



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, and Avaya Session Border Controller for Enterprise 7.2, with AT&T IP Flexible Reach - Enhanced Features Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, and Avaya Session Border Controller for Enterprise 7.2, with the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **MIS/PNT** transport connections.

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	9
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	20
5.2.	Locations	20
5.2.1.	Main Location	20
5.2.2.	CM-TG-5 Location	21
5.2.3.	Common Location	21
5.3.	Configure Adaptations	22
5.3.1.	Adaptation for Avaya Aura® Communication Manager Extensions	22
5.3.2.	Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service	24
5.4.	SIP Entities	25
5.4.1.	Avaya Aura® Session Manager SIP Entity	25
5.4.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk	27
5.4.3.	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	28
5.4.4.	Avaya Session Border Controller for Enterprise SIP Entity.....	28
5.4.5.	Avaya Aura® Messaging SIP Entity	28
5.5.	Entity Links	28
5.5.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	28
5.5.2.	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	29
5.5.3.	Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE	29
5.5.4.	Entity Link to Avaya Aura® Messaging	29
5.6.	Time Ranges – (Optional)	30
5.7.	Routing Policies	30
5.7.1.	Routing Policy for AT&T Routing to Avaya Aura® Communication Manager	30
5.7.2.	Routing Policy for Inbound Routing to Avaya Aura® Messaging.....	32
5.7.3.	Routing Policy for Outbound Calls to AT&T	32
5.8.	Dial Patterns	32
5.8.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager	32

5.8.2.	Matching Outbound Calls to AT&T	34
5.9.	Verify TLS Certificates – Session Manager	35
6.	Configure Avaya Aura® Communication Manager	38
6.1.	Verify Communication Manager System Settings	38
6.1.1.	System-Parameters Customer-Options	38
6.2.	System-Parameters Features	39
6.3.	Dial Plan	40
6.4.	IP Node Names	40
6.5.	IP Interface for procr	41
6.6.	IP Network Regions	41
6.6.1.	IP Network Region 1 – Local CPE Region	41
6.6.2.	IP Network Region 4 – AT&T Trunk Region	43
6.7.	IP Codec Parameters	43
6.7.1.	Codecs for IP Network Region 1 (calls within the CPE)	43
6.7.2.	Codecs for IP Network Region 4 (calls to/from AT&T)	44
6.8.	SIP Trunks	45
6.8.1.	SIP Trunk for Inbound/Outbound AT&T calls	45
6.8.2.	Local SIP Trunk (Avaya SIP Telephone and Messaging Access)	48
6.9.	Public Numbering	49
6.10.	Private Numbering	50
6.11.	Route Patterns	50
6.11.1.	Route Pattern for National Calls to AT&T	50
6.11.2.	Route Pattern for International Calls to AT&T	51
6.11.3.	Route Pattern for Service Calls to AT&T	52
6.11.4.	Route Pattern for Calls within the CPE	52
6.12.	Automatic Route Selection (ARS) Dialing	53
6.13.	Automatic Alternate Routing (AAR) Dialing	54
6.14.	Avaya G450 Media Gateway Provisioning	54
6.15.	Avaya Aura® Media Server Provisioning	55
6.16.	Save Translations	56
6.17.	Verify TLS Certificates – Communication Manager	57
7.	Configure Avaya Session Border Controller for Enterprise	58
7.1.	System Management – Status	60
7.2.	TLS Management	61
7.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	61
7.2.2.	Server Profiles	62
7.2.3.	Client Profiles	64
7.3.	Global Profiles	65
7.3.1.	Server Interworking – Avaya	65
7.3.2.	Server Interworking – AT&T	68
7.3.3.	Signaling Manipulation	69
7.3.4.	Server Configuration – Session Manager	71
7.3.5.	Server Configuration – AT&T	73
7.3.6.	Routing – To Session Manager	75
7.3.7.	Routing – To AT&T	76

7.3.8.	Topology Hiding – Enterprise Side	77
7.3.9.	Topology Hiding – AT&T Side.....	78
7.4.	Domain Policies	80
7.4.1.	Application Rules.....	80
7.4.2.	Media Rules	81
7.4.3.	Signaling Rules	83
7.4.4.	Endpoint Policy Groups – Enterprise Connection	84
7.4.5.	Endpoint Policy Groups – AT&T Connection.....	85
7.5.	Device Specific Settings.....	85
7.5.1.	Network Management.....	85
7.5.2.	Advanced Options.....	86
7.5.3.	Media Interfaces.....	87
7.5.4.	Signaling Interface	87
7.5.5.	Server Flows – For Session Manager	88
7.5.6.	Server Flows – For AT&T.....	89
8.	Verification Steps.....	89
8.1.	AT&T IP Flexible Reach – Enhanced Features	89
8.2.	Avaya Aura® Communication Manager	90
8.3.	Avaya Aura® Session Manager	91
8.4.	Avaya Session Border Controller for Enterprise.....	93
8.4.1.	System Status	93
8.4.2.	Protocol Traces	93
9.	Conclusion	95
10.	References.....	96

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, Avaya Aura® System Manager 8.0, and Avaya Session Border Controller for Enterprise 7.2, with the AT&T IP Flexible Reach - Enhanced Features service using AVPN or MIS/PNT transport connections.

Avaya Aura® Communication Manager 8.0 (Communication Manager) is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 8.0 (Session Manager) is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® System Manager 8.0 (System Manager) is the provisioning and management application for Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 7.2 (Avaya SBCE) is the point of connection between Session Manager and the AT&T IP Flexible Reach - Enhanced Features (IPFR-EF) service and is used to not only secure the SIP trunk, but also to adjust the SIP signaling and media 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 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 (Messaging) is used to provide voicemail capabilities for the CPE.
- An IPFR-EF service test lab circuit, to which the simulated enterprise was connected via AVPN transport.

¹ AVPN supports compressed RTP (cRTP).

² MIS/PNT does not support cRTP.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the AT&T Flexible Reach service did not include use of any specific encryption features as requested by AT&T.

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, 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 voice mail 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) **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 6.8.1**, where Communication Manager will retrieve the display information using the *From* header.
- 2) **T.38/G.729 fax is limited to 9600bps when using the G4xx Media Gateways.** A G450 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.
- 3) **Avaya SBCE inserts a=ptime:20 in the SIP SDP toward Communication Manager.** If no media packetization attribute (ptime) is included in the SIP Session Description Protocol (SDP), Avaya SBCE inserts “a=ptime:20”, specifying 20 milliseconds. AT&T includes a=maxptime:30 in the SIP SDP to recommend a ptime value of 30ms but does not specifically require a ptime value of 30. Although Communication Manager is configured to send ptime with a value of 30ms (See **Section 6.7.2**), it will send a ptime value of 20ms when it receives “a=ptime:20” from the Avaya SBCE. This causes the media packetization to be set to 20ms. No issues were found during testing due to this behavior.
- 4) **Removal of unnecessary SIP headers.** 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, Av-Secure-Indication.

- 5) **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues.** Certain Avaya SIP endpoints (e.g., 9641, 9621, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore, an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 7.3.3**).
- 6) **SIP OPTIONS** – AT&T IPFR-EF service is configured to send SIP OPTIONS messages with a Max-Forwards header value of “0”. This is by design from AT&T and Avaya SBCE responded correctly with “483 Too Many Hops”. AT&T considers this response acceptable to keep the trunk in service. However, an incident is logged on the Avaya SBCE for each OPTIONS message received with Max-Forwards=0. To prevent the incident log from being filled with these route failure messages, an optional Sigma script can be added to the Avaya SBCE to change the Max-Forwards value to an acceptable value to reach Communication Manager (see **Section 7.3.3**).
- 7) **Emergency 911/E911 Services Limitations and Restrictions** – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IPFR-EF to complete 911/E911 calls; therefore, it is the customer’s responsibility to ensure proper operation with the equipment/software vendor. While AT&T IPFR-EF services support 911/E911 calling capabilities under certain Calling Plans, there are circumstances when the 911/E911 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 8.0, System Manager 8.0, Session Manager 8.0, and Avaya SBCE 7.2.
- 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 G450 Media Gateway and Avaya Aura® Media Server are 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 Equinox® for Windows (SIP), as well as 2424 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 TLS to communicate with Avaya SBCE and with Communication Manager.
- Avaya Aura® Messaging was used in the reference configuration to provide voice mailbox capabilities. This solution is extensible to other messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Testing was performed using an IPFR-EF service test lab circuit.

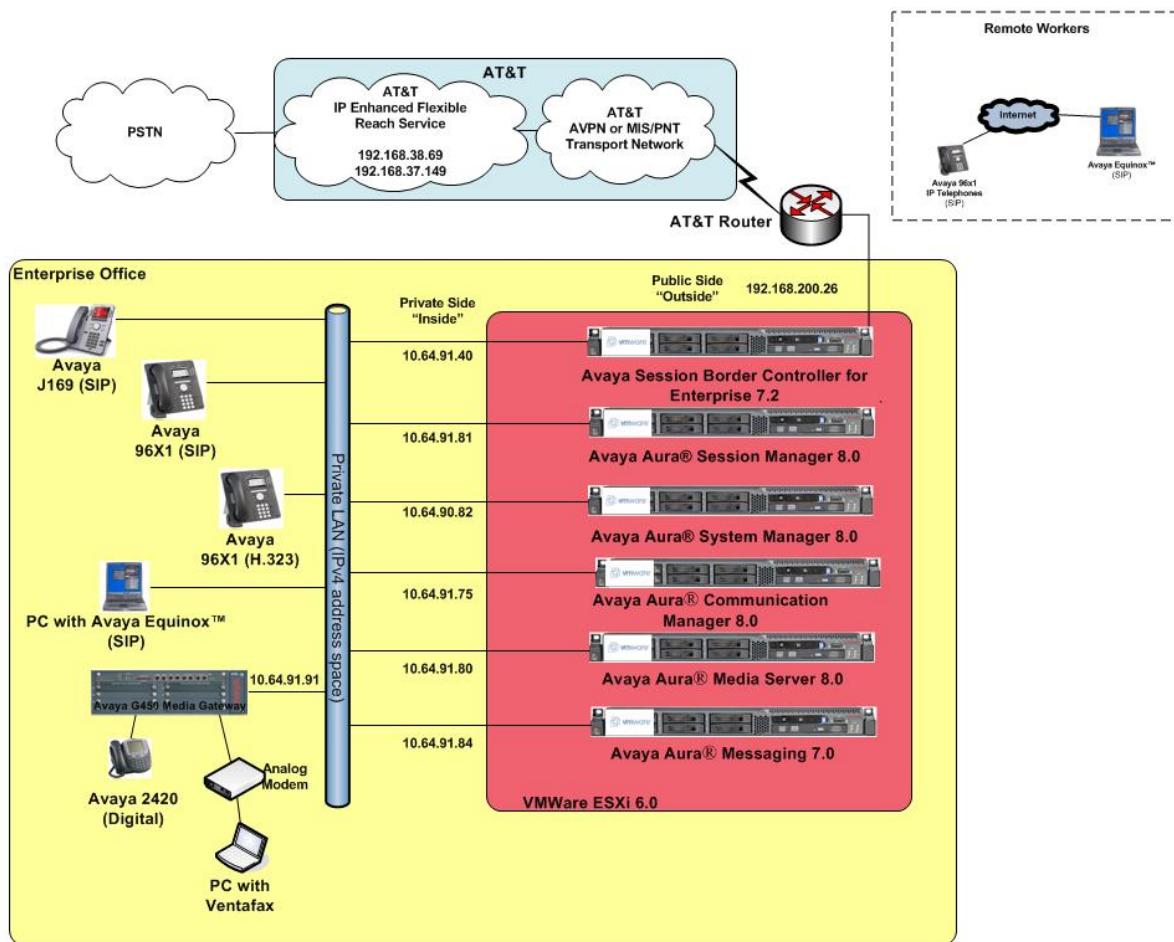


Figure 1: Reference configuration

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	10.64.91.81
Avaya Aura® Communication Manager	
IP Address	10.64.91.75
Avaya Aura® System Manager	
IP Address	10.64.90.82
Avaya Aura® Messaging	
IP Address	10.64.91.84
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Inside (Private) Interface	10.64.91.40
IP Address of Outside (Public) Interface	192.168.200.26 (see note below)
AT&T Border Element	
IP Addresses	192.168.38.69 192.168.37.149

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 actual IP addresses of the Avaya SBCE and AT&T BE are not included in this document. However, as placeholders in the following configuration sections, the IP addresses of **192.168.200.26** (Avaya SBCE public interface), **192.168.38.69** and **192.168.37.149** (AT&T BE IP addresses) are specified.

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

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

3.2.1. Inbound

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

1. A PSTN phone originates a call to an IPFR-EF service number.
2. The PSTN routes the call to the IPFR-EF service network.
3. The IPFR-EF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs IP address translations and any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone or fax endpoint.

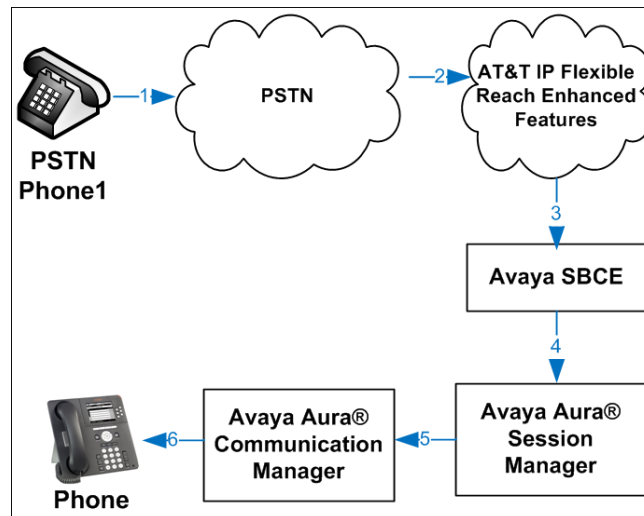


Figure 2: Inbound IPFR-EF Call

3.2.2. Outbound

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

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

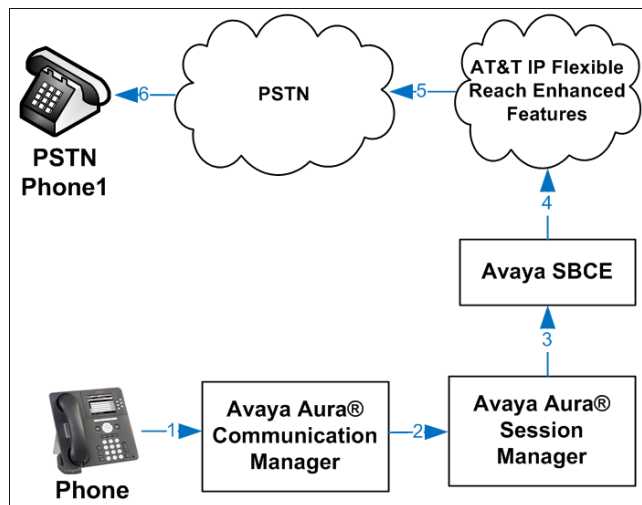


Figure 3: Outbound IPFR-EF Call

3.2.3. Call Forward Re-direction

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

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

1. 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. 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.
7. The IPFR-EF service places a call to the alternate destination, and upon answering Communication Manager connects the calling party to the target party.

