



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 7.0, Avaya Session Manager 7.0, and Avaya Session Border Controller for Enterprise 7.0, with AT&T IP Flexible Reach - Enhanced Features Service – Issue 1.1

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Aura® Session Border Controller for Enterprise 7.0, with the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Communication Manager 7.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 7.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. The Avaya Aura® Session Border Controller for Enterprise 7.0 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.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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	11
3.2.	AT&T IP Flexible Reach - Enhanced Features Service Call Flows	12
3.2.1.	Inbound	12
3.2.2.	Outbound.....	13
3.2.3.	Call Forward Re-direction	14
3.3.	AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow	15
3.4.	AT&T IP Flexible Reach - Enhanced Features – Attended/Unattended Transfer (Using Refer) Call Flow	16
4.	Equipment and Software Validated	17
5.	Configure Avaya Aura® Session Manager	18
5.1.	SIP Domain	19
5.2.	Locations	19
5.2.1.	Main Location.....	19
5.3.	Configure Adaptations	21
5.3.1.	Adaptation for Avaya Aura® Communication Manager Extensions	21
5.3.2.	Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service	23
5.3.3.	Adaptation for Meet-Me Conference Calls.....	24
5.3.4.	Adaptation for calls to Avaya Aura® Messaging.....	25
5.4.	SIP Entities.....	26
5.4.1.	Avaya Aura® Session Manager SIP Entity	26
5.4.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk	28
5.4.3.	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	29
5.4.4.	Avaya Aura® Communication Manager SIP Entity – Meet-Me Trunk.....	29
5.4.5.	Avaya Session Border Controller for Enterprise SIP Entity.....	29
5.4.6.	Avaya Aura® Messaging SIP Entity	29
5.5.	Entity Links	29
5.5.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	30
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)	31
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	33

5.7.3.	Routing Policy for Inbound Routing to Avaya Aura® Messaging.....	34
5.7.4.	Routing Policy for Outbound Calls to AT&T	34
5.8.	Dial Patterns	34
5.8.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager	34
5.8.2.	Matching Outbound Calls to AT&T	36
5.8.3.	Matching Inbound Calls to Avaya Aura® Communication Manager Meet-Me Conference	38
5.8.4.	Matching Inbound PSTN Calls to Avaya Aura® Messaging	39
6.	Configure Avaya Aura® Communication Manager	40
6.1.	Verify Communication Manager System Settings	40
6.1.1.	System-Parameters Customer-Options	41
6.2.	System-Parameters Features	43
6.3.	Dial Plan	45
6.4.	IP Node Names	46
6.5.	IP Network Regions	48
6.5.1.	IP Network Region 1 – Local CPE Region	48
6.5.2.	IP Network Region 2 – AT&T Trunk Region	50
6.6.	IP Codec Parameters	51
6.6.1.	Codecs for IP Network Region 1 (calls within the CPE)	51
6.6.2.	Codecs for IP Network Region 2 (calls to/from AT&T)	53
6.7.	SIP Trunks	53
6.7.1.	SIP Trunk for Inbound/Outbound AT&T calls	53
6.7.2.	Local SIP Trunk (Avaya SIP Telephone and Avaya Messaging Access)	59
6.7.3.	SIP Trunk for Meet-Me Conference Calls	60
6.8.	Private Numbering	61
6.9.	Public Unknown Numbering	62
6.10.	Route Patterns	63
6.10.1.	Route Pattern for Calls to AT&T	63
6.10.2.	Route Pattern for Calls within the CPE	64
6.11.	Automatic Route Selection (ARS) Dialing	65
6.12.	Automatic Alternate Routing (AAR) Dialing	66
6.13.	Avaya G430 Media Gateway Provisioning	67
6.14.	Meet-Me Conference Vector and Vector Directory Number (VDN)	69
6.14.1.	Meet-Me Vector	70
6.14.2.	Meet-Me VDN	70
6.15.	IP Interface for procr	71
6.16.	Save Translations	72
7.	Configure Avaya Session Border Controller for Enterprise	73
7.1.	System Management – Status	75
7.2.	Global Profiles	75
7.2.1.	Server Interworking – Avaya	76
7.2.2.	Server Interworking – AT&T	78
7.2.3.	Server Configuration – Session Manager	80
7.2.4.	Server Configuration – AT&T	81
7.2.5.	Routing – To Session Manager	82

7.2.6.	Routing – To AT&T	83
7.2.7.	Topology Hiding – Avaya Side	84
7.2.8.	Topology Hiding – AT&T Side.....	85
7.2.9.	Signaling Manipulation.....	86
7.3.	Domain Policies	86
7.3.1.	Application Rules.....	86
7.3.2.	Media Rules	87
7.3.3.	Signaling Rules	88
7.3.4.	Endpoint Policy Groups – Avaya Connection	89
7.3.5.	Endpoint Policy Groups – AT&T Connection.....	90
7.4.	Device Specific Settings.....	90
7.4.1.	Network Management.....	90
7.4.2.	Advanced Options.....	91
7.4.3.	Media Interfaces.....	92
7.4.4.	Signaling Interface	92
7.4.5.	Endpoint Flows – For Session Manager	93
7.4.6.	Endpoint Flows – For AT&T.....	93
8.	Verification Steps.....	95
8.1.	AT&T IP Flexible Reach – Enhanced Features	95
8.2.	Avaya Aura® Communication Manager	95
8.3.	Avaya Aura® Session Manager	96
8.4.	Avaya Session Border Controller for Enterprise.....	98
8.4.1.	System Status	98
8.4.2.	Protocol Traces	98
9.	Conclusion	100
10.	References.....	101
11.	Addendum 1 – Redundancy to Multiple AT&T Border Elements	102
11.1.	Secondary AT&T Border Element Server Configuration	102
11.2.	Add Secondary IP Address to Routing.....	103
11.3.	Configure End Point Flows – Server Flow - ATT_Secondary.....	104

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 7.0 (Communication Manager), Avaya Aura® Session Manager 7.0 (Session Manager), Avaya Aura® System Manager 7.0 (System Manager), and the Avaya Session Border Controller for Enterprise 7.0 (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 7.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 7.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® System Manager 7.0 is the provisioning/management application for Avaya Aura® Session Manager. The Avaya Aura® Session Border Controller for Enterprise 7.0 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, and fax machines (Ventafax application). Avaya Aura® Messaging is used to provide voicemail capabilities for the CPE.
- 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 between the PSTN, via the IPFR-EF network, and 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 T.38.
- 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, Communication Manager, and Avaya Messaging menu navigation.
- Telephony features such as hold, transfer, and conference.
- Basic Communication Manager EC500 “mobility” calls.
- 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.

- 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:
 - i) Create a “Meet-Me Conference” SIP trunk with NCR *disabled*, used exclusively for customers placing Meet-Me conference calls (see **Section 6.7.3**).
 - ii) Create a “general access” SIP trunk, with NCR *enabled*, for all other inbound and outbound calls (see **Section 6.7.1**). 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 may not display all the calling information. By default, Communication Manager expects a display update from the network in the PAI header. However, the subsequent network signaling does not contain a PAI header, and the From header must be used instead.
 - a) The recommended workaround is described in **Section 6.7.1**, where Communication Manager will retrieve the display information using the *From* header.
- 3) **IPFR-EF Simultaneous Ring and Sequential Ring – Secondary number uses Telephone Event payload type 101 and ptime of 20ms.** When the CPE endpoint associated with the IPFR-EF “secondary” number answers the call, the IPFR-EF service will send a re-Invite for this call dialog to change the Telephone Event Type from the preferred value of 100 to 101, and the ptime value from 30ms to 20ms. These values differ slightly from the IPFR-EF specification, and are noted here simply as an observation. Communication Manager was able to successfully negotiate to these new values, and no user-perceivable problems were observed from this behavior.
- 4) **IPFR-EF Call Forward Always (CFA/CFU) – No ringing heard for Ring Splash reminder.** When Call Forward is activated with the Ring Splash feature (ring reminder on call forward) through the IPFR-EF service, and a call is placed to the primary number, the CPE endpoint’s call appearance will flash briefly to indicate that the call has been forwarded; however, the IPFR-EF service sent a SIP CANCEL message before the endpoint had a chance to provide an audible ring tone.
- 5) **T.38/G.729 fax is limited to 9600bps when using the G4xx Media Gateways.** A G430 Media Gateway is used in the reference configuration. As a result T.38/G.729 fax was limited to 9600 bps. Also note that 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.

- 6) **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.
- 7) **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), Session Manager is provisioned to remove SIP headers not required by the AT&T IPFR-EF service (see **Section 5.3.2**). These headers are:
 - a) AV-Correlation-ID, AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Location, Remote-Party-ID.
- 8) **Emergency 911/E911 Services Limitations and Restrictions** – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) 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 7.0, System Manager 7.0, Session Manager 7.0, and the Avaya SBCE 7.0 are used in the reference configuration. Note that all of these Avaya components ran on a VMware (ESXi 5.5) platform.

- In the reference configuration System Manager provides a common administration interface for centralized management of Session Manager and 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. Avaya SIP endpoints register to Session Manager while Avaya H.323 endpoints register to Communication Manager.
- 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.
- Avaya Aura® Messaging was used in the reference configuration to provide voice mailbox 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.

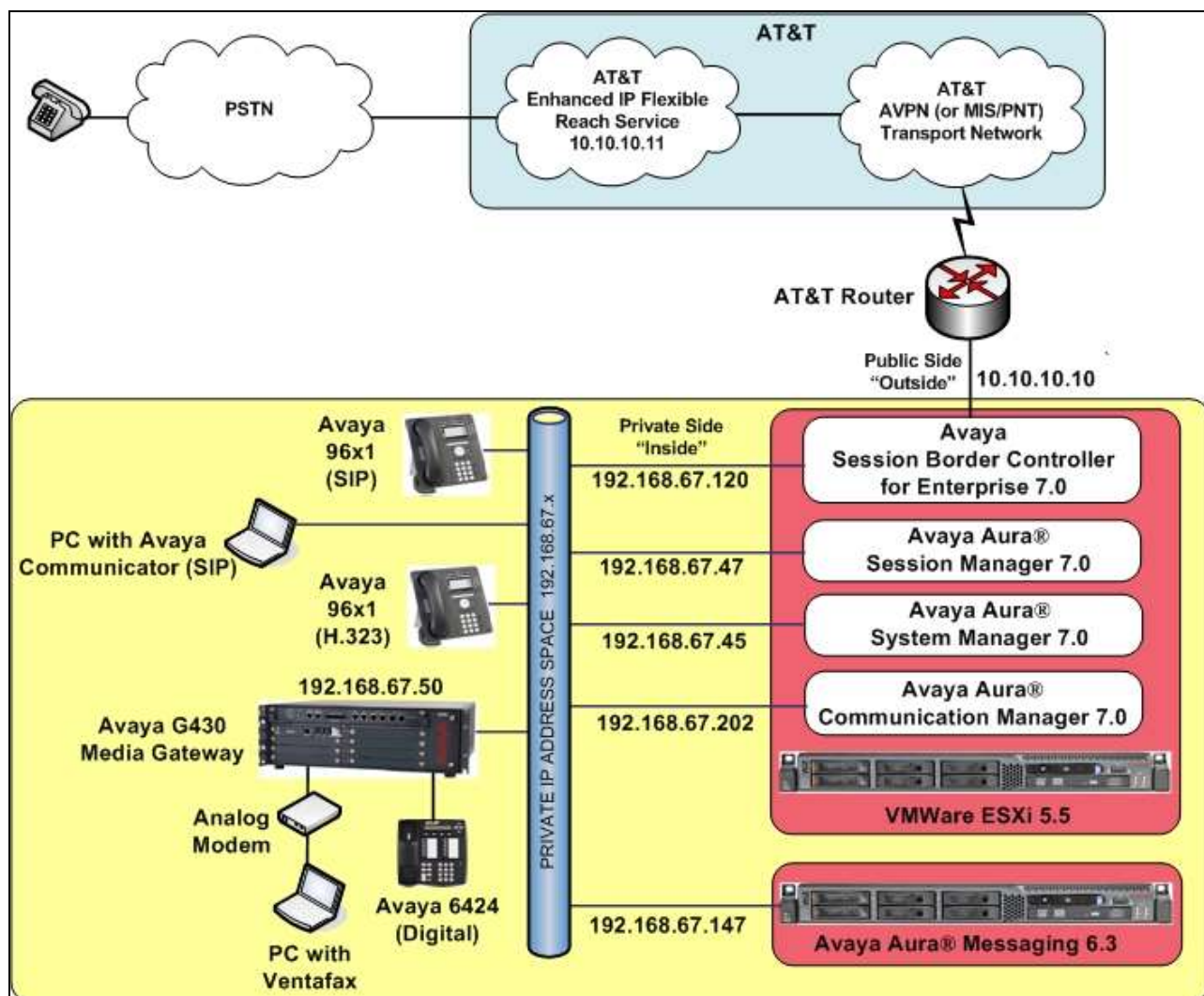


Figure 1: Reference configuration

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	
IP Address	192.168.67.47
Avaya Aura® Communication Manager	
IP Address	192.168.67.202
Avaya Aura® System Manager	
IP Address	192.168.67.45
Avaya Aura® Messaging	
IP Address	192.168.67.147
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	192.168.67.120

Table 1: Network 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.

