AT&T – Signaling Rule Request Headers Tab

The Remote-Address header inserted by the Avaya SBCE in INVITE is removed (see **Section 2.2, Item 3**).

Step 1 - Select **Domain Policies** from the menu on the left-hand side menu (not shown).

Step 2 - Select **Signaling Rules** (not shown).

Step 3 - From the Signaling Rules menu, select the **default** rule.

Step 4 - Select **Clone Rule** button

- Enter a name: **ATT_SR**

Step 5 - Click **Finish**

Step 6 - Highlight and edit the **ATT_SR** rule created in **Step 4**, enter the following:

- Select the **Request Headers** tab (not shown).
- Select the **Add In Header Control** button (not shown).
- Check the **Proprietary Request Header** box.
- For the **Header Name** field, enter **Remote-Address**.
- From the **Method Name** menu select **INVITE**.
- For **Header Criteria** select **Forbidden**.
- For **Presence Action** select **Remove Header**.

Step 7 - Click **Finish**.

The completed Request Headers form is shown below. Note that the Direction column shows “IN”, and that no Response Header manipulation is required.

Signaling Rules: ATT_SR

Buttons: Add, Filter By Device..., Rename, Clone, Delete

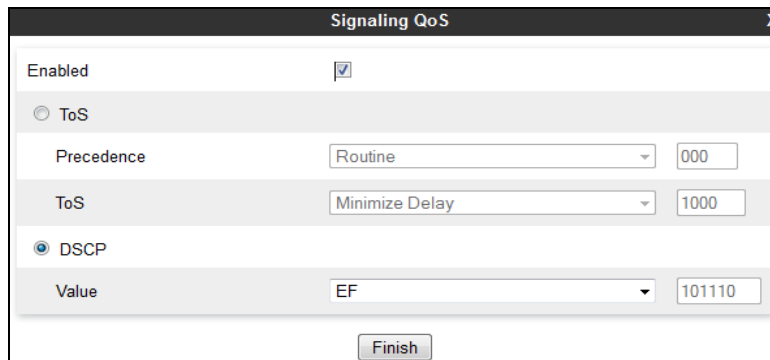
Left Menu: Signaling Rules, default, No-Content-Type..., **ATT_SR**, Avaya_SR

Tabbed Interface: General, Requests, Responses, **Request Headers**, Response Headers, Signaling QoS, UCID

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Remote-Address	ALL	Forbidden	Remove Header	Yes	OUT	Edit Delete

Step 8 - Highlight the **ATT_SR** rule, select the **Signaling QoS** tab and repeat **Steps 2 & 3** from **Section 7.3.3.1**.



The image shows a 'Signaling QoS' configuration window. It has a title bar with 'Signaling QoS' and a close button 'X'. Inside, there's a section 'Enabled' with a checked checkbox. Below that, there are two radio buttons: 'ToS' (selected) and 'DSCP'. Under 'ToS', there are two rows: 'Precedence' with a dropdown set to 'Routine' and a text box with '000', and 'ToS' with a dropdown set to 'Minimize Delay' and a text box with '1000'. Under 'DSCP', there's a 'Value' row with a dropdown set to 'EF' and a text box with '101110'. At the bottom right is a 'Finish' button.

7.3.4. Endpoint Policy Groups – Avaya Connection

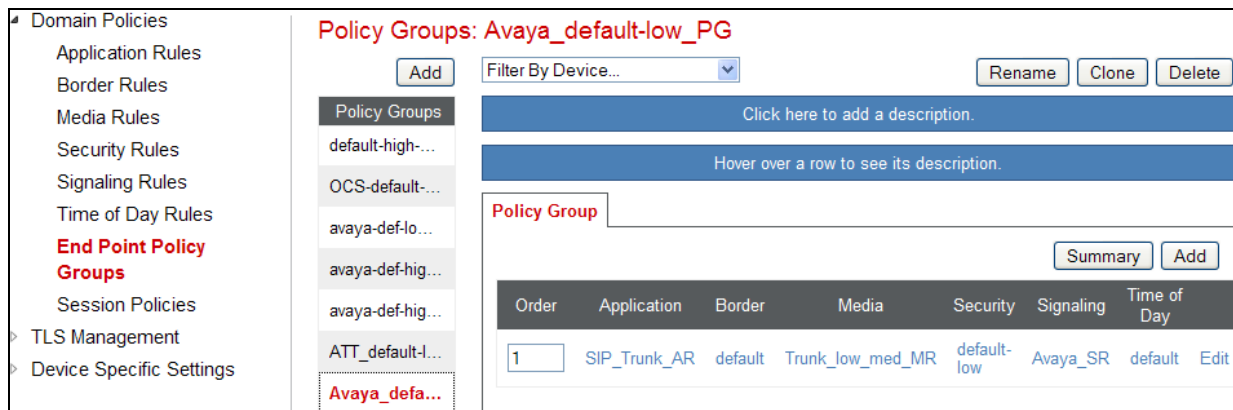
Step 1 - Select **Domain Policies** from the menu on the left-hand side.