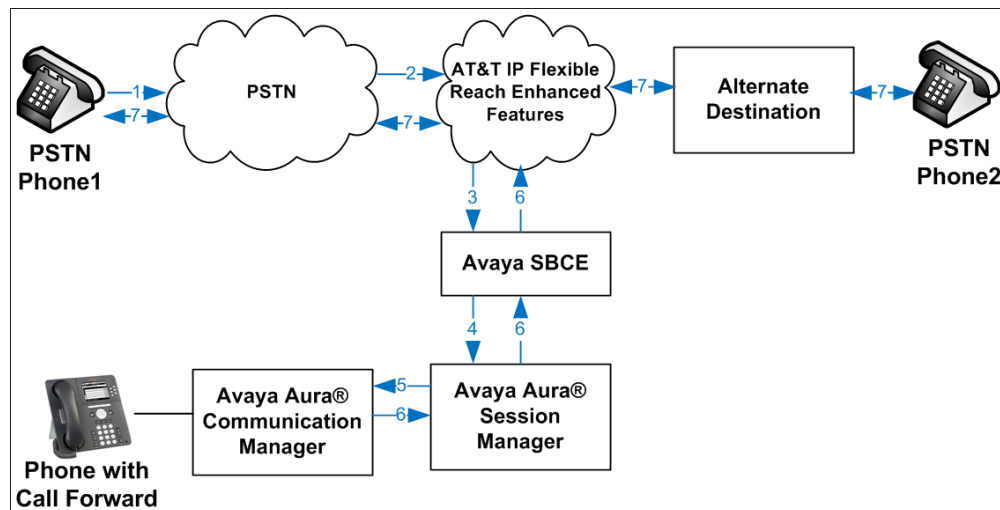


Figure 4: Station Re-directed (e.g., Call Forward) IPFR-EF Call

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 5** 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 IPFR-EF 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).

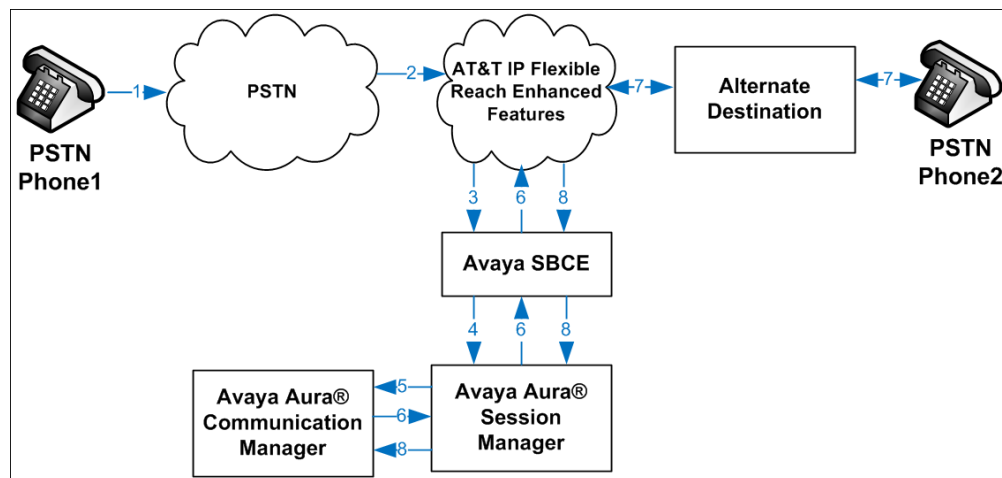


Figure 5: Network Based Blind Transfer Using Refer (Communication Manager Vector)

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 6** 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 initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network. Communication Manager completes the transfer, using Refer (*with the replaces parameter*), to the IPFR-EF service to connect the two active calls together.

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 initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network. Communication Manager redirects the call using a SIP Refer message when the transfer is completed by the station. The SIP Refer message specifies the active call to replace 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 replaces the call with the alternate destination specified in the Refer and connects the calling party to the alternate party.
8. IPFR-EF clears the existing calls to Communication Manager.

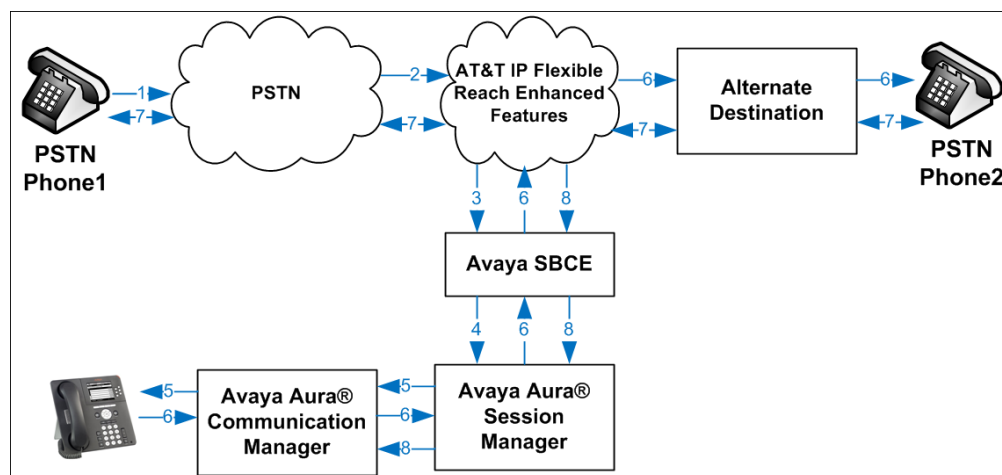


Figure 6: Attended/Unattended Transfer Using Refer (Communication Manager Station)

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0.0.931077
Avaya Aura® Communication Manager	8.0.0.0-R018x.00.0.822.0
Avaya Session Border Controller for Enterprise	7.2.2.0-07-14883
Avaya Aura® Messaging	7.0-00.0.441.0-017_0004 (SP 0)
Avaya Aura® Media Server	7.8.0.10 7.8.0.355
Avaya G450 Media Gateway	g450_sw_40_10_0
Avaya 96x1 IP Telephone	H.323 = 6.6604 SIP = 7.1.2.0.14
Avaya J100 Series IP Telephone	3.0.0.0.20
Avaya Equinox® for Windows (SIP)	3.4.0.152.46
Ventafax Home Version (Windows based Fax device)	7.9.255.613

Table 2: Equipment and Software Versions

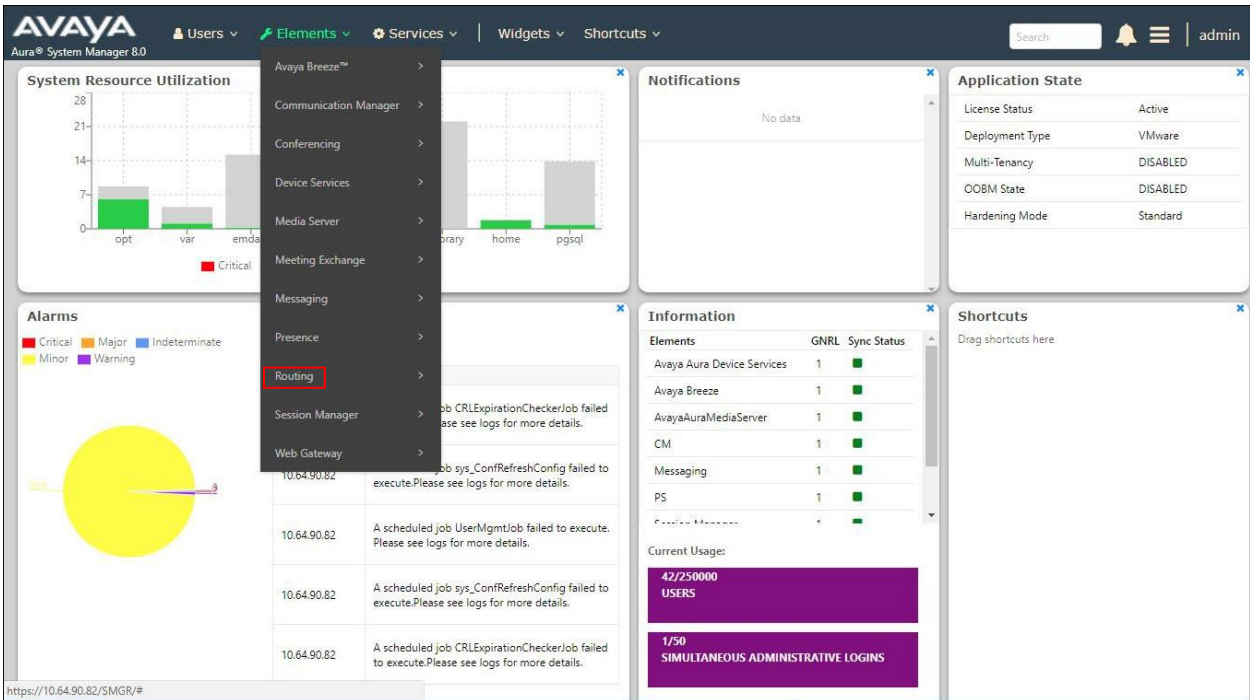
5. Configure Avaya Aura® Session Manager

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 Messaging.
- Define SIP Entities corresponding to Session Manager, Communication Manager, the Avaya SBCE, and Messaging.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, and Messaging, as well as the SIP trunks between the Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, Messaging, and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for inbound and outbound call routing.
- Verify TLS Certificates.

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, **Home** screen is displayed. From the **Home** screen, under the **Elements** heading, select **Routing**.



5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain **avayalab.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, **avayalab.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description.

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

The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', and 'Entity Links'. The main panel has a title 'Domain Management' and buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below these is a table with 1 item. The table has columns for 'Name', 'Type', and 'Notes'. The row shows 'avayalab.com' as the Name and 'sip' as the Type. At the bottom, it says 'Select : All, None'.

Name	Type	Notes
avayalab.com	sip	

5.2. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, and local SIP endpoints.
- **CM-TG-5** – Communication Manager trunk group 5 designated for AT&T.
- **Common** – Avaya SBCE

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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations (selected), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section has fields for 'Name' (Main) and 'Notes' (Avaya SIL). The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section has a 'Managed Bandwidth Units' dropdown (Kbit/sec), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked 'Audio Calls Can Take Multimedia Bandwidth' checkbox. The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)' (2000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (2000 Kbit/Sec), '* Minimum Multimedia Bandwidth' (64 Kbit/Sec), and '* Default Audio Bandwidth' (80 Kbit/sec). The 'Alarm Threshold' section has 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' dropdowns (both 80 %), and '* Latency before Overall Alarm Trigger' and '* Latency before Multimedia Alarm Trigger' fields (both 5 Minutes). The 'Location Pattern' section has 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' button. The table has columns for 'IP Address Pattern' and 'Notes'.

5.2.2. CM-TG-5 Location

To configure the Communication Manager Trunk Group 5 Location, repeat the steps in **Section 5.2.1** with the following changes:

- **Name** – Enter a descriptive name (e.g., **CM-TG-5**).

5.2.3. Common Location

To configure the Avaya SBCE Location, repeat the steps in **Section 5.2.1** with the following changes:

- **Name** – Enter a descriptive name (e.g., **Common**).

5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T. 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 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 History-Info header is removed automatically by the **ATTAdapter**.
 - Avaya SIP headers not required by AT&T are removed (see **Section 2.2, Item 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., **CM TG5 ATT IPFR**).
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' configuration page. On the left, a sidebar under 'Routing' has 'Adaptations' highlighted. The main panel has a 'General' tab. It contains several input fields: 'Adaptation Name' with the value 'CM TGS ATT IPFR', 'Module Name' with a dropdown menu showing 'DigitConversionAdapter', 'Module Parameter Type' with a dropdown arrow, 'Egress URI Parameters' as an empty text box, and 'Notes' with the value 'CM - ATT - IPFR'. At the top right of the main panel are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

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 range:** 30355593xx is a range of DNIS digits sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension range 59300 thru 59399.
 - Enter **30355593** in the **Matching Pattern** column.
 - Enter **10** in the **Min/Max** columns.
 - Enter **5** in the **Delete 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 10-digit DNIS numbers.

Digit Conversion for Outgoing Calls from SM

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*30355593	*10	*10		*5		destination ▼		10 digit DNIS to extension
<input type="checkbox"/>	*46955548	*10	*10		*5		destination ▼		10 digit DNIS to extension

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., **SBC1-Adaptation for ATT**).
2. Select **AttAdapter** from the **Module Name** drop-down menu (if no module name is present, select **<click to add module>** and enter **AttAdapter**). The AttAdapter will automatically remove History-Info headers, (which the IPFR-EF service does not support), sent by Communication Manager (see **Section 6.8.1**).

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-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-Id,P-Charging-Vector,P-Location,AV-Correlation-ID,Av-Secure-Indication**

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

Adaptation Details [Commit] [Cancel] [Help ?]

General

* **Adaptation Name:** SBC1-Adaptation for ATT

* **Module Name:** AttAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-Id,P-Charging-Vector,P-Location,AV-Correlation-ID,Av-Secure-Indication

Select : All, None

Egress URI Parameters:

Notes: SBC - ATT IPTF

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items [Filter: Enable]

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

Digit Conversion for Outgoing Calls from SM

Add Remove

0 Items [Filter: Enable]

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

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 TLS with port 5065), is for calls to/from AT&T and Communication Manager via the Avaya SBCE.
- Communication Manager for local trunk access (**Section 5.4.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager, as well as calls to Messaging.
- Avaya SBCE (**Section 5.4.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from the IPFR-EF service via the Avaya SBCE.
- Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Messaging.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5065), and to the Avaya SBCE (port 5061). 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., **SessionManager**).
- **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.61**).
- **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.
- **Minimum TLS Version** – Select **Use Global Setting**. In the reference configuration, the Session Manager Global Setting TLS version is 1.0 (not shown).

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 **Listen Port** section of the **SIP Entity Details** page. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 5.5**. Click on **Add** and provision entries as follows:

- **Port** – Enter **5061**
- **Protocol** – Select **TLS**
- **Default Domain** – Select a SIP domain administered in **Section 5.1** (e.g., **avayalab.com**)
- **Endpoint** – Check the checkbox to have this port be used for SIP endpoint registration.

Step 5 - Enter any notes as desired and leave all other fields on the page blank/default.

Step 6 - 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.

Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/> 5061	TLS	avayalab.com	<input checked="" type="checkbox"/>	TLS Endpoint

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., **CM-TG5**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 6.4** (e.g., **10.64.91.75**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM TG5 ATT IPFR** administered in **Section 5.3.1**.
- **Location** – Select Location **CM-TG-5** administered in **Section 5.2.2**.
- **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' page in the Avaya Aura Communication Manager interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'Commit' button. The 'General' section is active, showing fields for Name (CM-TG5), FQDN or IP Address (10.64.91.75), Type (CM), Notes (Trunk Group 5 - ATT IPFR), Adaptation (CM TG5 ATT IPFR), Location (CM-TG-5), Time Zone (America/Denver), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (checkbox), Call Detail Recording (none), Loop Detection Mode (On), Loop Count Threshold (5), Loop Detection Interval (in msec) (200), SIP Link Monitoring (Use Session Manager Configuration), and CRLF Keep Alive Monitoring (Use Session Manager Configuration). The 'Loop Detection' and 'Monitoring' sections are also visible.

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., **CM-TG3**).
- **Location** – Select Location **Main** administered in **Section 5.2.1**.
- **Adaptations** – Leave this field blank.

5.4.4. 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-ATT**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.40**, see **Section 7.5.1**).
- **Type** – Select **SIP Trunk**.
- **Location** – Select Location **Common** administered in **Section 5.2.3**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for ATT** (**Section 5.3.2**).

5.4.5. Avaya Aura® Messaging SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **Aura Messaging**).
- **FQDN or IP Address** – Enter the IP address of Messaging (e.g., **10.64.91.54**, see **Section 3.1**).
- **Type** – Select **Messaging**.
- **Location** – Select Location **Main** administered in **Section 5.2.1**.

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 Avaya SBCE (**Section 5.5.3**).
- Session Manager to Messaging (**Section 5.5.4**).

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 to CM TG5**).

- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g., **SessionManager**).
- **Protocol** – Select **TLS** (see **Section 6.8.1**).
- **SIP Entity 1 Port** – Enter **5065**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **CM-TG5**).
- **SIP Entity 2 Port** – Enter **5065** (see **Section 6.8.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

Step 3 - Click on **Commit**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
SM to CM TG5	Session Manager	TLS	5065	CM-TG5	5065	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

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 to CM TG3**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local entity (e.g., **CM-TG3**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 6.8.2**).