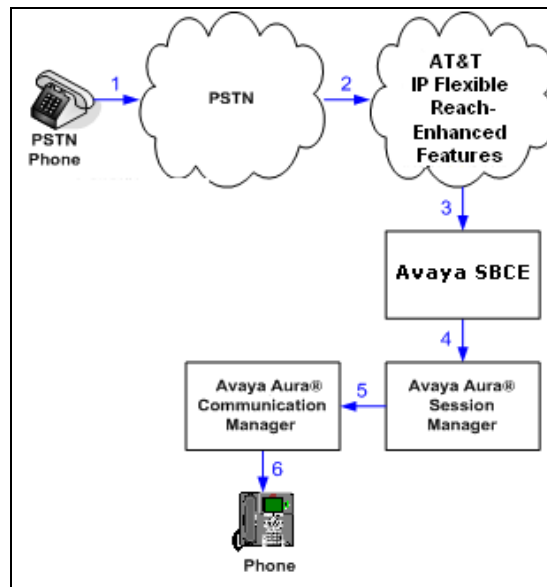


Figure 2: Inbound IPFR-EF Call

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.

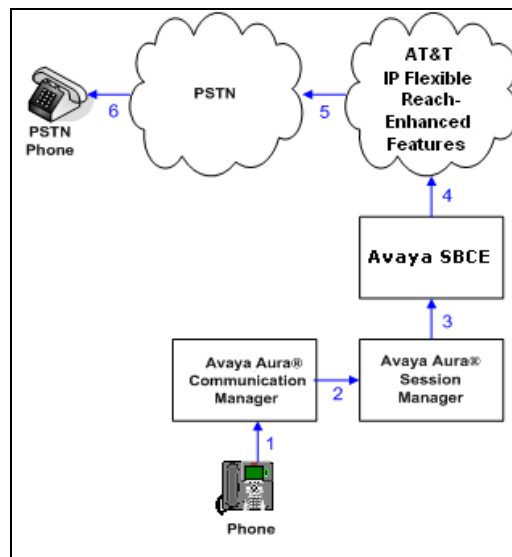


Figure 3: Outbound IPFR-EF Call

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 6.7**).

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.

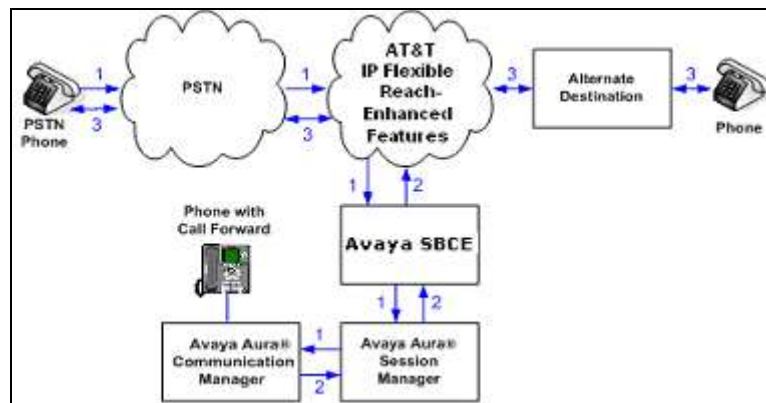


Figure 4: Station Re-directed (e.g., Call Forward) IPFR-EF Call

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).

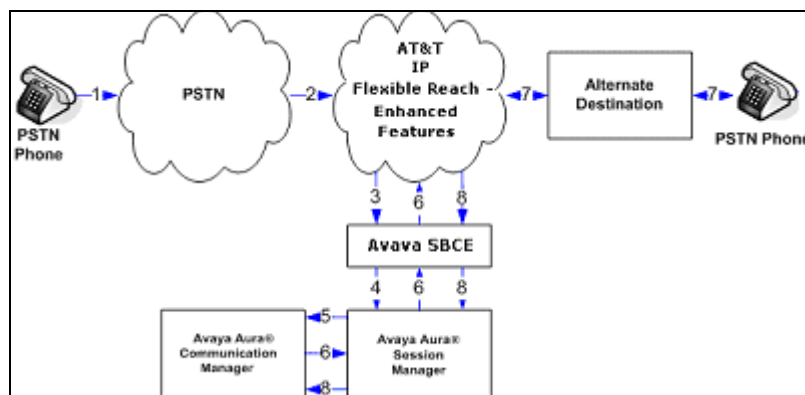


Figure 5: Network Based Blind Transfer Using Refer (Communication Manager Vector)

3.4. AT&T IP Flexible Reach - Enhanced Features – Attended/Unattended Transfer (Using Refer) Call Flow

This section describes the call flow for IPFR-EF using SIP Refer to perform an Attended or Unattended Transfer. 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 station. The station answers the call and, transfers it back out to a second PSTN destination. Communication Manager generates using Refer (*with the replaces parameter*), back to the IP E-IPFR service for routing to the new 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. Communication Manager routes the call to a station.
6. The station answers the call and then transfers it to a new PSTN destination. Communication Manager redirects 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 existing call to Communication Manager.

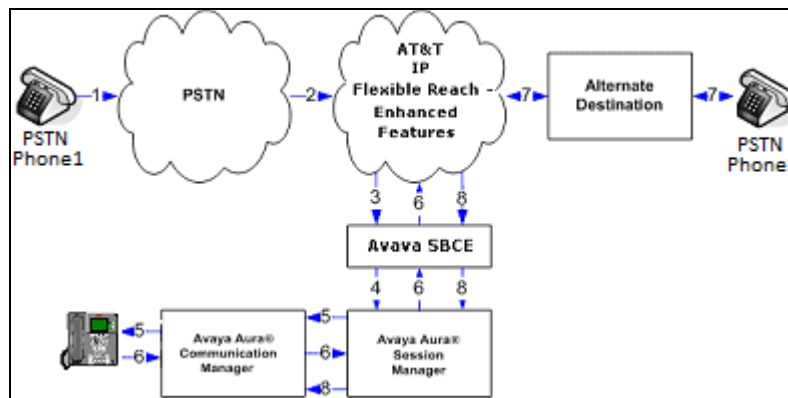


Figure 5: Attended/Unattended Transfer Using Refer (Communication Manager Vector)

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">Avaya Aura® Session ManagerAvaya Aura® System ManagerAvaya Aura® Communication ManagerAvaya Session Border Controller for Enterprise	<ul style="list-style-type: none">VMware ESXi 5.5<ul style="list-style-type: none">7.0.0.0.7000077.0.0.0.16266R017x.00.0.441.0 and SP1 (22477)7.0.0-21-6602
Dell R610 <ul style="list-style-type: none">System PlatformAvaya Aura® Messaging	<ul style="list-style-type: none">6.3.7.0.010056.3-03.0.141.0-348
Avaya G430 Media Gateway	<ul style="list-style-type: none">g430_sw_37_19_0
Avaya 96x1 IP Telephone	<ul style="list-style-type: none">H.323 = 6.6029SIP = 7.0.0.38
Avaya Communicator for Windows (SIP)	<ul style="list-style-type: none">2.1.2.75
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none">7.0.202.494

Table 2: Equipment and Software Versions

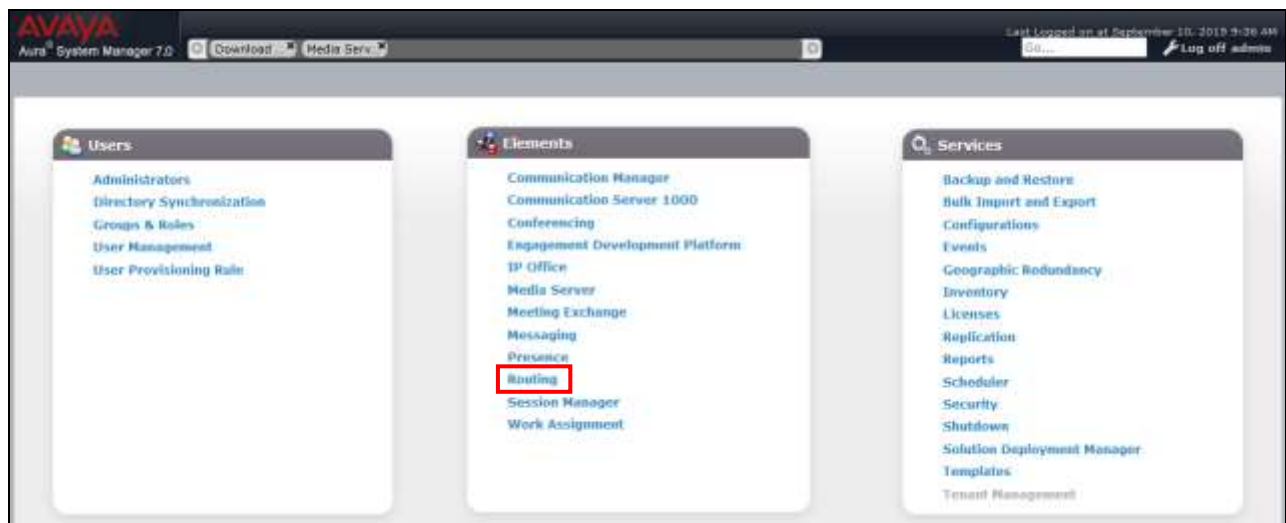
5. Configure Avaya Aura® Session Manager

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 a Location for Customer Premises Equipment (CPE).
- 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, 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.



5.2. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager, the Avaya SBCE, the G430 Media Gateway, and telephones.

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

Home / Elements / Routing / Locations

Location Details

General

* Name:

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

Maximum Multimedia Bandwidth (Inter-Location):

* Minimum Multimedia Bandwidth:

* Default Audio Bandwidth:

Alarm Threshold

Overall Alarm Threshold:

Multimedia Alarm Threshold:

* Latency before Overall Alarm Trigger:

* Latency before Multimedia Alarm Trigger:

Location Pattern

Add
Remove

☐ IP Address Pattern

Notes

Select : All, None

Commit
Cancel

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 DNIS number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDN.
- 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**.
 - Avaya SIP headers not required by AT&T are removed (see **Section 2.2, Item 5**).
- 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 (see **Section 2.2, Item 1**).
- 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., **ACM_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**).

The screenshot shows the 'Adaptation Details' page in the Session Manager configuration interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations (highlighted), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. The breadcrumb path at the top is 'Home / Elements / Routing / Adaptations'. There are 'Commit' and 'Cancel' buttons in the top right corner. The form fields are as follows: 'Adaptation Name' is a text field containing 'ACM_public'; 'Module Name' is a dropdown menu showing 'DigitConversionAdapter'; 'Module Parameter Type' is a dropdown menu that is currently empty; 'Egress URI Parameters' is a text field that is empty; and 'Notes' is a text area that is empty.

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/Communication manager extensions.

Step 5 - Click on **Commit**.

Note – 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 Request URI, *not* the number that was dialed.

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*5553161	*7	*7		*7	19001	destination		Sequential Primary
<input type="checkbox"/>	*5553162	*7	*7		*7	19002	destination		Sequential Secondary
<input type="checkbox"/>	*5553163	*7	*7		*7	19003	destination		
<input type="checkbox"/>	*5553164	*7	*7		*7	19004	destination		
<input type="checkbox"/>	*5553165	*7	*7		*7	19020	destination		Simul Primary
<input type="checkbox"/>	*5553166	*7	*7		*7	19021	destination		Simul Secondary

Select : All, None

Commit Cancel

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 6.7.1**).

Step 2 - In the **Module Parameter Type**: field select **Name-Value Parameter** from the menu.

Step 3 - In the **Name-Value Parameter** table, enter the following:

1. **Name** – Enter **eRHdrs**
2. **Value** – Enter the following Avaya headers to be removed by Session Manager. Note that each header name is separated by a comma.
 - **AV-Correlation-ID,AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-ID,P-Location,Reason,Remote-Party-ID**

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

The screenshot displays the 'General' tab of an adaptation configuration page. At the top, the 'Adaptation Name' is set to 'ATT'. Below it, the 'Module Name' is set to 'AttAdapter' from a dropdown menu. The 'Module Parameter Type' is set to 'Name-Value Parameter'. A table for Name-Value Parameters is shown with one entry: Name 'eRHdrs' and Value 'AV-Correlation-ID,AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-ID,P-Location,Reason,Remote-Party-ID'. Below this table are fields for 'Egress URI Parameters' and 'Notes'. The 'Digit Conversion for Incoming Calls to SM' section is empty, showing '0 Items' and a 'Filter: Enable' button. The 'Digit Conversion for Outgoing Calls from SM' section is also empty, showing '0 Items' and a 'Filter: Enable' button. Both sections have a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes.