Step 2 - Select **End Point Policy Groups**.

Step 3 - Select **Add**.

- **Name:** Avaya_default-low_PG.
- **Application Rule:** SIP_Trunk_AR (created in Section 7.3.1).
- **Border Rule:** default.
- **Media Rule:** Trunk_low_med_MR (created in Section 7.3.2).
- **Security Rule:** default-low.
- **Signaling Rule:** Avaya_SR (created in Section 7.3.3).
- **Time of Day:** default.

Step 4 - Select **Finish** (not shown). The completed **Policy Groups** screen is shown below.



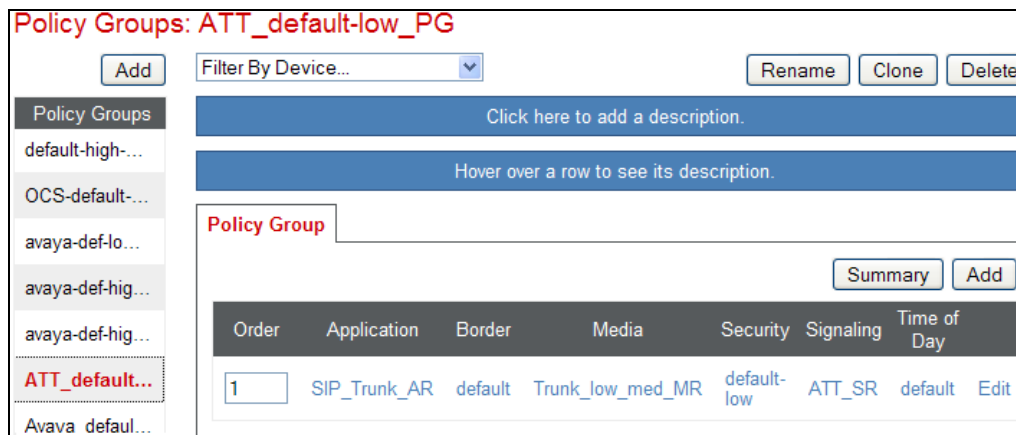
The image shows the 'Policy Groups: Avaya_default-low_PG' screen. On the left is a sidebar menu with 'Domain Policies' expanded, showing 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', 'Signaling Rules', 'Time of Day Rules', 'End Point Policy Groups' (highlighted in red), 'Session Policies', 'TLS Management', and 'Device Specific Settings'. The main area has a title 'Policy Groups: Avaya_default-low_PG' in red. Below it is an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. There's a blue bar with 'Click here to add a description.' and another with 'Hover over a row to see its description.' Below that is a 'Policy Group' section with a 'Summary' button and an 'Add' button. At the bottom is a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day. The first row has values: 1, SIP_Trunk_AR, default, Trunk_low_med_MR, default-low, Avaya_SR, default, and an 'Edit' link.

7.3.5. Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps 1 through 4 from Section 7.3.4 with the following changes:

- **Group Name:** ATT_default-low_PG.
- **Signaling Rule:** ATT_SR (created in Section 7.3.3).

Step 2 - Select **Finish** (not shown).