5.5.3. 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 to SBCE**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE entity (e.g., **SBCE-ATT**).
- **SIP Entity 2 Port** – Enter **5061**.

5.5.4. 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 Messaging (e.g., **SM to AAM**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.5** for the Aura® Messaging entity (e.g., **Aura Messaging**).
- **SIP Entity 2 Port** – Enter **5061**.

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.

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

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 Aura® Messaging (**Section 5.7.2**).
- Outbound calls to AT&T/PSTN (**Section 5.7.3**).

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., **To CM-TG5**), 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.

Name	FQDN or IP Address	Type	Notes
CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR

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

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 (**CM-TG5**), and click on **Select**.

SIP Entities				
13 Items				
	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	Aura Messaging	10.64.91.84	Messaging	Aura Messaging
<input type="radio"/>	Breeze	10.64.91.18	Avaya Breeze	
<input type="radio"/>	CM-TG1	10.64.91.75	CM	Trunk Group 1 - CM to Vz-IPT
<input type="radio"/>	CM-TG2	10.64.91.75	CM	Trunk Group 2 - Vz-Toll-Free inbound
<input type="radio"/>	CM-TG3	10.64.91.75	CM	Trunk Group 3 - CM to Enterprise
<input type="radio"/>	CM-TG4	10.64.91.75	CM	Trunk Group 4 - ATT IPTF
<input type="radio"/>	CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR
<input type="radio"/>	IP500	10.64.19.70	Other	IP Office
<input type="radio"/>	Presence	10.64.91.18	Presence Services	
<input type="radio"/>	SBC1	10.64.91.50	SIP Trunk	Avaya SBC-1 to PSTN
<input type="radio"/>	SBC2	10.64.91.100	SIP Trunk	Avaya SBC-2 to PSTN
<input type="radio"/>	SBCE-ATT	10.64.91.40	SIP Trunk	SBCE for AT&T testing
<input type="radio"/>	SBCE-Toll Free	10.64.91.41	SIP Trunk	SBCE for IPTF testing
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.

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

Routing Policy Details

Commit Cancel

General

Name: To CM-TG5
Disabled:
Retries: 0
Notes: Trunk Group 5 PSTN to CM

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR

Time of Day

Add Remove View Gaps/Overlaps

1 Item

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
2	24/7								00:00	23:59	

Select: All, None

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

This routing policy is for inbound calls to Aura® 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 5.4.5** for Aura® Messaging (e.g., **AAM**).

5.7.3. 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., **To SBCE-ATT**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE SIP Entity (e.g., **SBCE-ATT**).

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**).

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

In the reference configuration inbound calls from the IPFR-EF service sent 10 DNIS digits in the SIP Request URI (for security purposes, these digits are represented in this document as 303555xxxx). 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 **303555**. Note – The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 303-555-xxxx numbers into their corresponding Communication Manager extensions.
- **Min and Max** – Enter **10**.
- **SIP Domain** – Select **avayalab.com**, the SIP domain name configured in **Section 5.1**.

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:** 303555

* **Min:** 10

* **Max:** 10

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: AT&T DIDs

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"/>	Common	SBC to PSTN	To CM-TG5	2	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN5 to CM

Select : All, None

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 the location assigned to the Avaya SBCE in **Section 5.4.4** (e.g., **Common**).

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., **To CM-TG5**), and click on **Select**.

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

4 Items Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5
<input checked="" type="checkbox"/>	Common	SBC to PSTN
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1

Select : All, None

Routing Policies

11 Items Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AAM	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 PSTN1 to CM
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 VzIPCC to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input type="checkbox"/>	To CM TG4	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM
<input checked="" type="checkbox"/>	To CM-TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN5 to CM
<input type="checkbox"/>	To IP500	<input type="checkbox"/>	IP500	
<input type="checkbox"/>	To SBC1	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	To SBC2	<input type="checkbox"/>	SBC2	
<input type="checkbox"/>	To SBCE-ATT	<input type="checkbox"/>	SBCE-ATT	
<input type="checkbox"/>	to SBCE TollFree	<input type="checkbox"/>	SBCE-Toll Free	

Select : All, None

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.

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 469555

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: AT&T DID's

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To CM-TG5	2	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN5 to CM

Select : All, None

Denied Originating Locations

Add Remove

0 Items Filter: Enable

<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 1xxxxyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes *7 and *9 (e.g., *71yyyzzxxxx & *91yyyzzxxxx) 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., +). This will match any outbound call prefixed with a plus sign (+), such as an E.164 formatted number.

- Enter a **Min** pattern of **12**.
- Enter a **Max** pattern of **36**.
- 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 5.7.3** (e.g., **To SBCE-ATT**).

Dial Pattern Details Commit Cancel

General

* Pattern:
 * Min:
 * Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

4 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5	To SBCE-ATT	0	<input type="checkbox"/>	SBCE-ATT	
<input type="checkbox"/>	Main	Avaya SIL	To SBC2	1	<input type="checkbox"/>	SBC2	
<input type="checkbox"/>	Main	Avaya SIL	To SBC1	0	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1	To SBCE-ATT	0	<input type="checkbox"/>	SBCE-ATT	

Select : All, None

Step 2 - Repeat **Step 1** to add patterns for IPFR-EF Call Forward access codes with patterns ***7** and ***9**, and **Min=2/Max=36**.

Step 3 - Repeat **Step 1** to add any additional outbound patterns as required.

Dial Patterns

New Edit Delete Duplicate More Actions

43 Items Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	0	1	36	<input type="checkbox"/>			avayalab.com	0+ NANPA
<input type="checkbox"/>	*7	2	36	<input type="checkbox"/>			-ALL-	ATT -IPFlex feature code
<input type="checkbox"/>	*9	2	36	<input type="checkbox"/>			-ALL-	ATT -IPFlex feature code
<input type="checkbox"/>	x11	3	3	<input type="checkbox"/>			avayalab.com	Outbound Services
<input type="checkbox"/>	911	3	3	<input checked="" type="checkbox"/>	All Emergency	1	-ALL-	
<input type="checkbox"/>	9999	4	36	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	1411	4	4	<input type="checkbox"/>			avayalab.com	Outbound PSTN Information
<input type="checkbox"/>	15555	5	5	<input checked="" type="checkbox"/>	test EMERG	1	-ALL-	Test emergency outbound
<input type="checkbox"/>	12xxx	5	5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	11000	5	5	<input type="checkbox"/>			-ALL-	Messaging Pilot number
<input type="checkbox"/>	7	5	5	<input type="checkbox"/>			-ALL-	CM VDNs
<input type="checkbox"/>	89	5	5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	50	5	5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	14xxx	5	5	<input type="checkbox"/>			-ALL-	Enterprise Extensions
<input type="checkbox"/>	5551212	7	7	<input type="checkbox"/>			avayalab.com	Outbound Directory Service

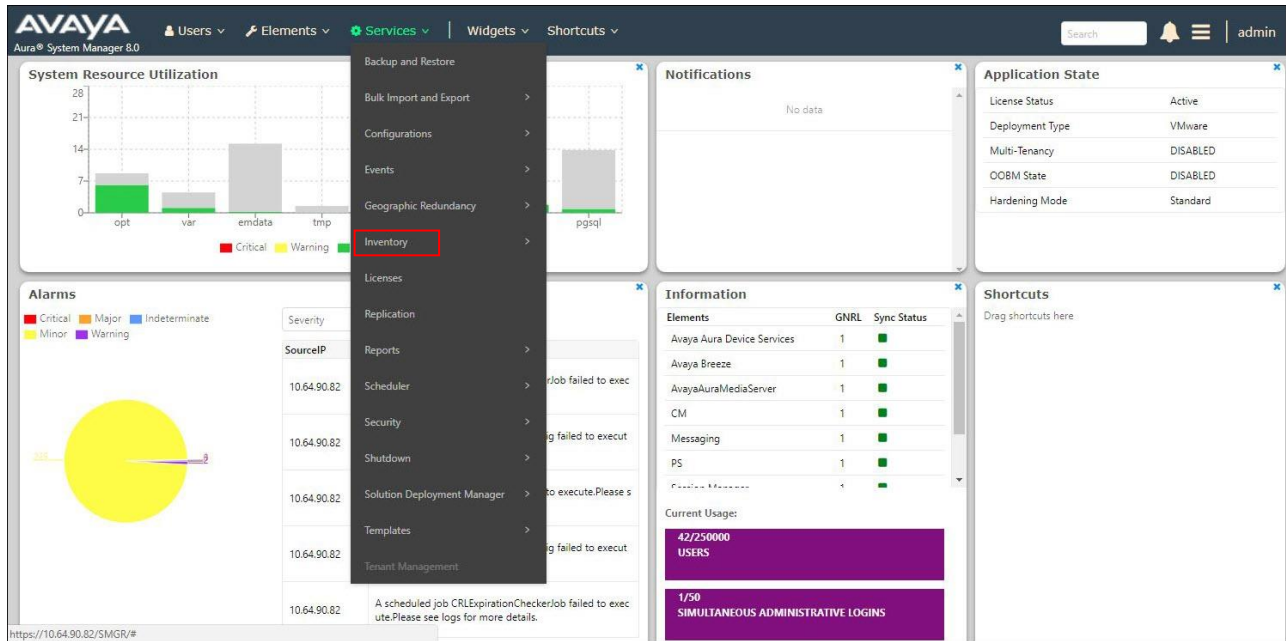
Select : All, None Page 1 of 3

5.9. Verify TLS Certificates – Session Manager

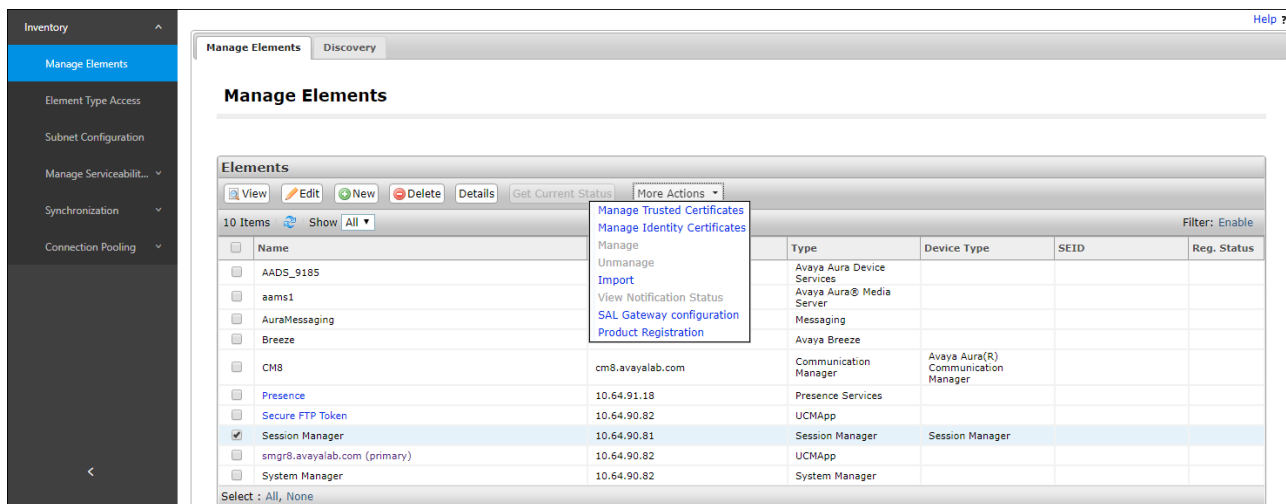
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

The following procedures show how to verify the certificates used by Session Manager.

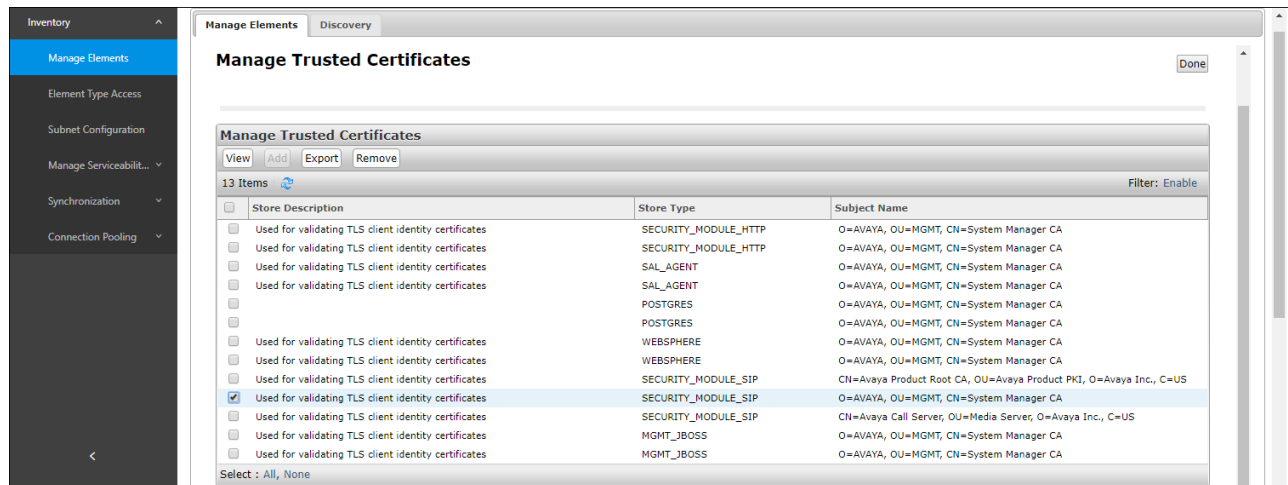
Step 1 - From the **Home** screen, under the **Services** heading, select **Inventory**.



Step 2 - In the left pane under **Inventory**, click on **Manage Elements** and select the Session Manager element, e.g., **SessionManager**. Click on **More Actions** → **Manage Trusted Certificates**.

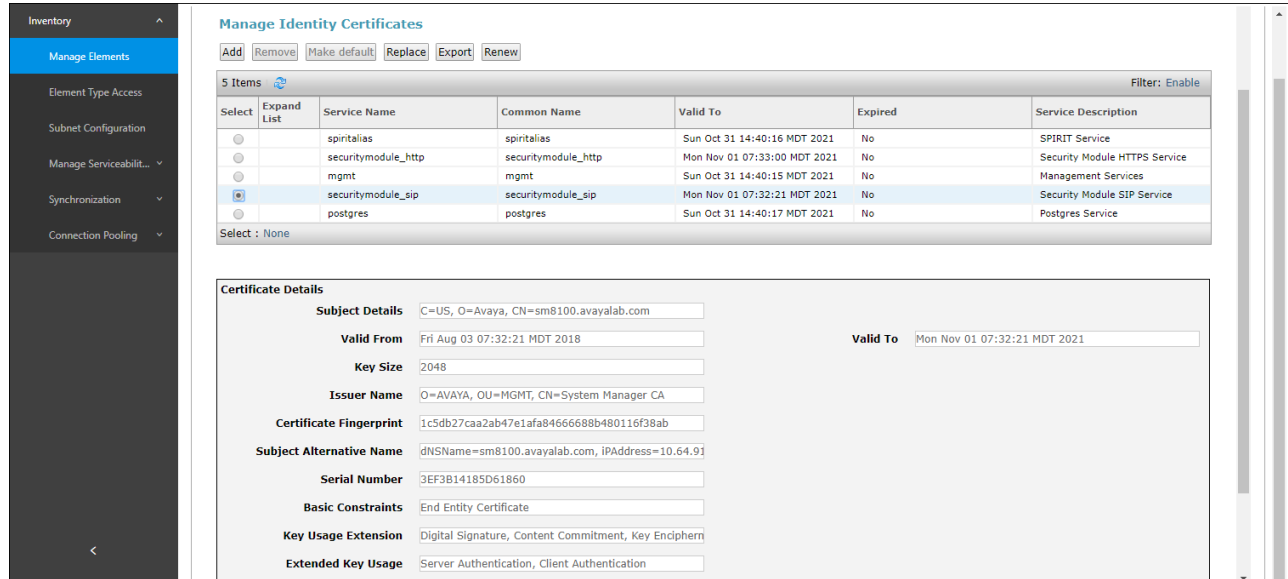


Step 3 - Verify the System Manager Certificate Authority certificate is listed in the trusted store, **SECURITY_MODULE_SIP**. Click **Done** to return to the previous screen.