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 designated for Meet-Me conference sessions. 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.

The screenshot displays the 'General' configuration page for an adaptation. The 'Adaptation Name' is 'Main_Meet-Me' and the 'Module Name' is 'DigitConversionAdapter'. Below this, there are fields for 'Module Parameter Type', 'Egress URI Parameters', and 'Notes'. The 'Digit Conversion for Incoming Calls to SM' section is empty. The 'Digit Conversion for Outgoing Calls from SM' section contains a table with one row of configuration data.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 5553180	* 7	* 7		* 7	19000	destination		Meet-Me Conference VDN

At the bottom of the page, there are 'Commit' and 'Cancel' buttons.

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 2 - 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 (36000 is the Avaya Messaging access number used in the reference configuration).
 - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
 - Enter any desired notes.

Step 3 - Click on **Commit**.

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

The screenshot shows the 'Adaptation Details' page with the following configuration:

- General**
 - Adaptation Name: AAM_Digits
 - Module Name: DigitConversionAdapter
 - Module Parameter Type: (empty)
 - Egress URI Parameters: (empty)
 - Notes: (empty)
- Digit Conversion for Incoming Calls to SM**
 - 0 items
- Digit Conversion for Outgoing Calls from SM**
 - 1 item
 - Matching Pattern: *5553170
 - Min: *10
 - Max: *10
 - Phone Context: (empty)
 - Delete Digits: *10
 - Insert Digits: 36000
 - Address to modify: destination
 - Adaptation Data: (empty)
 - Notes: (empty)

Buttons: Add, Remove, Filter: Enable, 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., **asm**).
- **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.

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., **customera.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.

Port	Protocol	Default Domain	Notes
5060	TCP	customera.com	
5061	TLS	customera.com	
5062	TCP	customera.com	
5080	TCP	customera.com	

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., **ACM_public**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 6.4** (e.g., **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **ACM_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' configuration page with the 'General' tab selected. The page includes fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, SIP Timer B/F, Credential name, Securable, Call Detail Recording, Loop Detection Mode, SIP Link Monitoring, Supports Call Admission Control, Shared Bandwidth Manager, Primary Session Manager Bandwidth Association, and Backup Session Manager Bandwidth Association. The 'Commit' and 'Cancel' buttons are in the top right corner.

SIP Entity Details [Commit] [Cancel]

General

* **Name:** ACM_public

* **FQDN or IP Address:** 192.168.67.202

Type: CM

Notes:

Adaptation: ACM_public

Location: Main

Time Zone: America/New_York

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

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

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., **ACM_local**).
- **Adaptations** – Leave this field blank.

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., **ACM_Meet-Me**).
- **Adaptations** – Select Adaptation **Main_Meet-Me** (**Section 5.3.3**).

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., **SBCE**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **192.168.67.120**, see **Section 7.4.1**).
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **ATT** (**Section 5.3.2**).

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** – Select **Other** (or **Modular Messaging**).
- **Adaptations** – Select Adaptation **AAM_Digits** (**Section 5.3.4**).

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., **sm_ACM_public_5062**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g., **asm**).
- **Protocol** – Select **TCP** (see **Section 6.7.1**).
- **SIP Entity 1 Port** – Enter **5062**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **ACM_public**).
- **SIP Entity 2 Port** – Enter **5062** (see **Section 6.7.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

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., **sm_ACM_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., **ACM_local**).
- **SIP Entity 2 Port** – Enter **5060** (see **Section 6.7.2**).

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., **sm_ACM_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., **ACM_Meet-Me**).
- **SIP Entity 2 Port** – Enter **5080** (see **Section 6.7.3**).

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., **sm_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., **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., **sm_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 6.7.2**).

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 displays the 'Time Ranges' configuration interface. On the left, a navigation pane lists various routing-related settings, with 'Time Ranges' currently selected. The main content area features a header with 'Time Ranges' and a set of action buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below this is a table for managing time ranges. The table has columns for a checkbox, Name, and days of the week (Mo, Tu, We, Th, Fr, Sa, Su), followed by Start Time, End Time, and Notes. One entry is shown with the name '24/7', all days of the week selected, a start time of 00:00, an end time of 23:59, and the note 'Time Range 24/7'. At the bottom of the table, there is a 'Select' dropdown menu currently set to 'All'.

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

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., **ACM_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.



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 (**ACM_Public**), and click on **Select**.



	Name	FQDN or IP Address	Type	Notes
⊙	AA-M	192.168.67.147	Modular Messaging	
⊙	ACM_local	192.168.67.202	CM	
⊙	ACM_Meet-Me	192.168.67.202	CM	Meet-Me Conference without NCR
●	ACM_public	192.168.67.202	CM	
⊙	asm	192.168.67.47	Session Manager	
⊙	SBCE	192.168.67.120	SIP Trunk	

Select : None

- 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.
- Step 8** - No **Regular Expressions** were used in the reference configuration.
- Step 9** - Click on **Commit**.

Note – Once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

The screenshot shows the 'Routing Policy Details' form. The 'General' section includes fields for 'Name' (ACM03_PUBLIC), 'Disabled' (unchecked), 'Ranking' (2), and 'Notes' (from AT&T). The 'SIP Entity as Destination' section has a 'Select' button. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlap' buttons, and a table with columns for Name, Rank, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The 'Ranking' field in the table is highlighted with a red box and contains the value '2'. The 'Dial Patterns' section includes 'Add' and 'Remove' buttons and a table with columns for Pattern, Ptn, Ptn, Emergency Call, SIP Domain, Originating Location, and Notes. The 'Regular Expressions' section includes 'Add' and 'Remove' buttons and a table with columns for Pattern, Rank Order, Deny, and 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:

- Enter a descriptive **Name** (e.g., **ACM_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., **ACM_Meet-Me**).
- In the **Time of Day** section, change the ranking number to **1**.

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. Repeat the steps in **Section 5.7.1** with the following differences:

- 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**).

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:

- Enter a descriptive **Name** for routing calls to the AT&T IPFR-EF service via the Avaya SBCE (e.g., **SBCE**), 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., **SBCE**).

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 DNIS digits in the SIP Request URI (for security purposes, these digits are represented in this document as **555xxxx**). The DNIS pattern must be matched for further call processing. Depending on customer deployments, the IPFR-EF service may send different DNIS digit lengths.

Note – Be sure to match on the DNIS digits specified in the AT&T Request URI, not the DID dialed digits. 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** – 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.

Step 3 - Scrolling down to the **Originating Location and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

Step 4 - In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to *All Originating 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., **ACM_Public**), and click on **Select**.

Name	Disabled	Destination	Notes
ACM_Local	<input type="checkbox"/>	ACM_local	
ACM_Hest-Ha	<input type="checkbox"/>	ACM_Hest-Ha	
ACM_Public	<input type="checkbox"/>	ACM_public	
SBCE	<input type="checkbox"/>	SBCE	
To_AAH	<input type="checkbox"/>	AA-M	

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

Step 7 - Repeat **Steps 1-6** for any additional inbound dial patterns from AT&T.

Note – No **Denied Original Locations** are specified in the reference configuration.

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

<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"/>	Main		ACN_Public		<input type="checkbox"/>	ACN_public	from AT&T

Select: All, None

Denied Originating Locations

Add Remove

0 Items

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

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 1xxxxyyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes *7 and *9 (e.g., *71yyyzzzxxxx & *91yyyzzzxxxx) are specified.

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., **SBCE**).

Note – No **Denied Original Locations** are specified in the reference configuration.

General Commit Cancel

* Pattern: 1732

* Min: 11

* Max: 11

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain: -ALL-

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-		SBCE	0	<input type="checkbox"/>	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"/>	011	12	16	<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"/>	*7	14	14	<input type="checkbox"/>			-ALL-	IPFR Call Forward Busy
<input type="checkbox"/>	*9	14	14	<input type="checkbox"/>			-ALL-	IPFR Call Forward RNA

Select : All, None

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 Request 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 changes:

- 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 **All** Locations.
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy **ACM_Meet-Me** (Section 5.7.2).

The screenshot shows the 'Dial Pattern Details' configuration page. The 'General' section is active, showing the following fields:

- Pattern:** 5553180
- Min:** 7
- Max:** 7
- Emergency Call:** ☐
- Emergency Priority:**
- Emergency Type:**
- SIP Domain:** -ALL-
- Notes:** Meet-Me conf

The 'Originating Locations and Routing Policies' section shows a table with 1 item:

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

The 'Denied Originating Locations' section shows 0 items.

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 checked="" type="checkbox"/>	-ALL-		To_AAM	0	<input type="checkbox"/>	AA-M	

Select: All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

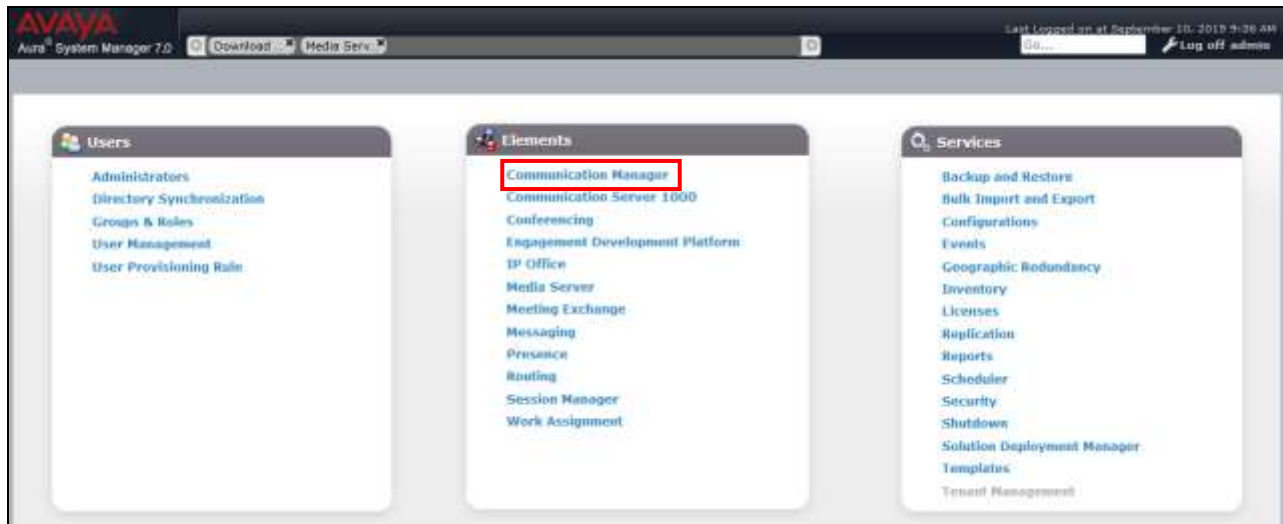
<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

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. These Application Notes assume that basic Communication Manager administration have already been performed. Consult [5 - 7] for more information.

Note – Unless otherwise noted, the following procedures are performed using System Manager.

Communication 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 **Communication Manager**.



Note – In the following sections, only the specified parameters are applicable to these Application Notes. Other parameter values may or may not match based on local configurations.

6.1. Verify Communication Manager System Settings

Note – This section describes steps to verify Communication Manager feature settings that are required for the reference configuration described in these Application Notes. Depending on access privileges and licensing, some or all of the following settings might only be viewed, and not modified. If any of the required features are not set, and cannot be configured, contact an authorized Avaya account representative to obtain the necessary licenses/access.

6.1.1. System-Parameters Customer-Options

Note – Parameters on this form may only be viewed. Licensing or privileged access is required to change values.

Step 1 - From the **Communication Manager** menu, select **Parameters** → **System Parameters** **Customer-Options**.

Step 2 - At the top of the page, select the appropriate Communication Manager system.

Step 3 - In the **System Parameters – Customer Options List** section, select the parameter line to activate the **View** button. Click on the **View** button.

Home / Elements / Communication Manager / Parameters / System Parameters - Customer Options

Search

System Parameters - Customer Options

Select device(s) from Communication Manager List

2 Items Show All Filter: Enable

Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version	CMT Notification
1000	192.168.67.202	September 13, 2015 11:05:22 PM -04:00	10:00 pm SUN SEP 13, 2015	Incremental	Completed		R017x.00.0.441.0	true

Select: All, None

Show List

System Parameters - Customer Options List

1 Item Show All Filter: Enable

Platform	Abbreviated Dialing Enhanced List	ABS	AES/AAR Partitioning	AES/AAR Dialing without FAC	Audible Message Waiting	Hospitality (Basic
20	true	true	true	false	true	true

Select: None

Step 4 - The **system-parameters customer-options** form is displayed. Click the **Next Page** button, and 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

Enter Refresh Cancel Clear Field Help Edit Prev Page **Next Page** More Actions

Info:

display system-parameters customer-options Page 2 of 12

OPTIONAL FEATURES

IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks:	12000 0
Maximum Concurrently Registered IP Stations:	18000 2
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 3
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

(NOTE: You must logout login to effect the permission changes.)