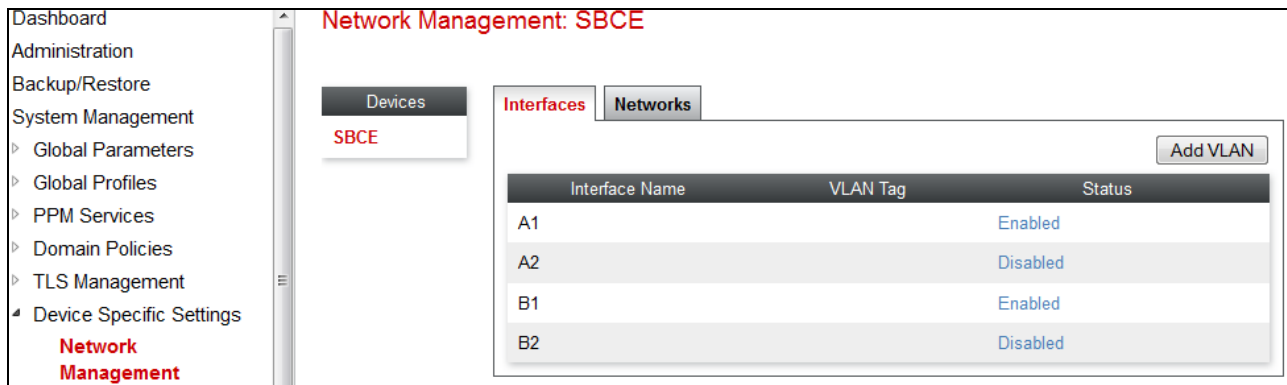


7.4. Device Specific Settings

7.4.1. Network Management

Step 1 - Select **Device Specific Settings** → **Network Management** from the menu on the left-hand side.

Step 2 - The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.



Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

Network Management: SBCE

Devices **Interfaces** **Networks**

SBCE

Add

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
Network_A1	192.168.70.1	255.255.255.0	A1	192.168.70.120	Edit	Delete
Network_B1	135.16.170.54	255.255.255.240	B1	135.16.170.55	Edit	Delete

7.4.2. Advanced Options

In **Section 7.4.3**, the media UDP port ranges required by AT&T are configured (**16384 – 32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be defined in **Section 7.4.3**.

Step 1 - Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side.

Step 2 - Select the **Port Ranges** tab.

Step 3 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 4 - Scroll to the bottom of the window and select **Save** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).

Advanced Options: SBCE

Devices **SBCE**

CDR Listing Feature Control SIP Options **Port Ranges** RTCP Monitoring

Changes to the settings below require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Port Range Configuration

Signaling Port Range	12000	-	16000
Config Proxy Internal Signaling Port Range	42000	-	51000
Listen Port Range	9000	-	9999
HTTP Port Range	10000	-	10200
OCS FTP Listen Port Range	6891	-	6901

7.4.3. Media Interfaces

As mentioned in **Section 7.4.2**, the AT&T IPFR-EF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, though only the outside port range is required by the AT&T IPFR-EF service.

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).

Step 2 - Select **Media Interface**.

Step 3 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** **Inside_Trunk_MI**.
- **IP Address:** **192.168.70.120** (Avaya SBCE A1 address).
- **Port Range:** **16384 – 32767**.

Step 4 - Click **Finish** (not shown).

Step 5 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** **Outside_Trunk_MI**.
- **IP Address:** **10.10.10.10** (Avaya SBCE B1 address).
- **Port Range:** **16384 – 32767**.

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).

The completed **Media Interface** screen is shown below.

The screenshot shows the 'Media Interface: SBCE' configuration page. On the left is a navigation menu with 'Media Interface' selected. The main area has a 'Media Interface' tab and a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table with two entries: 'Inside_Trunk_MI' and 'Outside_Trunk_MI'. Each entry has 'Edit' and 'Delete' links. An 'Add' button is in the top right corner of the table area.

Name	Media IP	Port Range	Edit	Delete
Inside_Trunk_MI	192.168.70.120	16384 - 32767	Edit	Delete
Outside_Trunk_MI	10.10.10.10	16384 - 32767	Edit	Delete

7.4.4. Signaling Interface

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).

Step 2 - Select **Signaling Interface**.

Step 3 - Select **Add** (not shown) and enter the following:

- **Name:** **Inside_Trunk_SI**.
- **IP Address:** **192.168.70.120** (Avaya SBCE A1 address).
- **TCP Port:** **5060**.