Step 4 - With Session Manager selected, click on **More Actions** → **Manage Identity Certificates** (not shown).

Step 5 - Verify the **Security Module SIP** service has a valid identity certificate signed by System Manager. If the **Subject Details** and **Subject Alternative Name** fields of the System Manager signed certificate need to be updated, click **Replace**, otherwise click **Done**.



6. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult Error! Reference source not found. - [9] for more information.

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

6.1. 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

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

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

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	4000	0	
Maximum Concurrently Registered IP Stations:	2400	2	
Maximum Administered Remote Office Trunks:	4000	0	
Maximum Concurrently Registered Remote Office Stations:	2400	0	
Maximum Concurrently Registered IP eCons:	68	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	2400	3	
Maximum Video Capable IP Softphones:	2400	10	
Maximum Administered SIP Trunks:	4000	60	
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	80	0	

Step 2 - On Page 6 of the form, verify that the **Processor Ethernet field is 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		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? n	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
Private Networking? y	Uniform Dialing Plan? y	
Processor and System MSP? y	Usage Allocation Enhancements? y	
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		
(NOTE: You must logoff & login to effect the permission changes.)		

6.2. System-Parameters Features

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

change system-parameters features	Page 1 of 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? all	
DID/Tie/ISDN/SIP Intercept Treatment: attendant	
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred	
Automatic Circuit Assurance (ACA) Enabled? n	
Abbreviated Dial Programming by Assigned Lists? n	
Auto Abbreviated/Delayed Transition Interval (rings): 2	
Protocol for Caller ID Analog Terminals: Bellcore	
Display Calling Number for Room to Room Caller ID Calls? n	

6.3. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

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

- 5-digit extensions with a **Call Type** of **ext** beginning with:
 - The digits **1, 5, 7** and **8** for Communication Manager extensions.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code ***xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 6.8**.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	5	ext						
2	5	ext						
3	5	ext						
4	5	ext						
5	5	ext						
60	3	ext						
66	2	fac						
7	5	ext						
8	5	ext						
9	1	fac						
*	3	dac						

6.4. IP Node Names

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

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

- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.81**).
- Media Server (e.g., **AMS** and **10.64.91.80**). The Media Server node name is only needed if a Media Server is present.

change node-names ip		IP NODE NAMES		Page 1 of 2	
Name	IP Address				
AMS	10.64.91.80				
SM	10.64.91.81				
default	0.0.0.0				
procr	10.64.91.75				
procr6	::				

6.5. IP Interface for procr

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

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

display ip-interface procr		Page	1	of	2
IP INTERFACES					
Type: PROCR		Target socket load: 4800			
Enable Interface? y		Allow H.323 Endpoints? y			
Network Region: 1		Allow H.248 Gateways? y			
		Gatekeeper Priority: 5			
IPV4 PARAMETERS					
Node Name: procr		IP Address: 10.64.91.75			
Subnet Mask: /24					

6.6. IP Network Regions

Network Regions are used to group various Communication Manager resources such as codecs, UDP port ranges, and inter-region communication. In the reference configuration, two network regions are used. Region 1 for the CPE access, and region 4 for SIP trunk access.

6.6.1. IP Network Region 1 – Local CPE Region

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

- Enter a descriptive name (e.g., **Enterprise**).
- Enter the enterprise domain (e.g., **avaya.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).

Note – The port range for Region 1 does not have to be in the range required by AT&T. However, the same range was used here in the reference configuration.

6.6.2. IP Network Region 4 – AT&T Trunk Region

Repeat the steps in **Section 6.6.1** with the following changes:

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

- Enter a descriptive name (e.g., **AT&T**).
- Enter **4** for the **Codec Set** parameter.

Step 2 - On **Page 4** of the form:

- Set codec set **4** for **dst rgn 1**.
- Note that **dst rgn 4** is pre-populated with codec set **4** (from page 1 provisioning).

change ip-network-region 4										Page 4 of 20		
Source Region: 4										Inter Network Region Connection Management		
										I	M	
										G	A	t
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	A	G	c			
1	4	y	NoLimit				n			t		
2	4	y	NoLimit				n			t		
3	3	y	NoLimit				n			t		
4	4										all	

6.7. IP Codec Parameters

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

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., **1**). On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, **G.729A**, and **G.729B** are included in the codec list. Note that the packet interval size will default to 20ms. Set the **Media Encryption** based on customer requirements. In the reference configuration, **1-srtp-aescm128-hmac80** was the preferred crypto suite, with **none** set as the second option.

change ip-codec-set 1					Page 1 of 2	
Codec Set: 1					IP MEDIA PARAMETERS	
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)			
1: G.722-64K		2	20			
2: G.711MU	n	2	20			
3: G.729A	n	2	20			
4: G.729B	n	2	20			
Media Encryption				Encrypted SRTCP: enforce-unenc-srtcp		
1: 1-srtp-aescm128-hmac80						
2: none						

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

change ip-codec-set 1		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia: 15360:Kbits			
Maximum Call Rate for Priority Direct-IP Multimedia: 15360:Kbits			
	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	
SIP 64K Data	n	0	20

6.7.2. Codecs for IP Network Region 4 (calls to/from AT&T)

This IP codec set will be used for IPFR-EF calls. Repeat the steps in **Section 6.7.1** with the following changes:

- Provision the codecs in the order shown below. Note that the order of G.729A and G.729B codecs may be reversed as required.
- Set **Frames Per Pkt** to **3**. This will auto-populate **30** for the **Packet Size (ms)** field, and specify a PTIME value of 30 in the SDP (recommended by AT&T). See **Section 2.2** for limitations.

change ip-codec-set 4		Page 1 of 2	
IP CODEC SET			
Codec Set: 4			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.729A	n	3	30
2: G.729B	n	3	30
3: G.711MU	n	3	30
Media Encryption		Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80			
2: none			

change ip-codec-set 4		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? n			
	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	
SIP 64K Data	n	0	20

6.8. SIP Trunks

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

- Inbound/outbound AT&T access – SIP Trunk 5
 - Note that this trunk will use TLS port 5065 as described in **Section 5.5.1**.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 3
 - Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

Note – Although TLS 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 TLS transport protocols in the CPE.

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

This section describes the steps for administering the SIP trunk to Session Manager used for IPFR-EF calls. Trunk 5 is defined. This trunk corresponds to the **CM-TG5** SIP Entity defined in **Section 5.4.2**.

6.8.1.1 Signaling Group 5

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **4**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- 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 **5065**.
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 6.6.2**.
- **Far-end Domain** – Enter **avayalab.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.
- **Initial IP-IP Direct Media** is set to **n**.
- **H.323 Station Outgoing Direct Media** is set to **n**.
- Use the default parameters on **page 2** of the form (not shown).

add signaling-group 5		Page 1 of 2
SIGNALING GROUP		
Group Number: 4	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	Clustered? n
Peer Detection Enabled? y	Peer Server: SM	
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: 5065	Far-end Listen Port: 5065	
	Far-end Network Region: 4	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

6.8.1.2 Trunk Group 5

Step 1 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **5**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **ATT IPFR**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***05**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 6.8.1.1** (e.g., **2**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

add trunk-group 5		Page 1 of 21
TRUNK GROUP		
Group Number: 5	Group Type: sip	CDR Reports: y
Group Name: ATT IPFR	COR: 5	TN: 1 TAC: *05
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: 5	
	Number of Members: 10	

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

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

add trunk-group 5	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	
Caller ID for Service Link Call to H.323 1xC: station-extension	

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

- Set **Numbering Format** to **public**.

add trunk-group 5	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: public	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

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

- Verify **Network Call Redirection** is set to **y**.
- 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 1** 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.

add trunk-group 5	PROTOCOL VARIATIONS	Page 4 of 21
<div style="text-align: right;">Mark Users as Phone? n</div>		
<div style="text-align: right;">Prepend '+' to Calling/Alerting/Diverting/Connected Number? n</div>		
<div style="text-align: right;">Send Transferring Party Information? n</div>		
<div style="text-align: right;">Network Call Redirection? y</div>		
<div style="text-align: right;">Build Refer-To URI of REFER From Contact For NCR? n</div>		
<div style="text-align: right;">Send Diversion Header? y</div>		
<div style="text-align: right;">Support Request History? y</div>		
<div style="text-align: right;">Telephone Event Payload Type: 100</div>		
<div style="text-align: right;">Shuffling with SDP? n</div>		
<div style="text-align: right;">Convert 180 to 183 for Early Media? n</div>		
<div style="text-align: right;">Always Use re-INVITE for Display Updates? n</div>		
<div style="text-align: right;">Identity for Calling Party Display: From</div>		
<div style="text-align: right;">Block Sending Calling Party Location in INVITE? n</div>		
<div style="text-align: right;">Accept Redirect to Blank User Destination? n</div>		
<div style="text-align: right;">Enable Q-SIP? n</div>		
<div style="text-align: right;">Interworking of ISDN Clearing with In-Band Tones: keep-channel-active</div>		
<div style="text-align: right;">Request URI Contents: may-have-extra-digits</div>		

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

Trunk 3 corresponds to the **CM-TG3** SIP Entity defined in **Section 5.4.3**.

6.8.2.1 Signaling Group 3

Repeat the steps in **Section 6.8.1.1** with the following changes:

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **3**).

Step 2 - Set the following parameters on page 1:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.6.1**.

6.8.2.2 Trunk Group 3

Repeat the steps in **Section 6.8.1.2** with the following changes:

Step 1 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **3**). On **Page 1** of the **trunk-group** form:

- **Group Name** – Enter a descriptive name (e.g., **SM Enterprise**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***03**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Section 6.8.2.1** (e.g., **3**).

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

- Same as **Section 6.8.1.2**

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

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

Step 4 - 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.

6.9. Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 6.8.1.2**), 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 - Enter **change public-unknown-numbering 5 ext-digits xxxxx**, where xxxxx is the 5-digit extension number to change.

Step 2 - Add each Communication Manager station extension and their corresponding IPFR-EF DNIS numbers (for the public trunk to AT&T). Communication Manager will insert these AT&T DNIS numbers in E.164 format into the From, Contact, and PAI headers as appropriate. In the reference configuration, a range of extensions were added as follows:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the first two digits for Communication Manager extensions (e.g., **54** for extension range 54xxx, and **59** for extension range 59xxx).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **5**).
- **Private Prefix** – Enter the corresponding IPFR-EF DNIS number prefix (e.g., **146955** and **130355**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

change public-unknown-numbering 5 ext-digits 5					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	14	5	17325552754	11	Total Administered: 46
5	50	4	173255	11	Maximum Entries: 240
5	54	5	146955	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	59	5	130355	11	
5	10001	2	18665553221	11	
					Communication Manager automatically inserts a '+' digit in this case.

6.10. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 6.8.2.2**), is used to send Communication Manager local extension numbers to Session Manager, for inclusion in any SIP headers directed to SIP endpoints and Messaging.

Step 1 - Add all 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 extension patterns defined in the Dial Plan in **Section 6.3** (e.g., **54** and **59**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).
- **Total Len** - Enter the total number of digits after the digit conversion (e.g., **5**).

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total CPN Len	
5	10	3		5	Total Administered: 6
5	11	3		5	Maximum Entries: 540
5	12	3		5	
5	54	3		5	
5	59	3		5	

6.11. Route Patterns

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

6.11.1. Route Pattern for National Calls to AT&T

This form defines the public SIP trunk, based on the route-pattern selected by the ARS table in **Section 6.12**. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks. In the

reference configuration, route pattern 1 is used for national calls, route pattern 2 is used for international calls, and route pattern 4 is used for service calls and IPFR-EF Call Forward feature access codes.

Step 1 - Enter the **change route-pattern 1** command to configure a route pattern for national calls and enter the following parameters:

- In the **Grp No** column, enter **5** for public trunk 5, and the **FRL** column enter **0** (zero).
- In the **Pfx Mrk** column, enter **1** to ensure 1 + 10 digits are sent to the service provider for FNPA calls.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.

change route-pattern 1										Page 1 of 3
Pattern Number: 1 Pattern Name: To PSTN SIP Trk										
SCCAN? n Secure SIP? n Used for SIP stations? n										
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG	IXC	
1: 5	0		1				p	n	user	
2:								n	user	
3:								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			none

6.11.2. Route Pattern for International Calls to AT&T

Repeat the steps in **Section 6.11.1** to add a route pattern for international calls with the following changes:

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

- In the **Grp No** column, enter **5** for public trunk 5, and the **FRL** column enter **0** (zero).
- In the **Pfx Mrk** column, leave blank (default).
- In the **No. Del Digits** column, enter **3** to have Communication Manager remove the international 011 prefix from the number.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.

change route-pattern 2															Page 1 of 3			
Pattern Number: 2															Pattern Name: 011 to E.164			
SCCAN? n															Secure SIP? n		Used for SIP stations? n	
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits			DCS/	IXC							
						Dgts			Intw									
1:	5	0				3	p			n	user							
2:										n	user							
3:										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				none					

6.11.3. Route Pattern for Service Calls to AT&T

Repeat the steps in **Section 6.11.1** to add a route pattern for x11 and IPFR-EF Call Forward feature access codes calls with the following changes:

Step 1 - Enter the **change route-pattern 4** command and enter the following parameters:

- In the **Grp No** column, enter **5** for public trunk 5, and the **FRL** column enter **0** (zero).
- In the **Pfx Mrk** column, leave blank (default).
- In the **Inserted Digits** column, leave blank (default).

change route-pattern 4															Page 1 of 3			
Pattern Number: 4															Pattern Name: Service Numbers			
SCCAN? n															Secure SIP? n		Used for SIP stations? n	
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits			DCS/	IXC							
						Dgts			Intw									
1:	5	0								n	user							
2:										n	user							
3:										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				none					

6.11.4. 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 6.13** (e.g., calls to Avaya SIP telephone extensions or Messaging).

Step 1 - Repeat the steps in **Section 6.11.1** with the following changes:

- In the **Grp No** column enter **3** for SIP trunk 3 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the **Pfx Mrk** column, leave blank (default).
- In the **Inserted Digits** column, leave blank (default).
- In the **Numbering Format** column, across from line **1**: enter **lev0-pvt**.

change route-pattern 3											Page 1 of 3		
Pattern Number: 3						Pattern Name: ToSM Enterprise							
SCCAN? n		Secure SIP? n		Used for SIP stations? y									
Primary SM: SM				Secondary SM:									
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted				DCS/	IXC	
No		Mrk	Lmt	List	Del	Digits				QSIG			
										Dgts	Intw		
1:	3	0										n	user
2:											n	user	
3:											n	user	
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	lev0-pvt		none		

6.12. 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 6.11**).

Step 1 - Enter the **change ars analysis 1720** command and enter the following:

- In the **Dialed String** column enter a matching dial pattern (e.g., 1720). Note that the best match will route first, that is 1720555xxxx will be selected before 17xxxxxxxxx.
- 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., 1).
- In the **Call Type** column enter **fnpa** (selections other than **fnpa** may be appropriate, based on the digits defined here).