Step 5 - On **Page 4** of the form, verify that the **ARS** feature is enabled.

display system-parameters customer-options Page 4 of 12

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?	y	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		

(NOTE: You must logoff login to effect the permission changes.)

Step 6 - On **Page 5** 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 5 of 12

OPTIONAL FEATURES

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

(NOTE: You must logoff login to effect the permission changes.)

Step 7 - On **Page 6** of the form, verify that the **Private Networking** and **Processor Ethernet** fields are set to **y**.

display system-parameters customer-options Page 6 of 12

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	Wideband Switching?	y
Processor Ethernet?	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.)

Step 8 - When the settings review is complete, click on the **Cancel** button (see the screenshot in **Step 4**). Note that attempting to leave the form without clicking Cancel will result in a system request to “Leave Page” or “Stay on Page”.

6.2. System-Parameters Features

Step 1 - Following the procedures in **Section 6.1**, select **Parameters** → **System-Parameters Features**, and select **View**. Note that changes can be made to the values on this form (depending on access privileges), by clicking on **Edit**.

Home / Elements / Communication Manager / Parameters / System Parameters - Features Help ?

System Parameters - Features

Select device(s) from Communication Manager List Show List

System Parameters - Features List

View Edit New

1 Item Show All Filter: Enable

Terminal Translation Initialization (TTI) Enabled	EMU Inactivity Interval for Deactivation(hours)	Switch Name	System
true			scm

Select : None

Step 2 - On page 1, verify that **Trunk-to-Trunk Transfer** is set to **all**.

display system-parameters features Page 1 of 19

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

Step 3 - On **page 19**, verify that **SIP Endpoint Managed Transfer** is set to **n**.

change system-parameters features Page 19 of 19

FEATURE-RELATED SYSTEM PARAMETERS

IP PARAMETERS

Direct IP-IP Audio Connections?	<input type="checkbox"/> y	IP Audio Hairpinning?	<input type="checkbox"/> n
Synchronization over IP?	<input type="checkbox"/> n		
SIP Endpoint Managed Transfer?	<input type="checkbox"/> n		
Expand ISDN Numbers to International for 1XCES?	<input type="checkbox"/> n		

CALL PICKUP

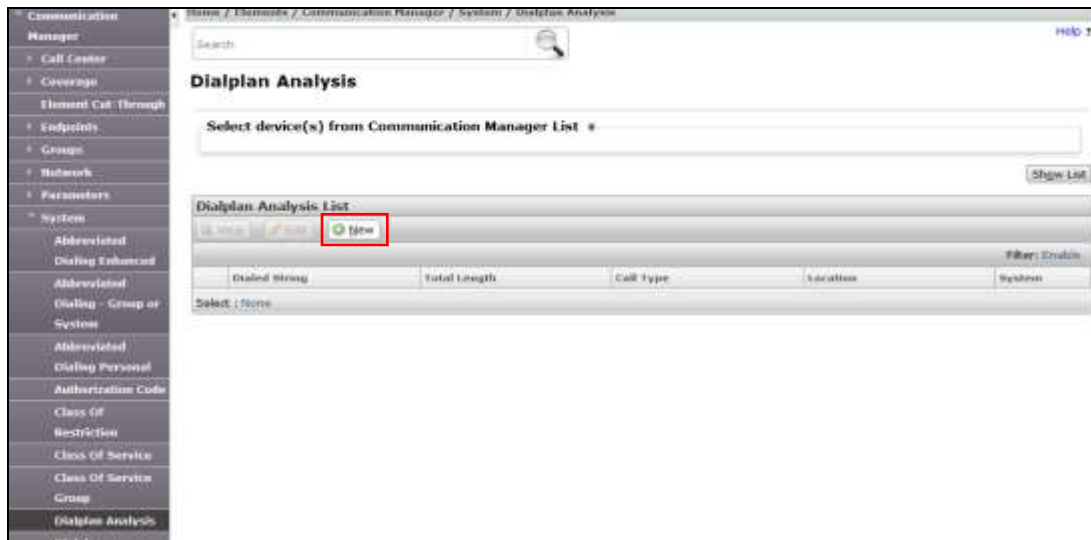
Maximum Number of Digits for Directed Group Call Pickup:	<input type="text"/> 2		
Call Pickup on Intercom Calls?	<input type="checkbox"/> y	Call Pickup Alerting?	<input type="checkbox"/> n
Temporary Bridged Appearance on Call Pickup?	<input type="checkbox"/> y	Directed Call Pickup?	<input type="checkbox"/> n
Extended Group Call Pickup:	<input type="text"/> none		
Enhanced Call Pickup Alerting?	<input type="checkbox"/> n		
Display Information With Bridged Call?	<input type="checkbox"/> n		
Keep Bridged Information on Multiline Displays During Calls?	<input type="checkbox"/> n		
PIN Checking for Private Calls?	<input type="checkbox"/> n		

6.3. Dial Plan

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

Step 1 - From the Communication Manager menu, select **System** → **Dialplan Analysis**.

Step 2 - Select **New**.



Step 3 - Select the appropriate Communication Manager system, and select **Add(+)**.



Step 4 - Provision the dial plan as follows:

- 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 6.7**.
- 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**.

Step 5 - Click on **Enter**.

acm

change dialplan analysis

Enter Refresh Cancel Clear Field Help Edit Prev Page Next Page More Actions

Info:

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	dac						
9	1	dac						
*	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 - From the Communication Manager menu, select **Network → Node Names**.

Step 2 - Select **New**.

Communication Manager

- Call Center
- Coverage
- Element Call Through
- Endpoints
- Concepts
- Network
 - Automatic
 - Alternate Routing
 - Analysis
 - Automatic
 - Alternate Routing
 - Digit Compression
 - Automatic Route Selection Analysis
 - Automatic Route Selection Digit Conversion
 - Automatic Route Selection Full
 - Data Modules
 - IP Codes Sets
 - IP Interfaces
 - IP Network Maps
 - IP Network
 - Regions
 - Node Names**

Search

Node Names

Select device(s) from Communication Manager List

Show List

Node Names List

New

Filter: Search

Type	Name	IP Address	System
Select: None			

Step 3 - Select the appropriate Communication Manager system, enter **ip** in the **Enter Qualifier** field, and select **Add(+)**.

Select device from Communication Manager List

Select a CM from the following list

2 Items

Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
am	192.168.67.202	September 14, 2015 11:00:23 PM -04:00	Incremental	Completed		R017x.00.0.441.0

Enter Qualifier: ip

Add(+) Cancel

* Required

Step 4 - Provision the Node Names as follows:

- Avaya SBCE private (A1) network interface (e.g., **SBCE** and **192.168.67.120**).
- Session Manager SIP signaling interface (e.g., **SM** and **192.168.67.47**).
- Avaya Messaging (e.g., **AAM** and **192.168.67.147**).

Step 5 - Click on **Enter**.

Note that other entries in the list are defined during Communication Manager installation.

change node-names ip

Enter Refresh Cancel Clear Field Help Edit Prev Page Next Page More Actions

Info:

change node-names ip Page 1 of 2

Name	IP Address
AAM	192.168.67.147
SBCE	192.168.67.120
SM	192.168.67.47
default	0.0.0.0
gateway	192.168.67.1
procr	192.168.67.202
procr6	11

(12 of 12 administered node-names were displayed)

Use 'list node-names' command to see all the administered node-names

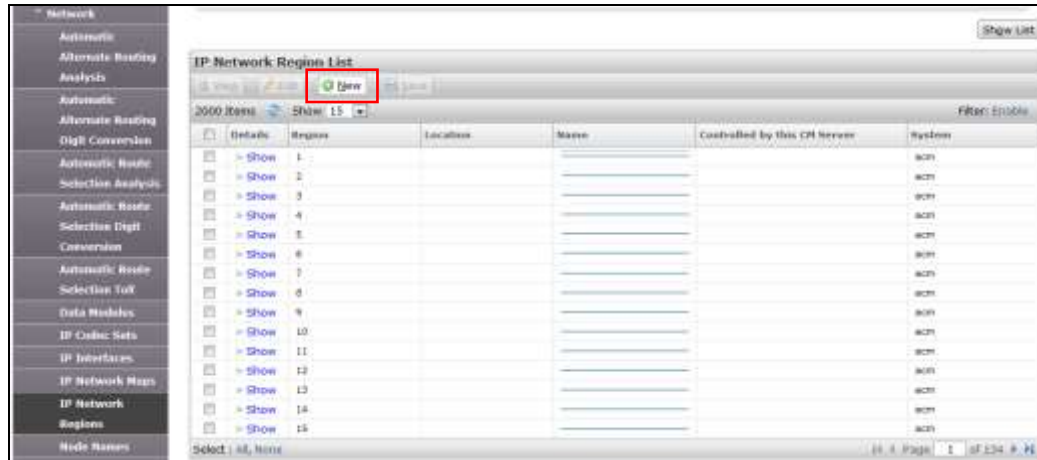
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

6.5. IP Network Regions

Network Regions are used to group various Communication Manager resources such as codecs, UDP port ranges, and inter-region communication. In 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).

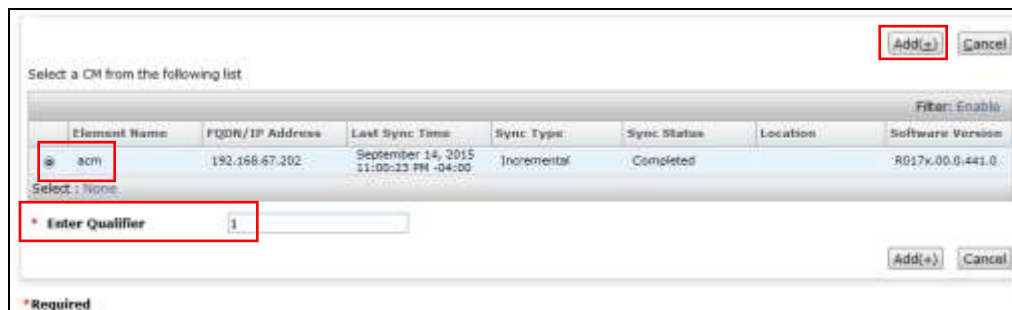
Step 1 - From the Communication Manager menu, select **Network** → **IP Network Regions**.

Step 2 - Select **New**.



6.5.1. IP Network Region 1 – Local CPE Region

Step 3 - Select the appropriate Communication Manager system, enter **1** in the **Enter Qualifier** field, and select **Add(+)**.



Step 4 - Region 1 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).

The screenshot shows the 'change ip-network-region 1' configuration page. The page title is 'change ip-network-region 1' and it is page 1 of 20. The form is titled 'IP NETWORK REGION'. The 'Region' is set to '1'. The 'Location' is '1'. The 'Authoritative Domain' is 'customera.com'. The 'Name' is 'Main'. The 'Stub Network Region' is 'n'. The 'MEDIA PARAMETERS' section includes 'Codec Set' (1), 'UDP Port Min' (16384), and 'UDP Port Max' (32767). The 'DIFFSERV/TOS PARAMETERS' section includes 'Call Control PHB Value' (46), 'Audio PHB Value' (46), and 'Video PHB Value' (26). The '802.1P/Q PARAMETERS' section includes 'Call Control 802.1p Priority' (6), 'Audio 802.1p Priority' (6), and 'Video 802.1p Priority' (5). The 'H.323 IP ENDPOINTS' section includes 'H.323 Link Bounce Recovery?' (Y), 'Idle Traffic Interval (sec)' (20), 'Keep-Alive Interval (sec)' (5), and 'Keep-Alive Count' (5). The 'AUDIO RESOURCE RESERVATION PARAMETERS' section includes 'RSVP Enabled?' (n). The 'Intra-region IP-IP Direct Audio' and 'Inter-region IP-IP Direct Audio' are both set to 'yes'. The 'IP Audio Hairpinning?' is set to 'n'.

Step 5 - On **page 2** of the form:

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

Step 6 - 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. Click on **Enter** (not shown).

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

Note that Region 2 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 6.5.1** with the following changes:

Step 6 - Select the appropriate Communication Manager system, enter **2** in the **Enter Qualifier** field, and select **Add(+)**.

Step 7 - On **Page 1** of the form (not shown):

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

Step 8 - 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

dst codec direct WAN-BW-limits

Intervening Dyn

Video A Gc

rgn set WAN Units Total

Regions CAC

Norm Prio Shr R L e

1 2 y NoLimit

2 2

n t

all

Step 9 - Click on **Enter** (not shown). The completed form is shown below.

