



## Avaya Solution & Interoperability Test Lab

# **Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1 with AT&T IP Flexible Reach - Enhanced Features using IPv6 – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1, with the AT&T IP Flexible Reach - Enhanced Features service, using IPv6 and AT&T's **AVPN** or **MIS/PNT** transport connections.

The AT&T Flexible Reach is one of several 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.....	6
2.1.	Interoperability Compliance Testing.....	7
2.2.	Test Results .....	8
2.3.	Support .....	10
2.4.	SIP Message – Packet Optimization .....	10
3.	Reference Configuration.....	11
3.1.	Illustrative Configuration Information .....	13
3.2.	Call Flows .....	14
3.2.1.	Inbound Call.....	14
3.2.2.	Outbound Call.....	15
3.2.3.	Call Forward Redirection.....	16
3.2.4.	Network Based Blind Transfer Call Flow (Communication Manager Vector).....	17
3.2.5.	Network Based Attended/Unattended Transfer Call Flow initiated by Communication Manager Station.....	18
4.	Equipment and Software Validated .....	19
5.	Configure Avaya Aura® Communication Manager.....	20
5.1.	Enable IPv6 addressing .....	20
5.2.	Verify Licensed Features .....	21
5.3.	System-Parameters Features .....	23
5.4.	System-Parameters IP-Options .....	24
5.5.	Processor Ethernet Configuration .....	24
5.6.	Node Names .....	25
5.7.	Dial Plan.....	26
5.8.	IP Network Regions .....	27
5.8.1.	IP Network Region 1 – Local CPE Region .....	27
5.8.2.	IP Network Region 6 – AT&T Trunk Region .....	29
5.9.	IP Codec Sets .....	30
5.9.1.	Codecs for IP Network Region 1 (calls within the CPE).....	30
5.9.2.	Codecs for IP Network Region 6 (calls to/from AT&T) .....	31
5.10.	SIP Trunks .....	32
5.10.1.	SIP Trunk for Inbound/Outbound AT&T calls .....	32
5.10.2.	Local SIP Trunk (Avaya SIP Telephone, Messaging Access, etc.) .....	36
5.11.	Public Numbering.....	37
5.12.	Private Numbering.....	38
5.13.	Route Patterns.....	38
5.13.1.	Route Pattern for National Calls to AT&T .....	38
5.13.2.	Route Pattern for International Calls to AT&T.....	39
5.13.3.	Route Pattern for Service Calls to AT&T .....	40
5.13.4.	Route Pattern for Calls within the CPE.....	40
5.14.	Automatic Route Selection (ARS) Dialing .....	41
5.15.	Automatic Alternate Routing (AAR) Dialing .....	41
5.16.	Avaya G450 Media Gateway Provisioning.....	42
5.17.	Avaya Aura® Media Server Provisioning.....	43
5.18.	Save Translations.....	46

5.19.	Verify TLS Certificates – Communication Manager .....	47
6.	Configure Avaya Aura® Session Manager .....	48
6.1.	System Manager Login and Navigation .....	49
6.2.	Enable Session Manager IPv6 Support .....	50
6.3.	SIP Domain .....	51
6.4.	Locations .....	52
6.4.1.	Main Location .....	52
6.4.2.	CM-TG-7 Location .....	52
6.4.3.	SBCE-IPv6 Location .....	52
6.5.	Configure Adaptations .....	53
6.5.1.	Adaptation for Avaya Aura® Communication Manager Extensions .....	53
6.5.2.	Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service .....	55
6.6.	SIP Entities .....	56
6.6.1.	Avaya Aura® Session Manager SIP Entity .....	56
6.6.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk .....	58
6.6.3.	Avaya Session Border Controller for Enterprise SIP Entity .....	59
6.6.4.	Avaya Aura® Communication Manager SIP Entity – Local Trunk .....	60
6.7.	Entity Links .....	61
6.7.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk .....	61
6.7.2.	Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE .....	62
6.7.3.	Entity Link to Avaya Aura® Communication Manager – Local Trunk .....	62
6.8.	Time Ranges – (Optional) .....	63
6.9.	Routing Policies .....	63
6.9.1.	Routing Policy for Inbound Calls to Avaya Aura® Communication Manager .....	63
6.9.2.	Routing Policy for Outbound Calls to AT&T .....	65
6.10.	Dial Patterns .....	66
6.10.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager .....	66
6.10.2.	Matching Outbound Calls to AT&T .....	68
6.11.	Security Module Configuration .....	69
6.12.	Verify TLS Certificates – Session Manager .....	70
7.	Configure Avaya Session Border Controller for Enterprise .....	72
7.1.	Device Management – Status .....	73
7.2.	TLS Management .....	75
7.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	75
7.2.2.	Server Profiles .....	76
7.2.3.	Client Profiles .....	77
7.3.	Network Management .....	78
7.4.	Advanced Options .....	80
7.5.	Media Interfaces .....	81
7.6.	Signaling Interfaces .....	83
7.7.	Server Interworking Profiles .....	84
7.7.1.	Server Interworking Profile – Enterprise .....	84
7.7.2.	Server Interworking – AT&T .....	85
7.8.	Signaling Manipulation .....	87
7.9.	SIP Server Profiles .....	88

7.9.1.	SIP Server Profile – Session Manager .....	88
7.9.2.	SIP Server Profile – AT&T.....	90
7.10.	Routing Profiles.....	92
7.10.1.	Routing Profile – Session Manager.....	92
7.10.2.	Routing Profile – AT&T .....	93
7.11.	Topology Hiding Profiles .....	94
7.11.1.	Topology Hiding – Enterprise.....	94
7.11.2.	Topology Hiding – AT&T .....	95
7.12.	Application Rules .....	95
7.13.	Media Rules.....	96
7.13.1.	Media Rule – Enterprise.....	96
7.13.2.	Media Rule – AT&T .....	99
7.14.	Signaling Rules.....	100
7.14.1.	Signaling Rule – Enterprise.....	100
7.14.2.	Signaling Rule – AT&T .....	100
7.15.	Endpoint Policy Groups.....	101
7.15.1.	End Point Policy Group – Enterprise .....	101
7.15.2.	Endpoint Policy Group – AT&T.....	102
7.16.	Endpoint Flows – Server Flows .....	102
7.16.1.	Server Flows – Enterprise .....	103
7.16.2.	Server Flow – AT&T .....	104
8.	AT&T IP Flexible Reach – Enhanced Features Configuration .....	105
9.	Verification Steps.....	105
9.1.	AT&T IP Flexible Reach – Enhanced Features .....	105
9.2.	Avaya Aura® Communication Manager Verification .....	106
9.3.	Avaya Aura® Session Manager Verification.....	108
9.4.	Avaya Session Border Controller for Enterprise Verification .....	110
9.4.1.	Incidents.....	110
9.4.2.	Server Status .....	111
9.4.3.	Diagnostic .....	112
9.4.4.	Protocol Traces .....	112
10.	Conclusion .....	114
11.	References.....	115
12.	Appendix A – Configuration for Fax Testing.....	116
12.1.	Configuration Changes for T.38 Fax .....	116
12.2.	Configuration Changes for G.711 Fax .....	118
13.	Appendix B – Avaya SBCE – SigMa Script File .....	120

# 1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise Release 8.1, with the AT&T IP Flexible Reach - Enhanced Features service using IPv6, over AT&T's AVPN or MIS/PNT transport connections.

Avaya Aura® Communication Manager 8.1 (Communication Manager) is the telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 8.1 (Session Manager) is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise.

The Avaya Session Border Controller for Enterprise 8.1 (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.

Avaya Aura applications support dual stack architecture, where IPv4 and IPv6 can be supported simultaneously. These Application Notes show a configuration where IPv6 is used in the SIP trunk between the Avaya SBCE public side and the IPFR Border Element. On the enterprise (private) side, both IPv4/IPv6 are used, with IPv6 being implemented over an existing platform already supporting IPv4 addresses.

The AT&T Flexible Reach service is one of several 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 AVPN<sup>1</sup> or MIS/PNT<sup>2</sup> transport services.

**Note** – The AT&T IP Flexible Reach - Enhanced Features service will be referred to as IPFR-EF in the remainder of this document.

---

<sup>1</sup> AVPN supports compressed RTP (cRTP).

<sup>2</sup> MIS/PNT does not support cRTP.

## 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, connected to the simulated enterprise via AVPN transport.

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 IP Flexible Reach service did not include use of any specific encryption features as requested by AT&T.

## 2.1. Interoperability Compliance Testing

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 AT&T IPFR-EF network. Calls were made between the PSTN, via the AT&T IPFR-EF network, and the CPE.

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

- Inbound and outbound voice calls between telephones controlled by the CPE and the PSTN using G.729A and G.711MU codecs. Phone types included SIP, H.323, digital and analog telephones at the enterprise.
- DTMF using RFC 2833
  - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system).
  - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Aura® Messaging, Communication Manager vector digit collection steps).
- Requests for privacy 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.
- Additional PSTN numbering plans (e.g., operator assist, toll-free and International).
- Telephony features such as hold, transfer, and conference.
- SIP Diversion Header for call redirection.
  - Call Forwarding
  - EC500
- Long duration calls.
- Inbound/Outbound fax calls using T.38 and G.711 pass-through.
- 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.
- Direct IP-to-IP media redirection in the enterprise (shuffling).
- Use of Alternative Network Address Types (ANAT) for SDP negotiation in the enterprise.

An Avaya Remote Worker endpoint (Avaya IX™ Workplace Client for Windows SIP softphone) 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. The configuration of the Remote Worker environment is beyond the scope of this document.

**Note** – Documents used to provision the test environment are listed in **Section 11**. In the following sections, references to these documents are indicated by the notation [x], where x is the document reference number.

## 2.2. Test Results

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

- 1) **IPFR-EF Call Forward Always (CFA/CFU) – No ringing heard for Ring Splash reminder.** When Call Forward is activated with the Ring Splash feature (ring reminder on call forward) through the IPFR-EF service, and a call is placed to the primary number, no indication is seen on the CPE endpoint. The c-line in the SDP of the Ring Splash SIP INVITE has a domain name “anonymous.invalid” instead of an IPv6 address, and this was rejected by the Avaya SBCE. A workaround is to include an Avaya SBCE Signaling Manipulation Rule to change the domain name to an IPv6 address (See **Section 7.8**). After the script is applied, the CPE endpoint’s call appearance will flash briefly to indicate that the call has been forwarded, but the IPFR-EF service may send a CANCEL before the endpoint has had a chance to provide an audible ring tone.
- 2) **Avaya SBCE does not change the Diversion header from sips to sip.** When TLS/SRTP is used within the enterprise, the SIP headers include the SIPS URI scheme for Secure SIP. The Avaya SBCE converts these header schemes from SIPS to SIP when it sends the SIP message toward AT&T. However, for call forward and EC500 calls, the Avaya SBCE was not changing the Diversion header scheme as expected. This caused these call types that require a Diversion header to fail, since Secure SIP is not supported on the SIP trunk to AT&T. This anomaly is currently under investigation by the Avaya SBCE development team. A workaround is to include an Avaya SBCE Signaling Manipulation (SigMa) script on the AT&T SIP Server profile on the Avaya SBCE, to convert “sips” to “sip” in the Diversion header. See **Section 7.8**.
- 3) **Faxes do not complete when using Alternative Network Address Type on the Avaya SBCE.** During the compliance test, both IPv4 and/or IPv6 addresses were used across different devices on the private network. The Alternative Network Address Type (ANAT) feature was enabled in Communication Manager and the Avaya SBCE as a mechanism to achieve media level interworking between IPv4 and IPv6 on the enterprise network. See **Section 5.8** and **Section 7.13**. During fax testing, it was observed that the Avaya SBCE rejected the T.38 re-INVITEs arriving from Communication Manager or AT&T when ANAT was enabled on the SBCE, and faxes failed. This issue is currently under investigation by Avaya. Inbound and outbound faxes using T.38 and G.711 pass-through were tested successfully, using the alternate configuration described in **Section 12** (Appendix A).
- 4) **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.
- 5) **Avaya SBCE inserts a=ptime:20 in the SIP SDP toward Communication Manager.** AT&T includes a=maxptime:30 in the SIP SDP to recommend a ptime value of 30ms, but does not specify a ptime value in the SDP. If no media packetization attribute (ptime) is included in the SIP Session Description Protocol (SDP), Avaya SBCE inserts “a=ptime:20”, specifying 20 milliseconds. Although Communication Manager can be configured to send ptime with a value of 30ms (See **Section 5.9.2**), 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.



- 6) **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 SigMa script (**Section 7.8**) is used to remove these headers.
- 7) **Emergency 911/E911 Services Limitations and Restrictions.** Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor. While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at <http://new.serviceguide.att.com>. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

## 2.3. Support

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

<https://www.business.att.com/products/sip-trunking.html>. 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.

## 2.4. SIP Message – Packet Optimization

To support advanced SIP telephony features in the Avaya Aura® enterprise environment, certain proprietary headers may be included in the SIP message sent toward the AT&T IPFR-EF service. These extra headers can cause the SIP message to become larger than the specified Maximum Transmission Unit (MTU) in some network equipment and create fragmented UDP packets. These fragmented packets may not be re-assembled properly on the far-end when packets arrive out of order. To prevent fragmented packets, any unnecessary or proprietary headers should be removed from the SIP message before being sent to AT&T. Session Manager can remove these headers by specifying the “*eRHdrs*” parameter within the “AttAdapter” adaptation. See **Section 6.5.2**.

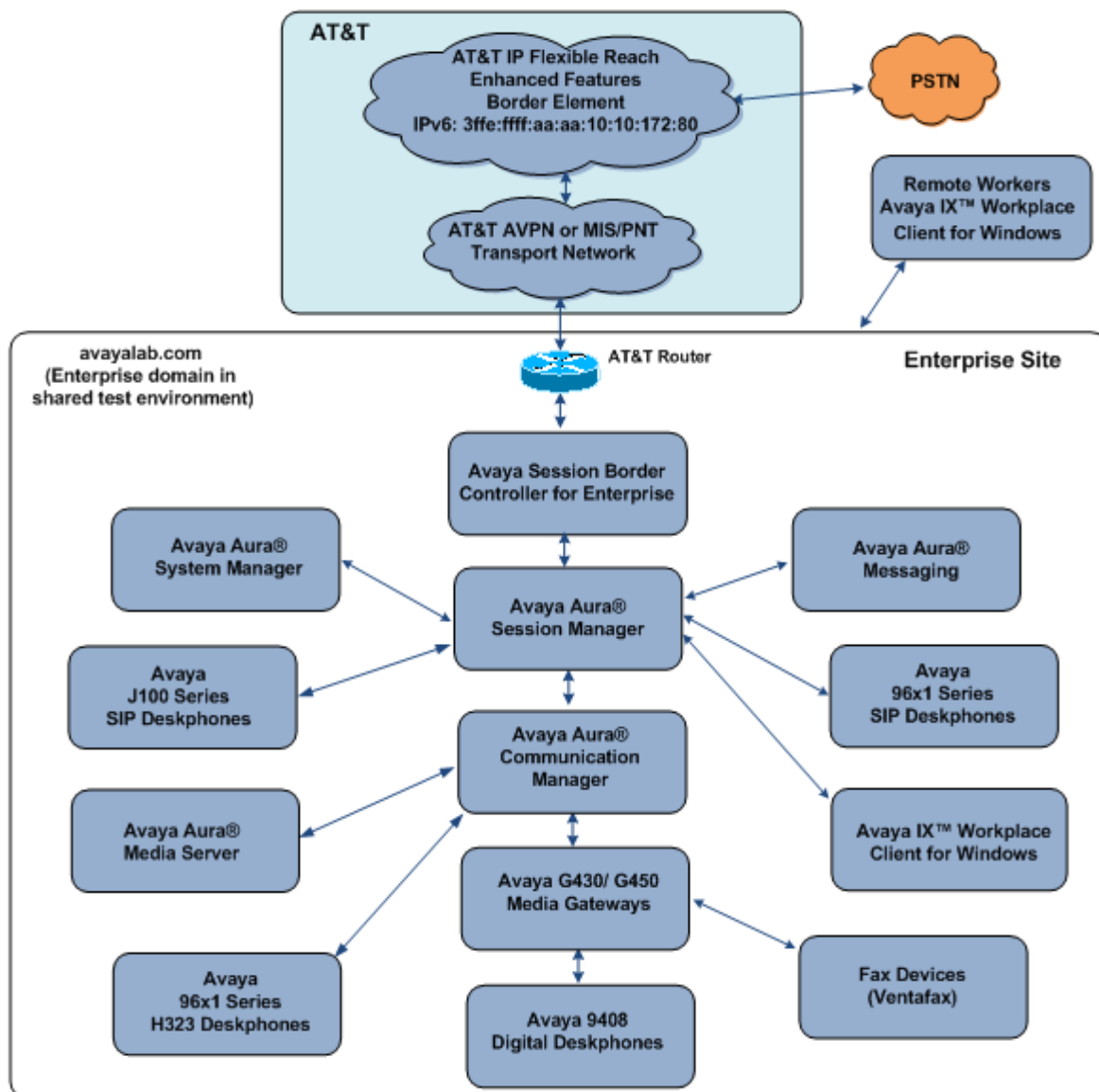
In the sample configuration, the following headers were removed:

- AV-Global-Session-ID
- Alert-Info
- Endpoint-View
- P-AV-Message-Id
- P-Charging-vector
- P-Location
- AV-Secure-Indication

To help reduce the packet size further, the Avaya SBCE can remove the Avaya “*gsid*” and “*epv*” parameters that may be included within the Contact header of outbound messages, by applying a Sigma script to the AT&T SIP server profile. See **Section 7.8**.

### 3. Reference Configuration

**Figure 1** illustrates the sample configuration used for the compliance testing, with the AT&T IPFR-EF service test lab circuit, connected to the simulated enterprise site via AVPN transport.



**Figure 1: Reference configuration**

The following components were used in the reference configuration:

- Avaya Session Border Controllers for Enterprise
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya G430 Media Gateway
- Avaya Media Server
- Avaya Aura® Messaging
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle
- Avaya IX™ Workplace Client for Windows
- Avaya Digital Phones
- Ventafax fax software

Avaya Aura® System Manager provides a common administration interface for centralized management of Session Manager and 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.

Note that Avaya G450 and G430 Media Gateways, and an Avaya Media Server are used in the reference configuration. This solution is extensible to other Avaya Media Gateways.

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.

Avaya Aura applications support dual stack architecture, where IPv4 and IPv6 can be supported simultaneously in a mixed environment. In addition, the IP address type (family) used in media stream negotiations is set independently of the SIP signaling address family. The Alternate Network Address Type (ANAT) feature is supported, as a mechanism to achieve media level interworking between devices using IPv4 and IPv6 addresses.

In the reference configuration, IPv6 and SIP/UDP is used for signaling between the IPFR-EF service Border Element (BE) and the public side of the Avaya SBCE. IPv6 and RTP is used for the media.

For illustration purposes, these Application Notes show a configuration where IPv6 is implemented on the enterprise side, over an existing platform already using IPv4 addresses. Signaling between Session Manager, the Avaya SBCE and Communication Manager specifically associated to the IPFR-EF trunk is configured to use IPv6 and SIP/TLS. Other SIP entities and endpoints in the reference configuration may continue to use IPv4/TLS. To ensure media interoperability with elements and endpoints on the private network which only operate at IPv4 addresses, ANAT and dual IPv6/IPv4 SRTP is used for the media on the enterprise.