Step 2 - Repeat **Step 1** 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 1720										Page 1 of 2
ARS DIGIT ANALYSIS TABLE										
Location: all										Percent Full: 1
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI	Reqd		
1720		11	11	1	fnpa		n			
18		11	11	1	fnpa		n			
19		11	11	1	fnpa		n			
1900		11	11	deny	fnpa		n			
1900555		11	11	deny	fnpa		n			
1xxx976		11	11	deny	fnpa		n			
*7		3	16	4	svcl		n			
*9		3	16	4	svcl		n			
311		3	3	4	svcl		n			
011		10	18	2	intl		n			
411		3	3	4	svcl		n			
5		10	10	1	fnpa		n			
511		3	3	4	svcl		n			
555		7	7	deny	hnpa		n			
5551212		7	7	1	svcl		n			

6.13. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

Step 1 - Enter the **change aar analysis 0** command and enter the following:

- **Dialed String** - In the reference configuration all SIP telephones used extensions in the range 54xxx, therefore enter **54**.
- **Min & Max** – Enter **5**
- **Route Pattern** – Enter **3**
- **Call Type** – Enter **lev0**

Step 2 - Repeat **Step 1** and create an entry for Messaging access extension (not shown).

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 1		
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
54		5	5	3	lev0		n	

6.14. Avaya G450 Media Gateway Provisioning

In the reference configuration, a G450 Media Gateway is provisioned. The G450 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 G450 registration to Communication Manager is shown below. For additional information on G450 provisioning, see [7].

Step 1 - Use SSH to connect to the G450 (not shown). Note that the Media Gateway prompt will contain “???” if the Media Gateway is not registered to Communication Manager (e.g., **G450-???(super)#**).

Step 2 - Enter the **show system** command and copy down the G450 serial number (e.g., **11N507727041**).

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., **10.64.91.75**, see **Section 6.4**).

Step 4 - Enter the **copy run start** command to save the G450 configuration.

Step 5 - From Communication Manager SAT, enter **add media-gateway x** where x is an available Media Gateway identifier (e.g., **1**).

Step 6 – On the Media Gateway form (not shown), enter the following parameters:

- Set **Type** = **g450**
- Set **Name** = a descriptive name (e.g., **G450-1**)
- Set **Serial Number** = the serial number copied from **Step 2** (e.g., **11N507727041**)
- 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 G450 to register to Communication Manager. When the Media Gateway registers, the G450 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., *G450-001(super)#*).

Step 7 - Enter the **display media-gateway 1** command and verify that the G450 has registered.

```
display media-gateway 1                                     Page 1 of 2
                                     MEDIA GATEWAY 10
                                     Type: g450
                                     Name: G450-1
                                     Serial No: 11N507727041
Link Encryption Type: any-ptls/tls      Enable CF? n
Network Region: 1                      Location: 1
Use for IP Sync? y                     Site Data:
Recovery Rule: 1

Registered? y
FW Version/HW Vintage: 40 .10 .0 /1
MGP IPV4 Address: 10.64.91.91
MGP IPV6 Address:
Controller IP Address: 10.64.91.75
MAC Address: b4:b0:17:90:61:d8

Mutual Authentication? optional
```

6.15. Avaya Aura® Media Server Provisioning

In the reference configuration, an Avaya Aura® Media Server is provisioned. The Media Server is located in the Main site and is used, along with the G450 Media Gateway, for local DSP resources, announcements, and Music On Hold.

Note – Only the Media Server provisioning associated with Communication Manager is shown below. See [8 and 9] for additional information.

Step 1 - Access the Media Server Element Manager web interface by typing “**https://x.x.x.x:8443**” (where x.x.x.x is the IP address of the Media Server) (not shown).

Step 2 - On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP → Node and Routes** and add the Communication Manager Procr interface IP address (e.g., **10.64.91.75**, see **Section 6.4**) as a trusted node (not shown).

Step 3 - On Communication Manager, enter the **add signaling-group x** command where x is an unused signaling group (e.g., **60**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**
- Verify that **Peer Detection Enabled?** – Set to **n**.
- **Peer Server** to **AMS**.
- **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 Media Server as administered in **Section 6.4** (e.g., **AMS**).
- **Near-end Listen Port** – Set to **9061**

- **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 6.6.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

```
add signaling-group 60                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 60           Group Type: sip
                          Transport Method: tls

Peer Detection Enabled? n Peer Server: AMS

Near-end Node Name: procr           Far-end Node Name: AMS
Near-end Listen Port: 9061         Far-end Listen Port: 5061
                                   Far-end Network Region: 1

Far-end Domain: 10.64.91.80
```

Step 4 - On Communication Manager, enter the **add media-server x** command where x is an available Media Server identifier (e.g., **1**). Enter the following parameters:

- **Signaling Group** – Enter the signaling group previously configured for Media Server (e.g., **60**).
- **Voip Channel License Limit** – Enter the number of VoIP channels for this Media Server (based on licensing) (e.g., **300**).
- **Dedicated Voip Channel Licenses** – Enter the number of VoIP channels licensed to this Media Server (e.g., **300**)
- Remaining fields are automatically populated based on the signaling group provisioning for the Media Server.

```
add media-server 1                                         Page 1 of 1
                                     MEDIA SERVER

Media Server ID: 1

Signaling Group: 60
Voip Channel License Limit: 300
Dedicated Voip Channel Licenses: 300

Node Name: AMS
Network Region: 1
Location: 1
Announcement Storage Area: ANNC-be99ad1a-1f39-41e5-ba04-000c29f8f3f3
```

6.16. Save Translations

After the Communication Manager provisioning is completed, enter the command **save translation**.

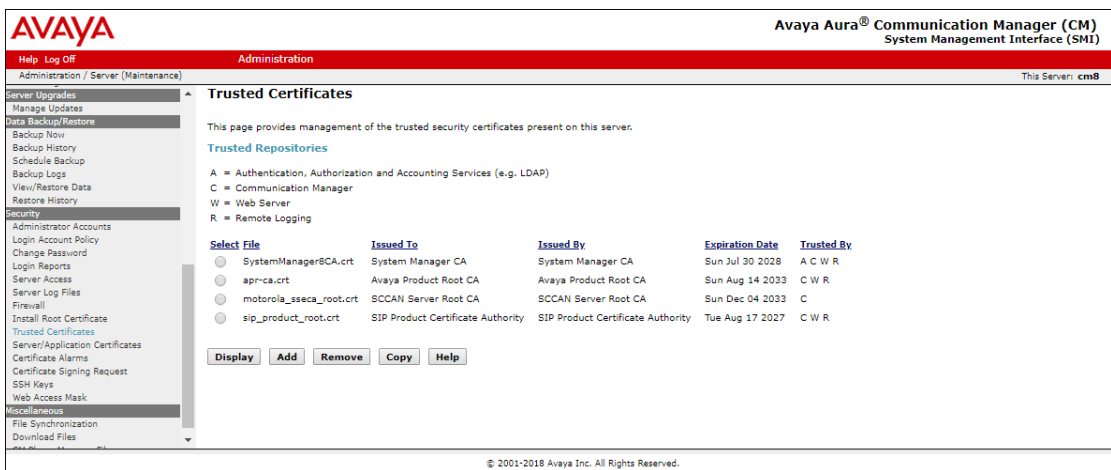
6.17. Verify TLS Certificates – Communication Manager

Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

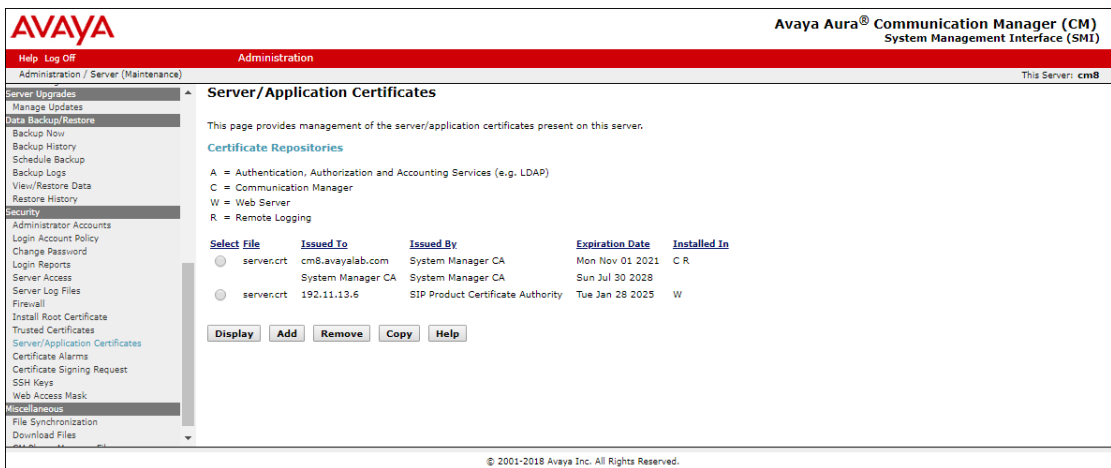
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. The following procedures show how to verify the certificates used by Communication Manager.

Step 1 - From a web browser, type in “https://<ip-address>”, where “<ip-address>” is the IP address or FQDN of Communication Manager. Follow the prompted steps to enter appropriate **Logon ID** and **Password** credentials to log in (not shown).

Step 2 - Click on **Administration** at the top of the page and select **Server (Maintenance)** (not shown). Click on **Security** → **Trusted Certificate** and verify the System Manager CA certificate is present in the Communication Manager trusted repository.



Step 3 - Click on **Security** → **Server/Application Certificates** and verify the System Manager CA certificate is present in the Communication Manager certificate repository.



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 [10] and [11] for additional information.

Note: The Avaya SBCE supports a Remote Worker configuration whereby Communication 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 10.64.91.40) 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 B2 (IP address 192.168.200.26).

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

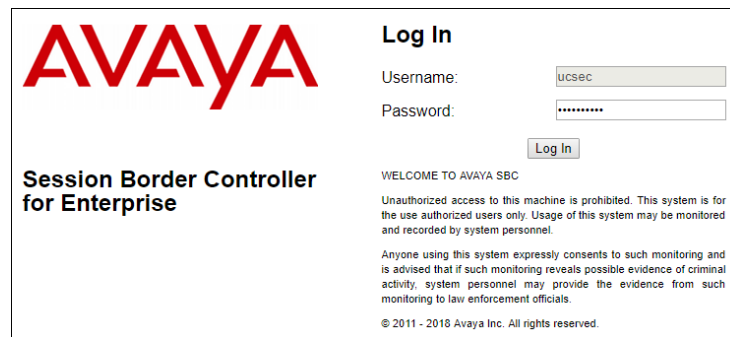
Step 1 - Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).

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



The screenshot shows the Avaya Session Border Controller for Enterprise login interface. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, a "WELCOME TO AVAYA SBC" message is followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Below this is a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2018 Avaya Inc. All rights reserved." is visible.

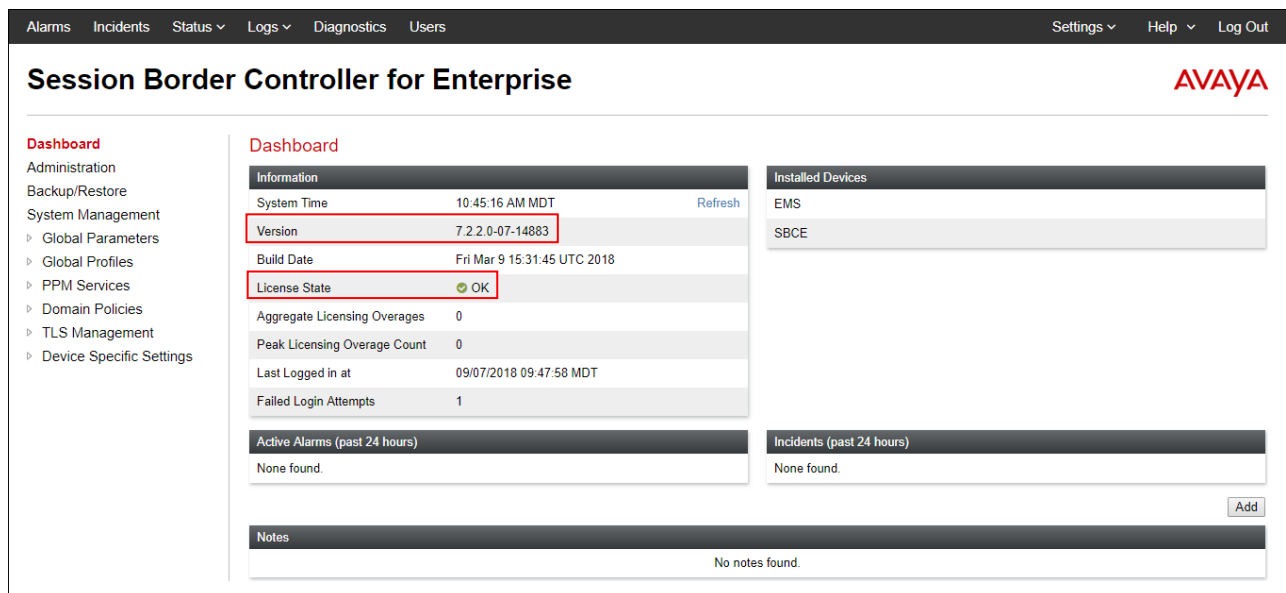
Step 3 - Enter the password and click on **Log In**.



The login screen for the Avaya Session Border Controller for Enterprise. It features the Avaya logo in red on the left. To the right, under the heading "Log In", are fields for "Username:" (containing "ucsec") and "Password:" (masked with dots). A "Log In" button is positioned below the password field. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a warning about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2018 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 for the Avaya Session Border Controller for Enterprise. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. A left-hand navigation menu lists various system management options. The main content area is divided into several sections: "Information" (showing system time, version 7.2.2.0-07-14883, build date, license state OK, and licensing overages), "Installed Devices" (listing EMS and SBCE), "Active Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (None found), and "Notes" (No notes found). The "Version" and "License State" fields in the Information section are highlighted with red boxes.

7.1. System Management – Status

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

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

The screenshot shows the 'System Management' section of the Avaya interface. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management (highlighted), Global Parameters, Global Profiles, PPM Services, and Domain Policies. The main area has tabs for 'Devices', 'Updates', 'SSL VPN', 'Licensing', and 'Key Bundles'. The 'Devices' tab is active, displaying a table with columns: Device Name, Management IP, Version, Status, and a row of action buttons. The table contains one entry for 'SBCE' with Management IP '10.64.90.40', Version '7.2.2.0-07-14883', and Status 'Commissioned'. The 'Restart Application' and 'View' buttons are highlighted with red boxes.

Device Name	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
SBCE	10.64.90.40	7.2.2.0-07-14883	Commissioned						

Step 2 - Click on **View** (shown above) to display the **System Information** screen. The following shows the relevant IP information highlighted in the shared test environment.

The screenshot displays the 'System Information: SBCE' window. It is divided into several sections: General Configuration, Device Configuration, License Allocation, Network Configuration, and DNS Configuration. The Network Configuration section contains a table with IP addresses and interfaces, where the first two rows are highlighted with red boxes. The Management IP(s) section shows the IP #1 (IPv4) as 10.64.90.40.

Appliance Name	SBCE
Box Type	SIP
Deployment Mode	Proxy

HA Mode	No
Two Bypass Mode	No

Standard Sessions	50
Requested: 50	
Advanced Sessions	50
Requested: 50	
Scopia Video Sessions	5
Requested: 5	
CES Sessions	0
Requested: 0	
Transcoding Sessions	50
Requested: 50	
Encryption	<input checked="" type="checkbox"/>

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.91.40	10.64.91.40	255.255.255.0	10.64.91.1	A1
				A1
192.168.200.26	192.168.200.26	255.255.255.248	192.168.200.25	B2
				B1
				B1
				B1

Primary DNS	10.64.90.201
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.64.91.40

IP #1 (IPv4)	10.64.90.40
--------------	-------------

7.2. TLS Management

Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

In the reference configuration, TLS transport is used for the communication between Session Manager and Avaya SBCE. The following procedures show how to create the client and server profiles.