IP Network Region List					
					
2000 Items			Show: 15	Filter: Enable	
	Details	Region	Location	Name	Controlled by this CM Server
	Show	1	1	Men	acm
	Show	2	1	ATT	acm
	Show	3			acm

6.6. IP Codec Parameters

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

Step 1 - From the Communication Manager menu, select **Network → IP Codec Sets**.

Step 2 - Select Codec Set 1, and click on the **Edit button.**

[illegible]

Step 3 - On **Page 1** of the **ip-codec-set** form, set the codec list as shown below. Note that the packet interval size will default to 20ms (**Frames Per Pkt = 2**).

change ip-codec-set 1

Info:

change ip-codec-set 1 Page 1 of 2

IP CODEC SET

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size[ms]
1: G.711MU	n	2	20
2: G.729A	n	2	20
3: G.729B	n	2	20
4:			

Step 4 - On **Page 2** of the form, set **FAX Mode** to **t.38-standard**, and **ECM** to **y**.

Step 5 - Leave the remaining values default, and click on **Enter** (not shown).

change ip-codec-set 1 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? ☐

	Mode	Redundancy	Packet Size[ms]
FAX	t.38-standard	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
STP 64K Data	n	0	20

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

This IP codec set will be used for IPFR-EF calls. Repeat the steps in **Section 6.6.1** with the following changes:

Step 6 - Select Codec Set **2**, and click on the **Edit** button.

Step 7 - On **Page 1** of the **ip-codec-set** form, set the codec list as shown below. Set the packet interval size to 30ms (**Frames Per Pkt = 3**). **Page 2** is the same as in **Section 6.6.1**.

change ip-codec-set 2		Page 1 of 2	
IP CODEC SET			
Codec Set: 2			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.729B	<input type="text" value="n"/>	<input type="text" value="3"/>	30
2: G.729A	<input type="text" value="n"/>	<input type="text" value="3"/>	30
3: G.711MU	<input type="text" value="n"/>	<input type="text" value="3"/>	30
4: <input type="text"/>	<input type="text"/>	<input type="text"/>	

Note that the order of G.729B and G.729A may be reversed as required.

6.7. 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.

6.7.1. 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. Trunk 2 is defined. This trunk corresponds to the **ACM_Public** SIP Entity defined in **Section 5.4.2**.

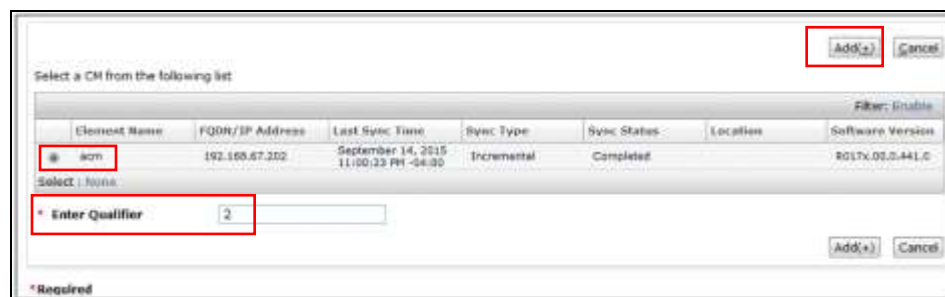
6.7.1.1 Signaling Group 2

Step 1 - From the Communication Manager menu, select **Network → Signaling Groups**.

Step 2 - Select **New**.



Step 3 - Select the appropriate Communication Manager system, enter **2** in the **Enter Qualifier** field, and select **Add(+)**.



Step 4 - Provision the following parameters:

- **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 system 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., **SM**).
- **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 6.5.2**.
- **Far-end Domain** – Enter **customer.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 (via the SBCE), a loss of audio can occur when this option is enabled.

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

acm

change signaling-group 2

Enter Refresh Cancel Clear Field Help Edit Prev Page Next Page More Actions

Info:

change signaling-group 2 Page 1 of 2

SIGNALING GROUP

Group Number: 2 Group Type: sip

MS Enabled? n Transport Method: tcp

Q-SIP? n

IP Video? n

Peer Detection Enabled? y Peer Server: SM

Enforce SIPs URI for SRTP? y

Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y

Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

Alert Incoming SIP Crisis Calls? n

Near-end Node Name: procr Far-end Node Name: SM

Near-end Listen Port: 5062 Far-end Listen Port: 5062

Far-end Network Region: 2

Far-end Domain: customera.com

Bypass If IP Threshold Exceeded? n

Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n

DTMF over IP: rtp-payload Direct IP-IP Audio Connections? y

Session Establishment Timer(min): 3 IP Audio Hairpinning? n

Enable Layer 3 Test? y Initial IP-IP Direct Media? y

H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 10

Step 5 - Click on **Enter**.

6.7.1.2 Trunk Group 2

Step 6 - From the Communication Manager menu, select **Network → Trunk Groups**.

Step 7 - Select **New**.

Group Number	Trunk Group Name	Group Type	Trunk Number	TAC	Number of Members	CDR	CDR	Outgoing Display	Group Length	System
Select: 23 Items										

Step 8 - Select the appropriate Communication Manager system, enter **2** in the **Enter Qualifier** field, and select **Add(+)**.

Client Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
acm	192.168.67.202	September 14, 2015 11:00:23 PM -04:00	Incremental	Completed		R017x.03.0.441.0

Select: None

* Enter Qualifier: 2

Add(+) Cancel

Step 9 - 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**).

acm

change trunk-group 2

Enter Refresh Cancel Clear Field Help Edit Prev Page Next Page More Actions ▾

Info:

change trunk-group 2 Page 1 of 21

TRUNK GROUP

Group Number: 2 Group Type: sip CDR Reports: y

Group Name: ATT COR: 1 TN: 1 TAC: 602

Direction: two-way Outgoing Display? n

Dial Access? n Night Service:

Queue Length: 0

Service Type: public-ntwrk Auth Code? n

Member Assignment Method: auto

Signaling Group: 2

Number of Members: 10

Step 10 - 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.

change trunk-group 2 Page 2 of 21

Group Type: sip

TRUNK PARAMETERS

Unicode Name: auto

Redirect On OPTIM Failure: 5000

SCCAN? n Digital Loss Group: 18

Preferred Minimum Session Refresh Interval(sec): 900

Disconnect Supervision - In? y Out? y

XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n

Step 11 - On Page 3 of the Trunk Group form:

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

Note – Typically a trunk defined as **public-ntwrk** (see **Step 9** 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 6.8**).

change trunk-group 2 Page 3 of 21

TRUNK FEATURES

ACA Assignment? Measured: Maintenance Tests?

Numbering Format: UUI Treatment:

Replace Restricted Numbers? Replace Unavailable Numbers?

Hold/Unhold Notifications? Modify Tandem Calling Number:

Show ANSWERED BY on Display?

Step 12 - 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**.

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.

change trunk-group 2 Page 4 of 21

PROTOCOL VARIATIONS

Mark Users as Phone?	<input type="text" value="n"/>
Prepend '+' to Calling/Alerting/Diverting/Connected Number?	<input type="text" value="n"/>
Send Transferring Party Information?	<input type="text" value="n"/>
Network Call Redirection?	<input type="text" value="y"/>
Build Refer-To URI of REFER From Contact For NCR?	<input type="text" value="n"/>
Send Diversion Header?	<input type="text" value="y"/>
Support Request History?	<input type="text" value="y"/>
Telephone Event Payload Type:	<input type="text" value="100"/>
Convert 180 to 183 for Early Media?	<input type="text" value="n"/>
Always Use re-INVITE for Display Updates?	<input type="text" value="n"/>
Identity for Calling Party Display:	<input type="text" value="From"/>
Block Sending Calling Party Location in INVITE?	<input type="text" value="n"/>
Accept Redirect to Blank User Destination?	<input type="text" value="n"/>
Enable Q-SIP?	<input type="text" value="n"/>
Interworking of ISDN Clearing with In-Band Tones:	<input type="text" value="keep-channel-active"/>
Request URI Contents:	<input type="text" value="may-have-extra-digits"/>

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

Trunk 1 corresponds to the ACM_Local SIP Entity defined in Section 5.4.3.

6.7.2.1 Signaling Group 1

Repeat the steps in Section 6.7.1.1 with the following changes:

Step 1 - Select the appropriate Communication Manager system, enter **1** in the **Enter Qualifier** field, and select **Add(+)**.

Step 2 - Set the following parameters on page 1:

- **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 6.5.1.

6.7.2.2 Trunk Group 1

Repeat the steps in Section 6.7.1.2 with the following changes:

Step 1 - Select the appropriate Communication Manager system, enter **1** in the **Enter Qualifier** field, and select **Add(+)**.

Step 2 - Set the following parameters on page 1:

- **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 Section 6.7.2.1 (e.g., **1**).

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

- Same as Section 6.7.1.2

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

- Same as **Section 6.7.1.2**

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.

6.7.3. SIP Trunk for Meet-Me Conference Calls

Trunk 5 corresponds to the **ACM_Meet-Me** SIP Entity defined in **Section 5.4.4**.

6.7.3.1 Signaling Group 5

Repeat the steps in **Section 6.7.1.1** with the following changes:

Step 1 - Select the appropriate Communication Manager system, enter **5** in the **Enter Qualifier** field, and select **Add(+)**.

Step 2 - Set the following parameters on page 1:

- **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 6.5.2**.

6.7.3.2 Trunk Group 5

Repeat the steps in **Section 6.7.1.2** with the following changes:

Step 3 - Select the appropriate Communication Manager system, enter **5** in the **Enter Qualifier** field, and select **Add(+)**.

Step 4 - Set the following parameters on page 1:

- **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 **Section 6.7.3.1** (e.g., **5**).

Step 5 - On **Page 2** of the **Trunk Group** form:


- Same as **Section 6.7.1.2**.

Step 6 - On **Page 3** of the **Trunk Group** form:

- Same as **Section 6.7.1.2**.

Step 7 - On **Page 4** of the **Trunk Group** form:

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



Group Number	Trunk Group Name	Group Type	Tenant Number	TAC	Number of Members	CDR	CDR	Outgoing Display	Queue Length	System
1	Local	sp	1	801	10	1	true	false	0	com
2	ATT	sp	1	602	10	1	true	false	0	com
5	Meet-Me_Conf	sp	1	605	10	1	true	false	0	com

6.8. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 6.7.1.2**), 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 - From the Communication Manager menu, select **Element Cut-Through**.

Step 2 - Select the appropriate Communication Manager system.



Step 3 - The Element Cut-Through command line interface will open. Enter the command **change private-numbering 0**, and click on the **Send** button.



Step 4 - Add an entry for 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 5 - Repeat **Step 4** and enter the Avaya Messaging access extension (e.g., **36000**).

Step 6 - 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., **7325553170**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 7 - Click on **Enter**.

Note that the **attd** entry appears by default.

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len
0	attd		0	1
5	19	1		5
5	36000	1		5
5	19001	2	7325553170	10
5	19002	2	7325554071	10
5	19003	2	7325554072	10
5	19004	2	7325553174	10
5	19005	2	7325553171	10

6.9. Public Unknown Numbering

Even though the SIP trunks defined in **Section 6.7** used Private numbering, extension entries must be defined in the public-unknown-numbering table as well.

Step 1 - From the Communication Manager menu, select **Element Cut-Through**.

Step 2 - Select the appropriate Communication Manager system.

Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version	CM Notification
192.168.67.262	192.168.67.262	September 14, 2015 11:55:23 PM -04:05	10:05 am MON SEP 14, 2015	Incremental	Completed		8017x.00.0.441.8	true

Step 3 - The Element Cut-Through command line interface will open. Enter the command ***change public-unknown-numbering 0***, and click on the **Send** button.

Command:

Step 4 - Add an entry for 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 and public trunk groups (e.g., **1-2**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 5 - Repeat **Step 4** and enter the Avaya Messaging access extension (e.g., **36000**).

change public-unknown-numbering 0				
NUMBERING - PUBLIC/UNKNOWN FORMAT				
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len
5	19	1-2		5
5	36000	1-2		5

Step 6 - Click on **Enter**.

6.10. Route Patterns

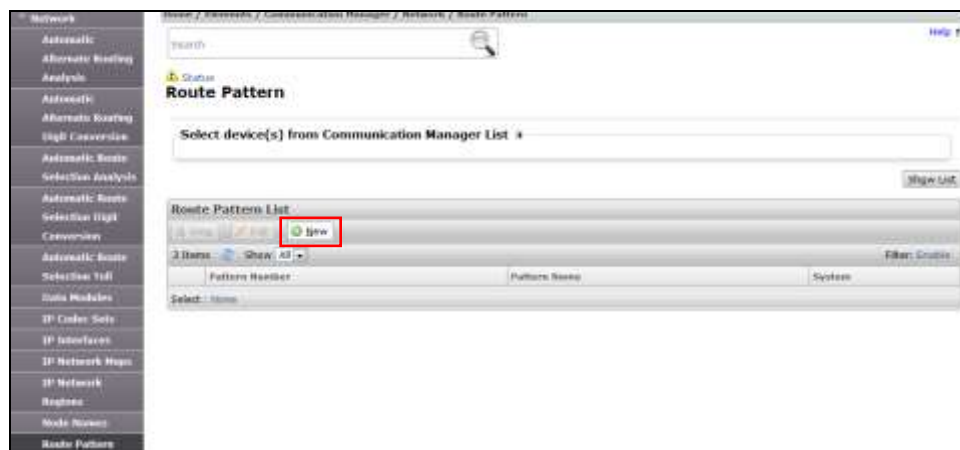
Route Patterns are used to direct outbound calls via the public or local CPE SIP trunks.