Step 4 - Click **Finish** (not shown).

Step 5 - Select **Add** again, and enter the following:

- **Name: Outside_Trunk_SI.**
- **IP Address: 10.10.10.10** (Avaya SBCE B1 address).
- **UDP Port: 5060.**

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**).

Signaling Interface: SBCE

Devices
SBCE

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Inside_Trunk_SI	192.168.70.120	5060	5060	---	None	Edit Delete
Outside_Trunk_SI	10.10.10.10	---	5060	---	None	Edit Delete

7.4.5. Endpoint Flows – For Session Manager

Step 1 - Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side (not shown).

Step 2 - Select the **Server Flows** tab (not shown).

Step 3 - Select **Add**, (not shown) and enter the following:

- **Flow Name: SM_Trunk.**
- **Server Configuration: SM_Trunk_SC** (Section 7.2.3).
- **URI Group: ***
- **Transport: ***
- **Remote Subnet: ***
- **Received Interface: Outside_Trunk_SI** (Section 7.4.4).
- **Signaling Interface: Inside_Trunk_SI** (Section 7.4.4).
- **Media Interface: Inside_Trunk_MI** (Section 7.4.3).
- **End Point Policy Group: Avaya_default-low_PG** (Section 7.3.4).
- **Routing Profile: ATT_RP** (Section 7.2.6).
- **Topology Hiding Profile: Avaya_TH** (Section 7.2.7).
- Let other values default.

Step 4 - Click **Finish** (not shown).

View Flow: SM_Trunk		View Flow: SM_Trunk	
Criteria		Profile	
Flow Name	SM_Trunk	Signaling Interface	Inside_Trunk_SI
Server Configuration	SM_Trunk_SC	Media Interface	Inside_Trunk_MI
URI Group	*	End Point Policy Group	Avaya_default-low_PG
Transport	*	Routing Profile	ATT_RP
Remote Subnet	*	Topology Hiding Profile	Avaya_TH
Received Interface	Outside_Trunk_SI	File Transfer Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any

7.4.6. Endpoint Flows – For AT&T

Step 1 - Repeat steps 1 through 4 from Section 7.4.5, with the following changes:

- **Flow Name:** ATT.
- **Server Configuration:** ATT_SC (Section 7.2.4).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Inside_Trunk_SI (Section 7.4.4).
- **Signaling Interface:** Outside_Trunk_SI (Section 7.4.4).
- **Media Interface:** Outside_Trunk_MI (Section 7.4.3).
- **End Point Policy Group:** ATT_default-low_PG (Section 7.3.5).
- **Routing Profile:** SM_RP (Section 7.2.5).
- **Topology Hiding Profile:** ATT_TH (Section 7.2.8).

View Flow: ATT		View Flow: ATT	
Criteria		Profile	
Flow Name	ATT	Signaling Interface	Outside_Trunk_SI
Server Configuration	ATT_SC	Media Interface	Outside_Trunk_MI
URI Group	*	End Point Policy Group	ATT_default-low_PG
Transport	*	Routing Profile	SM_RP
Remote Subnet	*	Topology Hiding Profile	ATT_TH
Received Interface	Inside_Trunk_SI	File Transfer Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any

The completed **End Point Flows** screen is shown below.

DMZ Services

- Domain Policies
- TLS Management
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows**
 - Session Flows
 - DMZ Services
 - TURN/STUN Service
 - SNMP
 - Syslog Management
 - Advanced Options
 - Troubleshooting

Devices

SBCE

Subscriber Flows

Server Flows

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP	View Clone Edit Delete

Server Configuration: SM_Trunk_SC

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya_default-low_PG	ATT_RP	View Clone Edit

8. Verification Steps

The following steps may be used to verify the configuration:

8.1. AT&T IP Flexible Reach – Enhanced Features

The following scenarios may be executed to verify Communication Manager, Session Manager, Avaya SBCE, and the AT&T IPFR-EF service interoperability:

- Place inbound and outbound calls, answer the calls, and verify that two-way talk path exists.
- Verify that calls remain stable and disconnect properly.
- Verify basic call functions such as hold, transfer, and conference.
- Verify the use of DTMF signaling.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to voicemail (e.g., Avaya Messaging). Retrieve voicemail messages either locally or from PSTN.
- Using the appropriate IPFR-EF access numbers and codes, verify that the following features are successful:
 - Network based Simultaneous Ring – The “primary” and “secondary” endpoints ring, and either may be answered.
 - Network based Sequential Ring (Locate Me) – Verify that after the “primary” endpoint rings for the designated time, the “secondary” endpoint rings and may be answered.
 - 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) – Verify that based on each feature criteria, calls are successfully redirected and may be answered.
- Inbound / Outbound T.38 fax.
- SIP OPTIONS monitoring of the health of the SIP trunk.
- Incoming and outgoing calls using the G.729 (A or B) and G.711 ULAW codecs.
- If applicable, verify Remote Worker configurations are successful.

8.2. Avaya Aura® Communication Manager

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

- Tracing a SIP trunk.
 1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., 602). Note that in the trace shown below, Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 19001, before sending the INVITE to Communication Manager.

```
list trace tac 602
```

Page 1

LIST TRACE

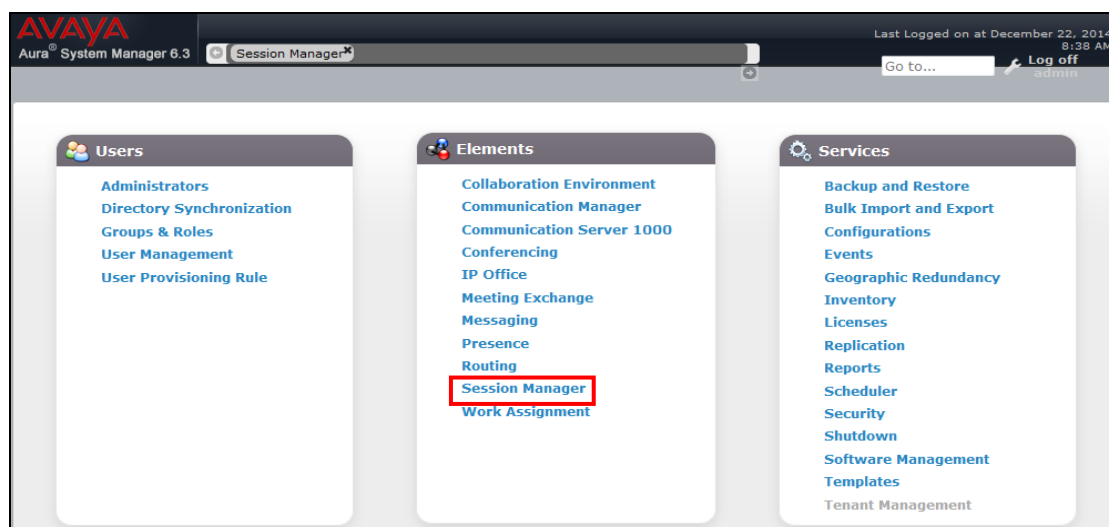
```
time      data
15:55:06 TRACE STARTED 04/19/2013 CM Release String cold-02.0.823.0-20396
15:55:16 SIP<INVITE sip:19001@customera.com SIP/2.0
15:55:16      Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16      7ok0
15:55:16      active trunk-group 2 member 1      cid 0x2e9
15:55:16 SIP>SIP/2.0 180 Ringing
15:55:16      Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16      G729B ss:off ps:30
15:55:16      rgn:2 [192.168.70.120]:16388
15:55:16      rgn:1 [192.168.67.50]:16392
15:55:16      xoip options: fax:T38 modem:off tty:US  uid:0x5000b
15:55:16      xoip ip: [192.168.67.50]:16392
15:55:18 SIP>SIP/2.0 200 OK
15:55:18      Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:18      7ok0
15:55:18      active station      19001 cid 0x2e9
15:55:18 SIP<ACK sip:7325553940@192.168.67.202:5062;transport=tcp SI
15:55:18 SIP<P/2.0
15:55:18      Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:18      7ok0
```

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

8.3. Avaya Aura® Session Manager

The Session Manager configuration may be verified via System Manager.