### 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.

Component	Illustrative Value in these Application Notes
<b>Avaya Aura® Communication Manager</b>	
IP Address (procr)	10.64.91.75
IPv6 Address (procr6)	fd22:305b:b390:14e6::5
<b>Avaya Aura® Session Manager</b>	
IPv4 Address	10.64.91.81
IPv6 Address	fd22:305b:b390:14e6::6
<b>Avaya Aura® Media Server</b>	
IPv4 Address	10.64.91.86
IPv6 Address	fd22:305b:b390:14e6::7
<b>Avaya G450 Media Gateway</b>	
IPv4 Address	10.64.91.91
IPv6 Address	fd22:305b:b390:14e6::9
<b>Avaya G430 Media Gateway</b>	
IPv4 Address	10.5.5.150
<b>Avaya Session Border Controller for Enterprise (SBCE)</b>	
IPv4 Address of Inside (Private) Interface A1	10.64.91.40
IPv6 Address of Inside (Private) Interface A1	fd22:305b:b390:14e6::1a
IPv6 Address of Outside (Public) Interface	3ffe:ffff:bb:bb::240 (see note below)
<b>AT&amp;T Border Element</b>	
IP Address	3ffe:ffff:aa:aa:10:10:172:80

**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 public IPv6 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 **3ffe:ffff:bb:bb::240** (Avaya SBCE public interface) and **3ffe:ffff:aa:aa:10:10:172:80** (AT&T BE IPv6 address) are specified.

**Note** – The IPv6 addresses on the private enterprise network were generated using a pseudo-random algorithm for the assignment of “almost unique” local IPv6 unicast addresses, as described in RFC4193. These IP addresses have local significance only, and they are not expected to be routable on the global Internet.

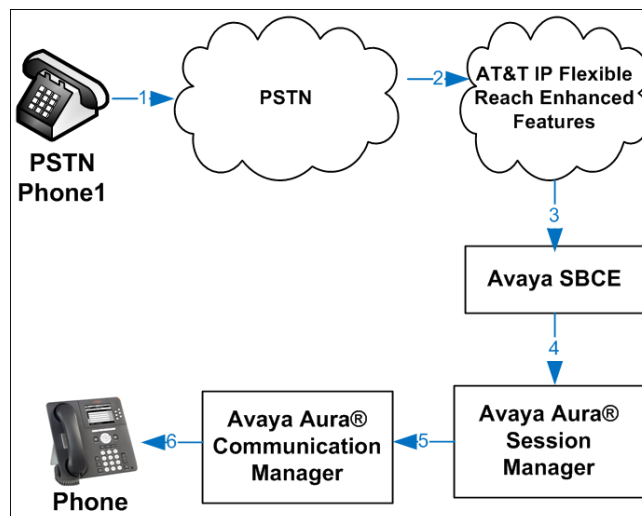
## 3.2. Call Flows

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

### 3.2.1. Inbound Call

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.

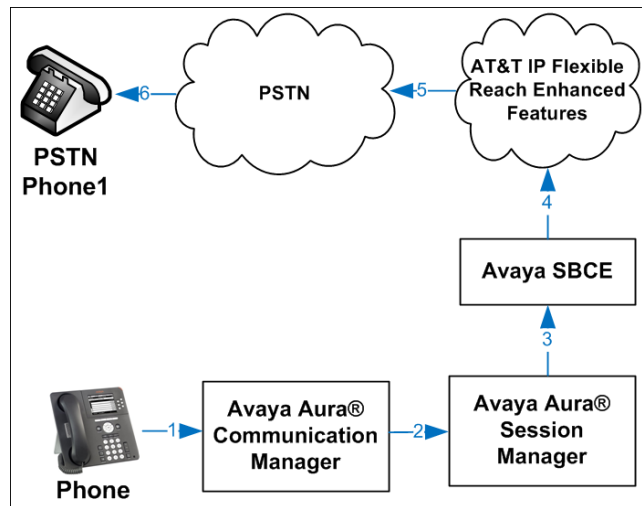


**Figure 2: Inbound IPFR-EF Call**

### 3.2.2. Outbound Call

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.



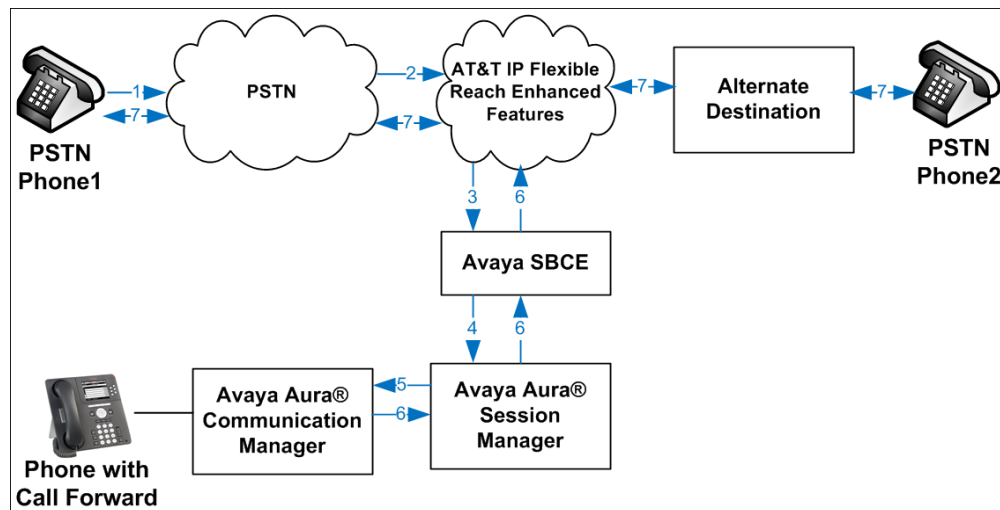
**Figure 3: Outbound IPFR-EF Call**

### 3.2.3. Call Forward Redirection

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 5.10.1**).

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.



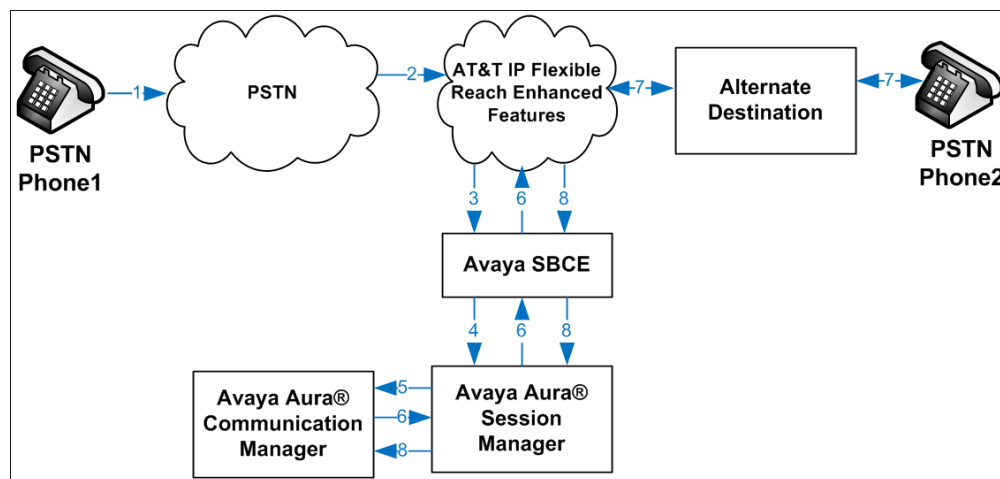
**Figure 4: Station Re-directed (e.g., Call Forward) IPFR-EF Call**



### 3.2.4. Network Based Blind Transfer Call Flow (Communication Manager Vector)

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 REFER message specifies the alternate destination in its Refer-To header, 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).

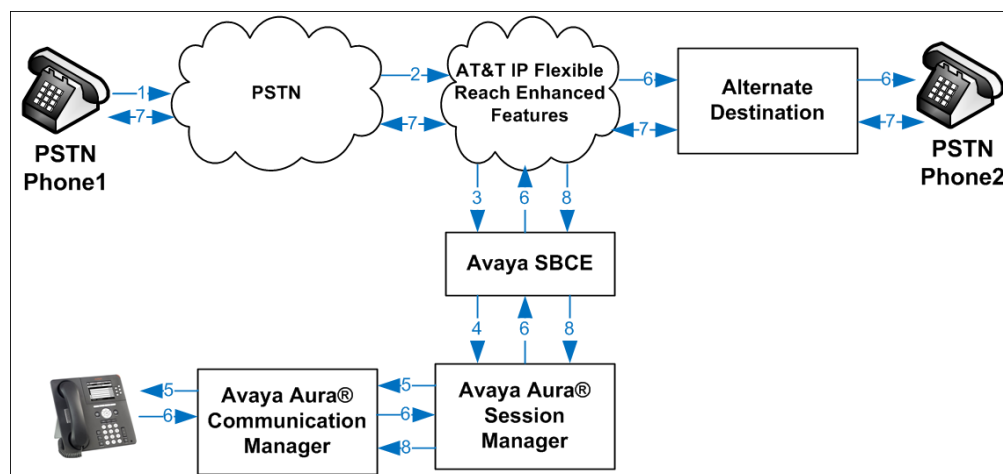


**Figure 5: Network Based Blind Transfer Using REFER (Communication Manager Vector)**

### 3.2.5. Network Based Attended/Unattended Transfer Call Flow initiated by Communication Manager Station

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 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® System Manager	8.1.2.0.0611097 (Feature Pack 2)
Avaya Aura® Session Manager	8.1.2.0.812033
Avaya Aura® Communication Manager	8.1.2.0.0-FP2 (Patch 26095)
Avaya Session Border Controller for Enterprise	8.1.0.0.14-18490
Avaya Aura® Media Server	8.0.2.93
Avaya Aura® Messaging	7.1.Service Pack 2
Avaya G450 Media Gateway	41.24.0
Avaya G430 Media Gateway	41.24.0
Avaya 96x1 Series IP Deskphone (H.323)	6.8304
Avaya 96x1 Series IP Deskphone (SIP)	7.1.8.0.9
Avaya J129 IP Deskphone (SIP)	4.0.4.0.10
Avaya IX™ Workplace Client for Windows	3.7.6.10.1
Avaya 9408 Digital Deskphone	20.06
Fax device	Ventafax 7.10

**Table 2: Equipment and Software Versions**

## 5. 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 both the Communication Manager SMI web page and the 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]Error! Reference source not found. in the References section for additional 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.

### 5.1. Enable IPv6 addressing

This section describes the steps to enable IPv6 addressing in 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** – On the Communication Manager SMI page, select **Administration** → **Server (Maintenance)**. On the menu on the left hand side, navigate to **Server Configuration** → **Network Configuration**.

- In the **IPv6 is Currently:** box, select **enabled** from the drop-down menu. Click **Change**. The system displays the IPv6 text boxes for each field.
- Enter the IPv6 values for the default gateway, IP address and prefix.
- Click **Change**.

**AVAYA** Avaya Aura® Communication Manager (CM) System Management Interface (SMI)

Help Log Off Administration

Administration / Server (Maintenance) This Server: cm8

### Network Configuration

This implementation is used to configure the IP related settings for this server. Please note that some changes made on this page may affect settings on other pages under the "Server Configuration" category - please make sure to check all pages for an accurate configuration.

**Notes**

- The host name and ID of each server in the system must be unique.
- The below fields are used to indicate how each Ethernet port is to be used (functional assignment) and to configure the IP related settings of each port. Ethernet ports may be used for multiple purposes, except for the port assigned to the laptop, which must be dedicated to only that purpose.
- An Ethernet port can be configured without a functional assignment. However, any port intended for use with the Communication Manager application must be assigned the correct functional assignment.
- Note that any configuration data obtained from an external source will be displayed read-only. To change these settings, please navigate to the external source used to configure the settings.
- A restart of Communication Manager is needed after the server has been successfully configured. Click the **Restart CM** button below to do so. Please note that this should be done after all configuration is completed. Too many restarts may escalate to a full Communication Manager reboot.
- This server is reporting to be the **ACTIVE** server. This server will be unavailable for telephony processing when configuration changes are submitted.

Host Name: cm8

DNS Domain: avayaalab.com

Search Domain List: avayaalab.com (comma separated)

Primary DNS: 10.64.19.201

Secondary DNS:

Tertiary DNS:

Server ID: 1 (Range 1 to 256)

IPv6 is currently: **enabled**

Default Gateway: IPv4: 10.64.91.1 IPv6: fd22:305b:b390:1446:0:0:1

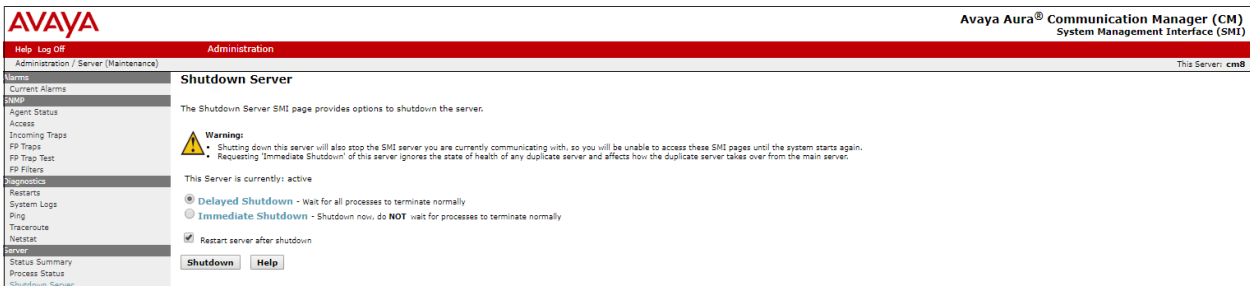
eth0: IPv4 Address: 10.64.91.75 Mask: 255.255.255.0 IPv6 Address: fd22:305b:b390:1446:: Prefix: /64 Functional Assignment: Corporate LAN/Processor Ethernet/Control Network

eth1: IPv4 Address: / Mask: IPv6 Address: Prefix: / Functional Assignment:

**Change Restart CM Help**

**Step 3** – Communication Manager needs to be rebooted for the IPv6 settings to take effect. This will be service affecting.

- On the **Server** section, click **Shutdown Server**.
- Make sure that **Restart server after shutdown** is checked.
- Click **Shutdown**.



## 5.2. Verify Licensed Features

**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.

**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** – Using the System Access Terminal (SAT) interface, 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:	1000	2		
Maximum Administered Remote Office Trunks:	4000	0		
Max Concurrently Registered Remote Office Stations:	1000	0		
Maximum Concurrently Registered IP eCons:	68	0		
Max Concur Reg Unauthenticated H.323 Stations:	100	0		
Maximum Video Capable Stations:	2400	0		
Maximum Video Capable IP Softphones:	1000	6		
<b>Maximum Administered SIP Trunks:</b>	<b>4000</b>	<b>75</b>		
Max Administered Ad-hoc Video Conferencing Ports:	4000	0		
Max Number of DS1 Boards with Echo Cancellation:	80	0		

**Step 2 - On Page 4 of the form, verify that ARS is enabled.**

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
<b>ARS? y</b>	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? y		

**Step 3 - On Page 5 of the form, verify that the Enhanced EC500, IP Trunks, and ISDN-PRI, features are enabled. If the use of SIP REFER messaging will be required verify that the ISDN/SIP Network Call Redirection feature is enabled. If the use of SRTP will be required verify that the Media Encryption Over IP feature is enabled.**

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y	<b>IP Stations? y</b>	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
<b>Enhanced EC500? y</b>	<b>ISDN/SIP Network Call Redirection? y</b>	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	<b>ISDN-PRI? y</b>	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	<b>Media Encryption Over IP? y</b>	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
<b>IP Trunks? y</b>		
IP Attendant Consoles? y		

**Step 4** - 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? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
<b>Processor Ethernet? y</b>	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

### 5.3. 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	
<b>Trunk-to-Trunk Transfer: all</b>	
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	

## 5.4. System-Parameters IP-Options

Enter the **change system-parameters ip-options** command to enable Alternate Network Address Type (ANAT) at the system level. Communication Manager uses ANAT as a mechanism to achieve interworking between IPv4 and IPv6 at the media level (SDP). ANAT can also be controlled at the specific IP Network Region form (Section 5.8).

**Step 1** – On **Page 3** of the form, set **ANAT Enabled** to **y**.

change system-parameters ip-options		Page	3	of	4
IP-OPTIONS SYSTEM PARAMETERS					
SNMP PARAMETERS					
Download Flag? n					
Community String:					
SOURCE ADDRESSES					
1.		4.			
2.		5.			
3.		6.			
SERVICES DIAL PAD PARAMETERS			ALTERNATIVE NETWORK ADDRESS TYPES		
Download Flag? n			<b>ANAT Enabled? y</b>		
Password: *					
MUSIC/ANNOUNCEMENTS IP-CODEC PREFERENCES					
Prefer use of G.711 by Music Sources? n					
Prefer use of G.711 by Announcement Sources? n					
Prefer use of G.711 by IP Endpoints Listening to Music? n					
Prefer use of G.711 by IP Endpoints Listening to Announcements? n					

## 5.5. Processor Ethernet Configuration

Use the **change ip-interface procr** command to verify the Processor Ethernet (procr) parameters defined during installation, and to enable the IPv6 (procr6) interface.

**Step 1** – On **Page 1** of the form, verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H.248 Gateways?** fields are set to **y**. In the reference configuration the procr interface is assigned to **Network Region: 1**. Default values are used for the remaining parameters in this page.

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



**Step 2** - On **Page 2** of the form, under **IPV6 PARAMETERS**, note that **Node Name procr6** is already assigned, and the **IP Address** shows the value entered in **Section 5.1**.

- Set **Enable Interface** to **y**

change ip-interface procr		Page 2 of 2
IP INTERFACES		
Speed: ?		
Duplex: Full		
IPV6 PARAMETERS		
Node Name: procr6		
IP Address: fd22:305b:b390:14e6::5		
Subnet Mask: /64		
Enable Interface? y		

## 5.6. Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration the Processor Ethernet based Communication Manager platform is used. Note that both IPv4 and IPv6 addresses are present in the test environment. Also note the Communication Manager **procr** and **procr6** interfaces IP addresses, as shown in **Section 5.1**. The **procr6** address will be used to define the Communication Manager SIP Entity in **Section 6.6**.

**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. In the example below, **SM** and **10.64.91.81** correspond to the Session Manager IPv4 address configured during the initial installation. A new node name and IPv6 address are added, to be used on the Signaling Group to Session Manager, later in **Section 5.10.1**. (e.g., **SM-IPv6** and **fd22:305b:b390:14e6::6**)
- Media Server (e.g., **AMS801** and **10.64.91.86**). The Media Server node name is only needed if a Media Server is present.

change node-names ip		Page	1 of	2
		IP NODE NAMES		
Name	IP Address			
AMS801	10.64.91.86			
IPOSE	10.64.19.170			
SM	10.64.91.81			
SM-IPv6	fd22:305b:b390:14e6::6			
default	0.0.0.0			
procr	10.64.91.75			
procr6	fd22:305b:b390:14e6::5			

## 5.7. 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 5.10**.

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						

## 5.8. IP Network Regions

Network regions provide a means to logically group resources such as codecs, UDP port ranges, and inter-region communication. In the shared Communication Manager configuration used for the testing, the Avaya Media Gateways and Media Server are in region 1. To provide testing flexibility, network region 6 was associated to components used specifically for the AT&T SIP trunk access.