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 - From the Communication Manager menu, select **Network → Route Pattern**.

Step 2 - Select **New**.



Step 3 - Select the appropriate Communication Manager system, enter **2** in the **Enter Qualifier** field, and select **Add(+)**.

Select a CM from the following list

Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
acm	192.168.67.202	September 14, 2015 11:00:23 PM -04:00	Incremental	Completed		R017x.00.0.441.0

Select : None

Enter Qualifier: 2

Add(+) Cancel

Step 4 - Enter the following parameters:

- In the **Grp No** column enter **2** for public trunk 2, and the **FRL** column enter **0** (zero).
- In the **Numbering Format** column, across from line **1**: enter **unk-unk**.

change route-pattern 2 Page 1 of 3

Pattern Number: 2 Pattern Name:

SCCAN? ☐ Secure SIP? ☐ Used for SIP stations? ☐

Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DC5/ IXC
No								QSIG
								Intw
1:	2	0		1				n user
2:								n user
3:								n user
4:								n user
5:								n user
6:								n user

BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbering LAR

0 1 2 M 4 W Request Dgts Format

1: y y y y y n n rest unk-unk none

Step 5 - Click on **Enter**.

6.10.2. Route Pattern for Calls within the CPE

This form defines the Route pattern for 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 6 - Repeat the steps in **Section 6.10.1** with the following changes:

- 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**.

6.11. Automatic Route Selection (ARS) Dialing

The ARS table is selected based on the caller dialing the ARS access code (e.g., **9**) as defined in **Section 6.3**. The access code is removed and the ARS table matches the remaining outbound dialed digits and sends them to the designated route-pattern (see **Section 6.10**).

Step 1 - From the Communication Manager menu, select **Network** → **Automatic Route Selection Analysis**.

Step 2 - Select **New**.



Dialed String	Total Min	Total Max	Route Pattern	Location	System
720	10	10	2	atl	AC70
1421	4	4	2	atl	AC70
311	3	3	2	atl	AC70
333	10	10	2	atl	AC70
5	10	10	2	atl	AC70
4	10	10	2	atl	AC70
7	?	?	2	atl	AC70

Step 3 - Select the appropriate Communication Manager system, enter new dial string (e.g., **1732**) in the **Enter Qualifier** field, and select **Add(+)**.



Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
acn	192.168.67.202	September 20, 2015 11:00:05 PM -06:00	Incremental	Completed		R017x.00.0.441.0

Select : None

* Enter Qualifier: 1732

Enter Location:

* Required

Step 4 - For outbound dialing to AT&T enter the following:

- In the **Dialed String** column enter a matching dial pattern (e.g., **1732**). Note that the best match will route first, that is 1732555xxxx will be selected before 17xxxxxxxxxx.
- In the **Min** and **Max** columns enter the corresponding digit lengths, (e.g., **11** and **11**).
- In the **Route Pattern** column select a route-pattern to be used for these calls (e.g., **2**).
- In the **Call Type** column enter **hnpa** (selections other than **hnpa** may be appropriate, based on the digits defined here).

Step 5 - Repeat **Step 4** for all other outbound call strings. In addition, IPFR-EF Call Forward feature access codes *7 and *9 are defined here as well.

change ars analysis 1732

Enter Refresh Cancel Clear Field Help Edit Prev Page Next Page More Actions ▾

Info: Enter number between 1-999, or blank

change ars analysis 1732 Page 2 of 2

ARS DIGIT ANALYSIS TABLE

Location: all Percent Full: 1

Dialed String	Total		Route	Call	Node	ANI
	Min	Max	Pattern	Type	Num	Reqd
1732	11	11	2	hnpa		n
1800	11	11	2	hnpa		n
*7	13	13	2	hnpa		n
*9	13	13	2	hnpa		n

Step 6 - Click on **Enter**.

6.12. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

Step 1 - From the Communication Manager menu, select **Network** → **Automatic Alternate Routing Analysis**.

Step 2 - Select **New**.

Groups Network Automatic Alternate Routing Analysis Automatic

Automatic Alternate Routing Analysis List

Filter: Enable

Dialed String	Total Min	Total Max	Route Pattern	Location	Add Required	System

Step 3 - Select the appropriate Communication Manager system, enter new dial string (e.g., **19**) in the Enter **Qualifier** field, and select **Add(+)**.

Select a CM from the following list

1 Item

Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
*cm	192.168.87.202	September 20, 2015 11:00:05 PM +08:00	Incremental	Completed		R017x.00.0.441.0

Select: None

* Enter Qualifier 19

Enter Location

Add(+) Cancel

* Required

Step 4 - Enter the following to define Communication Manager extensions:

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

Step 5 - Repeat **Step 4**, and create an entry for Avaya Messaging access extension **36000**.

The screenshot shows a web interface titled "change aar analysis 19". At the top, there are buttons: Enter, Refresh, Cancel, Clear Field, Help, Edit, Prev Page, Next Page, and More Actions. Below these is an "Info:" section. The main content area is titled "change aar analysis 19" and "AAR DIGIT ANALYSIS TABLE". It shows "Location: all" and "Percent Full: 1". Below this is a table with columns: Dialed String, Total (Min, Max), Route Pattern, Call Type, Node Num, and ANI Req'd. The table contains two rows of data:

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
19	5	5	1	unku		n
36000	5	5	1	unku		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)#**).

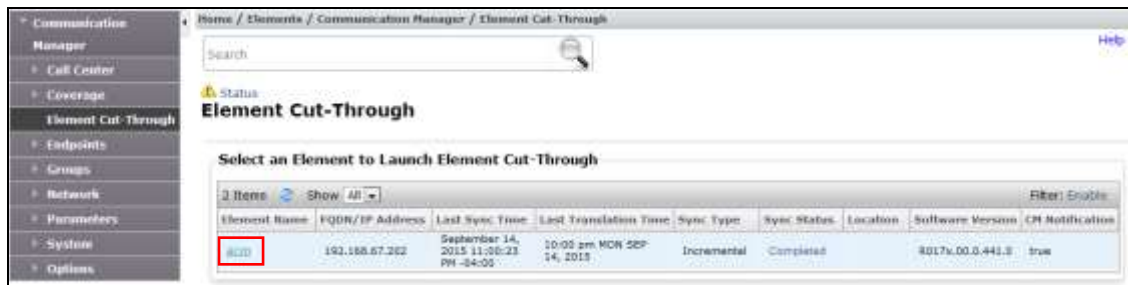
Step 2 - Enter the **show system** command and copy down the G430 serial number (e.g., **11N509736520**).

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 start** command to save the G430 configuration.

Step 5 - From the Communication Manager menu, select **Element Cut-Through**.

Step 6 - Select the appropriate Communication Manager system.



Step 7 - The Element Cut-Through command line interface will open. Enter the command ***add media-gateway x*** where x is an available Media Gateway identifier (e.g., **1**), and click on the **Send** button.



Step 8 - The Media Gateway form will open (not shown). Enter the following parameters:

- Set **Type** = **g430**
- Set **Name** = a descriptive name (e.g., **G430-1**)
- Set **Serial Number** = the serial number copied from **Step 2** (e.g., **11N509736520**).
- Set the **Link Encryption Type** parameter as desired (**any-ptls/tls** 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 8** (e.g., **G430-001(super)#**).

Step 9 - Enter the **display media-gateway 1** command from the Element Cut-Through command line interface, and verify that the G430 has registered.

Command:

Info:

display media-gateway 1

Page 1 of 2

MEDIA GATEWAY 1

Type: g430

Name: G430-1

Serial No: 11N509736520

Link Encryption Type: any-ptls/tls Enable CF? n

Network Region: 1 Location: 1

Recovery Rule: 1 Site Data:

Registered? y

FW Version/HW Vintage: 37.19.0 / 1

MGP IPv4 Address: 192.168.67.50

MGP IPv6 Address:

Controller IP Address: 192.168.67.202

MAC Address: b4:b0:17:8f:3a:49

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.

The screenshot shows a web interface for configuring a 'CALL VECTOR'. At the top, there's a title 'change vector 6' and a row of buttons: Enter, Refresh, Cancel, Clear Field, Help, Edit, Prev Page, Next Page, and More Actions. Below this is an 'Info' section with the text 'Select suggested values from dropdown'. The main content area is titled 'change vector 6' and 'CALL VECTOR', with a page indicator 'Page 1 of 6'. The configuration includes fields for 'Number: 6' and 'Name: MeetMeConf'. A series of checkboxes are present for various features: 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), and Variables? (y). Below these are step-by-step actions: 01 wait-time 5 secs hearing ringback; 02 collect 6 digits after announcement 11001; 03 goto step 5 if digits = meet-me-access; 04 goto step 2 if unconditionally; 05 route-to meetme; and 06 stop.

6.14.2. Meet-Me VDN

Note that this VDN extension is specified in the Dial Pattern in **Section 6.3**.

The screenshot shows the 'Edit Vector Directory Number (VDN)' configuration page. At the top right are buttons for Commit, Schedule, Reset, and Cancel. The form is divided into two tabs: 'Basic Information (B)' and 'Variables Information (V)'. Under 'Basic Information', there are fields for 'System' (ACM), 'Extension' (19000), and 'Name' (MeetMeConf). The 'Variables Information' tab is active, showing fields for 'Destination' (Vector Number 6), 'Meet-me Conferencing?' (checked), 'COR' (1), 'Tenant Number' (1), 'Conference Access Code' (123456), 'Conference Controller' (14006), 'Conference Type' (6-party), 'Route-to Number', and 'Unanswered Conference Timeout'.

6.15. IP Interface for procr

Verify the Processor Ethernet (procr) parameters defined during installation.

Step 1 - From the Communication Manager menu, select **Network → IP Interfaces**.

Step 2 - Select the **PROCR Type** and select **View**.



Step 3 - Verify the following parameters:

- **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.



6.16. Save Translations

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

Step 1 - From the Communication Manager menu, select **Element Cut-Through**.

Step 2 - Select the appropriate Communication Manager system.



Step 3 - The Element Cut-Through command line interface will open. Enter the command *save translation all*, and click on the **Send** button.



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.

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.

As described in **Section 3**, the reference configuration places the private interface A1 (IP address 192.168.67.120) 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. A disclaimer paragraph follows, stating that the system is restricted to authorized users and that unauthorized access is prohibited. Another paragraph mentions that system use may be monitored for administrative and security reasons. A final paragraph states that all users must comply with corporate instructions regarding information assets. At the bottom, a copyright notice reads "© 2011 - 2013 Avaya Inc. All rights reserved."

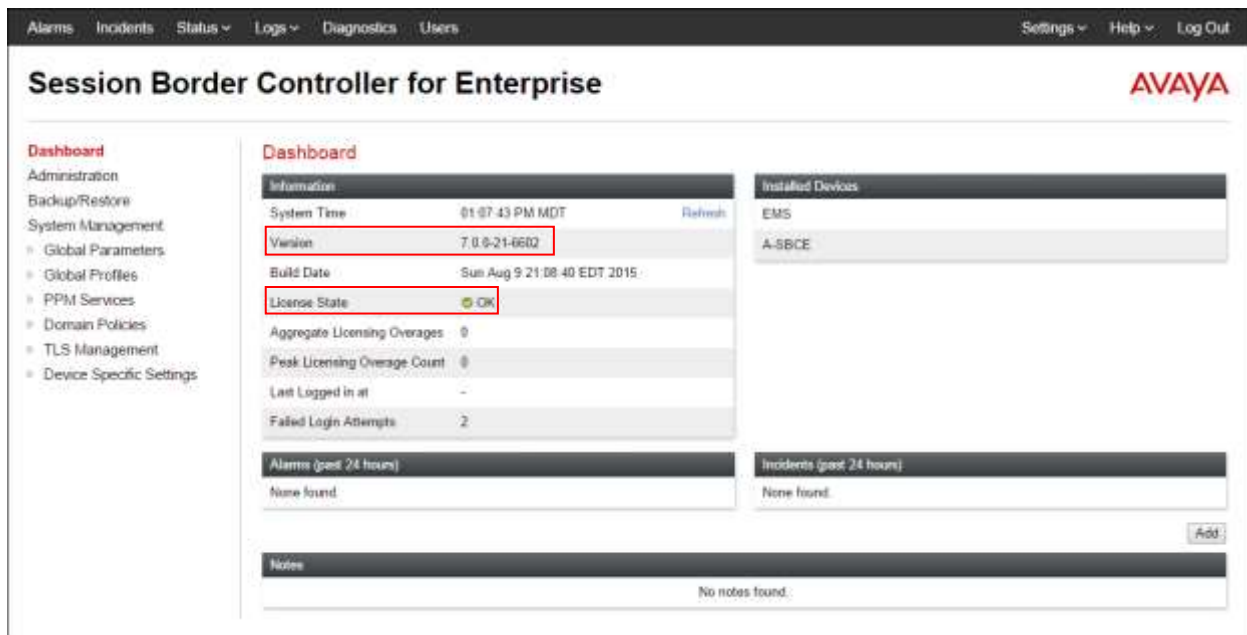
Step 3 - Enter the password and click on **Log In**.