Step 1 – Using the procedures described in **Section 5**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



Step 2 – The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns all show good status.

In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **4** Entities defined.

Session Manager Dashboard
This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances
Service State: [Dropdown] Shutdown System: [Dropdown] As of 10:35 AM

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	Version
sm63	Core	✓	0/0/0	Up	Accept New Service	0/4	0	1/1	✓	✓	6.3.11.0.631103

Select: All, None

Step 3 - Clicking on the **0/4** entry (shown above) in the **Entity Monitoring** column, results in the following display:

All Entity Links for Session Manager: sm63

Summary View

Status Details for the selected Session Manager:

8 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	ACM63_local	192.168.67.202	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	ACM63_Meet-Me	192.168.67.202	5080	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	ACM63_public	192.168.67.202	5062	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	A-SBCE	192.168.70.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP

Note the **A-SBCE** Entity from the list of monitored entities above. The **Reason Code** column indicates that Session Manager has received a **SIP 405 Method Not Allowed** response to the SIP **OPTIONS** it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Also note that the Avaya SBCE sends the Session Manager generated **OPTIONS** on to the AT&T IPFR-EF Border Element, and it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends it back to Session Manager.

Another useful tool is to select **System Tools** → **Call Routing Test** (not shown) from the left hand menu. This tool allows specific call criteria to be entered, and the simulated routing of this call through Session Manager is then verified.

8.4. Avaya Session Border Controller for Enterprise

8.4.1. System Status

Various system conditions monitored by the Avaya SBCE may be displayed as follows.

Step 1 – Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the Dashboard screen.

8.4.2. Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to Device Specific Settings → Advanced Options → Troubleshooting → Trace

Step 2 - Select the **Packet Capture** tab and select the following:

- Select the desired **Interface** from the drop down menu (e.g., **All**).
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**)
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields
- Click **Start Capture** to begin the trace.

Note – Specifying **All** in the **Interface** field will result in the Avaya SBCE capturing traffic from both the A1 and B1 interfaces defined in the reference configuration. Also, when specifying the **Maximum Number of Packets to Capture**, be sure to estimate a number large enough to include all packets for the duration of the test.

Trace: SBCE

Devices
SBCE

Packet Capture
Captures

Packet Capture Configuration

Status	Ready
Interface	Any
Local Address IP[Port]	All :
Remote Address *, *Port, IP, IP-Port	*
Protocol	All
Maximum Number of Packets to Capture	5000
Capture Filename Using the name of an existing capture will overwrite it.	TEST.pcap

Start Capture
Clear

The capture process will initialize and then display the following **In Progress** status window:

Trace: SBCE

Devices
SBCE

Call Trace
Packet Capture
Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status	In Progress
Interface	Any
Local Address IP[Port]	All :
Remote Address *, *Port, IP, IP-Port	*
Protocol	All
Maximum Number of Packets to Capture	5000
Capture Filename Using the name of an existing capture will overwrite it.	TEST.pcap

Stop Capture

Step 3 – Run the test.

Step 4 – When the test is completed, select **Stop Capture** button shown above.

Step 5 - Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.

Step 6 - Click on the **File Name** link to download the file and use Wireshark to open the trace.

Trace: SBCE

Devices
SBCE

Packet Capture
Captures

Last Modified
Descending
Sort
Reset
Refresh

File Name	File Size (bytes)	Last Modified	
TEST_20150106085556.pcap	94,208	January 6, 2015 9:56:11 AM EST	Delete

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.3, can be configured to interoperate successfully with the AT&T IP Flexible Reach – Enhanced Features service, within the constraints described in **Section 2.2**.