### 5.8.1. 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., **avayalab.com**) in the **Authoritative Domain** field (see **Section 6.3**).
- 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.

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

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

- Verify that **RTCP Reporting to Monitor Server Enabled** is set to **y**.
- Set **ANAT Enabled** to **y**.

<b>change ip-network-region 1</b>	<b>Page 2 of 20</b>
IP NETWORK REGION	
<b>RTCP Reporting to Monitor Server Enabled? y</b>	
RTCP MONITOR SERVER PARAMETERS	
Use Default Server Parameters? y	
ALTERNATIVE NETWORK ADDRESS TYPES	
<b>ANAT Enabled? y</b>	

**Step 3** - On **page 4** of the form:

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **6** in the **dst rgn** column, enter **6** for the codec set (this means region 1 is permitted to talk to region 6 and it will use codec set 6 to do so). The **direct WAN** and **Units** columns will self-populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

change ip-network-region 1										Page 4 of 20		
Source Region: 1		Inter Network Region Connection Management							I	M		
									G	A t		
<b>dst rgn</b>	<b>codec set</b>	<b>direct WAN</b>	<b>WAN-BW-limits Units</b>	<b>Video Total Norm</b>	<b>Prio Shr</b>	<b>Intervening Regions</b>	<b>Dyn CAC</b>	<b>A R</b>	<b>G L</b>	<b>c e</b>		
<b>1</b>	<b>1</b>							all				
2	2	y	NoLimit				n	t				
3	1	y	NoLimit				n	t				
4	4	y	NoLimit				n	t				
5												
<b>6</b>	<b>6</b>	y	NoLimit				n	y	t			
7	7	y	NoLimit				n	y	t			
8												

## 5.8.2. IP Network Region 6 – AT&T Trunk Region

Repeat the steps in **Section 5.8.1** with the following changes:

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

- Enter a descriptive name (e.g., **IPv6 to SM-ATT**).
- Enter **6** for the **Codec Set** parameter.

**Step 2** – On **Page 2** (not shown):

- Verify that **RTCP Reporting to Monitor Server Enabled** is set to **y**.
- Set **ANAT Enabled** to **y**.

**Step 3** – On **Page 4** of the form:

- Set codec set **6** for **dst rgn 1**.
- Note that **dst rgn 6** is pre-populated with codec set **6** (from page 1 provisioning).

change ip-network-region 6										Page 4 of 20		
Source Region: 6		Inter Network Region Connection Management							I	M		
									G	A t		
<b>dst rgn</b>	<b>codec set</b>	<b>direct WAN</b>	<b>WAN-BW-limits Units</b>	<b>Video Total Norm</b>	<b>Prio Shr</b>	<b>Intervening Regions</b>	<b>Dyn CAC</b>	<b>A R</b>	<b>G L</b>	<b>c e</b>		
<b>1</b>	<b>6</b>	y	NoLimit				n	y	t			
2												
3	3	y	NoLimit				n	y	t			
4												
5												
<b>6</b>	<b>6</b>							all				
7												

## 5.9. IP Codec Sets

Use the **change ip-codec-set** command to define a list of codecs to use for calls within the enterprise, and for calls between the enterprise and the service provider.

### 5.9.1. 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** and **G.729A** 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.

<b>change ip-codec-set 1</b>		<b>Page 1 of 2</b>	
IP Codec Set			
Codec Set: 1			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.722-64K		2	20
2: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>
3: <b>G.729A</b>	<b>n</b>	<b>2</b>	<b>20</b>
4: G.729B	n	2	20
5:			
6:			
7:			
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**.

**Step 3** - For **Media Connection IP Address Type Preferences**, enter **IPv4** as the first preference and **IPv6** as the second preference.

<b>change ip-codec-set 1</b>		<b>Page 2 of 2</b>	
IP MEDIA PARAMETERS			
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	Redun- dancy	Packet Size (ms)
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>	<b>ECM: y</b>
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20
Media Connection IP Address Type Preferences			
1: <b>IPv4</b>			
2: <b>IPv6</b>			

## 5.9.2. Codecs for IP Network Region 6 (calls to/from AT&T)

This IP codec set will be used for IPFR-EF calls. Repeat the steps in **Section 5.9.1** with the following changes:

- Provision the codecs in the order shown below.
- 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.
- Set the **Media Connection IP Address Type Preferences**. When using a mixed IPv4-IPv6 topology, generally is a good practice to use IPv4 first and IPv6 second as the preference on the SDP. In the reference configuration, and in order to enforce the use of IPv6 by the media on the enterprise during the testing with AT&T IPFR, **IPv6** was used at the first preference and **IPv4** as the second preference in this IP codec set, used for the IPFR-EF calls.

change ip-codec-set 6

Page 1 of 2

IP CODEC SET

Codec Set: 6

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

Media Encryption

1: 1-srtp-aescm128-hmac80

2: none

Encrypted SRTCP: enforce-unenc-srtcp

change ip-codec-set 6

Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

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

Media Connection IP Address Type Preferences

1: IPv6

2: IPv4

## 5.10. 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 7. This trunk uses IPv6, TLS port 5067.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 3. This trunk uses IPv4, TLS port 5061.

**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 6.6** regarding the use of TLS transport protocols in the CPE.

### 5.10.1. 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 Group 7 is defined. This trunk corresponds to the **CM-TG7** SIP Entity defined in **Section 6.6.2**.

#### 5.10.1.1 Signaling Group 7

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **7**), 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 IPv6 node name of the Processor Ethernet (**procr6**) noted in **Section 5.5**.
- **Far-end Node Name** – Set to the IPv6 node name of Session Manager as administered in **Section 5.6** (e.g., **SM-IPv6**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5067**.
- **Far-end Network Region** – Set the IP network region to **6**, as set in **Section 5.8.2**.
- **Far-end Domain** – Enter **avayalab.com**. This is the domain provisioned for Session Manager in **Section 6.3**.
- **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).



<b>add signaling-group 7</b>		<b>Page 1 of 2</b>
SIGNALING GROUP		
Group Number: 7	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: procr6	Far-end Node Name: SM-IPv6	
Near-end Listen Port: 5067	Far-end Listen Port: 5067	
	Far-end Network Region: 6	
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	IP Audio Hairpinning? n
Session Establishment Timer(min): 3	Initial IP-IP Direct Media? n	Alternate Route Timer(sec): 6
Enable Layer 3 Test? y		
H.323 Station Outgoing Direct Media? n		

### 5.10.1.2 Trunk Group 7

**Step 1** - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 7). 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 IPv6**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **\*07**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 5.10.1.1** (e.g., 7).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

<b>add trunk-group 7</b>		<b>Page 1 of 21</b>
TRUNK GROUP		
Group Number: 7	Group Type: sip	CDR Reports: y
Group Name: ATT IPFR IPv6	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: *07
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 7	
	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.

<b>add trunk-group 7</b>	<b>Page 2 of 21</b>
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
<b>Preferred Minimum Session Refresh Interval(sec): 900</b>	
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**.

<b>add trunk-group 7</b>	<b>Page 3 of 21</b>
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
<b>Numbering Format: public</b>	
	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**).

**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 6.5.2**). Alternatively, History Info may be disabled here.

<b>add trunk-group 7</b>	<b>Page 4 of 21</b>
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
<b>Network Call Redirection? y</b>	
Build Refer-To URI of REFER From Contact For NCR? n	
<b>Send Diversion Header? y</b>	
Support Request History? y	
<b>Telephone Event Payload Type: 100</b>	
Shuffling with SDP? n	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

## 5.10.2. Local SIP Trunk (Avaya SIP Telephone, Messaging Access, etc.)

Trunk Group 3 corresponds to the CM-TG3 SIP Entity defined in Section 6.6.4.

### 5.10.2.1 Signaling Group 3

Repeat the steps in Section 5.10.1.1 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 Node Name** – Set to the Processor Ethernet IPv4 node name (**procr**) noted in Section 06.
- **Far-end Node Name** – Set to the IPv4 node name of Session Manager as administered in Section 5.6 (e.g., SM).
- **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 5.8.1.

### 5.10.2.2 Trunk Group 3

Repeat the steps in Section 5.10.1.2 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 5.10.2.1 (e.g., 3).

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

- Same as Section 5.10.1.2.

**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.

## 5.11. Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 5.10.1.2**), 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 a Communication Manager extensions (e.g., **89321**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **7**).
- **Private Prefix** – Enter the corresponding IPFR-EF DNIS number prefix (e.g., **17325552753**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

change public-unknown-numbering 5 ext-digits 89321					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	89321	7	17325552753	11	Total Administered: 46
5	89324	7	17325552754	11	Maximum Entries: 240
					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.
					Communication Manager automatically inserts a '+' digit in this case.

## 5.12. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 5.10.2.2**), 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 5.7** (e.g., **54** and **89** are the local extension patterns used in the reference configuration).
- **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 Len	
5	10	3		5	Total Administered: 6
5	11	3		5	Maximum Entries: 540
5	12	3		5	
5	54	3		5	
5	89	3		5	

## 5.13. Route Patterns

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

### 5.13.1. 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 5.14**. 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 **7** for public trunk 7, 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 FRL NPA		Pfx Hop Toll No.		Inserted		DCS/ IXC									
No		Mrk Lmt List Del		Digits		QSIG									
				Dgts		Intw									
1: 7		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							

### 5.13.2. Route Pattern for International Calls to AT&T

Repeat the steps in **Section 5.13.1** 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 **7** for public trunk 7, 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	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits			QSIG				
						Dgts				Intw				
1:	7	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			

### 5.13.3. Route Pattern for Service Calls to AT&T

Repeat the steps in **Section 5.13.1** to add a route pattern for x11 and IPFR-EF Call Forward feature access codes calls that do not require a leading plus sign, with the following changes:

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

- In the **Grp No** column, enter **7** for public trunk 7, 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 FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
  No      Mrk Lmt List Del  Digits      QSIG
                                Dgts      Intw
1: 7      0
2:
3:

      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
```

### 5.13.4. 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 5.15** (e.g., calls to Avaya SIP telephone extensions or Messaging).

**Step 1** - Repeat the steps in **Section 5.13.1** 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
2:
3:

      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
```



## 5.14. 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 5.7**. 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 5.13**).

**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 17xxxxxxxxxx.
- In the **Min** and **Max** columns enter the corresponding digit lengths, (e.g., **11** and **11**).
- In the Route Pattern column select a route-pattern to be used for these calls (e.g., **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 Req'd
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

## 5.15. 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	

## 5.16. Avaya G450 Media Gateway Provisioning

In the reference configuration, an Avaya G450 Media Gateway is provisioned. The G450 is used for local DSP resources, announcements, Music On Hold, etc.

**Note** – An Avaya G450 and a G430 Media Gateways were used in the reference configuration. The G450 was provisioned to use IPv4 and IPv6 addresses, while the G430 used IPv4 addresses only.

**Note** – Only the Media Gateway provisioning associated with the enabling of IPv6 on the G450 and registration to Communication Manager is shown below. It is assumed that the G450 IPv4 address has already been configured. For additional information for the provisioning of the Media Gateway see [8] in the References section.

**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.

**Step 3** – To set the G450 IPv6 address:

- Enter **interface vlan 1**.
- At the *G450-???(super-if:Vlan 1)#* prompt, set the G450 IPv6 address and prefix length. Enter **ipv6 address fd22:305b:b390:14e6::9 64**.
- Enter **ipv6 admin-state up**.
- Enter **pmi6** and then **exit**.

**Step 4** – Back at the *G450-???(super)#* prompt, enter the media gateway MGC list with both the Communication manager procr and procr6 IP addresses (see **Section 5.5**):

- Enter **set mgc list 10.64.91.75+fd22:305b:b390:14e6::5**

**Step 6** – Enter the **copy run start** command to save the G450 configuration.

**Step 7** – Enter **reset** to reset the media gateway.

**Step 8** - From the Communication Manager SAT, enter **add media-gateway x** where x is an available Media Gateway identifier (e.g., **2**).

**Step 9** – On the Media Gateway form, enter the following parameters:

- Set **Type** = **g450**.
- Set **Name** = a descriptive name (e.g., **G450-2**).
- Set **Serial Number** = enter the serial number copied from **Step 2**.
- 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 9** (e.g., *G450-002(super)#*).

**Step 10** - Enter the **display media-gateway 2** command and verify that the G450 has registered

```
display media-gateway 2                                     Page 1 of 2
                                     MEDIA GATEWAY 2

Type: g450
Name: G450-2
Serial No: 11N507727041
Link Encryption Type: any-ptls/tls      Enable CF? n
Network Region: 1                      Location: 1
Use for IP Sync? n                     Site Data:
Recovery Rule: 1

Registered? y
FW Version/HW Vintage: 41 .24 .0 /2
MGP IPV4 Address: 10.64.91.91
MGP IPV6 Address: fd22:305b:b390:14e6::9
Controller IP Address: 10.64.91.75
MAC Address: b4:b0:17:90:61:d8

Mutual Authentication? optional
```

## 5.17. Avaya Aura® Media Server Provisioning

In the reference configuration, an Avaya Aura® Media Server is used, along with a G450 and a G430 Media Gateways, for local DSP resources, announcements, and Music On Hold.

**Note** – Only the Media Server provisioning associated with enabling IPv6 and the connectivity to Communication Manager is shown below. It is assumed that the Media Server initial configuration, including the assignment of an IPv4 address has already been completed. See [9] and [10] in the References section for additional information.

Perform the following steps on the Avaya Media Server, to enable the IPv6 on the server:

**Step 1** – Use SSH to connect to the Media Server Linux shell. Use the customer account to login.

**Step 2** – Enter the **netSetup** command. Follow the on screen prompts to confirm existing network settings, and update the new IPv6 configuration. In the example below, **10.64.91.86** is the Media Server IPv4 address and **fd22:305b:b390:14e6::7** the IPv6 address.

```
Verify responses:

Server hostname:      ams801
Server IP address:    10.64.91.86
Netmask/prefix:       255.255.255.0/24
Gateway:              10.64.91.1
DNS Domain:           avayalab.com
Primary DNS Server:
IPv6 auto config:     off
Server IPv6 address:  fd22:305b:b390:14e6::7
IPv6 prefix:          64
IPv6 gateway address: fd22:305b:b390:14e6::1

Enter selection (c=continue; u=update responses; a=abort) [u]:c
```

**Step 3** – Once the changes are completed, type **reboot** to restart the Media Server.

**Step 4** - 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).

**Step 5** - On the Media Server Element Manager, navigate to **System Configuration → Network Settings → IP Interface Assignment**. Set the parameters under **IPv4 Interfaces**, **IPv6 Interfaces** and **Media Interface Preference** as on the screen below, and click **Save**.

The screenshot shows the Avaya Aura Media Server web interface. The left sidebar contains a navigation menu with categories like System Status, Applications, Cluster Configuration, and System Configuration. The main content area is titled 'IP Interface Assignment' and includes a breadcrumb trail: Home > System Configuration > Network Settings > IP Interface Assignment. Below the title, there are three tabs: IPv4 Interfaces, IPv6 Interfaces, and Media Interface Preference. The IPv4 Interfaces section has fields for Signaling, Media, Cluster, and OAM, all set to 10.64.91.86 and [eth0]. The IPv6 Interfaces section has fields for Signaling and Media set to fd22:305b:b390:14e6::7 [eth0], while Cluster and OAM are set to Not Configurable. The Media Interface Preference section has a Transport field set to Dual IPv4/IPv6, and two preference fields for Remote and Local Offers, both set to their respective defaults. At the bottom right, there are buttons for Save, Cancel, and Restore Defaults.

**Step 6** – In the reference configuration, TLS transport is used for the communication between Communication Manager and the Media Server, using System Manager signed identity certificates. Navigate to **Security → Certificate Management → Trust Store** and verify the System Manager CA certificate is present in the trust repository.

The screenshot shows the Avaya Aura Media Server web interface for the Trust Store. The left sidebar shows the navigation menu with 'Security' expanded. The main content area is titled 'Trust Store' and includes a breadcrumb trail: Home > Security > Certificate Management > Trust Store. Below the title, there are buttons for Import..., Delete, Import CRL..., and Download CRL. A table lists the certificates in the trust store:

	Name	Issued By	Subject	Expiration Date
<input type="checkbox"/>	Avaya Product Root CA	/C=US/O=Avaya Inc./OU=Avaya Product PKI/CN=Avaya Product Root CA	/C=US/O=Avaya Inc./OU=Avaya Product PKI/CN=Avaya Product Root CA	Sun Aug 14 05:25:36 MDT 2033
<input type="checkbox"/>	Avaya SIP CA	/C=US/O=Avaya Inc./OU=SIP Product Certificate Authority/CN=SIP Product Certificate Authority	/C=US/O=Avaya Inc./OU=SIP Product Certificate Authority/CN=SIP Product Certificate Authority	Tue Aug 10 16:45:28 MDT 2027
<input type="checkbox"/>	SMGR8	/CN=System Manager CA/OU=MGMT/O=AVAYA	/CN=System Manager CA/OU=MGMT/O=AVAYA	Sun Jul 30 13:05:37 MDT 2028

**Step 7** –On Communication Manager, enter the **add signaling-group x** command where x is an unused signaling group (e.g., **80**), 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 5.6**.
- **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 5.6** (e.g., **AMS801**).
- **Near-end Listen Port** – Set to **9061** (default).
- **Far-end Listen Port** – Set to **5061** (default).
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.8.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

```
add signaling-group 80                                     Page 1 of 2
                                                         SIGNALING GROUP

Group Number: 80           Group Type: sip
                          Transport Method: tls

Peer Detection Enabled? n Peer Server: AMS

Near-end Node Name: procr           Far-end Node Name: AMS801
Near-end Listen Port: 9061         Far-end Listen Port: 5061
                                Far-end Network Region: 1

Far-end Domain: 10.64.91.86
```