7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Step 1 - Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu includes 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', and 'TLS Management'. Under 'TLS Management', 'Certificates' is selected and highlighted in red. The main content area is titled 'Certificates' and features two buttons: 'Install' and 'Generate CSR'. Below these buttons, there are four sections: 'Installed Certificates' showing 'sbc40.crt' with 'View' and 'Delete' links; 'Installed CA Certificates' showing 'GSSCPSMGRCA.pem' and 'SystemManagerCA.pem' with 'View' and 'Delete' links; 'Installed Certificate Revocation Lists' with a message 'No certificate revocation lists have been installed.'; and 'Installed Keys' showing 'sbc40.key' with a 'Delete' link.

7.2.2. Server Profiles

Step 1 - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbc40.crt**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

The screenshot shows a dialog box titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a red warning box with the following text: "WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems." Below the warning, the dialog is organized into sections. The "TLS Profile" section contains a "Profile Name" text field with the value "sbc40-server" and a "Certificate" dropdown menu currently showing "sbc40.crt". The "Certificate Verification" section contains a "Peer Verification" dropdown menu set to "None". Below this, there is a list box for "Peer Certificate Authorities" containing "GSSCPSMGRCA.pem" and "SystemManagerCA.pem". There is an empty list box for "Peer Certificate Revocation Lists". At the bottom of this section is a "Verification Depth" text field with the value "0". A "Next" button is located at the bottom center of the dialog.

The following screen shows the completed TLS **Server Profile** form:

The screenshot displays a web application interface for configuring TLS Server Profiles. On the left is a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (expanded), Certificates, Client Profiles, **Server Profiles** (highlighted), and Device Specific Settings. The main content area is titled "Server Profiles: sbc40-server" and includes an "Add" button. Below the title is a list of server profiles, with "sbc40-server" selected. The selected profile is shown in a detailed view with the following sections and fields:

- Server Profile** (tab)
- TLS Profile**
 - Profile Name: sbc40-server
 - Certificate: sbc40.crt
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: HIGH:IDH:IDH:IMD5:1aNULL:1eNULL:@STRENGTH

An "Edit" button is located at the bottom right of the profile details.

7.2.3. Client Profiles

Step 1 - Select **TLS Management** → **Server Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbc40.crt**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManagerCA.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.

The screenshot shows a window titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a warning message in an orange box: "WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems." Below the warning, the form is organized into sections. The "TLS Profile" section contains a "Profile Name" text field with the value "sbc40-client" and a clear button (X), and a "Certificate" dropdown menu showing "sbc40.crt". The "Certificate Verification" section has a "Peer Verification" label with the value "Required". Below this is a "Peer Certificate Authorities" list box containing two entries: "GSSCPSMGRCA.pem" and "SystemManagerCA.pem", with the latter selected and highlighted in blue. There is also a "Peer Certificate Revocation Lists" text area which is currently empty. The "Verification Depth" is set to "1" in a text field. The "Extended Hostname Verification" checkbox is unchecked. The "Custom Hostname Override" text field is also empty. At the bottom right of the form is a "Next" button.

The following screen shows the completed TLS **Client Profile** form:

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left-hand menu shows the navigation structure, with 'Client Profiles' highlighted under 'TLS Management'. The main content area is titled 'Client Profiles: sbc40-client'. It features a list of client profiles with 'sbc40-client' selected. The details for this profile are shown in a form with the following sections:

- TLS Profile**
 - Profile Name: sbc40-client
 - Certificate: sbc40.crt
- Certificate Verification**
 - Peer Verification: Required
 - Peer Certificate Authorities: SystemManagerCA.pem
 - Peer Certificate Revocation Lists: ---
 - Verification Depth: 1
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: HIGH:IDH:IDH:IMD5:1aNULL:1eNULL:@STRENGTH

Buttons for 'Add', 'Delete', and 'Edit' are visible at the top and bottom of the form.

7.3. Global Profiles

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

7.3.1. 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.

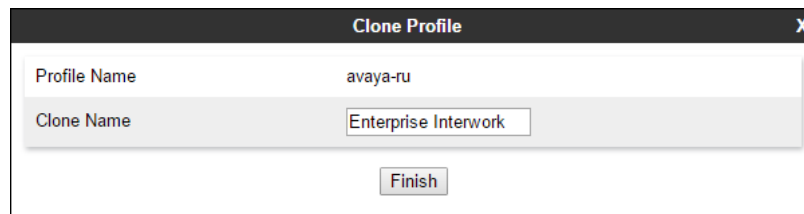
Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left-hand menu shows the navigation structure, with 'Server Interworking' highlighted under 'Global Profiles'. The main content area is titled 'Interworking Profiles: avaya-ru'. It features a list of interworking profiles with 'avaya-ru' selected. The details for this profile are shown in a form with the following sections:

- General**
 - Hold Support: NONE
 - 180 Handling: None

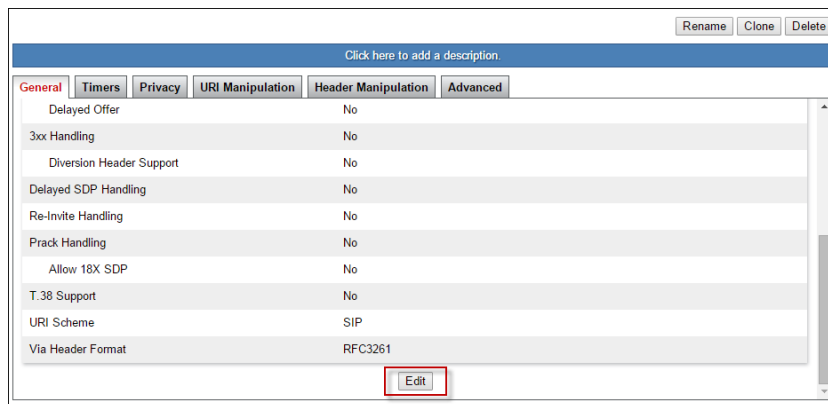
Buttons for 'Add', 'Clone', and 'Edit' are visible at the top of the form. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.'

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



A dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two input fields: "Profile Name" with the value "avaya-ru" and "Clone Name" with the value "Enterprise Interwork". Below these fields is a "Finish" button.

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



A profile configuration screen for "Enterprise Interwork". At the top right are buttons for "Rename", "Clone", and "Delete". Below them is a blue bar with the text "Click here to add a description." and a tabbed interface with tabs for "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is selected, showing a list of settings:

Setting	Value
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

At the bottom center is an "Edit" button, which is highlighted with a red rectangle.

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

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

Editing Profile: Enterprise Interwork

General

Hold Support ☒ None
☐ RFC2543 - c=0.0.0.0
☐ RFC3264 - a=sendonly

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group

Send Hold ☐

Delayed Offer ☐

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

Prack Handling ☐

Allow 18X SDP ☐

T.38 Support ☒

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261
☐ RFC2543

Finish

Step 6 - Returning to the Interworking Profile screen, select the **Advanced** tab, accept the default values, and click **Finish**.

7.3.2. Server Interworking – AT&T

Repeat the steps shown in **Section 7.3.1** 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-Interworking**) 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-Interworking

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 None

Diversion Manipulation ☐

Diversion Condition None

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

MOBX Re-INVITE Handling ☐

DTMF

DTMF Support

☒ None
☐ SIP Notify
☐ RFC 2833 Relay & SIP Notify
☐ SIP Info
☐ RFC 2833 Relay & SIP Info
☐ Inband

Finish

7.3.3. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, one signaling manipulation script is used.

Note – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 7.4.3**) does not meet the desired result. Refer to **[10]** for information on the Avaya SBCE scripting language.

Step 1 - As described in **Section 2.2, Item 4**), Avaya SIP endpoints may send requests with Endpoint-View headers containing private network information. These are removed in **Section 5.3.2**. However, an “epv” parameter is also inserted into the Contact header of these requests. This parameter also contains private network information. The following signaling manipulation is used to remove this “epv” parameter from the Contact header, along with the “gsid” parameter. The “gsid” parameter was removed to further reduce packet size.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **contact_param_bandwidth**). The following script is defined:

```

Title contact_param_bandwidth Save
1 within session "ALL"
2 {
3     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4     {
5
6         //Remove gsid and epv parameters from Contact header to hide internal topology
7         remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
8         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
9     }

```

Step 2 - As described in **Section 2.2, Item 5)**, some Avaya SIP endpoints may send Bandwidth headers that may cause issues with the AT&T network. The following signaling manipulation script is added to the script defined in **Step 1** above, to remove these Bandwidth headers.

1. The following script is added:

```

Title contact_param_bandwidth Save
1 within session "ALL"
2 {
3     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4     {
5
6         //Remove gsid and epv parameters from Contact header to hide internal topology
7         remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
8         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
9
10        //Remove Bandwidth from SDP
11        %BODY[1].regex_replace("b=(TIAS|AS|CT):(\d+)\r\n","");
12    }
13 }

```

Step 3 - As described in **Section 2.2, Item 6)**, AT&T sends SIP OPTIONS messages with Max-Forwards header with a value of "0". The following signaling manipulation script is added to the script defined in **Step 1** above, to change the Max-Forwards header value to "30" for AT&T SIP OPTIONS messages.

1. The following script is added:

```

Title contact_param_bandwidth Save
1 within session "ALL"
2 {
3     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4     {
5
6         //Remove gsid and epv parameters from Contact header to hide internal topology
7         remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
8         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
9
10        //Remove Bandwidth from SDP
11        %BODY[1].regex_replace("b=(TIAS|AS|CT):(\d+)\r\n","");
12    }
13 }
14
15 //OPTIONAL - Change AT&T Max-Forwards value from 0 to 30
16 within session "OPTIONS"
17 {
18     act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
19     {
20         %HEADERS["Max-Forwards"][1] = "30";
21     }
22 }

```

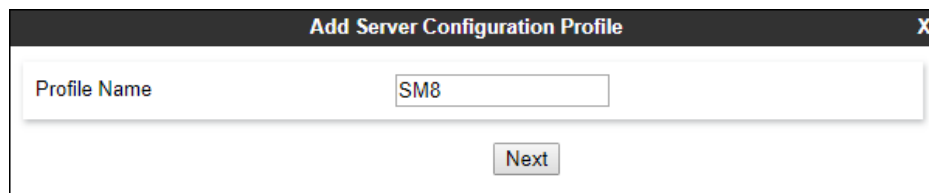
Step 4 - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the AT&T Server Configuration in **Section 7.3.5, Step 3**.

7.3.4. Server Configuration – Session Manager

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

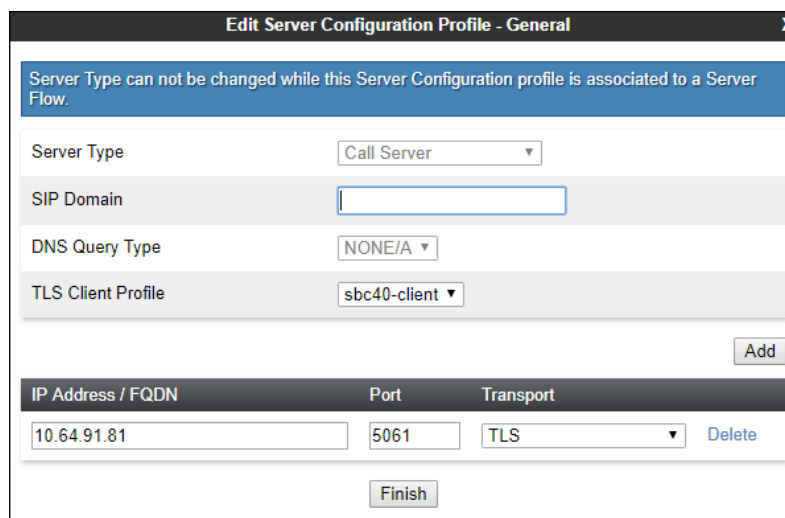
Step 1 - Select **Global Profiles → Server Configuration** from the left-hand menu.

Step 2 - Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM8**) and click **Next**.



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

- Select **Server Type: Call Server**
- **SIP Domain:** Leave blank (default)
- **DNS Query Type:** Select **NONE/A** (default)
- **TLS Client Profile:** Select the profile create in **Section 7.2.3** (e.g., **sbc40-client**)
- **IP Address/FQDN:** **10.64.91.81** (Session Manager network IP address)
- **Transport:** Select **TLS**
- **Port:** **5061**
- Select **Next** (not shown)



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

- Select **Next** to accept default values

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

- Select **Enterprise Interwork** (created in **Section 7.3.1**), for **Interworking Profile**
- Check **Enable Grooming**
- In the **Signaling Manipulation Script** field select **None**
- Select **Finish**

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

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Enterprise Interwork ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Finish

7.3.5. 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 7.3.4**, 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-trk-svr**) and select **Next** (not shown).

Step 2 - On the **General** window, enter the following:

- **Server Type:** Select **Trunk Server**
- **IP Address/FQDN:** **192.168.38.69** (AT&T Border Element IP address)
- **Transport:** Select **UDP**
- **Port:** **5060**

Step 3 – For the additional AT&T Border Element IP addresses, click **Add** and enter the following:

- **IP Address/FQDN:** **192.168.37.149** (AT&T Border Element IP address)
- **Transport:** Select **UDP**
- **Port:** **5060**
- Select **Next** until the Heartbeat tab is reached

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

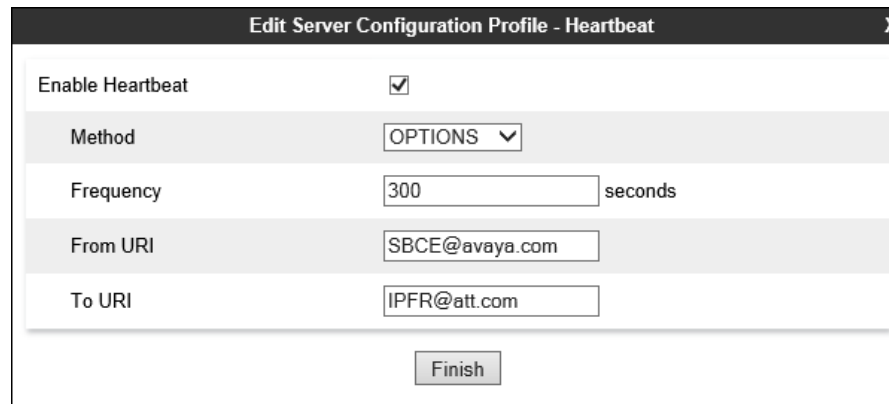
Add

IP Address / FQDN	Port	Transport	
192.168.38.69	5060	UDP	Delete
192.168.37.149	5060	UDP	Delete

Finish

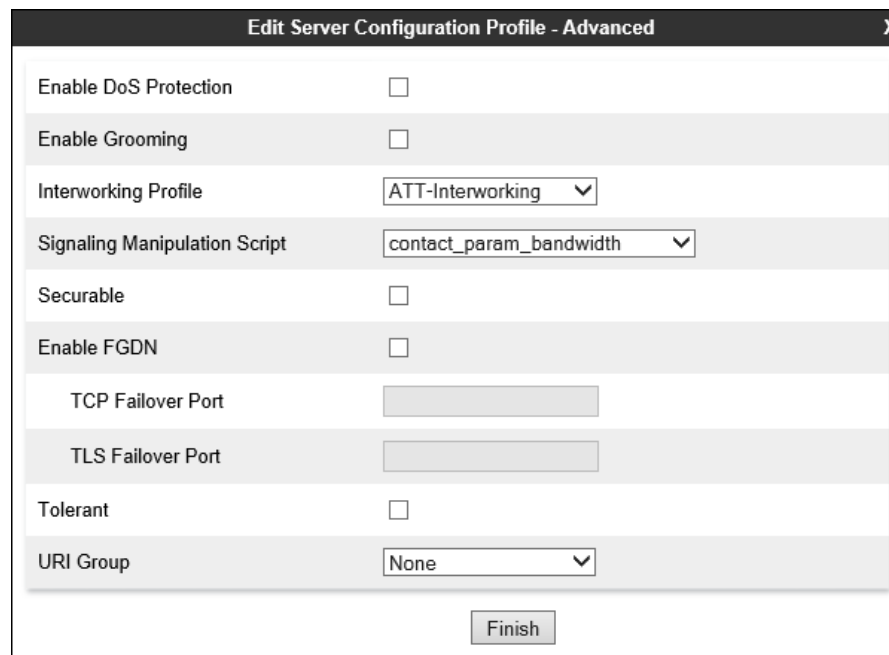
Step 3 - On the **Heartbeat** window, enter the following.