Testing was performed on a production AT&T IP Flexible Reach – Enhanced Features service circuit. The reference configuration shown in these Application Notes 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. Deploying Avaya Aura® Session Manager, Release 6.3, Issue 6, November 2014
2. Administering Avaya Aura® Session Manager, Release 6.3, Issue 7, September 2014
3. Deploying Avaya Aura® System Manager on System Platform, Release 6.3, Issue 4, June 2014
4. Administering Avaya Aura® System Manager for Release 6.3.10, Release 6.3, Issue 6, November 2014

Avaya Aura® Communication Manager

5. Deploying Avaya Aura® Communication Manager on System Platform, Release 6.3, 18-604394, Issue 6, June 2014
6. Administering Avaya Aura® Communication Manager, Release 6.3, 03-300509, Issue 10, June 2014
7. Administering Avaya G430 Branch Gateway, Release 6.3, 03-603228, Issue 5, October 2013

Avaya Session Border Controller for Enterprise

8. Administering Avaya Session Border Controller for Enterprise, Release 6.3, Issue 4, October 2014
9. Deploying Avaya Session Border Controller for Enterprise, Release 6.3, Issue 4, October 2014
10. Application Notes, “*Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communications Manager Rel. 6.3 and Avaya Aura® Session Manager Rel. 6.3, Issue 1.0*”
<http://origin-support.avaya.com/css/P8/documents/100183254>

Avaya Aura® Messaging

11. Administering Avaya Aura® Messaging, Release 6.3.2, Issue 1, December 2014

AT&T IP Flexible Reach - Enhanced Features Service:

12. AT&T IP Flexible Reach - Enhanced Features Service description -
<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>

11. Addendum 1 – Redundancy to Multiple AT&T Border Elements

The AT&T IPFR-EF service may provide multiple network Border Elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T Border Elements **10.10.10.11** and **10.10.10.12**, the Avaya SBCE is provisioned as follows to include the secondary trunk connection to 10.10.10.12 (the primary AT&T trunk connection to 10.10.10.11 is defined in **Section 7.2.4**).

11.1. Secondary AT&T Border Element Server Configuration

Step 1 - Repeat the steps shown in **Section 7.2.4** with the following changes:

- Add a new **Server Configuration** (e.g., **ATT_Secondary_SC**)

Step 2 - On the **Add Server Configuration Profile – General** tab:

- Enter the IP address of the AT&T Secondary Border Element (e.g., **10.10.10.12**). The completed General tab is shown below.

The screenshot shows the 'Server Configuration: ATT_Secondary_SC' form with the 'General' tab selected. On the left, a sidebar lists 'Server Profiles' with 'ATT_Secondary_SC' highlighted. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab contains a 'Server Type' dropdown set to 'Trunk Server'. Below is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. A single row is present with values '10.10.10.12', '5060', and 'UDP'. An 'Edit' button is at the bottom right of the table. At the top right of the form are 'Rename', 'Clone', and 'Delete' buttons.

IP Address / FQDN	Port	Transport
10.10.10.12	5060	UDP

Step 3 - On the **Heartbeat** tab:

- Check **Enable Heartbeat**.
- **Method: OPTIONS**
- **Frequency: As desired (e.g., 60 seconds).**
- **From URI: secondary@customer.com**
- **To URI: secondary@customer.com**
- Select **Next** (not shown)

Step 4 - On the **Advanced** Tab, click **Finish** (not shown). The completed Heartbeat tab is shown below.

The screenshot shows the 'Server Configuration: ATT_Secondary_SC' form with the 'Heartbeat' tab selected. The 'General' tab is also visible. The 'Heartbeat' tab contains a checkbox 'Enable Heartbeat' which is checked. Below are fields for 'Method' (OPTIONS), 'Frequency' (60 seconds), 'From URI' (secondary@customer.com), and 'To URI' (secondary@customer.com). An 'Edit' button is at the bottom right.

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	secondary@customer.com
To URI	secondary@customer.com

Step 5 - Select the **AT&T Server Configuration** created in **Section 7.2.4** (e.g., **ATT_SC**), and select the **Heartbeat Tab**

Step 7 - Select **Edit** (not shown) and repeat **Steps 3 & 4**, using the information shown below, and then click **Finish** (not shown).

General	Authentication	Heartbeat	Advanced
Enable Heartbeat		<input checked="" type="checkbox"/>	
Method		OPTIONS	
Frequency		60 seconds	
From URI		primary@customera.com	
To URI		primary@customera.com	

11.2. Add Secondary IP Address to Routing

Step 1 - Select **Global Profiles → Routing** from the left-hand menu.

Step 2 - Select the Routing profile created in **Section 7.2.6** (e.g., **ATT_RP**).