**Step 8** - 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., 80).
- **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: 80
Voip Channel License Limit: 300
Dedicated Voip Channel Licenses: 300
Node Name: AMS801
Network Region: 1
Location: 1
Announcement Storage Area: ANNC-be99ad1a-1f39-41e5-ba04-000c29f8f3f3
```

## 5.18. Save Translations

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

## 5.19. 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. Follow the steps below 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.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', and 'Administration'. The left sidebar shows a tree view with 'Administration / Server (Maintenance)' selected. The main content area is titled 'Trusted Certificates' and contains a table of trusted repositories. The table has columns for 'Select File', 'Issued To', 'Issued By', 'Expiration Date', and 'Trusted By'. The table lists three certificates: 'SystemManager8CA.crt', 'apr-ca.crt', and 'motorola\_sseca\_root.crt'. Below the table are buttons for 'Display', 'Add', 'Remove', 'Copy', and 'Help'.

Select File	Issued To	Issued By	Expiration Date	Trusted By
<input type="radio"/> SystemManager8CA.crt	System Manager CA	System Manager CA	Sun Jul 30 2028	A C W R
<input type="radio"/> apr-ca.crt	Avaya Product Root CA	Avaya Product Root CA	Sun Aug 14 2033	C W R
<input type="radio"/> motorola_sseca_root.crt	SCCAN Server Root CA	SCCAN Server Root CA	Sun Dec 04 2033	C
<input type="radio"/> sip_product_root.crt	SIP Product Certificate Authority	SIP Product Certificate Authority	Tue Aug 17 2027	C W R

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

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', and 'Administration'. The left sidebar shows a tree view with 'Administration / Server (Maintenance)' selected. The main content area is titled 'Server/Application Certificates' and contains a table of server/application certificates. The table has columns for 'Select File', 'Issued To', 'Issued By', 'Expiration Date', and 'Installed In'. The table lists two certificates: 'server.crt' and 'server.crt'. Below the table are buttons for 'Display', 'Add', 'Remove', 'Copy', and 'Help'.

Select File	Issued To	Issued By	Expiration Date	Installed In
<input type="radio"/> server.crt	cm8.avayalab.com	System Manager CA	Mon Nov 01 2021	C R
<input type="radio"/> server.crt	System Manager CA	System Manager CA	Sun Jul 30 2028	W

## 6. 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] in the References section for further details.

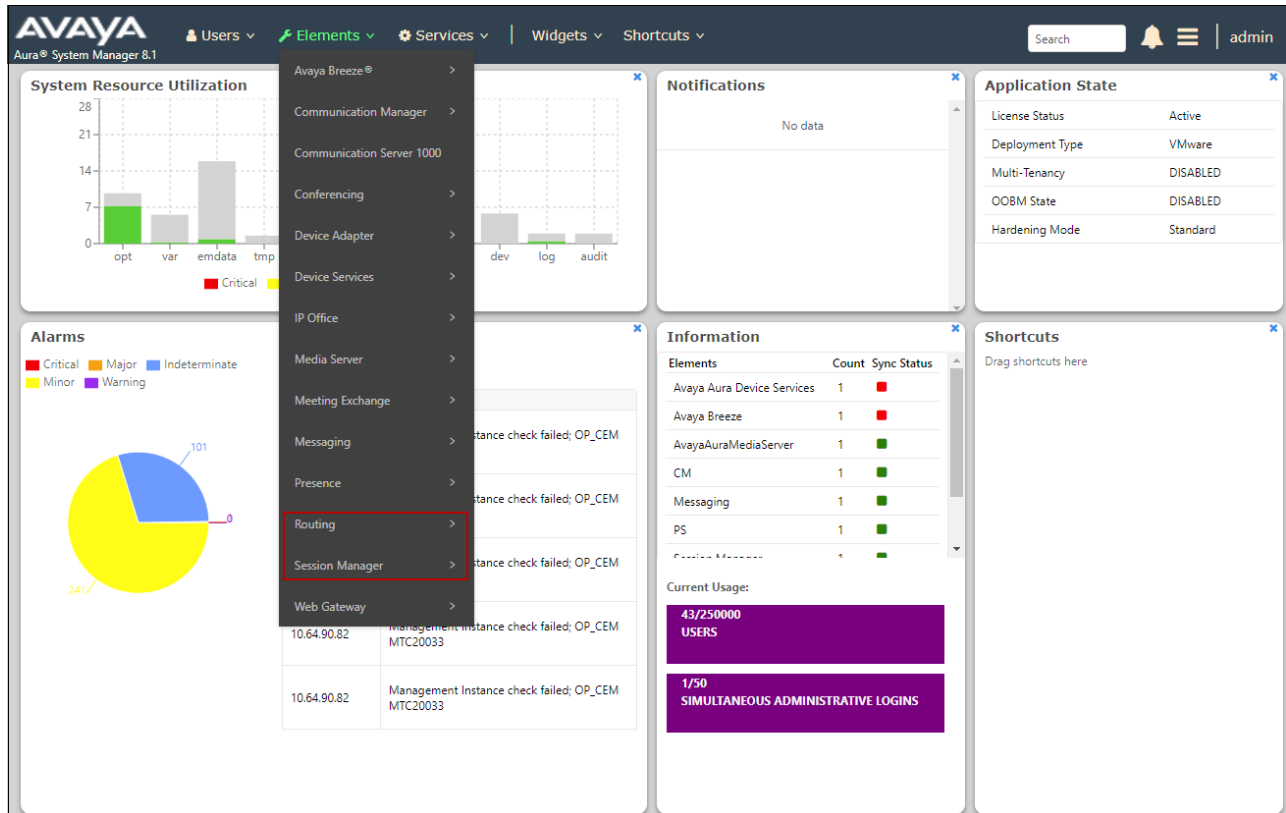
This section provides the procedures for configuring Session Manager to process inbound and outbound calls between Communication Manager and the Avaya SBCE. In the reference configuration, all Session Manager provisioning is performed via System Manager.

- Enable IPv6 support.
- 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 and the Avaya SBCE.
- Define SIP Entities corresponding to Session Manager, Communication Manager and the Avaya SBCE.
- Define Entity Links describing the SIP trunks between Session Manager and Communication Manager, as well as the SIP trunks between Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for inbound and outbound call routing.
- Security Module configuration.
- Verify TLS Certificates.



## 6.1. System Manager Login and Navigation

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. Most items discussed in this section will be located under the **Session Manager** and **Routing** menus, under the **Elements** heading shown below.



## 6.2. Enable Session Manager IPv6 Support

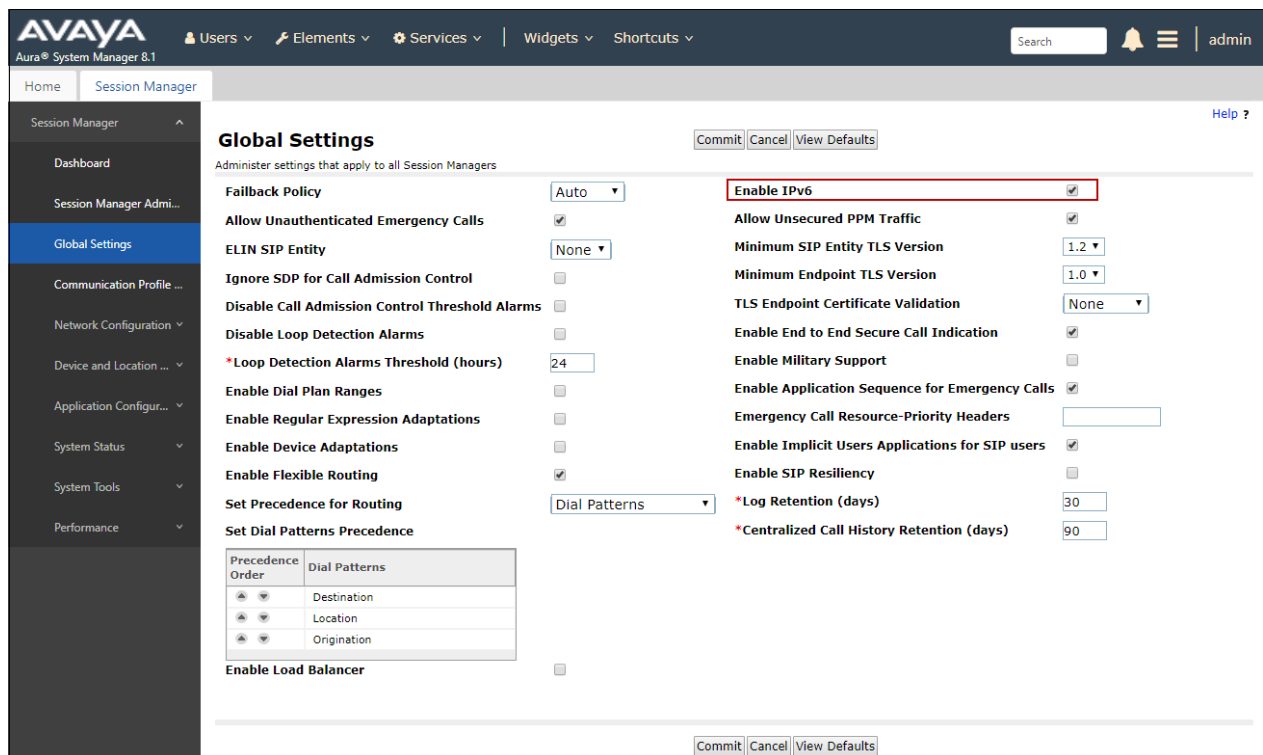
Session Manager supports dual stack architecture, therefore it can connect simultaneously to SIP entities and endpoints that use IPv4 and IPv6 addresses. Support for IPv6 in Session Manager is disabled by default.

Follow the steps below to enable IPv6 in Session Manager:

**Step 1** – From the **Home** screen, under the **Elements** heading, select **Session Manager** → **Global Settings**.

**Step 2** – Check the **Enable IPv6** box.

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



**AVAYA** Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Session Manager

Session Manager

Dashboard

Session Manager Admin...

**Global Settings**

Communication Profile ...

Network Configuration

Device and Location ...

Application Configur...

System Status

System Tools

Performance

**Global Settings** Commit Cancel View Defaults

Administer settings that apply to all Session Managers

**Fallback Policy** Auto

**Enable IPv6** ☒

**Allow Unauthenticated Emergency Calls** ☒

**ELIN SIP Entity** None

**Ignore SDP for Call Admission Control** ☐

**Disable Call Admission Control Threshold Alarms** ☐

**Disable Loop Detection Alarms** ☐

**\*Loop Detection Alarms Threshold (hours)** 24

**Enable Dial Plan Ranges** ☐

**Enable Regular Expression Adaptations** ☐

**Enable Device Adaptations** ☐

**Enable Flexible Routing** ☒

**Set Precedence for Routing** Dial Patterns

**Set Dial Patterns Precedence**

Precedence Order	Dial Patterns
1	Destination
2	Location
3	Origination

**Enable Load Balancer** ☐

**Allow Unsecured PPM Traffic** ☒

**Minimum SIP Entity TLS Version** 1.2

**Minimum Endpoint TLS Version** 1.0

**TLS Endpoint Certificate Validation** None

**Enable End to End Secure Call Indication** ☒

**Enable Military Support** ☐

**Enable Application Sequence for Emergency Calls** ☒

**Emergency Call Resource-Priority Headers**

**Enable Implicit Users Applications for SIP users** ☒

**Enable SIP Resiliency** ☐

**\*Log Retention (days)** 30

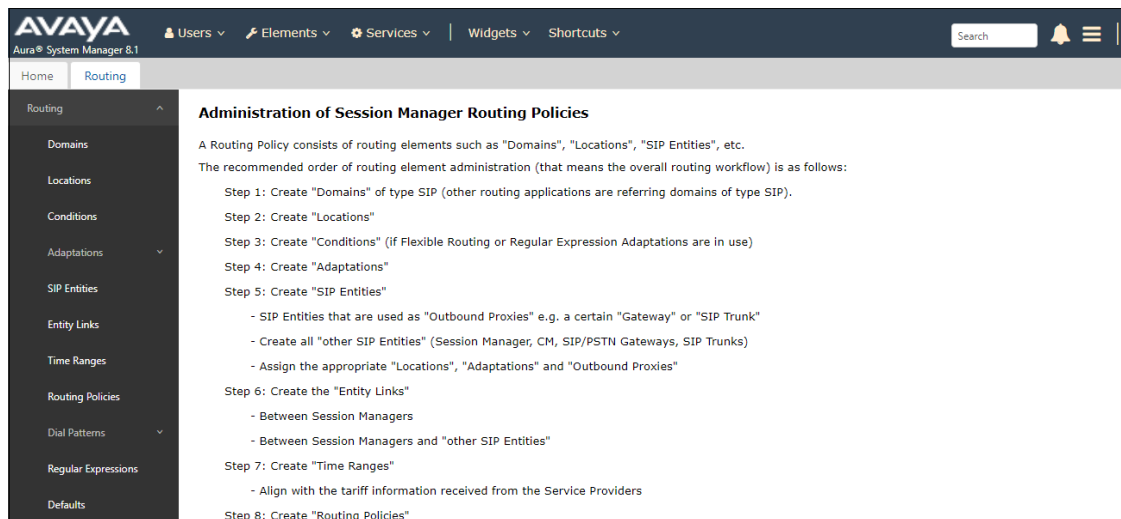
**\*Centralized Call History Retention (days)** 90

Commit Cancel View Defaults

## 6.3. SIP Domain

From the **Home** screen, under the **Elements** heading in the center, select **Routing**.

The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in the following section will be located under the **Routing** element shown below.

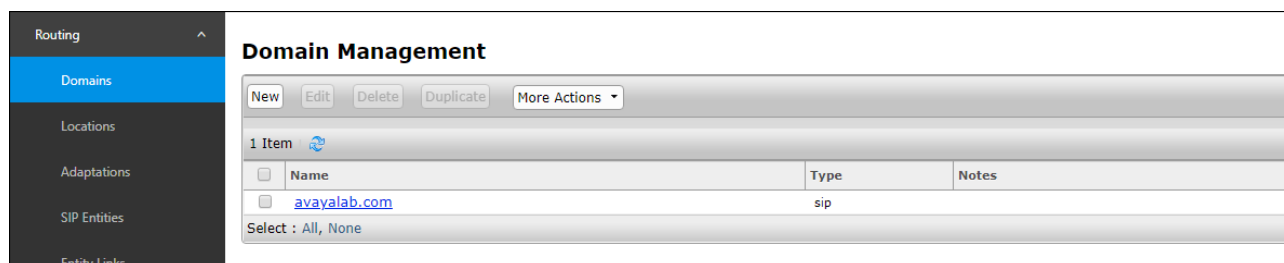


**Step 1** - Select **Domains** from the left navigation menu. In the reference configuration, domain **avayalab.com** was defined.

**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.



## 6.4. 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-7** – Communication Manager trunk group 7 designated for AT&T.
- **SBCE-IPv6** – Avaya SBCE

### 6.4.1. 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** - Click **Commit** to save.

The screenshot displays the Avaya System Manager 8.1 web interface. The left-hand navigation pane is expanded to show the 'Locations' menu item. The main content area is titled 'Location Details' and contains several sections for configuring a new location. The 'General' section includes fields for 'Name' (set to 'Main') and 'Notes' (set to 'Avaya SIL'). The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section includes fields for 'Managed Bandwidth Units' (set to 'kbit/sec'), 'Total Bandwidth', and 'Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'. The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', 'Latency before Overall Alarm Trigger', and 'Latency before Multimedia Alarm Trigger'. The 'Location Pattern' section at the bottom includes an 'Add' button, a 'Remove' button, and a table with one row containing 'IP Address Pattern' and 'Notes'.

### 6.4.2. CM-TG-7 Location

To configure the Communication Manager Trunk Group 7 Location, repeat the steps in **Section 6.4.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **CM-TG-7**).

### 6.4.3. SBCE-IPv6 Location

To configure the Avaya SBCE Location, repeat the steps in **Section 6.4.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **SBCE-IPv6**).

## 6.5. 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 6.5.1**) - 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 6.5.2**) - 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 2.4**).

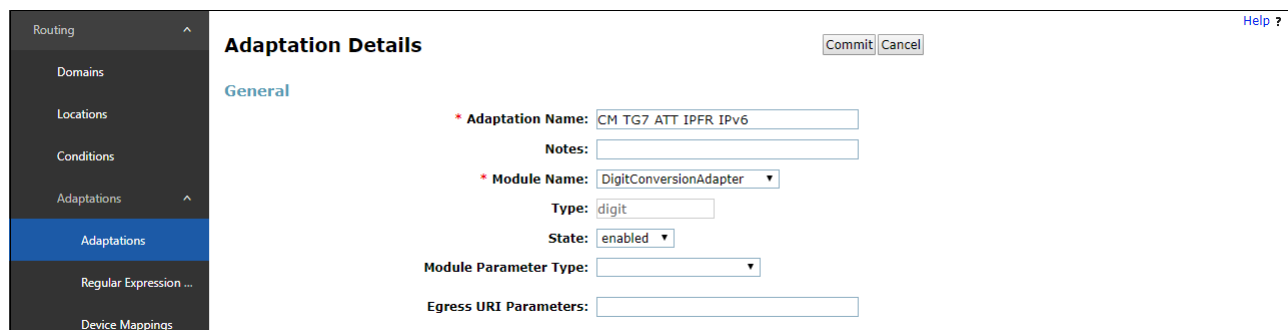
### 6.5.1. Adaptation for Avaya Aura® Communication Manager Extensions

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 TG7 ATT IPFR IPv6**).
2. Select **DigitConversionAdapter** from the **Module Name** drop-down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).



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

1. **Example 1 – destination extension:** 7325552753 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension 89321.
  - Enter **7325552753** in the **Matching Pattern** column.
  - Enter **10** in the **Min/Max** columns.
  - Enter **10** in the **Delete Digits** column.
  - Enter **89321** in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.

**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"/>	* 7325552753	* 10	* 10		* 10	89321	destination ▼		
<input type="checkbox"/>	* 7325552754	* 10	* 10		* 10	89324	destination ▼		

Select : All, None

Commit Cancel

## 6.5.2. 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 6.5.1** 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 5.10.1**).

**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.

The screenshot shows the 'Adaptation Details' configuration page. The left sidebar contains a navigation menu with options like Domains, Locations, Conditions, Adaptations, Regular Expression..., Device Mappings, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Adaptations' section is selected.

The main content area is titled 'Adaptation Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible:

- Adaptation Name:** SBC1-Adaptation for ATT
- Notes:** SBC - ATT
- Module Name:** AttAdapter (selected from a dropdown)
- Type:** digit
- State:** enabled
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table for 'Name-Value Parameters' with 'Add' and 'Remove' buttons. The table has columns for 'Name' and 'Value'. One entry is present:

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-

Below the table is a 'Select' dropdown set to 'All, None' and an 'Egress URI Parameters' field.

At the bottom, there are two sections for 'Digit Conversion':

- Digit Conversion for Incoming Calls to SM:** Includes an 'Add' button, a table with 0 items, and a 'Filter: Enable' link.
- Digit Conversion for Outgoing Calls from SM:** Includes a 'Remove' button, a table with 0 items, and a 'Filter: Enable' link.

Each digit conversion table has columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes.

## 6.6. SIP Entities

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

- Session Manager (**Section 6.6.1**).
- Communication Manager for AT&T trunk access (**Section 6.6.2**) – This entity, and its associated Entity Link (using IPv6 and TLS with port 5067), is for calls to/from AT&T and Communication Manager via the Avaya SBCE.
- Avaya SBCE (**Section 6.6.33**) – This entity, and its associated Entity Link (using IPv6 and TLS with port 5061), is for calls to/from the IPFR-EF service via the Avaya SBCE.
- Communication Manager for local trunk access (**Section 6.6.44**) – This entity, and its associated Entity Link (using IPv4 and TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager, as well as calls to Messaging.

**Note** – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5067), 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.

### 6.6.1. 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., **Session Manager**).
- **IP Address Family**: Since Session Manager connects to SIP entities that use IPv4 and IPv6 addresses, select **both**. Note that field is only present after IPv6 has been enabled in Session Manager (**Section 6.2**).
- **IPv4 Address** – Enter the IPv4 address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.81**).
- **IPv6 Address** – Enter the IPv6 address of Session Manager signaling interface (e.g. **fd22:305b:b390:14e6:6**)
- **Type** – Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 6.4.1**).
- **Time Zone** – Select the time zone in which Session Manager resides.
- **Minimum TLS Version** – Select the TLS version, or select **Use Global Settings** to use the default TLS version, configurable at the global level (**Elements**→**Session Manager**→**Global Settings**).

**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.



Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

### SIP Entity Details

Commit Cancel

**General**

\* Name: Session Manager

\* IP Address Family: Both

\* IPv4 Address: 10.64.91.81

IPv6 Address: fd22:305b:b390:14e6::6

SIP FQDN:

Type: Session Manager

Notes:

Location: Main

Outbound Proxy:

Time Zone: America/Denver

Minimum TLS Version: Use Global Setting

Credential name:

**Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

**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 6.7**. Click on **Add** and provision entries as follows:

- **Port** – Enter **5061**
- **Protocol** – Select **TLS**
- **Default Domain** – Select a SIP domain administered in **Section 6.23** (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 6.7**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

Listen Ports

Add Remove

1 Item Filter: Enable

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

Select : All, None

## 6.6.2. 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-TG7**).
- **IP Address Family**: Select **IPv6**.
- Check the **Tolerance** box. With this setting, Session Manager will allow messages on this entity that may contain IP addresses of the opposite address family (IPv4) in some of the headers, without modifying them.
- **FQDN or IPv6 Address** – Enter the IPv6 address of Communication Manager Processor Ethernet (procr6) interface, described in **Section 5.6** (e.g., **fd22:305b:b390:14e6::5**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM TG7 ATT IPFR IPv6** administered in **Section 6.5.1**.
- **Location** – Select Location **CM-TG-7** administered in **Section 6.4.2**.
- **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, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. At the top right of the main area are 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields and settings:

- Name:** CM-TG7
- IP Address Family:** IPv6 (dropdown), **Tolerance:** ☒
- FQDN or IPv6 Address:** fd22:305b:b390:14e6::5
- Type:** CM (dropdown)
- Notes:** CM IPv6 trunk for AT&T IPFR
- Adaptation:** CM TG7 ATT IPFR IPv6 (dropdown)
- Location:** CM-TG7 (dropdown)
- Time Zone:** America/Denver (dropdown)
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting (dropdown)
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** none (dropdown)

Below the 'General' section is the 'Loop Detection' section with the following settings:

- Loop Detection Mode:** On (dropdown)
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200

At the bottom is the 'Monitoring' section with the following settings:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration (dropdown)

### 6.6.3. Avaya Session Border Controller for Enterprise SIP Entity

Repeat the steps in **Section 6.6.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **SBCE-ATT-IPFR- IPv6**).
- **FQDN or IPv6 Address** – Enter the IPv6 address of the A1 (private) interface of the Avaya SBCE (e.g., **fd22:305b:b390:1436::1a**). See **Section 7.6**.
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for ATT** (**Section 6.5.2**).
- **Location** – Select Location **SBCE IPv6** administered in **Section 6.4.3**.

**SIP Entity Details** Commit Cancel

**General**

\* Name:

\* IP Address Family:  Tolerance: ☒

\* FQDN or IPv6 Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

**Loop Detection**

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

**Monitoring**

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

#### 6.6.4. Avaya Aura® Communication Manager SIP Entity – Local Trunk

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 6.6.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **CM-TG3**).
- **IP Address Family** – Select **IPv4**.
- **FQDN or IPv4 Address** – Enter the IPv4 address of Communication Manager Processor Ethernet (procr) interface, described in **Section 06** (e.g., **10.64.19.75**)
- **Adaptations** – Leave this field blank.
- **Location** – Select Location **Main** administered in **Section 6.4.1**.

**SIP Entity Details** Commit Cancel

**General**

\* Name:

\* IP Address Family:  Tolerance: ☐

\* FQDN or IPv4 Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Minimum TLS Version:

Credential name:

Securable: ☒

Call Detail Recording:

**Loop Detection**

Loop Detection Mode:

**Monitoring**

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

## 6.7. Entity Links

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

- Session Manager to Communication Manager Public trunk (**Section 6.7.1**).
- Session Manager to Avaya SBCE (**Section 6.7.2**).
- Session Manager to Communication Manager Local trunk (**Section 6.7.3**).