- Check **Enable Heartbeat**
- **Method:** **OPTIONS**
- **Frequency:** **300** seconds
- **From URI:** Enter a descriptive URI, e.g., **SBCE@avaya.com**
- **To URI:** Enter a descriptive URI, e.g., **IPFR@att.com**



Step 4 - On the **Advanced** window, enter the following.

- Select **ATT-Interworking** (created in **Section 7.3.2**), for **Interworking Profile**.
- Select **contact_param_bandwidth** (created in **Section 7.3.3**) for **Signaling Manipulation Script**.
- Select **Finish**.

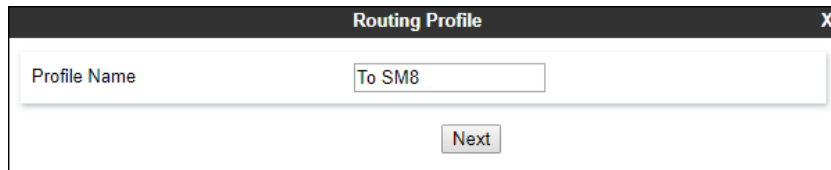


7.3.6. Routing – To Session Manager

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

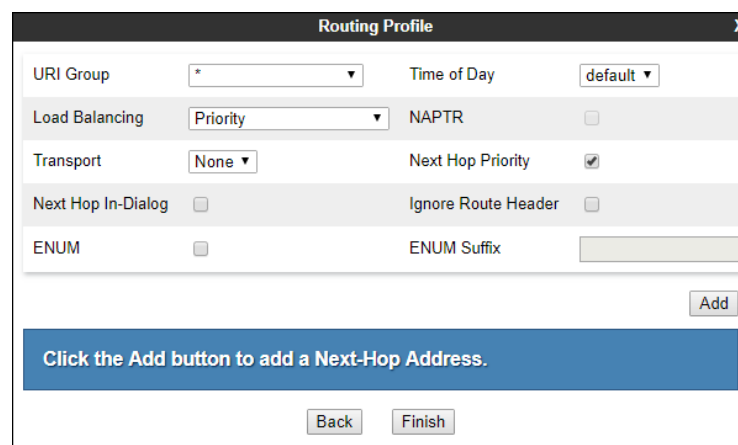
Step 1 - Select **Global Profiles** → **Routing** from the left-hand menu, and select **Add** (not shown)

Step 2 - Enter a **Profile Name**: (e.g., **To SM8**) and click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "To SM8". Below the input field is a button labeled "Next".

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



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. The window contains several configuration options: "URI Group" with a dropdown menu showing "*", "Time of Day" with a dropdown menu showing "default", "Load Balancing" with a dropdown menu showing "Priority", "NAPTR" with a checkbox, "Transport" with a dropdown menu showing "None", "Next Hop Priority" with a checked checkbox, "Next Hop In-Dialog" with an unchecked checkbox, "Ignore Route Header" with an unchecked checkbox, "ENUM" with an unchecked checkbox, and "ENUM Suffix" with a text input field. At the bottom right is an "Add" button. Below the "Add" button is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the bottom of the window are "Back" and "Finish" buttons.

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

- **Priority/Weight** = **1**
- **Server Configuration** = **SM8** (from **Section 7.3.4**).
- **Next Hop Address**: Verify that the **10.64.91.81:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** fields are grayed out.
- Click on **Finish**.

Profile : To SM8 - Edit Rule

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"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	SM8	10.64.91.81:5061 (TLS)	None	Delete

Finish

7.3.7. Routing – To AT&T

Repeat the steps in **Section 7.3.6**, 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., **To ATT IPFR**).

Step 2 - On the **Next-Hop Address** window, populate the following fields:

- **Priority/Weight = 1**
- **Server Configuration = ATT-trk-svr (from Section 7.3.5).**
- **Next Hop Address: select 192.168.38.69:5060 (UDP).**

Step 3 - For the additional AT&T Border Element, click **Add** and enter the following:

- **Priority/Weight = 2**
- **Server Configuration = ATT-trk-svr (from Section 7.3.5).**
- **Next Hop Address: select 192.168.37.149:5060 (UDP).**

Step 4 - Click **Finish**.

Profile : To ATT IPFR - Edit Rule

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"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	ATT-trk-svr	192.168.38.69:5060 (UDP)	None	Delete
2	ATT-trk-svr	192.168.37.149:5060 (UDP)	None	Delete

Finish

7.3.8. Topology Hiding – Enterprise Side

The **Topology Hiding** screen 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.

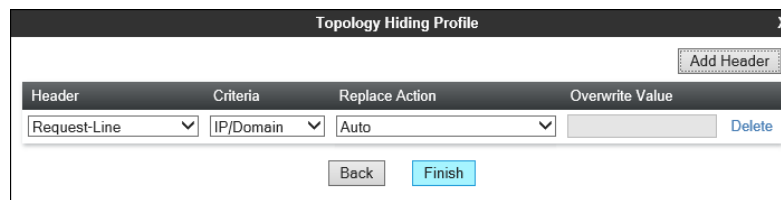
Step 1 - Select **Global Profiles → Topology Hiding** from the left-hand side menu.

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

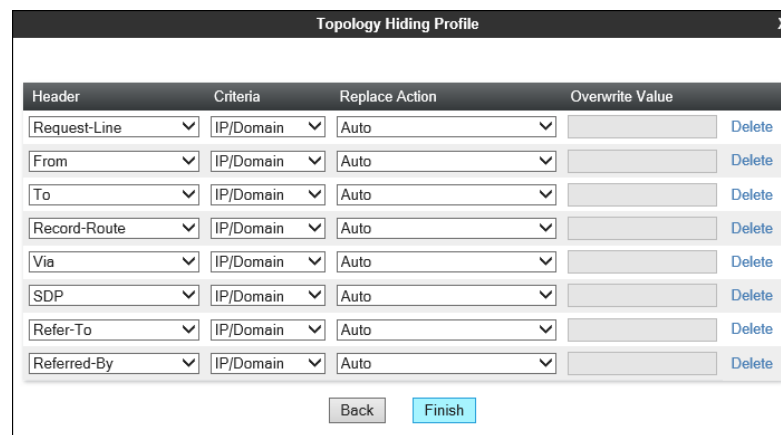


The screenshot shows a window titled "Topology Hiding Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Enterprise-Topology". Below the input field is a button labeled "Next".

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



The screenshot shows the "Topology Hiding Profile" window with the "Add Header" button in the top right corner. Below the button is a table with the following columns: "Header", "Criteria", "Replace Action", "Overwrite Value", and "Delete". The table contains one row with the following values: "Request-Line" for Header, "IP/Domain" for Criteria, "Auto" for Replace Action, an empty field for Overwrite Value, and a "Delete" button. At the bottom of the window are "Back" and "Finish" buttons.



The screenshot shows the "Topology Hiding Profile" window with the "Add Header" button in the top right corner. Below the button is a table with the following columns: "Header", "Criteria", "Replace Action", "Overwrite Value", and "Delete". The table contains eight rows with the following values: "Request-Line", "From", "To", "Record-Route", "Via", "SDP", "Refer-To", and "Referred-By" for Header; "IP/Domain" for Criteria; "Auto" for Replace Action; an empty field for Overwrite Value; and a "Delete" button. At the bottom of the window are "Back" and "Finish" buttons.

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

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

Finish

7.3.9. Topology Hiding – AT&T Side

Repeat the steps in **Section 7.3.8**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

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

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

Finish

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy Policy, and RADIUS. The main content area is titled 'Topology Hiding Profiles: SIP-Trunk-Topology'. It features a list of profiles on the left: default, cisco_th_profile, Enterprise-Topology, SIP-Trunk-Topology (highlighted with a red box), and IPOSE-Topology. An 'Add' button is located above this list. On the right, there is a description field with the placeholder text 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a 'Topology Hiding' tab with a table showing header criteria and their replacement actions. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The rows are: From (IP/Domain, Auto, ---), Request-Line (IP/Domain, Auto, ---), Referred-By (IP/Domain, Auto, ---), Record-Route (IP/Domain, Auto, ---), SDP (IP/Domain, Auto, ---), Refer-To (IP/Domain, Auto, ---), Via (IP/Domain, Auto, ---), and To (IP/Domain, Auto, ---). An 'Edit' button is located at the bottom right of the table.

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

7.4. 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.

7.4.1. 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**
- Click **Finish** (not shown). The completed **Application Rule** is shown below.

The screenshot shows the 'Application Rules: sip-trunk' configuration page. On the left is a navigation menu with 'Domain Policies' expanded and 'Application Rules' selected. The main area shows a list of application rules on the left, with 'sip-trunk' highlighted. The right side displays the configuration for the 'sip-trunk' rule, including a table for Application Type (Audio, Video) and a Miscellaneous section for CDR Support and RTCP Keep-Alive.

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	Off
RTCP Keep-Alive	No

7.4.2. Media Rules

Media Rules are used to define media encryption and QoS parameters. Separate media rules are created for AT&T and Session Manager.

7.4.2.1 Enterprise – Media Rule

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

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

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

- In the **Clone Name** field enter **enterprise med rule**
- Click **Finish**. The newly created rule will be displayed.

Step 4 - Highlight the **enterprise med rule** just created (not shown):

- Select the **Encryption** tab (not shown).
- Click the **Edit** button and the **Media Encryption** window will open.
- Select **RTP** from the drop-down for **Preferred Format #2** in the Audio and Video Encryption sections.
- In the **Miscellaneous** section, check **Capability Negotiation**.
- Click **Finish**

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^A <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^A <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input checked="" type="checkbox"/>

Finish

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

The screenshot shows the 'Media QoS' configuration window. It has a title bar 'Media QoS' with a close button 'X'. Inside, there's a section 'Media QoS Marking'. Under this, 'Enabled' is checked. Below that, there are two radio buttons: 'ToS' (unselected) and 'DSCP' (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). Under 'DSCP', there are two rows: 'Audio' (EF, 101110) and 'Video' (EF, 101110). At the bottom, there is a 'Finish' button.

7.4.2.2 AT&T – Media Rule

Repeat the steps in **Section 7.4.2.1**, with the following changes, to create a Media Rule for AT&T.

1. From the Media Rules menu, select the **default-low-med** rule
2. In the **Clone Name** field enter **att med rule**

The completed **att med rule** screen is shown below.

The screenshot shows the 'Media Rules' configuration screen. On the left is a sidebar with a menu: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies (Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, End Point Policy Groups, Session Policies), TLS Management, and Device Specific Settings. The 'Media Rules' section is selected. The main area is titled 'Media Rules: att med rule'. It has an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this is a blue bar with the text 'Click here to add a description.' There are four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Both sections have 'Preferred Formats' set to 'RTP' and 'Interworking' checked. There is also a 'Miscellaneous' section with 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right.

7.4.3. Signaling Rules

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

7.4.3.1 Enterprise – 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.

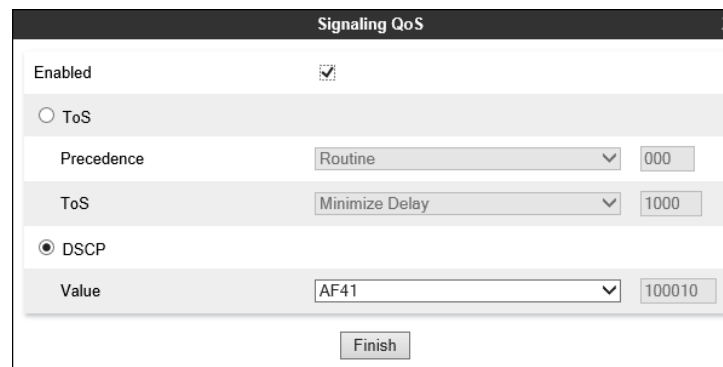
Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

- In the **Rule Name** field enter **enterprise sig rule**
- Click **Finish**. The newly created rule will be displayed (not shown).

Step 4 - Highlight the **enterprise sig 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 = AF41**

Step 5 - Click **Finish**.



The screenshot shows the 'Signaling QoS' configuration window. It has a title bar with 'Signaling QoS' and a close button. The window contains several settings: 'Enabled' is checked with a checkbox; 'ToS' is selected with a radio button; 'Precedence' is set to 'Routine' in a dropdown menu with a value of '000'; 'ToS' is set to 'Minimize Delay' in a dropdown menu with a value of '1000'; 'DSCP' is selected with a radio button; 'Value' is set to 'AF41' in a dropdown menu with a value of '100010'. A 'Finish' button is at the bottom right.

7.4.3.2 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).

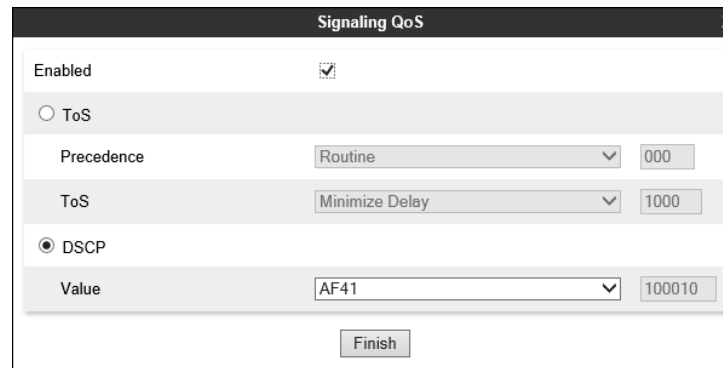
Step 3 - From the Signaling Rules menu, select the **default** rule.

Step 4 - Select **Clone Rule** button

- Enter a name: **att sig rule**

Step 5 - Click **Finish**

Step 6 - Highlight the **att sig rule**, select the **Signaling QoS** tab and repeat **Steps 4 & 5** from **Section 7.4.3.1**



The image shows a 'Signaling QoS' configuration window. It has a title bar with 'Signaling QoS' and a close button. Inside, there's a section 'Enabled' with a checked checkbox. Below that, there are three radio buttons: 'ToS', 'DSCP', and 'DSCP' (which is selected). Under 'ToS', there are fields for 'Precedence' (set to 'Routine') and 'ToS' (set to 'Minimize Delay'). Under 'DSCP', there is a 'Value' field (set to 'AF41'). At the bottom, there is a 'Finish' button.