Step 3 - Click **Edit** (not shown), and enter the following:

- **Priority / Weight** : enter **2**.
- **Server Configuration**: Select **ATT_Secondary_SC** from the drop-down menu.
- **Next Hop Address**: enter **10.10.10.12:5060**.
- **Transport**: enter **UDP**.
- Use default values for the rest of the parameters.

Step 4 - Click **Finish**. Note that after selecting Finish, the Transport field will clear and (UDP) will appear in the Next Hop Address field (shown below in the **ATT_SC** Server Configuration entry).

Note – If desired, the **Load Balancing** parameter may be used to modify how the two defined AT&T Border Elements are accessed. **Priority** was used in the Reference Configuration.

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
Add			
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT_SC	10.10.10.11:5060 (UDP)	None
2	ATT_Secondary_SC	10.10.10.12:5060	UDP
Finish			

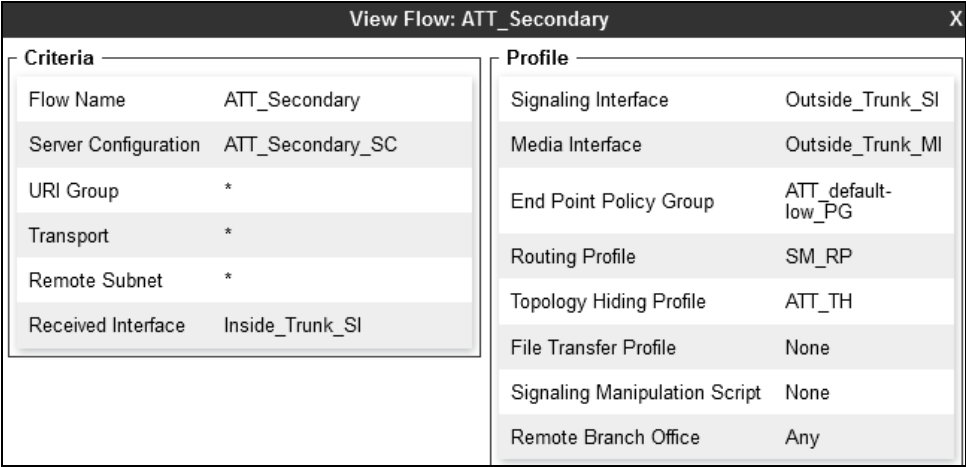
11.3. Configure End Point Flows – Server Flow - ATT_Secondary

Step 1 - Select **Device Specific Settings** → **Endpoint Flows** from the left-hand menu.

Step 2 - Select the **Server Flows** Tab, and select **Add Flow**. Repeating the steps in Section 7.4.6, enter the following:

- **Flow Name:** ATT_Secondary
- **Server Configuration:** ATT_Secondary_SC (Section 11.1).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Inside_Trunk_SI (Section 7.4.4).
- **Signaling Interface:** Outside_Trunk_SI (Section 7.4.4).
- **Media Interface:** Outside_trunk_MI (Section 7.4.3).
- **End Point Policy Group:** ATT_default-low_PG (Section 7.3.5).
- **Routing Profile:** SM_RP (Section 7.2.5).
- **Topology Hiding Profile:** ATT_TH (Section 7.2.8).
- Let other values default.

Step 3 - Click **Finish** (not shown). When completed, the Avaya SBCE will issue OPTIONS messages to the primary (10.10.10.11) and secondary (10.10.10.12) AT&T Border Elements.



Criteria	
Flow Name	ATT_Secondary
Server Configuration	ATT_Secondary_SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside_Trunk_SI

Profile	
Signaling Interface	Outside_Trunk_SI
Media Interface	Outside_Trunk_MI
End Point Policy Group	ATT_default-low_PG
Routing Profile	SM_RP
Topology Hiding Profile	ATT_TH
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any



Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	ATT	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP

Server Configuration: ATT_Secondary_SC

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	ATT_Secondary	*	Inside_Trunk_SI	Outside_Trunk_SI	ATT_default-low_PG	SM_RP

Server Configuration: SM_Trunk_SC

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile
1	SM_Trunk	*	Outside_Trunk_SI	Inside_Trunk_SI	Avaya default-low_PG	ATT_RP

©2015 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by TM 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.