**Note** – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.6**.

**Note** – See the information in **Section 6.6** regarding the transport protocols and ports used in the reference configuration.

### 6.7.1. 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 TG7**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.6.1** for Session Manager (e.g., **SessionManager**).
- **Protocol** – Select TLS (see **Section 5.10.1**).
- **SIP Entity 1 Port** – Enter **5067**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.6.2** for the Communication Manager public entity (e.g., **CM-TG7**).
- **SIP Entity 2 Port** – Enter **5067** (see **Section 5.10.1**).
- **IP Address Family** – Select **IPv6**.
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

**Step 3** - Click on **Commit**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	IP Address Family	DNS Override	Connection Policy
SM to CM TG7	Session Manager	TLS	5067	CM-TG7	5067	IPv6		trusted

## 6.7.2. 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 6.7.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to SBCE ATT FR IPv6**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.6.3** for the Avaya SBCE entity (e.g., **SBCE-ATT-IPFR-IPv6**).
- **SIP Entity 2 Port** – Enter **5061**.
- **IP Address Family** – Select **IPv6**.

The screenshot shows the 'Entity Links' configuration page in the Avaya management interface. The left sidebar has 'Entity Links' selected. The main area shows a table with one item. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, and Connection Policy. The row values are: Name: SM to SBCE ATT FR IPv6, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5061, SIP Entity 2: SBCE-ATT-IPFR-IPv6, Port: 5061, IP Address Family: IPv6, DNS Override: (unchecked), and Connection Policy: trusted. There are 'Commit' and 'Cancel' buttons at the top right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	IP Address Family	DNS Override	Connection Policy
SM to SBCE ATT FR IPv6	Session Manager	TLS	5061	SBCE-ATT-IPFR-IPv6	5061	IPv6	<input type="checkbox"/>	trusted

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

To configure this Entity Link, repeat the steps in **Section 6.7.1**, 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 6.6.44** for the Communication Manager local entity (e.g., **CM-TG3**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 5.10.2**).
- **IP Address Family** – Select **IPv4**.

The screenshot shows the 'Entity Links' configuration page in the Avaya management interface. The left sidebar has 'Entity Links' selected. The main area shows a table with one item. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, and Connection Policy. The row values are: Name: SM to CM TG3, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5061, SIP Entity 2: CM-TG3, Port: 5061, IP Address Family: IPv4, DNS Override: (unchecked), and Connection Policy: trusted. There are 'Commit' and 'Cancel' buttons at the top right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	IP Address Family	DNS Override	Connection Policy
SM to CM TG3	Session Manager	TLS	5061	CM-TG3	5061	IPv4	<input type="checkbox"/>	trusted

## 6.8. 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	

## 6.9. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (**Section 6.9.1**).
- Outbound calls to AT&T/PSTN (**Section 6.9.2**).

### 6.9.1. Routing Policy for Inbound Calls 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-TG7**), 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.

**Routing Policy Details**

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

**Step 4** - In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.6.2** for the Communication Manager public SIP Entity (**CM-TG7**), and click on **Select**.

SIP Entities

Select

Cancel

Help ?

SIP Entities

19 Items

Filter: Enable

	Name	IP Address Family	FQDN or IPv4 Address	FQDN or IPv6 Address	Type	Notes
<input type="radio"/>	Aura Messaging	IPv4	10.64.91.84		Messaging	Aura Messaging
<input type="radio"/>	Breeze	IPv4	10.64.91.18		Avaya Breeze	
<input type="radio"/>	CM-TG1	IPv4	10.64.91.75		CM	Trunk Group 1 - CM to Vz-IPT
<input type="radio"/>	CM-TG2	IPv4	10.64.91.75		CM	Trunk Group 2 - Vz-Toll-Free inbound
<input type="radio"/>	CM-TG3	IPv4	10.64.91.75		CM	Trunk Group 3 - CM to Enterprise
<input type="radio"/>	CM-TG4	IPv4	10.64.91.75		CM	Trunk Group 4 - ATT IPTF
<input type="radio"/>	CM-TG5	IPv4	10.64.91.75		CM	Trunk Group 5 - ATT IPFR
<input type="radio"/>	CM-TG6	IPv6		fd22:305b:b390:14e6::5	CM	CM IPv6 trunk for AT&T TF
<input checked="" type="radio"/>	CM-TG7	IPv6		fd22:305b:b390:14e6::5	CM	CM IPv6 trunk for AT&T IPFR
<input type="radio"/>	CM-TG9	IPv4	10.64.91.75		CM	Masergy
<input type="radio"/>	ExperiencePortal	IPv4	10.64.91.90		Voice Portal	
<input type="radio"/>	Presence	IPv4	10.64.91.18		Presence Services	
<input type="radio"/>	SBC1	IPv4	10.64.91.50		SIP Trunk	Avaya SBC-1 to PSTN
<input type="radio"/>	SBC2-100	IPv4	10.64.91.100		SIP Trunk	Avaya SBC-2 to PSTN
<input type="radio"/>	SBC2-101	IPv4	10.64.91.101		SIP Trunk	SBCE Masergy

Select : None

Page 1 of 2

**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 6.8**, and click on **Select**.

**Step 7** - Returning to the **Routing Policy Details** page in the **Time of Day** section, enter a **Ranking** of 0.

**Step 8** - No **Regular Expressions** were used in the reference configuration.

**Step 9** - Click on **Commit**.

**Note** – Once the **Dial Patterns** are defined (**Section 6.10**) they will appear in the **Dial Pattern** section of this form.

Routing Policy Details		Commit Cancel	Help ?								
General											
* Name: To CM TG7											
Disabled: <input type="checkbox"/>											
* Retries: 0											
Notes: Incoming from ATT FR IPv6											
SIP Entity as Destination											
Select											
Name	IP Address Family	FQDN or IPv4 Address	FQDN or IPv6 Address	Type	Notes						
CM-TG7	IPv6		fd22:305b:b390:14e6::5	CM	CM IPv6 trunk for AT&T IPFR						
Time of Day											
Add Remove View Gaps/Overlaps											
1 Item											
Filter: Enable											
<input type="checkbox"/> Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/> 0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	
Select : All, None											



## 6.9.2. Routing Policy for Outbound Calls to AT&T

This Routing Policy is used for Outbound calls to AT&T. Repeat the steps in **Section 6.9.1** 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 IPv6 FR**), 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 6.6.33** for the Avaya SBCE SIP Entity (e.g., **SBCE-ATT-IPFR-IPv6**).

**Routing Policy Details** [Commit] [Cancel] [Help ?](#)

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Name	IP Address Family	FQDN or IPv4 Address	FQDN or IPv6 Address	Type	Notes
SBCE-ATT-IPFR-IPv6	IPv6		fd22:305b:b390:14e6::1a	SIP Trunk	SBCE IPv6 FR Inside A1

**Time of Day**

[Add] [Remove] [View Gaps/Overlaps]

1 Item [Filter: Enable](#)

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

Select : All, None

## 6.10. 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 6.10.1**).
- Outbound calls to AT&T (**Section 6.10.2**).

### 6.10.1. 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 732555xxxx). 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 **732555**. Note – The Adaptation defined for Communication Manager in **Section 6.5.1** will convert the various 732-555-xxxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

**Dial Pattern Details** [Commit] [Cancel] Help ?

**General**

\* Pattern: 732555

\* Min: 10

\* Max: 10

Emergency Call: ☐

SIP Domain: avayalab.com

Notes:

**Originating Locations, Origination Dial Pattern Sets, and Routing Policies**

[Add] [Remove]

0 Items

Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
---------------------------	----------------------------	-----------------------------------	------------------------------------	---------------------	------	-------------------------	----------------------------	----------------------

**Denied Originating Locations and Origination Dial Pattern Sets**

[Add] [Remove]

**Step 3** - Scroll down to the **Originating Location, Origination Dial Patterns and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.

**Step 4** – In the **Originating Location** area, check the checkbox corresponding to the Avaya SBCE location, e.g., **SBCE-IPv6**.

**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 6.9.1** (e.g., **To CM-TG7**), and click on **Select** (not shown).

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

7 Items Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5
<input type="checkbox"/>	CM-TG7	ATT IPFR IPv6 trunk
<input type="checkbox"/>	Common-SBCs	SBC to PSTN
<input type="checkbox"/>	Experience Portal	
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1
<input checked="" type="checkbox"/>	SBCE-IPv6	

Select : All, None

**Origination Dial Pattern Sets**

1 Item Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Calls from local area code	

Select : None

**Routing Policies**

16 Items Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AAM	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM6 IPv6	<input type="checkbox"/>	CM-TG6	
<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 type="checkbox"/>	To CM-TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN to CM
<input type="checkbox"/>	To CM TG6	<input type="checkbox"/>	CM-TG6	Incoming ATT TF IPv6
<input checked="" type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Incoming from ATT FR IPv6
<input type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	ExperiencePortal	

**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.

## 6.10.2. 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., \*71yyyzzzxxxx & \*91yyyzzzxxxx) are specified.

**Step 1** – Repeat the steps shown in **Section 6.10.1**, 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 **10**.
- Enter a **Max** pattern of **36**.
- In the **Routing Policies** section of the **Originating Locations, Origination Dial Patterns and Routing Policies** page, check the checkbox for the Originating Location corresponding to the Communication Manager Trunk Group 7 (e.g., **CM-TG-7**) and the Routing Policy administered for routing calls to AT&T in **Section 6.9.2** (e.g., **To SBCE ATT IPV6 FR**).

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* Pattern: +

\* Min: 10

\* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: E.164 Public Numbers

**Originating Locations, Origination Dial Pattern Sets, and Routing Policies**

Add Remove Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CM-TG7	ATT IPFR IPV6 trunk			To SBCE ATT IPV6 FR	0	<input type="checkbox"/>	SBCE-ATT-IPFR-IPV6	

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.

## 6.11. Security Module Configuration

Verify and complete the Session Manager Security Module networking configuration.

**Step 1** – From the **Home** screen, navigate to **Elements** → **Session Manager** → **Session Manager Administration**.

**Step 2** – Select the Session Manager instance and click **Edit**.

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Session Manager Instances | Branch Session Manager Instances

Session Manager Instances

New View Edit Delete

1 Item Filter: Enable

Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
Session Manager	Normal	40	0	40	

Select : None

**Step 3** – In the **Security Module** area, the field **SIP Entity IP Address** is display only, showing the IPv4 addresses of the Session Manager Entity as configured in **Section 6.6.1**. Verify the **Network Mask** and **Default Gateway**. These IP addresses should have been configured during the Session Manager initial installation.

**Step 4** – The field **SIP Entity IPv6 Address** is display only, showing the IPv6 addresses of the Session Manager Entity as configured in **Section 6.6.1**. Enter the **IPv6 Network prefix length** (e.g., 64) and **IPv6 Default Gateway** (e.g., fd22:305b:b390:14e6::1) as shown on the screen below.

**Step 5** – Click on **Commit** to save the changes.

Home Session Manager

Session Manager Administration

Dashboard

Session Manager Admin...

Global Settings

Communication Profile ...

Network Configuration

Device and Location ...

Application Configur...

System Status

System Tools

Performance

Edit Session Manager

Commit Cancel

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Logging |

Expand All | Collapse All

General

SIP Entity Name Session Manager

Description

\*Management Access Point Host Name/IP 10.64.90.81

\*Direct Routing to Endpoints Enable

Data Center gsscp

Avaya Aura Device Services Server Pairing AADS\_9185

Maintenance Mode

Security Module

SIP Entity IP Address 10.64.91.81

\*Network Mask 255.255.255.0

\*Default Gateway 10.64.91.1

SIP Entity IPv6 Address fd22:305b:b390:14e6::6

\*IPv6 Network prefix length 64

\*IPv6 Default Gateway fd22:305b:b390:14e6::1

\*Call Control PHB 46

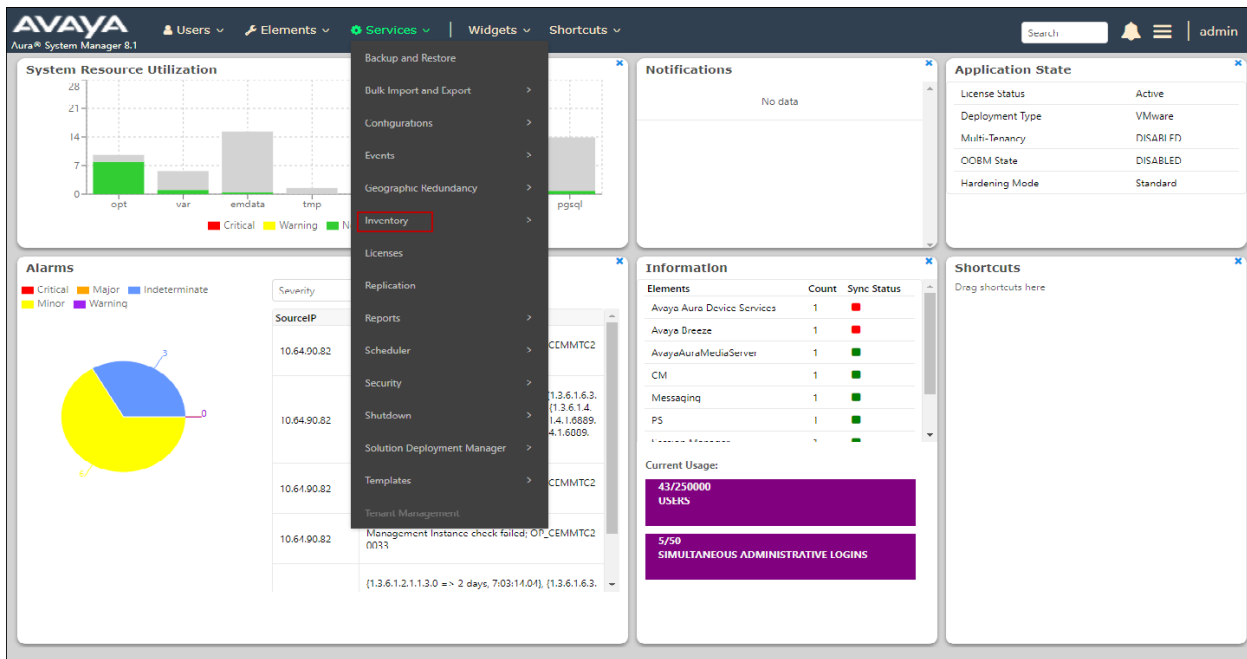
\*SIP Firewall Configuration SM 6.3.8.0

## 6.12. Verify TLS Certificates – Session Manager

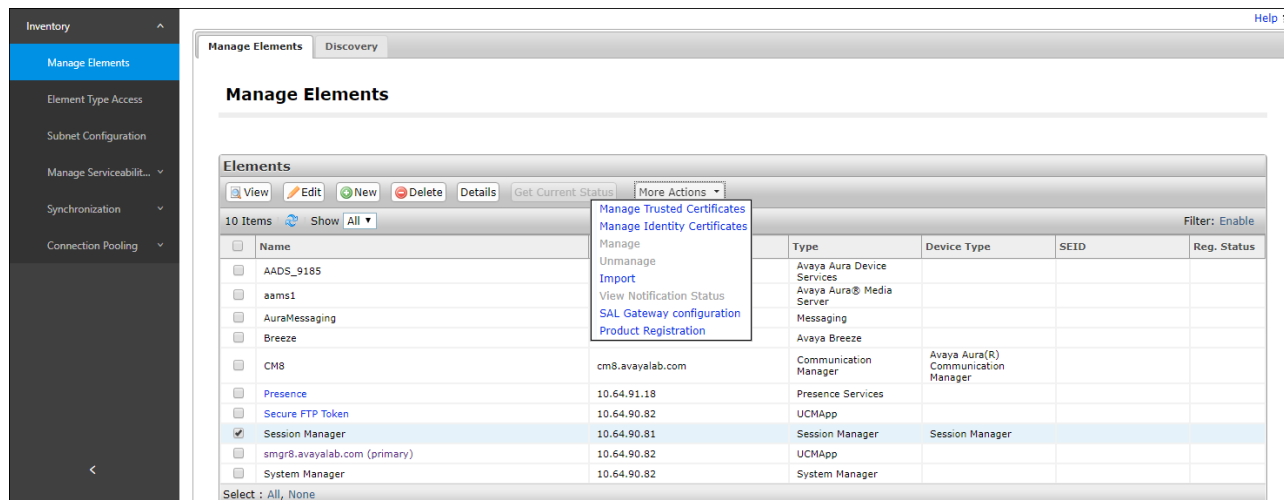
**Note** – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

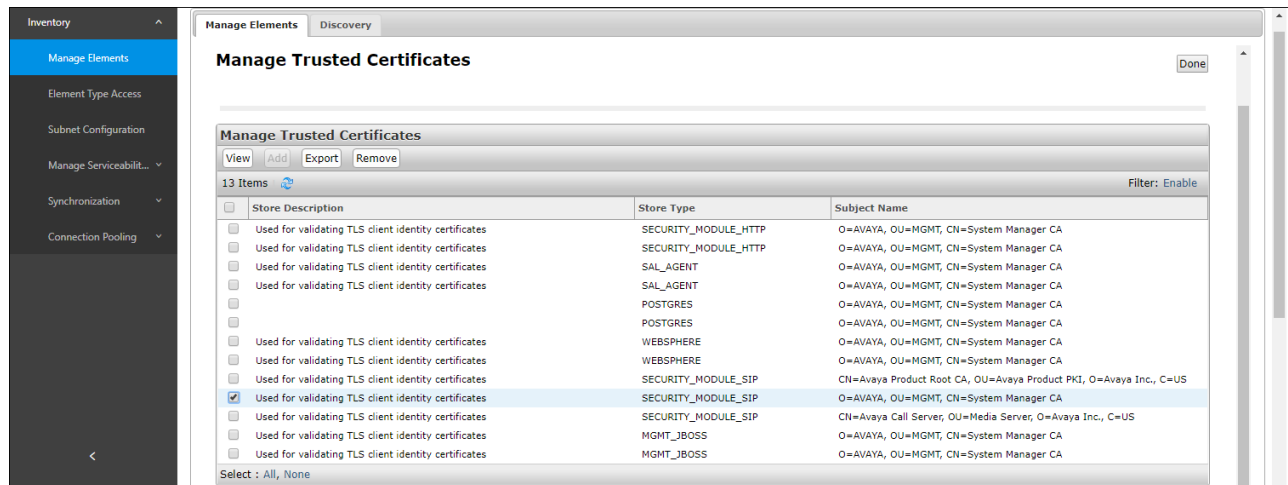
**Step 1** - From the **Home** screen, under the **Services** heading, select **Inventory**.



**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**.

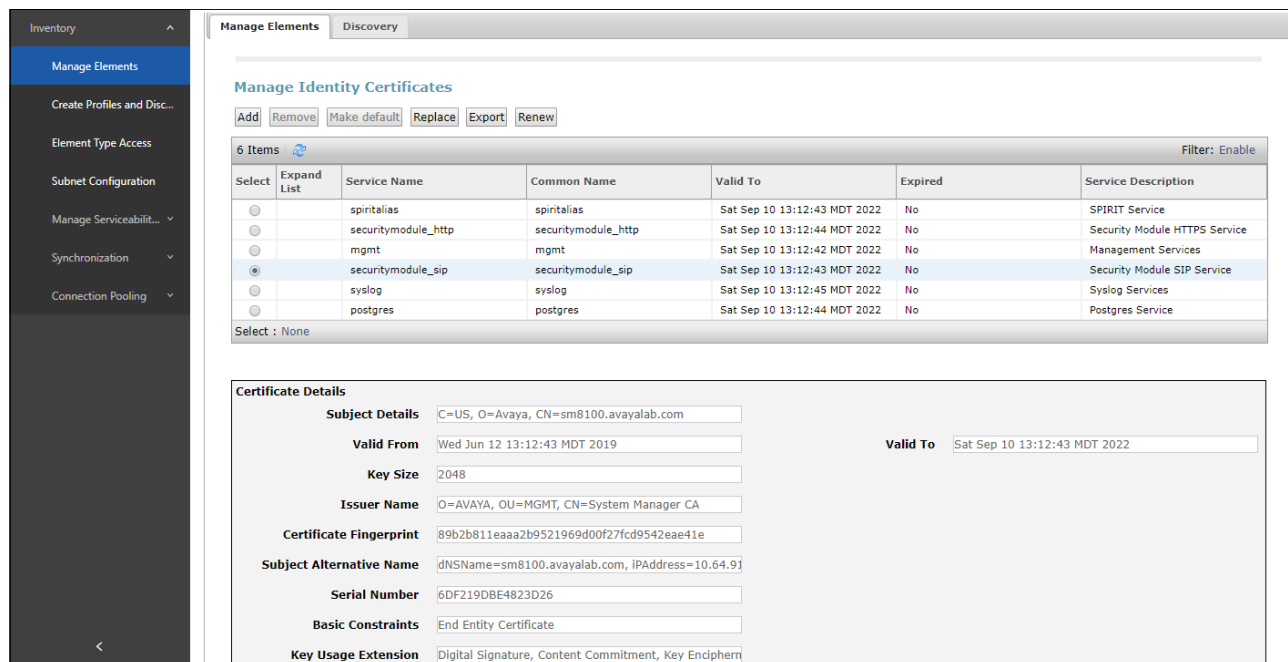


**Step 3** - Verify the System Manager Certificate Authority certificate is listed in the trusted store, **SECURITY\_MODULE\_SIP**. Click **Done** to return to the previous screen.



**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**.



## 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 [11] and [12] in the References section 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.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter <https://ipaddress/sbc> in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE. Log in using the appropriate credentials.



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, there is a "Log In" section with fields for "Username:" (containing "ucsec") and "Password:" (containing masked characters). A "Log In" button is positioned below the password field. Below the login fields, a "WELCOME TO AVAYA SBC" message is displayed, 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, a consent statement reads: "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 - 2019 Avaya Inc. All rights reserved." is visible.



The EMS Dashboard page of the Avaya SBCE will appear. 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 screenshot shows the Avaya Session Border Controller for Enterprise EMS Dashboard. The top navigation bar includes links for Device: EMS, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. The left-hand menu lists 'EMS Dashboard' with sub-options: Device Management, System Administration, Backup/Restore, and Monitoring & Logging. The main content area is titled 'Dashboard' and contains several sections:

- Information:** A table showing system details.
 

System Time	10:24:50 AM MDT	Refresh
Version	8.1.0.0-14-18490	
GUI Version	8.1.0.0-18490	
Build Date	Mon Feb 03 17:23:09 UTC 2020	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	03/27/2020 07:00:46 MDT	
Failed Login Attempts	0	
- Installed Devices:** A table showing the installed device.
 

EMS
SBCE8-70
- Active Alarms (past 24 hours):** None found.
- Incidents (past 24 hours):** None found.
- Notes:** No notes found.

## 7.1. Device Management – Status

**Step 1** - Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE8-70** is shown. Verify that the **Status** column shows **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 Avaya Session Border Controller for Enterprise EMS Dashboard, specifically the Device Management section. The left-hand menu now highlights 'Device Management'. The main content area is titled 'Device Management' and contains several tabs: Devices, Updates, SSL VPN, Licensing, and Key Bundles. The 'Devices' tab is selected, displaying a table of installed devices:

Device Name	Management IP	Version	Status	
SBCE8-70	10.64.90.70	8.1.0.0-14-18490	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

**Step 2** - Click on **View** to display the **System Information** screen. The screen shows the **Network Configuration, DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. In the shared test environment, the highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to AT&T.

System Information: SBCE8-70

General Configuration

Appliance NameSBCE8-70

Box TypeSIP

Deployment ModeProxy

Device Configuration

HA ModeNo

Two Bypass ModeNo

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	10	100
Advanced Sessions	10	100
Scopia Video Sessions	10	100
CES Sessions	10	100
Transcoding Sessions	10	100
CLID	---	
Encryption	Available: Yes <input checked="" type="checkbox"/>	

Network Configuration

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
10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1
				B1
3ffe:ffff:bb:bb::240	3ffe:ffff:bb:bb::240	64	3ffe:ffff:bb:bb::1	B1
				B1
				B2