The login page features the Avaya logo in red at the top left. To its right is the 'Log In' header. Below the header are two input fields: 'Username:' with a masked password '*****' and 'Password:' with an empty field. A 'Log In' button is positioned below the password field. On the left side, below the logo, is the text 'Session Border Controller for Enterprise'. On the right side, 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 modification 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 a paragraph about monitoring: '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 right, it states: '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.

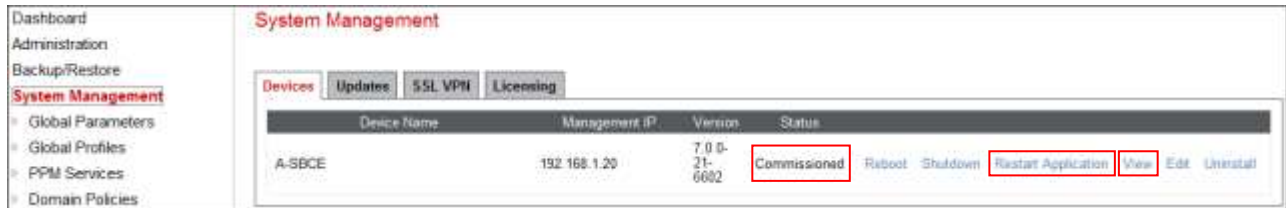


The dashboard has a top navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left sidebar lists menu items: Dashboard, Administration, Backup/Restore, System Management (Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings). The main content area is titled 'Dashboard' and contains several sections. The 'Information' section has a table with the following data: System Time (01:07:43 PM MDT), Version (7.0.0-21-6602), Build Date (Sun Aug 9 21:08:40 EDT 2015), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged In at (-), and Failed Login Attempts (2). The 'Installed Devices' section lists EMS and A-SBCE. The 'Alarms (past 24 hours)' and 'Incidents (past 24 hours)' sections both show 'None found'. There is an 'Add' button next to the incidents section. A 'Notes' section at the bottom shows 'No notes found'.

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.



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

System Information: A-SBCE

General Configuration		Device Configuration		License Allocation	
Appliance Name	A-SBCE	HA Mode	No	Standard Sessions <small>Requested: 500</small>	500
Box Type	SIP	Two Bypass Mode	No	Advanced Sessions <small>Requested: 500</small>	500
Deployment Mode	Proxy			Scopia Video Sessions <small>Requested: 500</small>	500
				CES Sessions <small>Requested: 0</small>	0
				Encryption	<input checked="" type="checkbox"/>

Network Configuration				
IP	Public IP	Netmask	Gateway	Interface
192.168.67.120	192.168.67.120	255.255.255.0	192.168.67.1	A1
10.10.10.10	10.10.10.10	255.255.255.0	10.10.10.1	B1

DNS Configuration		Management IP(s)	
Primary DNS	192.168.67.5	IP	192.168.63.64
Secondary DNS			
DNS Location	DMZ		
DNS Client IP	192.168.70.120		

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.

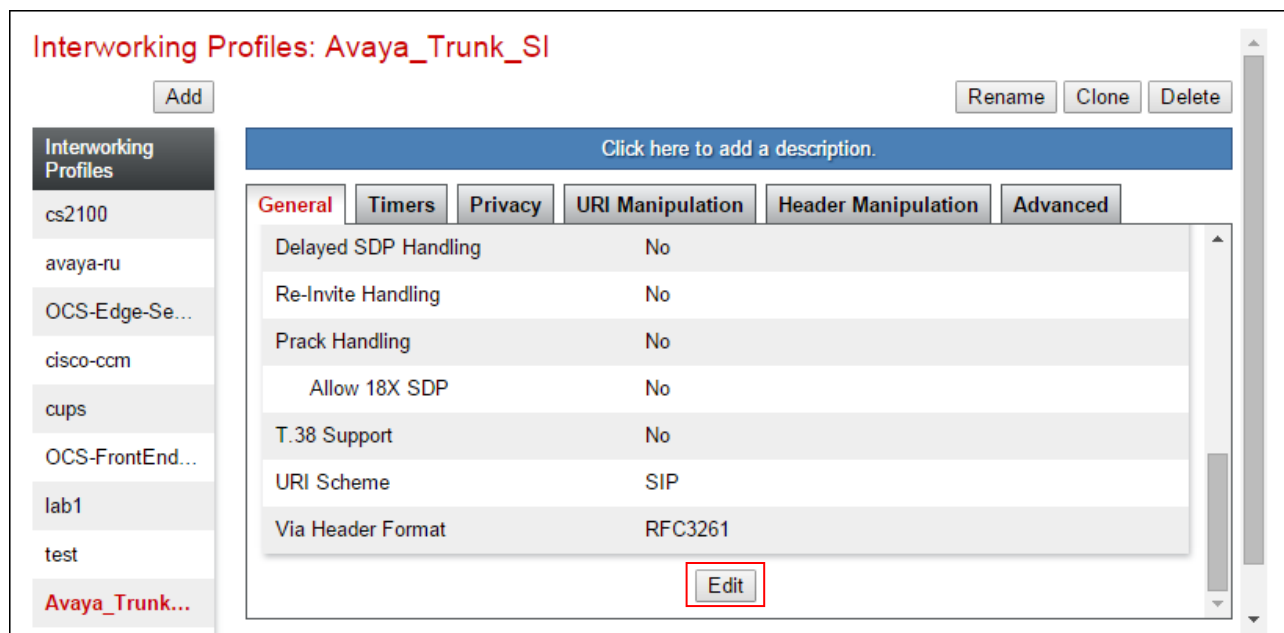
Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.



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 **Finish**.

The screenshot shows a dialog box titled "Editing Profile: Avaya_Trunk_SI" with a close button (X) in the top right corner. The "General" tab is selected. The settings are as follows:

Setting	Value
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"/>
Delayed Offer	<input 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"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<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

At the bottom of the dialog is a "Finish" button.

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

Editing Profile: Avaya_Trunk_SI

Record Routes

- ☐ None
- ☐ Single Side
- ☒ Both Sides
- ☐ Dialog-Initiate Only (Single Side)
- ☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions Avaya ▼

Diversion Manipulation ☐

Diversion Condition None ▼

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

DTMF

DTMF Support

- ☒ None
- ☐ SIP NOTIFY
- ☐ SIP INFO

Finish

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 **SIP Timers** and **Privacy** screens will open (not shown), accept default values for these screens by clicking **Next**.

Step 4 - The **Advanced/DTMF** screen will open:

- In the **Record Routes** field, check **Both Sides**.
- All other options can be left as default.
- Click **Finish**.

Editing Profile: ATT_Trunk_SI

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☐

Extensions

Diversion Manipulation ☐

Diversion Condition

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

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** 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". It has a text input field labeled "Profile Name" containing the text "SM_Trunk_SC". Below the input 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 a window titled "Edit Server Configuration Profile - General". It has a "Server Type" dropdown menu set to "Call Server". Below this is an "Add" button. Underneath is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "192.168.67.47", "5060", and "TCP". There is a "Delete" button next to the "Transport" dropdown. At the bottom are "Back" and "Next" buttons.

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**.
- Check **Enable Grooming**.
- 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.

Edit Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya_Trunk_SI

Signaling Manipulation Script None

Connection Type SUBID

Securable ☐

Finish

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** and enter a Profile Name (e.g., **ATT_SC**) and select **Next** (not shown).

Step 2 - On the **General** window, 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** until the Advanced tab is reached.

Global Parameters

- Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration**
 - Topology Hiding

Server Configuration: ATT_SC

Add

Server Profiles

SM_Trunk_SC

ATT_SC

Rename Clone Delete

General Authentication Heartbeat Advanced

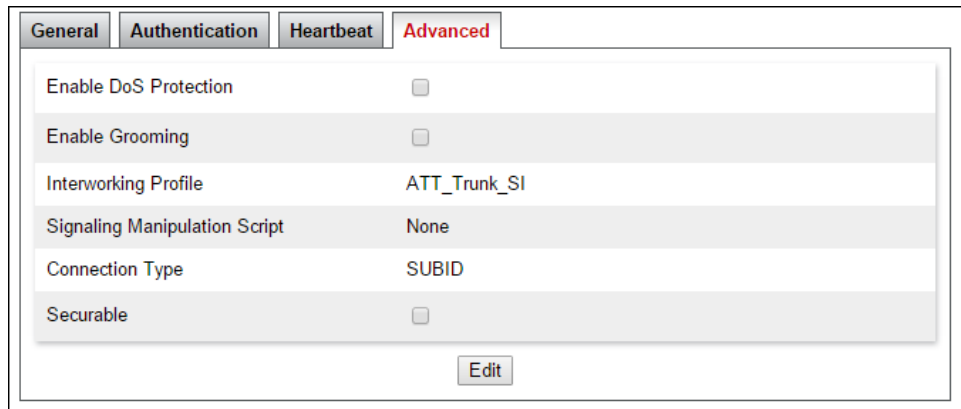
Server Type Trunk Server

IP Address / FQDN	Port	Transport
10.10.10.11	5060	UDP

Edit

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

- Select **ATT_Trunk_SI** (created in **Section 7.2.2**), for **Interworking Profile**.
- Select **Finish** (not shown).



The screenshot shows a configuration window with tabs: General, Authentication, Heartbeat, and Advanced (selected). The Advanced tab contains the following settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT_Trunk_SI
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	<input type="checkbox"/>

An **Edit** button is located at the bottom right of the configuration area.

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**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. It contains a text field labeled "Profile Name" with the value "SM_RP" entered. A **Next** button is located at the bottom right.

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



The screenshot shows a "Routing Profile" configuration window with the following settings:

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"/>

An **Add** button is at the bottom right. Below the settings is a blue banner that reads: "Click the Add button to add a Next-Hop Address." At the very bottom are **Back** and **Finish** buttons.

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**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	SM_Trunk_SC	192.168.67.47:5060 (TCP)	None

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, enter a Profile Name: (e.g., **ATT_RP**).

Step 2 - On the **Next-Hop Address** window, 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 (UDP)**.

Step 3 - Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT_SC	10.10.10.11:5060 (UDP)	None

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.10.10.11	UDP

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**.



The screenshot shows a window titled "Topology Hiding Profile". Inside, there is a "Profile Name" label followed by a text input field containing "Avaya_TH". Below the input field is a "Next" button.

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.



The screenshot shows the "Topology Hiding Profile" window. At the top right is an "Add Header" button. Below it is a table with four columns: "Header", "Criteria", "Replace Action", and "Override Value". The first row contains "Request-Line", "IP/Domain", "Auto", and an empty text field. To the right of the text field is a "Delete" button. At the bottom are "Back" and "Finish" buttons.

Header	Criteria	Replace Action	Override Value	
Request-Line	IP/Domain	Auto		Delete



The screenshot shows the "Topology Hiding Profile" window with the "Add Header" button removed. The table now contains eight rows of headers. Each row has a "Delete" button to its right. At the bottom are "Back" and "Finish" buttons.

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

Step 4 - Populate the fields as shown below, and click **Finish**. Note that **customerera.com** is the domain used by the CPE (see **Sections 5.1, 6.5, and 6.7**).