7.4.4. Endpoint Policy Groups – Enterprise Connection

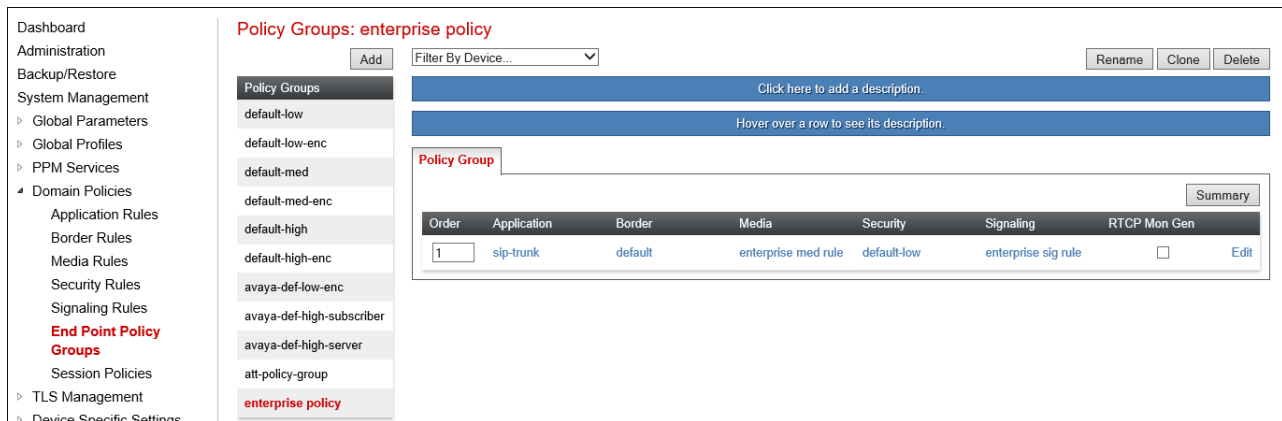
Step 1 - Select **Domain Policies** from the menu on the left-hand side.

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

Step 3 - Select **Add**.

- **Name:** enterprise policy
- **Application Rule:** sip-trunk (created in **Section 7.4.1**)
- **Border Rule:** default
- **Media Rule:** enterprise med rule (created in **Section 7.4.2**)
- **Security Rule:** default-low
- **Signaling Rule:** enterprise sig rule (created in **Section 7.4.3.1**)

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



The image shows the 'Policy Groups: enterprise policy' screen. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area shows a list of policy groups. The 'enterprise policy' group is selected and its details are shown in a table below.

Order	Application	Border	Media	Security	Signaling	RTCP Mon Gen	
1	sip-trunk	default	enterprise med rule	default-low	enterprise sig rule	<input type="checkbox"/>	Edit

7.4.5. Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps 1 through 4 from Section 7.4.4 with the following changes:

- **Group Name:** att-policy-group
- **Media Rule:** att med rule (created in Section 7.4.2.2)
- **Signaling Rule:** att sig rule (created in Section 7.4.3.2)

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

The screenshot shows the 'Policy Groups: att-policy-group' configuration page. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, End Point Policy Groups (highlighted), Session Policies, TLS Management, and Device Specific Settings. The main area has a 'Policy Groups' list on the left with 'att-policy-group' selected. The right side shows a table for the selected group. The table has columns: Order, Application, Border, Media, Security, Signaling, RTCP Mon Gen, and a Summary/Action column. The first row shows Order 1, Application sip-trunk, Border default, Media att med rule, Security default-low, Signaling att sig rule, RTCP Mon Gen checkbox, and an Edit link.

Order	Application	Border	Media	Security	Signaling	RTCP Mon Gen	Summary
1	sip-trunk	default	att med rule	default-low	att sig rule	<input type="checkbox"/>	Edit

7.5. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.5.1. 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 B2 (public) interfaces are used.

The screenshot shows the 'Network Management: SBCE' page. The left navigation menu is the same as in the previous screenshot, with 'Network Management' highlighted. The main area has two tabs: 'Interfaces' (selected) and 'Networks'. The 'Interfaces' tab shows a table with columns: Interface Name, VLAN Tag, and Status. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Enabled). There is an 'Add VLAN' button in the top right corner of the table area.

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Enabled

Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B2 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.

Network Management: SBCE

Devices SBCE

Interfaces Networks

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.40	Edit Delete
Outside-B2	192.168.200.25	255.255.255.248	B2	192.168.200.26	Edit Delete

7.5.2. Advanced Options

In **Section 7.5.3**, 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 7.5.3**.

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 **12000 – 16380**

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: SBCE

Devices SBCE

CDR Listing Feature Control SIP Options Network Options Port Ranges RTCP Monitoring Load Monitoring

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

Port Range Configuration	
Signaling Port Range	12000 - 16380
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	6000 - 6999
HTTP Port Range	51001 - 62000

Save

7.5.3. Media Interfaces

As mentioned in **Section 7.5.2**, 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-Media-Interface**
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.40**
- **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-B2-Media**
- **IP Address:** Select **Outside-B2 (B2, VLAN0)** and **192.168.200.26**
- **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 in the shared test environment is shown below.

Media Interface: SBCE			
Devices		Media Interface	
SBCE		Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management .	
		Add	
Name	Media IP Network	Port Range	
Outside-B2-Media	192.168.200.26 Outside-B2 (B2, VLAN 0)	16384 - 32767	Edit Delete
Inside-Media-Interface	10.64.91.40 Inside-A1 (A1, VLAN 0)	16384 - 32767	Edit Delete

7.5.4. 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-Sig-40**
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.40**
- **TLS Port:** **5061**
- **TLS Profile:** Select the TLS server profile created in **Section 7.2.2** (e.g., **sbc40-server**)

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

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

- **Name:** **Outside-B2-Signaling**
- **IP Address:** Select **Outside-B2 (B2, VLAN0)** and **192.168.200.26**

- **UDP Port: 5060**

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

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile
Outside-B2-Signaling	192.168.200.26 Outside-B2 (B2, VLAN 0)	---	5060	---	None
Inside-Sig-40	10.64.91.40 Inside-A1 (A1, VLAN 0)	---	---	5061	sbc40-server

7.5.5. Server 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:** Session Manager flow.
- **Server Configuration:** EnterpriseCallServer (Section 7.3.4).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Outside-B2-Signaling (Section 7.5.4).
- **Signaling Interface:** Inside-Sig-40 (Section 7.5.4).
- **Media Interface:** Inside-Media-Interface (Section 7.5.3).
- **End Point Policy Group:** enterprise policy (Section 7.4.4).
- **Routing Profile:** To ATT IPFR (Section 7.3.7).
- **Topology Hiding Profile:** Enterprise-Topology (Section 7.3.8).
- Let other values default.

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

View Flow: Session Manager flow			
Criteria		Profile	
Flow Name	Session Manager flow	Signaling Interface	Inside-Sig-40
Server Configuration	EnterpriseCallServer	Media Interface	Inside-Media-Interface
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	enterprise policy
Remote Subnet	*	Routing Profile	To ATT IPFR
Received Interface	Outside-B2-Signaling	Topology Hiding Profile	Enterprise-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any

7.5.6. Server Flows – For AT&T

Step 1 - Repeat steps 1 through 4 from **Section 7.5.5**, with the following changes:

- **Flow Name:** IPFR flow.
- **Server Configuration:** ATT-trk-svr (Section 7.3.5).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Inside-Sig-40 (Section 7.5.4).
- **Signaling Interface:** Outside-B2-Signaling (Section 7.5.4).
- **Media Interface:** Outside-B2-Media (Section 7.5.3).
- **End Point Policy Group:** att-policy-group (Section 7.4.5).
- **Routing Profile:** To SM (Section 7.3.6).
- **Topology Hiding Profile:** SIP-Trunk-Topology (Section 7.3.9).

View Flow: IPFR flow			
Criteria		Profile	
Flow Name	IPFR flow	Signaling Interface	Outside-B2-Signaling
Server Configuration	ATT-trk-svr	Media Interface	Outside-B2-Media
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	att-policy-group
Remote Subnet	*	Routing Profile	To SM
Received Interface	Inside-Sig-40	Topology Hiding Profile	SIP-Trunk-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any

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., Aura® 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.

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., *05). 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 14008, before sending the INVITE to Communication Manager.

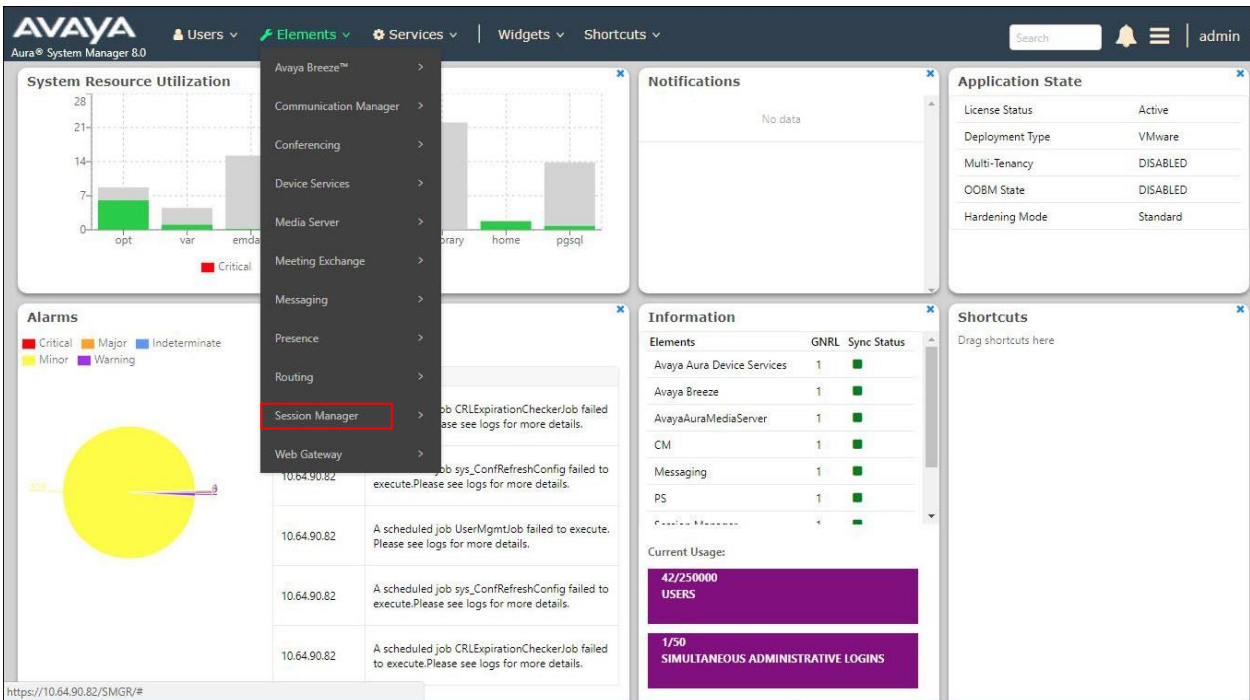
```
list trace tac *05                                     Page 1
LIST TRACE
time      data
10:00:13 TRACE STARTED 05/01/2018 CM Release String cold-01.0.532.0-24184
10:00:35 SIP<INVITE sips:14008@avayalab.com SIP/2.0
10:00:35      Call-ID: a373e03114bedb008ccbbe51c080a624
10:00:35      active trunk-group 5 member 1      cid 0x508
10:00:35      dial 14008
10:00:35      term station      14008 cid 0x508
10:00:35      Called party uses private-numbering
10:00:35 SIP>INVITE sips:14008@avayalab.com SIP/2.0
10:00:35      Call-ID: c8925424d5841e897220c292817b9
10:00:35 SIP<SIP/2.0 100 Trying
10:00:35      Call-ID: c8925424d5841e897220c292817b9
10:00:35 SIP<INVITE sips:14008@avayalab.com SIP/2.0
10:00:35      Call-ID: c8925424d5841e897220c292817b9
10:00:35 SIP>INVITE sips:14008@avayalab.com SIP/2.0
10:00:35      Call-ID: c8925424d5841e897220c292817b9
```

- 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 is **1** alarm out of the **14** Entities defined.

Session Manager

Dashboard

Session Manager Admin...

Global Settings

Communication Profile ...

Network Configuration

Device and Location ...

Application Configur...

System Status

Session Manager Dashboard

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

Session Manager Instances

Service State

Shutdown System

EASG

As of 10:43 AM

1 Item

Show

All

Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	1/14	0	7/7	⚠	✓	Normal	Enabled	8.0.0.0.800035

Select : All, None

Step 3 - Clicking on the **1/14** entry (shown above) in the **Entity Monitoring** column, results in the following display:

<div>Session Manager</div> <div>Dashboard</div> <div>Session Manager Admin...</div> <div>Global Settings</div> <div>Communication Profile ...</div> <div>Network Configuration ...</div> <div>Device and Location ...</div> <div>Application Configur...</div> <div>System Status</div> <div>System Tools</div> <div>Performance</div>										
Session Manager Entity Link Connection Status This page displays detailed connection status for all entity links from a Session Manager.										
Status Details for the selected Session Manager:										
All Entity Links for Session Manager: Session Manager Summary View										
14 Items Filter: Enable										
<input type="radio"/>	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status	
<input type="radio"/>	Aura Messaging	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	ExperiencePortal	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	Breeze	IPv4	10.64.91.18	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	CM-TG4	IPv4	10.64.91.75	5064	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	Presence	IPv4	10.64.91.18	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	CM-TG3	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	CM-TG2	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	CM-TG1	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	SBCE-ATT	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP	
<input type="radio"/>	SBCE-Toll Free	IPv4	10.64.91.41	5061	TLS	FALSE	UP	405 Method Not Allowed	UP	
<input type="radio"/>	CM-TG5	IPv4	10.64.91.75	5065	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	SBC2	IPv4	10.64.91.100	5061	TLS	FALSE	UP	403 Forbidden	UP	
<input type="radio"/>	SBC1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP	
<input type="radio"/>	IP500	IPv4	10.64.19.70	5061	TLS	FALSE	DOWN	408 Request Timeout	DOWN	
Select : None										

Note – The **SBCE-ATT** 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, Status, Logs, Diagnostics, and Users**. In addition, the most recent Incidents are listed in the lower right of the Dashboard screen.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) Dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main dashboard area is divided into several sections:

- Information:** System Time (10:50:40 AM MDT), Version (7.2.2.0-07-14883), Build Date (Fri Mar 9 15:31:45 UTC 2018), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (10/30/2018 08:41:28 MDT), and Failed Login Attempts (0).
- Installed Devices:** EMS, SBCE.
- Active Alarms (past 24 hours):** None found.
- Incidents (past 24 hours):** SBCE : Phone Stealth DDOS Detected.
- Notes:** No notes found.

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 B2 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: TEST.pcap
Using the name of an existing capture will overwrite it.

Start Capture Clear

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

Trace: 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: TEST.pcap
Using the name of an existing capture will overwrite it.

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	Packet Capture	Captures		
SBCE	Last Modified ▾	Descending ▾	Sort	Reset
				Refresh
File Name	File Size (bytes)	Last Modified		
TEST_20170612112410.pcap	270,336	June 12, 2017 11:24:50 AM MDT		Delete

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.2, 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 and Branch Session Manager in Virtualized Environment, Release 8.0, Issue 2, August 2018
- [2] Administering Avaya Aura® Session Manager, Release 8.0, Issue 2, August 2018
- [3] Deploying Avaya Aura® System Manager in Virtualized Environment, Release 8.0, Issue 2, September 2018
- [4] Administering Avaya Aura® System Manager for Release 8.0, Issue 4, September 2018

Avaya Aura® Communication Manager

- [5] Deploying Avaya Aura® Communication Manager in Virtualized Environment, Release 8.0, Issue 4, September 2018
- [6] Administering Avaya Aura® Communication Manager, Release 8.0, Issue 1, July 2018
- [7] Administering Avaya G450 Branch Gateway, Release 8.0, Issue 1, July 2018
- [8] Deploying and Updating Avaya Aura® Media Server Appliance, Release 8.0, Issue 2, July 2018
- [9] Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager, August 2015

Avaya Session Border Controller for Enterprise

- [10] Administering Avaya Session Border Controller for Enterprise, Release 7.2.2, Issue 9, April 2018
- [11] Deploying Avaya Session Border Controller for Enterprise, Release 7.2.2, Issue 7, April 2018

Avaya Aura® Messaging

- [12] Administering Avaya Aura® Messaging, Release 7.0.0, Issue 4, April 2018

AT&T IP Flexible Reach - Enhanced Features Service:

- [13] 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/>

©2018 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.