fd22:305b:b390:14e6::8	fd22:305b:b390:14e6::8	64	fd22:305b:b390:14e6::1	A1
fd22:305b:b390:14e6::1a	fd22:305b:b390:14e6::1a	64	fd22:305b:b390:14e6::1	A1

DNS Configuration

Primary DNS10.64.19.201

Secondary DNS

DNS LocationDMZ

DNS Client IP10.64.91.40

Management IP(s)

IP #1 (IPv4)10.64.90.70

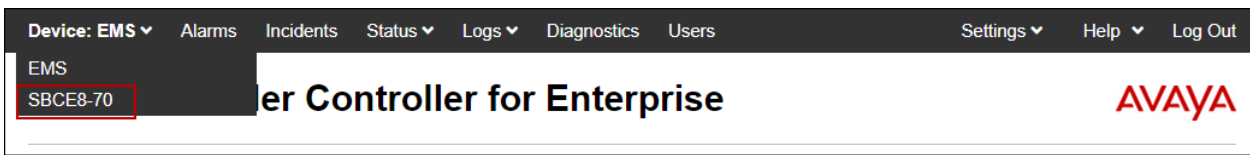
## 7.2. TLS Management

**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.

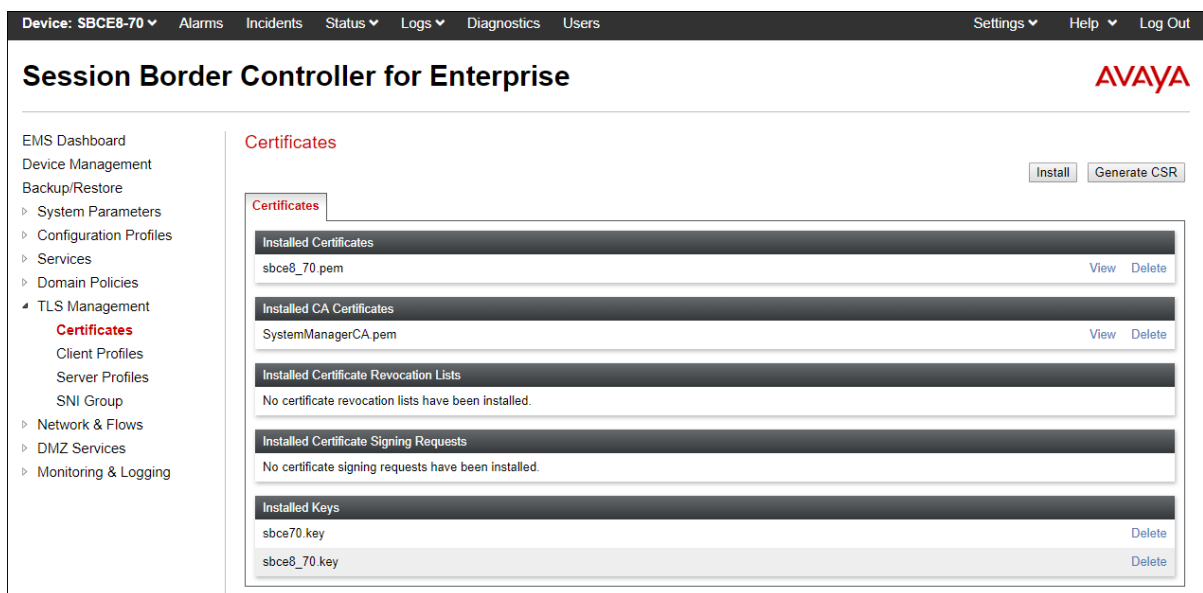
### 7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



**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.



## 7.2.2. Server Profiles

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

- **Profile Name:** enter a descriptive name. (e.g., **sbce8\_70Server**).
- **Certificate:** select the identity certificate, e.g., **sbce8\_70.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

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

The 'Edit Profile' dialog box shows the configuration for a TLS profile. At the top, there is a warning message: "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 'TLS Profile' section contains fields for 'Profile Name' (sbce8\_70Server), 'Certificate' (sbce8\_70.pem), 'SNI Options' (None), and 'SNI Group' (None). The 'Certificate Verification' section includes 'Peer Verification' (None), 'Peer Certificate Authorities' (SystemManagerCA.pem), 'Peer Certificate Revocation Lists' (empty), and 'Verification Depth' (0). A 'Next' button is at the bottom right.

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

The 'Session Border Controller for Enterprise' interface displays the 'Server Profiles: sbce8\_70Server' section. The 'Server Profiles' list shows 'sbce8\_70Server' with an 'Add' button. The 'Server Profile' details are shown in a table format:

Server Profile	
Click here to add a description.	
<b>TLS Profile</b>	
Profile Name	sbce8_70Server
Certificate	sbce8_70.pem
SNI Options	None
<b>Certificate Verification</b>	
Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>
<b>Renegotiation Parameters</b>	
Renegotiation Time	0
Renegotiation Byte Count	0
<b>Handshake Options</b>	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:IDH:ADH: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 a descriptive name (e.g., **sbce8\_70Client**)
- **Certificate:** select the identity certificate, e.g., **sbce8\_70.pem**, 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**.
- Enter 1 under **Verification Depth**. Click **Next**.

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

The 'Edit Profile' dialog box shows the configuration for a TLS Client Profile. At the top, a warning message states: '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.' The 'TLS Profile' section includes fields for 'Profile Name' (sbce8\_70Client), 'Certificate' (sbce8\_70.pem), and 'SNI' (Enabled). The 'Certificate Verification' section includes 'Peer Verification' (Required), 'Peer Certificate Authorities' (SystemManagerCA.pem), 'Peer Certificate Revocation Lists' (empty), 'Verification Depth' (1), 'Extended Hostname Verification' (disabled), and 'Server Hostname' (empty). A 'Next' button is at the bottom.

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

The 'Session Border Controller for Enterprise' interface shows the 'Client Profiles' section. The profile 'sbce8\_70Client' is selected. The 'Client Profile' form is displayed with the following details: 'Profile Name' (sbce8\_70Client), 'Certificate' (sbce8\_70.pem), 'SNI' (Enabled), 'Peer Verification' (Required), 'Peer Certificate Authorities' (SystemManagerCA.pem), 'Peer Certificate Revocation Lists' (---), 'Verification Depth' (1), 'Extended Hostname Verification' (disabled), 'Renegotiation Parameters' (Renegotiation Time: 0, Renegotiation Byte Count: 0), and 'Handshake Options' (Version: TLS 1.2, TLS 1.1, TLS 1.0; Ciphers: Default, FIPS, Custom; Value: HIGH IDH IADH IMD5 IaNULL IaNULL @STRENGTH). An 'Edit' button is at the bottom.

## 7.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Networks & Flows → Network Management**. On the **Networks** tab, verify/edit the IP addresses assigned to the interfaces. The following screen shows the enterprise interface is assigned to **A1** and the interface towards AT&T is assigned to **B1**.

**Step 1** - Select **Networks & Flows → Network Management** from the menu on the left-hand side.

**Step 2** - The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.



**Session Border Controller for Enterprise** AVAYA

EMS Dashboard  
Device Management  
Backup/Restore  
‣ System Parameters  
‣ Configuration Profiles  
‣ Services  
‣ Domain Policies  
‣ TLS Management  
‣ Network & Flows  
  **Network Management**  
  Media Interface

**Network Management**

**Interfaces** **Networks** Add VLAN

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 B1 interfaces. The following Avaya SBCE interfaces and associated IP addresses were used in the sample configuration:

- **Outside-B1-IPv6:** **3ffe:ffff:bb:bb::240** – IPv6 address configured toward the AT&T IPTF service. This address is known to AT&T. See **Section 3**.
- **Inside-A1-IPv6:** **fd22:305b:b390:14e6::1a**– IPv6 address configured for the AT&T IPFR-EF service toward the private network.
- **Inside-A1:** **10.64.91.40** – IPv4 address configured for AT&T IPFR-EF service toward the private network.

**Note:** Even though signaling between the Avaya SBCE and Session Manager in the reference configuration is configured to use IPv6 addresses, a secondary IPv4 interface toward the private network is used for direct media (shuffling) interoperability with devices and endpoints on the enterprise that use IPv4 addresses only.

## Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

Certificates

Client Profiles

Server Profiles

SNI Group

▸ Network & Flows

Network Management

### Network Management

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, 10.64.91.41	<a href="#">Edit</a> <a href="#">Delete</a>
Outside-B1	3ffe:ffff:bb:bb::1	64	B1	3ffe:ffff:bb:bb::240	<a href="#">Edit</a> <a href="#">Delete</a>
Outside-B1-IPv6	3ffe:ffff:bb:bb::1	64	B1	3ffe:ffff:bb:bb::240	<a href="#">Edit</a> <a href="#">Delete</a>
Inside-A1-IPv6	fd22:305b:b390:14e6::1	64	A1	fd22:305b:b390:14e6::8, fd22:305b:b390:14e6::1a	<a href="#">Edit</a> <a href="#">Delete</a>

## 7.4. Advanced Options

AT&T required the UDP port ranges of the media to be configured in the **16384 – 32767** range. However, by default ranges 12000 to 21000 and 22000 to 31000 are already allocated by the Avaya SBCE for internal use. The following steps reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T can be defined on the Avaya SBCE Media Interfaces (**Section 7.5**).

**Step 1** - Select **Network & Flows** → **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** - Select **Save**. Note that changes to these values require an application restart (see **Section 7.1**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. Under Network & Flows, the 'Advanced Options' link is highlighted. The main content area is titled 'Advanced Options' and contains several tabs: Periodic Statistics, Feature Control, SIP Options, Network Options, Port Ranges (selected), RTP Monitoring, and Load Monitoring. A warning message states: 'Changes to the settings below require an application restart before taking effect. Application restarts can be issued from Device Management.' Below this, the 'Port Range Configuration' section shows four rows with input fields for port ranges: Signaling Port Range (12000 - 16380), Config Proxy Internal Signaling Port Range (42000 - 51000), Listen Port Range (6000 - 6999), and HTTP Port Range (51001 - 62000). A 'Save' button is located at the bottom right of the configuration area.

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



## 7.5. Media Interfaces

Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. As mentioned in **Section 7.4**, 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.

Some ports in the range required by AT&T were already allocated by the Avaya SBCE for internal use, by default. **Section 7.4** shows the steps required to reallocate the port ranges used by the Avaya SBCE, so the range required by AT&T could be accommodated.

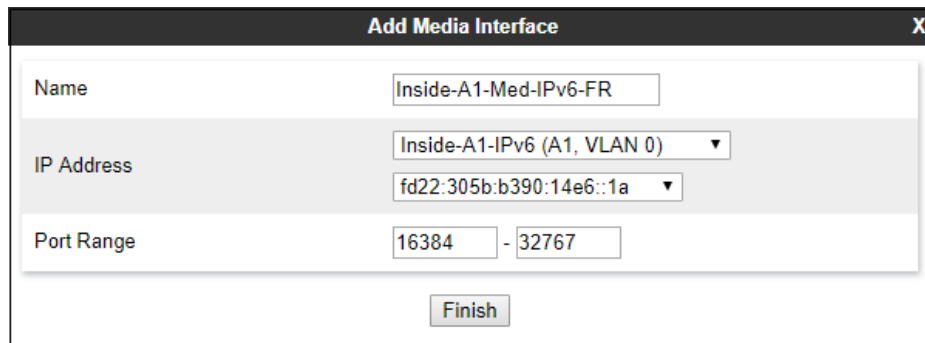
**Note:** In the reference configuration, both IPv6 and IPv4 media interfaces are created toward the private network. This is done for direct IP-IP media (shuffling) interoperability between the Avaya SBCE and devices and endpoints on the enterprise that operate only at IPv4. On the public side to the AT&T IPFR-EF trunk, only the IPv6 media interface is required.

**Step 1** - Select **Network & Flows → Media Interface** on the left-hand side menu,

**Step 2** - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Inside-A1-Med-IPv6-FR
- **IP Address:** Select **Inside-A1-IPv6 (A1, VLAN 0)** and **fd22:305b:b390:14e6::1a**
- **Port Range:** **16384 – 32767**

**Step 3** - Click **Finish**.



The screenshot shows a window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains three main configuration sections:

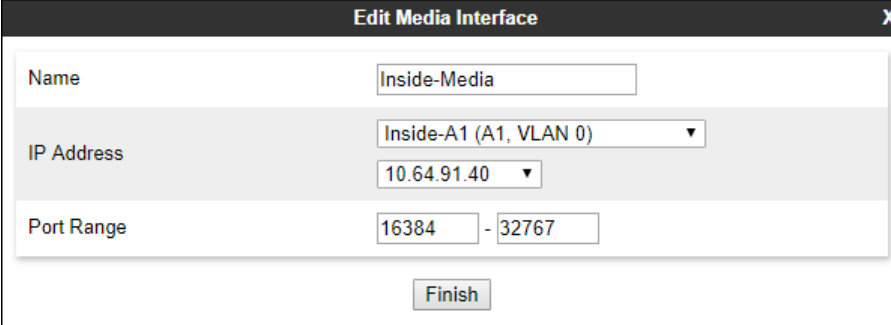
- Name:** A text input field containing "Inside-A1-Med-IPv6-FR".
- IP Address:** A section with two dropdown menus. The first dropdown is set to "Inside-A1-IPv6 (A1, VLAN 0)". The second dropdown is set to "fd22:305b:b390:14e6::1a".
- Port Range:** Two text input fields. The first contains "16384" and the second contains "32767", separated by a hyphen.

At the bottom center of the window is a button labeled "Finish".

**Step 4** - Select **Add** again (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Inside-Media
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.40**
- **Port Range:** 16384 – 32767

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

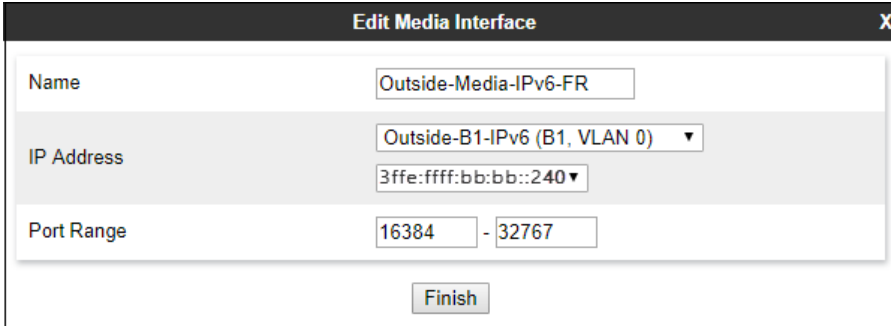


The screenshot shows a window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains three main sections: "Name" with a text field containing "Inside-Media"; "IP Address" with a dropdown menu showing "Inside-A1 (A1, VLAN 0)" and a text field below it containing "10.64.91.40"; and "Port Range" with two text fields containing "16384" and "32767" separated by a hyphen. A "Finish" button is located at the bottom center of the window.

**Step 6** - Select **Add** again (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Outside-Media-IPv6-FR
- **IP Address:** Select **Outside-B1-IPv6 (B1, VLAN0)** and **3ffe:ffff:bb:bb::240**
- **Port Range:** 16384 – 32767

**Step 7** - Click **Finish**.



The screenshot shows a window titled "Edit Media Interface" with a close button (X) in the top right corner. The window contains three main sections: "Name" with a text field containing "Outside-Media-IPv6-FR"; "IP Address" with a dropdown menu showing "Outside-B1-IPv6 (B1, VLAN 0)" and a text field below it containing "3ffe:ffff:bb:bb::240"; and "Port Range" with two text fields containing "16384" and "32767" separated by a hyphen. A "Finish" button is located at the bottom center of the window.

## 7.6. Signaling Interfaces

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

**Step 1** - Select **Network & Flows → Signaling Interface** from the menu on the left-hand side

**Step 2** - Select **Add** (not shown) and enter the following:

- **Name:** Inside-A1-Sig-IPv6-FR
- **IP Address:** Select **Inside-A1-IPv6 (A1, VLAN0)** and **fd22:305b:b390:14e6::1a**
- **TLS Port:** 5061
- **TLS Profile:** Select the TLS server profile created in **Section 7.2.2**.

**Step 3** - Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' dialog box with the following configuration:

Field	Value
Name	Inside-A1-Sig-IPv6-FR
IP Address	Inside-A1-IPv6 (A1, VLAN 0) fd22:305b:b390:14e6::1a
TCP Port	Leave blank to disable
UDP Port	Leave blank to disable
TLS Port	5061
TLS Profile	sbce8_70Server
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

**Step 4** - Select **Add** again, and enter the following:

- **Name:** Outside-Signaling-IPv6-FR
- **IP Address:** Select **Outside-B1-IPv6 (B1, VLAN0)** and **3ffe:ffff:bb:bb::240**
- **UDP Port:** 5060

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

The screenshot shows the 'Edit Signaling Interface' dialog box with the following configuration:

Field	Value
Name	Outside-Signaling-IPv6-FR
IP Address	Outside-B1-IPv6 (B1, VLAN 0) 3ffe:ffff:bb:bb::240
TCP Port	Leave blank to disable
UDP Port	5060
TLS Port	Leave blank to disable
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

## 7.7. Server Interworking Profiles

The Server Interworking profiles include parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for the enterprise and AT&T IPFR-EF service.

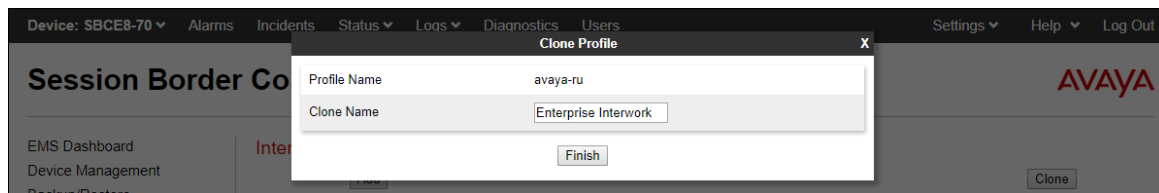
### 7.7.1. Server Interworking Profile – Enterprise

In the sample configuration, the enterprise Server Interworking profile was cloned from the default **avaya-ru** profile and then modified.

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

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

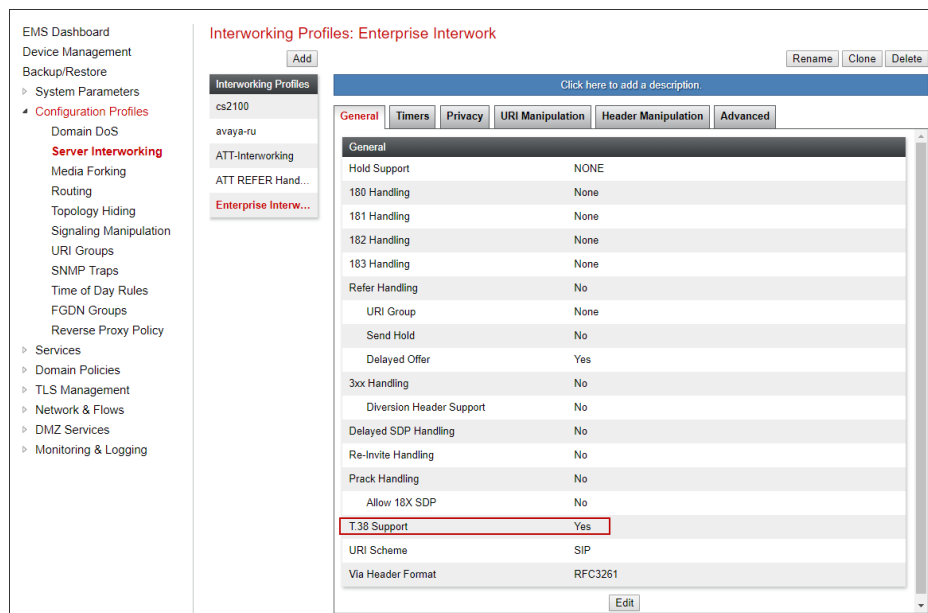
**Step 3** - Enter profile name: (e.g., **Enterprise Interwork**), and click **Finish** to continue.



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

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

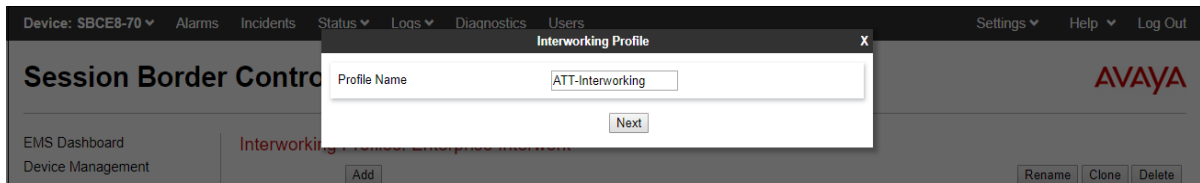
- Check **T38 Support**.
- All other options can be left with default values. Click **Finish** (not shown).



## 7.7.2. Server Interworking – AT&T

Repeat the steps shown in **Section Error! Reference source not found.** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

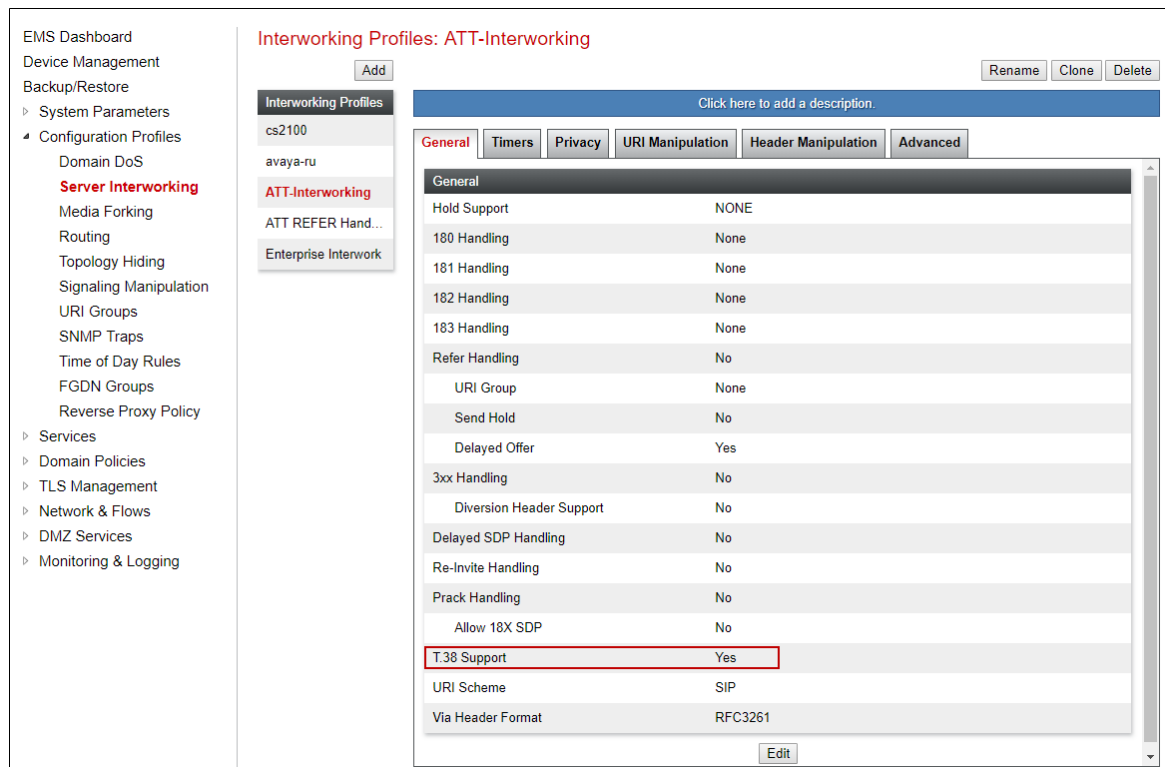
**Step 1** - Select **Add Profile** and enter a profile name: (e.g., **ATT-Interworking**) and click **Next**.



The screenshot shows the 'Session Border Controller' web interface. A modal dialog titled 'Interworking Profile' is open. It has a 'Profile Name' input field containing 'ATT-Interworking' and a 'Next' button. The background interface shows the 'Session Border Controller' title and the 'AVAYA' logo.

**Step 2** - The **General** screen will open:

- Default values are used with the exception of **T.38 Support** set to **Yes**



The screenshot shows the 'Interworking Profiles: ATT-Interworking' configuration screen. The 'General' tab is selected. The 'T.38 Support' option is highlighted with a red box, showing it is set to 'Yes'. The 'Add' button is visible at the top left of the configuration area.

Option	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
<b>T.38 Support</b>	<b>Yes</b>
URI Scheme	SIP
Via Header Format	RFC3261

**Step 3** – The **SIP Timers** and **Privacy** screens will open (not shown), accept default values for these screens by clicking **Next**.

**Step 4** – On the **Advanced/DTMF** tab:

- In the **Record Routes** field, check **Both Sides**.
- All other options can be left as default. Click **Finish** (not shown).

Interworking Profiles: ATT-Interworking

Buttons: Add, Rename, Clone, Delete

Interworking Profiles List:

- cs2100
- avaya-ru
- ATT-Interworking**
- ATT REFER Handl...
- Enterprise Interwork

Click here to add a description.

Tabs: General, Timers, Privacy, URI Manipulation, Header Manipulation, **Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No

**DTMF**

DTMF Support	None
--------------	------

Edit

## 7.8. Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, a 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 Server Interworking Profiles (**Section 7.7**) or Signaling Rules (**Section 7.14**) does not meet the desired result. Refer to References [11] for information on the Avaya SBCE scripting language.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor.

A Sigma script was created during the compliance test to correct the following interoperability issues:

- Remove the gsid and epv parameters from outbound Contact headers. See **Section Error!** Reference source not found..
- Remove the Bandwidth headers sent by some Avaya SIP endpoints. (**Section 2.2, item 6**).
- Change the Diversion header from SIPS to SIP towards AT&T. (**Section 2.2, item 2**)
- Convert the “anonymous.invalid” domain on the Ring Splash INVITE to an IPv6 address. (**Section 2.2, item 1**).

The details of the complete script appear on **Section 13**.

**Step 1** - Select **Configuration Profiles → Signaling Manipulation** from the menu on the left.

**Step 2** - Click **Add Script** (not shown) and the script editor window will open.

- Enter a name for the script in the **Title** box (e.g., **Script for IPFR-CM IPv6**).
- Copy and paste the script from **Section 13** in this document.

**Signaling Manipulation Editor** AVAYA

Title  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=(T|AS|CT):(\d+)\n\n","");
12
13  // fix call-fwd
14    %HEADERS["Diversion"][1].regex_replace("sips","sip");
15
16  }
17 }
18 within session "ALL"
19 {
20   act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
21   {
22
23   // RingSplash Fix
24    %BODY[1].regex_replace("anonymous.invalid","::");
25
26  }
```