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

Back Finish

7.2.8. Topology Hiding – AT&T Side

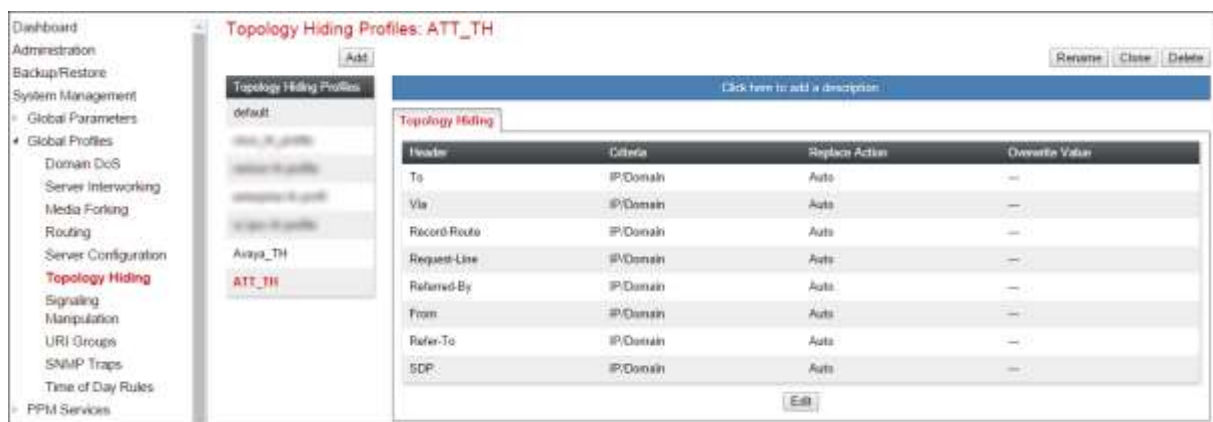
Repeat the steps in **Section 7.2.7**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

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

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

Back Finish

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



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.

SIP-Trunk_AR

Filter By Device ▼ Rename Clone Delete

[Click here to add a description](#)

Application Rule

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"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

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 screenshot shows the 'Media QoS' configuration window. It has a title bar 'Media QoS' with a close button. The window is divided into sections: 'Media QoS Reporting' with 'RTCP Enabled' checked; 'Media QoS Marking' with 'Enabled' checked and 'ToS' selected. Under 'ToS', there are four rows: 'Audio Precedence' (Routine, 000), 'Audio ToS' (Minimize Delay, 1000), 'Video Precedence' (Routine, 000), and 'Video ToS' (Minimize Delay, 1000). Below these is the 'DSCP' section with 'Audio' (EF, 101110) and 'Video' (EF, 101110). A 'Finish' button is at the bottom.

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

The screenshot shows the 'Media Rules: Trunk-low-med_MR' configuration window. It has a title bar 'Media Rules: Trunk-low-med_MR' with 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' buttons. The left sidebar lists 'Media Rules' with options: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'lab1', 'RW med rule', and 'Trunk-low-med_MR' (highlighted). The main area has tabs: 'Media Encryption', 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FECC'. The 'Media Encryption' tab is active, showing 'Audio Encryption' (Preferred Formats: RTP, Interworking: checked) and 'Video Encryption' (Preferred Formats: RTP, Interworking: checked). There is also a 'Miscellaneous' section with 'Capability Negotiation' (unchecked). An 'Edit' button is at the bottom.

7.3.3. Signaling Rules

In the reference configuration, Signaling Rules are used to define QoS parameters.

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).

Step 4 - 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 5 - Click **Finish**.



7.3.3.2 AT&T – Signaling Rule

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

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

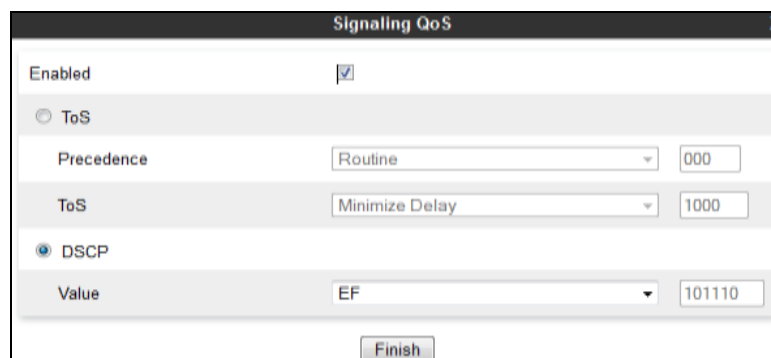
Step 3 - From the Signaling Rules menu, select the **default** rule.

Step 4 - Select **Clone Rule** button

- Enter a name: **ATT_SR**

Step 5 - Click **Finish**

Step 6 - Highlight the **ATT_SR** rule, select the **Signaling QoS** tab and repeat **Steps 4 & 5** from **Section 7.3.3.1**.



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 7.3.3.1).

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



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 7.3.3.2).

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: A-SBCE

Devices	Interfaces	Networks
A-SBCE		

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	192.168.67.1	255.255.255.0	A1	192.168.67.120, 192.168.67.121	Edit Delete
Network_B1	10.10.10.1	255.255.255.0	B1	10.10.10.10	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 **Signaling Port Range** row, change the range to **7000 – 16000**

Step 4 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 5 – In the **Listen Port Range** row, change the range to **6000 – 6999**.

Step 6 – In the **HTTP Port Range** row, change the range to **51001 – 62000**.

Step 7 - Scroll to the bottom of the window and select **Save**. Note that changes to these values require an application restart (see **Section 7.1**).

Advanced Options: A-SBCE

Device: A-SBCE

CDR Listing Feature Control SIP Options Network Options Port Ranges RTPC 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	7000 - 16000
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	6000 - 6999
HTTP Port Range	51001 - 62000

Save

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:** Select **Network_A1 (A1,VLAN0)** and **192.168.67.120**.
- **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:** Select **Network_B1 (B1,VLAN0)** and **10.10.10.10**.
- **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.

Name	Media IP Network	Port Range	
Inside_Trunk_MI	192.168.67.120 Network_A1 (A1, VLAN0)	16384 - 32767	Edit Delete
Outside_Trunk_MI	10.10.10.10 Network_B1 (B1, VLAN0)	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:** Select **Network_A1 (A1,VLAN0)** and **192.168.67.120**.
- **TCP Port:** **5060**.

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

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

- **Name:** **Outside_Trunk_SI**.
- **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.10.10**.
- **UDP Port:** **5060**.

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



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

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

Subscriber Flows		Server Flows	
Priority	Flow Name	URI Group	Received Interface
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
1	SM_Trunk
	URI Group
	*
	Received Interface
	Outside_Trunk_SI
	Signaling Interface
	Inside_Trunk_SI
	End Point Policy Group
	Avaya default-low_PG
	Routing Profile
	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 Element Cut-Through command line interface or 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

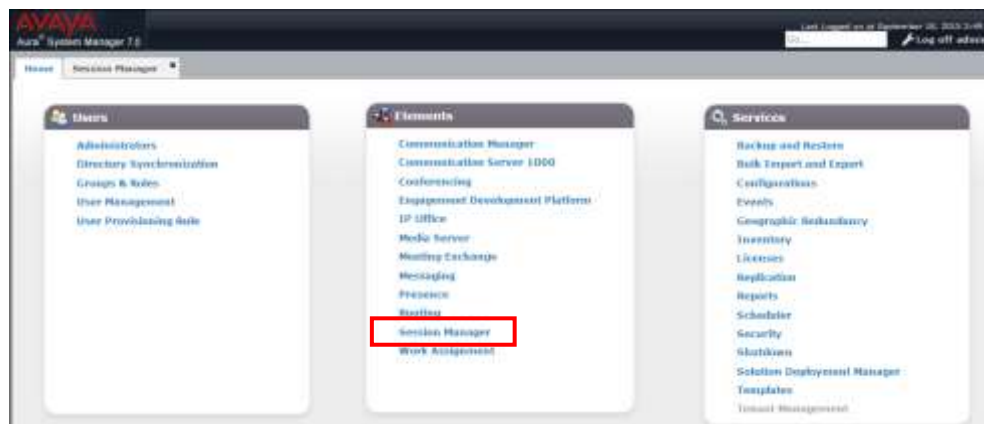
```
time      data
15:55:06 TRACE STARTED 04/19/2013 CM Release String cold-02.0.823.0-20396
15:55:16 SIP<INVITE sip:19001@customera.com SIP/2.0
15:55:16      Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16      7ok0
15:55:16      active trunk-group 2 member 1      cid 0x2e9
15:55:16 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 [192.168.67.120]: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	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	Licenses Mode	Version
SessionManager	Core	✓	0/0/0	Up	Accept New Service	0/4	0	7/6	✓	✓	Normal	7.0.0.0.700007

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

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

Note the **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.

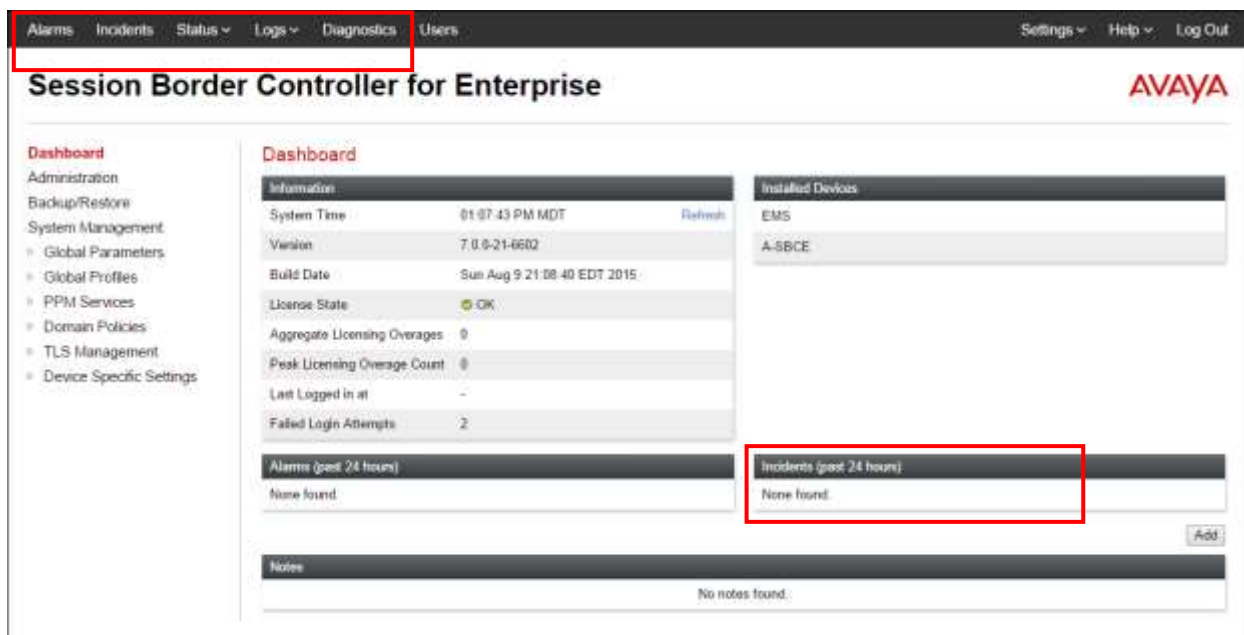
Another useful tool is to select **System Tools** → **Call Routing Test** (not shown) from the left hand menu. This tool allows specific call criteria to be entered, and the simulated routing of this call through Session Manager is then verified.

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 7.0, Avaya Aura® Session Manager 7.0, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0, 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 on VMware®, Release 7.0, Issue 1, August 2015
2. Administering Avaya Aura® Session Manager, Release 7.0, Issue 1, August 2015
3. Deploying Avaya Aura® System Manager, Release 7.0, September 2015
4. Administering Avaya Aura® System Manager for Release 7.0, Issue 1, August 2015

Avaya Aura® Communication Manager

5. Deploying Avaya Aura® Communication Manager in Virtualized Environment, Release 7.0
6. Administering Avaya Aura® Communication Manager, Release 7.0, 03-300509, Issue 1, August 2015
7. Administering Avaya G430 Branch Gateway, Release 7.0, 03-603228, Issue 1, August 2015

Avaya Session Border Controller for Enterprise

8. Administering Avaya Session Border Controller for Enterprise, Release 7.0, Issue 1, August 2015
9. Deploying Avaya Session Border Controller for Enterprise, Release 7.0, Issue 1, August 2015

Avaya Aura® Messaging

10. Administering Avaya Aura® Messaging, Release 6.3.3, Issue 1, August 2015

AT&T IP Flexible Reach - Enhanced Features Service:

11. 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' window. On the left, there is a 'Server Profiles' list with 'SM_Trunk_SC', 'ATT_SC', and 'ATT_Secondary_SC' (highlighted in red). The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing 'Server Type' as 'Trunk Server'. Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one row with the values '10.10.10.12', '5060', and 'UDP'. There are 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' 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@customera.com**
- **To URI: secondary@customera.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 'Heartbeat' tab of the 'Server Configuration: ATT_Secondary_SC' window. The 'Enable Heartbeat' checkbox is checked. Below it are fields for 'Method' (OPTIONS), 'Frequency' (60 seconds), 'From URI' (secondary@customera.com), and 'To URI' (secondary@customera.com). There is an 'Edit' button at the bottom.

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

- Click **Add** to create a second entry.
- **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.

View Flow: ATT_Secondary			
Criteria		Profile	
Flow Name	ATT_Secondary	Signaling Interface	Outside_Trunk_SI
Server Configuration	ATT_Secondary_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

©2016 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.