**Step 3** - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the AT&T SIP Server profile in **Section 7.9.2**.

## 7.9. SIP Server Profiles

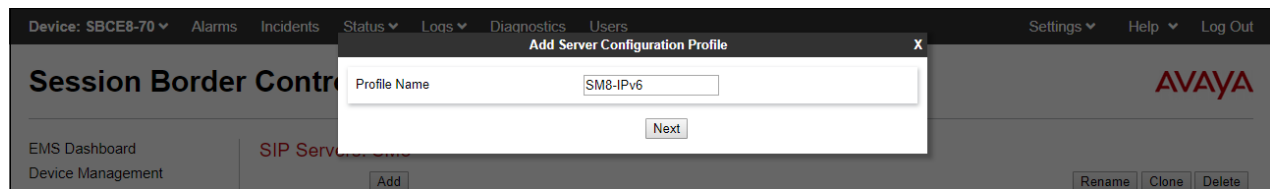
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

### 7.9.1. SIP Server Profile – Session Manager

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

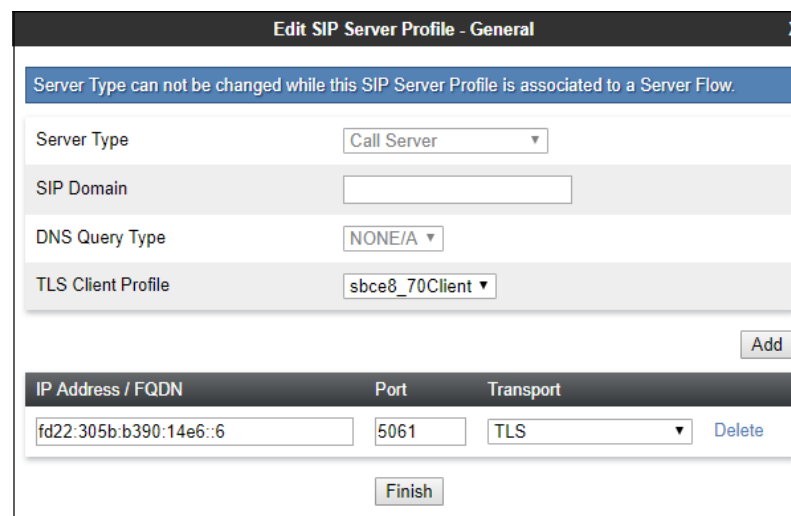
**Step 1** - Select **Services** → **SIP Servers** from the left-hand menu.

**Step 2** - Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM8-IPv6**) and click **Next**.



**Step 3** - The **Edit SIP Server 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., **sbce8\_70Client**)
- **IP Address/FQDN**: **fd22:305b:b390:14e6::6** (Session Manager Security Module IPv6 address). Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.



IP Address / FQDN	Port	Transport
fd22:305b:b390:14e6::6	5061	TLS





**Step 4** – Default values can be used on the **Authentication** tab.

**Step 5** – On the **Heartbeat** tab, check the **Enable Heartbeat** box to have the Avaya SBCE source “heartbeats” toward Session Manager. This configuration is optional.

- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward Session Manager.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.

The screenshot shows the 'Edit SIP Server Profile - Heartbeat' window. It contains the following fields and values:

Field	Value
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	sbce70@avayalab.com
To URI	sm8-6@avayalab.com

A 'Finish' button is located at the bottom right of the form.

**Step 6** – Default values are used on the **Registration** and **Ping** tabs.

**Step 7** – On the **Advanced** tab:

- Select the **Enterprise Interwork** (created in **Section 7.7.1**), for **Interworking Profile**.
- Since TLS transport is specified in **Step 3**, then the **Enable Grooming** option should be enabled.
- Select the **Tolerant** option, in order to support messages with headers with both IPv4 and IPv6 addresses in this server profile to the private network.
- Select **Finish**.

The screenshot shows the 'Edit SIP Server Profile - Advanced' window. It contains the following fields and values:

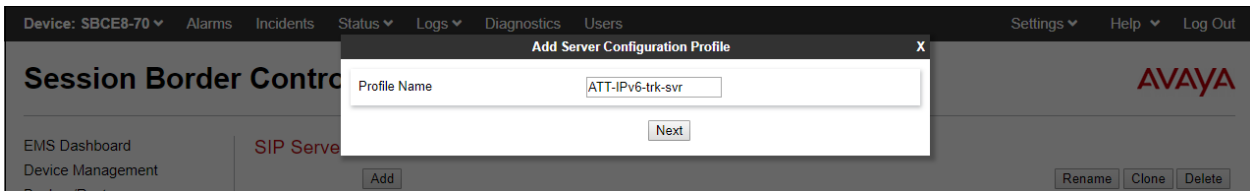
Field	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Enterprise Interwork
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant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

A 'Finish' button is located at the bottom right of the form.

## 7.9.2. SIP Server Profile – AT&T

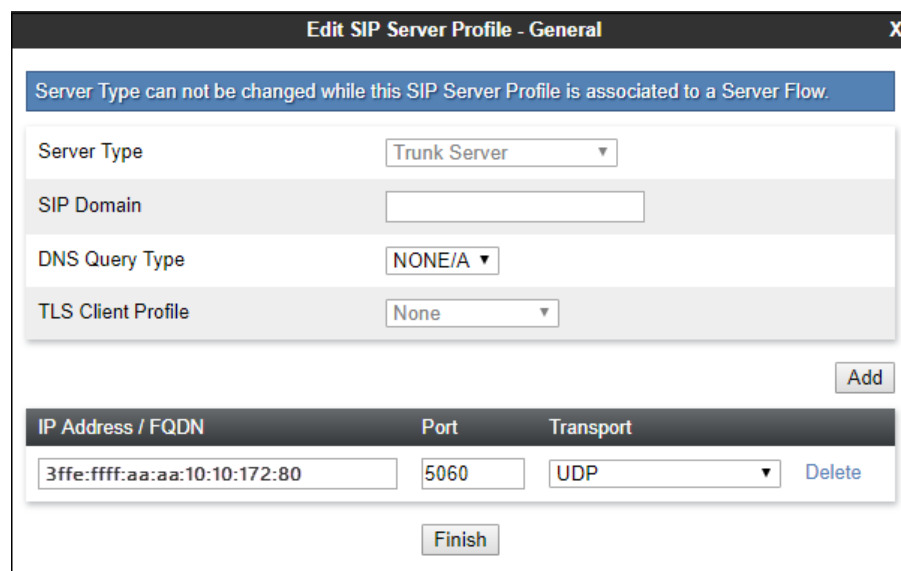
Repeat the steps in **Section 7.9.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to AT&T.

**Step 1** - Select **Add** and enter a Profile Name (e.g., **ATT-IPv6-trk-svr**) and select **Next**.



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

- Select **Server Type: Trunk Server**
- **IP Address/FQDN: 3ffe:ffff:aa:aa:10:10:172:80** (AT&T Border Element IPv6 address)
- **Port: 5060**
- Select **Transport: UDP**
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



**Step 3** – Default values can be used on the **Authentication** tab.

**Step 4** – On the **Heartbeat** tab, check the **Enable Heartbeat** box to have the Avaya SBCE source “heartbeats” toward AT&T. This configuration is optional.

- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward AT&T.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.

Enable Heartbeat ☒

Method OPTIONS ▾

Frequency 300 seconds

From URI SBCE@avaya.com

To URI ATTBE@att.com

Finish

**Step 5** - On the **Advanced** window, enter the following.

- **Enable Grooming** is not used for UDP connections and is left unchecked.
- Select **ATT-Interworking** (created in **Section Error! Reference source not found.**), for **Interworking Profile**.
- Select the **Script for IPTF-CM IPv6** (created in **Section Error! Reference source not found.**) for **Signaling Manipulation Script**.
- Since IPv6 only addresses are used on the trunk between the public side of the Avaya SBCE and the AT&T BE, **Tolerant** is not checked in this profile.
- Select **Finish**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile ATT-Interworking ▾

Signaling Manipulation Script Script for IPFR-CM IPv6 ▾

Securable ☐

Enable FGDN ☐

TCP Failover Port

TLS Failover Port

Tolerant ☐

URI Group None ▾

Finish

## 7.10. Routing Profiles

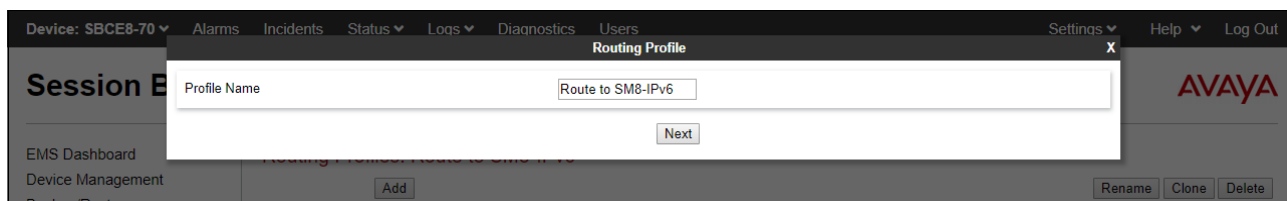
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and determine which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types. Separate Routing Profiles were created in the reference configuration for Session Manager and AT&T.

### 7.10.1. Routing Profile – Session Manager

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

**Step 1** - Select **Configuration Profiles → Routing** from the left-hand menu, and select **Add**.

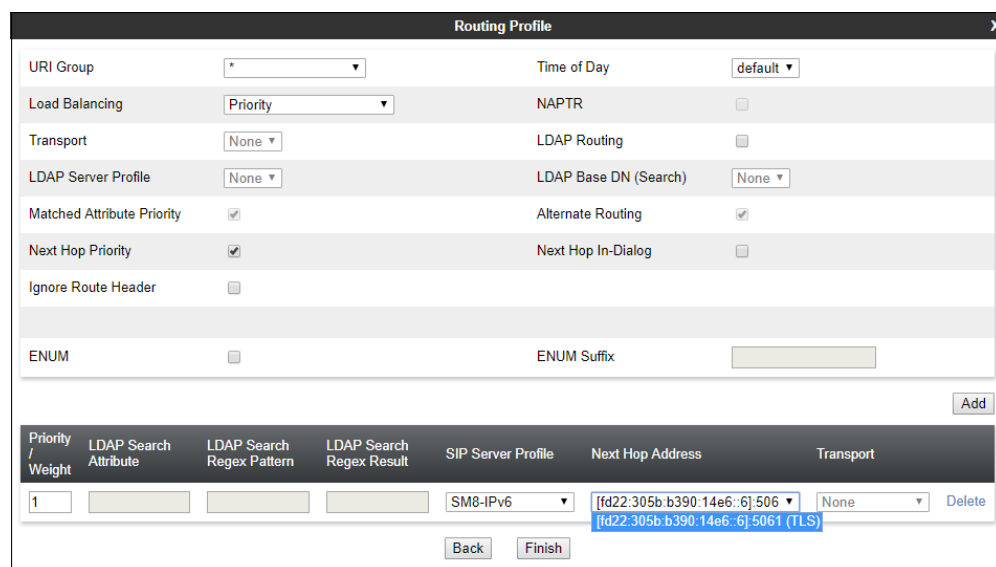
**Step 2** - Enter a **Profile Name**: (e.g., **Route to SM8-IPv6**) and click **Next**.



**Step 3** - The Routing Profile window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button.

**Step 4** - The **Next-Hop Address** section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight** = 1
- **SIP Server Profile** = **SM8-IPv6** (from **Section 7.9.1**).
- **Next Hop Address**: Verify that the **[fd22:305b:b390:14e6::6]:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IPv6 address). Also note that the **Transport** field is grayed out. Click on **Finish**.



## 7.10.2. Routing Profile – AT&T

Repeat the steps in **Section 7.10.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

**Step 1** - Enter a Profile Name: (e.g., **To ATT IPv6**).

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

- **Priority/Weight: 1**
- **SIP Server Profile:** **ATT-IPv6-trk-svr** (from **Section Error! Reference source not found.**).
- **Next Hop Address:** Verify that the **3ffe:ffff:aa:aa:10:10:172:80:5060 (UDP)** entry from the drop-down menu is selected (AT&T Border Element IP address).
- Click **Finish**.

URI Group	Time of Day
*	default
Load Balancing	NAPTR
Priority	<input type="checkbox"/>
Transport	LDAP Routing
None	<input type="checkbox"/>
LDAP Server Profile	LDAP Base DN (Search)
None	None
Matched Attribute Priority	Alternate Routing
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Next Hop Priority	Next Hop In-Dialog
<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ignore Route Header	
<input type="checkbox"/>	
ENUM	ENUM Suffix
<input type="checkbox"/>	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				ATT-IPv6-trk-svr	[3ffe:ffff:aa:aa:10:10:172:80]:5	None

Back Finish

## 7.11. Topology Hiding Profiles

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

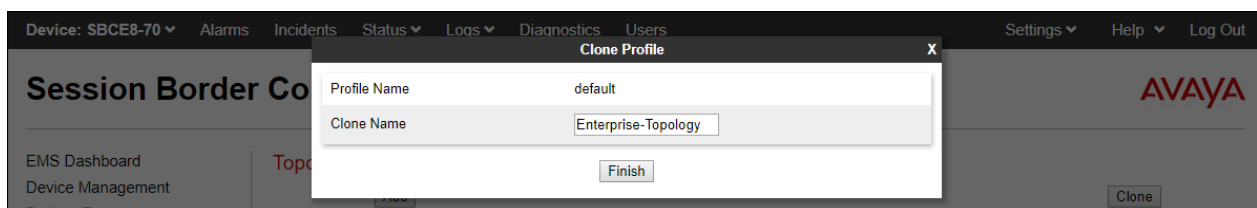
### 7.11.1. Topology Hiding – Enterprise

In the sample configuration, the enterprise Topology Hiding Profile was cloned from the **default** profile and then modified.

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

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

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



**Step 4** - Edit the newly created **Enterprise-Topology** profile.

**Step 5** - For the **Request-Line**, **To** and **From** headers select **Overwrite** under the **Replace Action** column. Enter the domain of the enterprise (e.g., **avayalab.com**) on the **Overwrite Value** field.

**Step 6** - Click **Finish**.

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

Finish

## 7.11.2. Topology Hiding – AT&T

Repeat the steps in **Section 7.11.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

**Step 1** - Enter a Profile Name (e.g., **SIP-Trunk-Topology**).

**Step 2** - Use the default values for all fields.

**Step 3** - Click **Finish**.

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

Finish

## 7.12. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

**Step 1** - Select **Domain Policies** → **Application Rules** from the left-hand side menu.

**Step 2** - Select the **default-trunk** rule.

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

- In the **Clone Name** field enter the new Application Rule name (e.g., **sip-trunk**).
- Click **Finish** (not shown). The completed **Application Rule** is shown below.

Session Border Controller for Enterprise

Application Rules: sip-trunk

Application Rules

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



## 7.13. Media Rules

Media Rules are used to define parameters in the media, like media encryption, QoS and Alternate Network Address Types (ANAT). Separate media rules are created for the enterprise and AT&T.

### 7.13.1. Media Rule – Enterprise

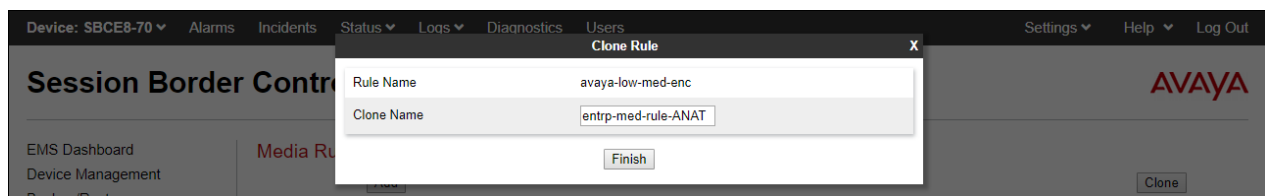
In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

**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, and the **Clone Rule** window will open.

- In the **Clone Name** field enter the new Media Rule name (e.g., **entrp-med-rule-ANAT**)
- Click **Finish**. The newly created rule will be displayed.



**Step 4** - On the enterprise Media Rule just created, select the **Encryption** tab.

- Click the **Edit** button and the **Media Encryption** window will open.
- In the **Audio Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Video Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Miscellaneous** section, select **Capability Negotiation**.

A screenshot of the 'Media Encryption' configuration window. It is divided into three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. In the 'Audio Encryption' section, 'Preferred Format #1' is set to 'SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80', 'Preferred Format #2' is set to 'RTP', 'Preferred Format #3' is set to 'NONE', 'Encrypted RTCP' is unchecked, 'MKI' is unchecked, 'Lifetime' is set to '2h', and 'Interworking' is checked. The 'Video Encryption' section has identical settings. In the 'Miscellaneous' section, 'Capability Negotiation' is checked. A 'Finish' button is at the bottom.

**Step 5** – Select the **Advanced** Tab.

- Select **ANAT Enabled**.
- Under **Local Preference** select **IPv6**.
- Select **Use Remote Preference**.

The screenshot shows a configuration window titled "Advanced" with a close button (X) in the top right corner. The window contains several sections with settings:

- Silencing**:
  - Silencing Enabled: ☐
  - Timeout:  second(s)
- Binary Floor Control Protocol**:
  - BFCP Enabled: ☐
- Far End Camera Control**:
  - FECC Enabled: ☐
- ANAT**:
  - ANAT Enabled: ☒
  - Local Preference: ☐ IPv4 ☒ IPv6
  - Use Remote Preference: ☒
- Media Line Compliance**:
  - Media Line Compliance Enabled: ☐

A "Finish" button is located at the bottom right of the window.

**Note:** when using a mixed IPv4-IPv6 topology, as the one shown on the enterprise side of the reference configuration, it is a good practice to use the same IPv4 preference across the Avaya SBCE enterprise media rule and the corresponding Communication Manager IP-codec-set (**ip-codec-set 6** in the example, **Section 5.9.2**). IPv6 was selected here to enforce the use of IPv6 addresses for the media during the compliance test with IPFR-EF, for verification purposes. Testing using IPv4 addresses for the media, with IPv4 selected as the local preference in both the Avaya SBCE enterprise media rule and Communication Manager **ip-codec-set 6** was also successfully performed during the compliance test.

**Step 6** - Click **Finish**.

The completed **entrp-med-rule-ANAT** is shown on the screen below.

## Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

Application Rules

Border Rules

**Media Rules**

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Media Rules: entrp-med-rule-ANAT

Add

RenameCloneDelete

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

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

Edit

## 7.13.2. Media Rule – AT&T

Repeat the steps in **Section 7.13.1**, with the following changes, to create a Media Rule for AT&T.

1. Clone the **default-low-med** rule
2. In the **Clone Name** field enter the new Media Rule name (e.g., **att-med-rule**)
3. Leave all fields at their default values.

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

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

Application Rules

Border Rules

**Media Rules**

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

Media Rules: att-med-rule

Add

Rename Clone Delete

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

Audio Encryption

Preferred Formats RTP

Interworking ☒

Video Encryption

Preferred Formats RTP

Interworking ☒

Miscellaneous

Capability Negotiation ☐

Edit

DSCP values **EF** for expedited forwarding (default value) are used for Media **QoS**.

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

Application Rules

Border Rules

**Media Rules**

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

TLS Management

Media Rules: att-med-rule

Add

Rename Clone Delete

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

Audio DSCP EF

Video QoS

Video DSCP EF

Edit

## 7.14. Signaling Rules

Signaling Rules are used to define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message, and to specify QoS parameters for the SIP signaling packets.

### 7.14.1. Signaling Rule – Enterprise

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

**Step 2** - 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 the new Signaling Rule name (e.g., **enterprise-sig-rule**)
- Click **Finish**.

Signaling Rule **enterprise-sig-rule** show below was left unchanged from the default rule.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), Charging Rules, End Point Policy Groups, Session Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main area is titled 'Signaling Rules: enterprise-sig-rule' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' options. A list of signaling rules is shown: 'default', 'No-Content-Type-Ch...', 'att-sig-rule', 'enterprise-sig-rule' (highlighted in red), and 'ATT-TF-408-test-sig'. The configuration for 'enterprise-sig-rule' is displayed in a tabbed interface with tabs for General, Requests, Responses, Request Headers, Response Headers, Signaling QoS, and UCID. The 'General' tab is active, showing 'Inbound' and 'Outbound' sections with 'Requests' and 'Non-2XX Final Responses' set to 'Allow'. The 'Content-Type Policy' section has 'Enable Content-Type Checks' checked, and 'Action' and 'Multipart Action' set to 'Allow'. An 'Exception List' is also present.

### 7.14.2. Signaling Rule – AT&T

Signaling Rule **att-sig-rule** was similarly cloned from the **default** rule and used for AT&T. Note that the DSCP value **AF41** for assured forwarding (default value) is set for **Signaling QoS**.

The screenshot displays the 'Session Border Controller for Enterprise' web interface for the 'att-sig-rule'. The navigation menu is the same as in the previous screenshot. The main area is titled 'Signaling Rules: att-sig-rule' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' options. The list of signaling rules shows 'att-sig-rule' highlighted in red. The configuration for 'att-sig-rule' is displayed in a tabbed interface with tabs for General, Requests, Responses, Request Headers, Response Headers, Signaling QoS, and UCID. The 'Signaling QoS' tab is active, showing 'Signaling QoS' checked, 'QoS Type' set to 'DSCP', and 'DSCP' set to 'AF41'. An 'Edit' button is visible at the bottom.

## 7.15. Endpoint Policy Groups

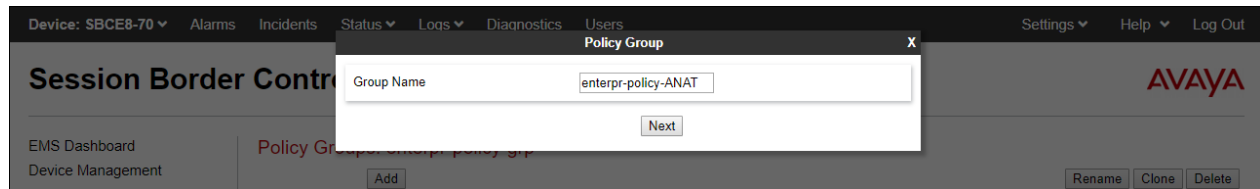
The rules created within the Domain Policies are assigned to an End Point Policy Group. The End Point Policy Group is then applied to a Server Flow in **Section 7.16**.

### 7.15.1. End Point Policy Group – Enterprise

**Step 1** - Select **Domain Policies → End Point Policy Groups** from the left-hand side menu.

**Step 2** - Select **Add**.

- Enter a name for the Policy Group (e.g., **enterpr-policy-ANAT**)
- Click **Next**.

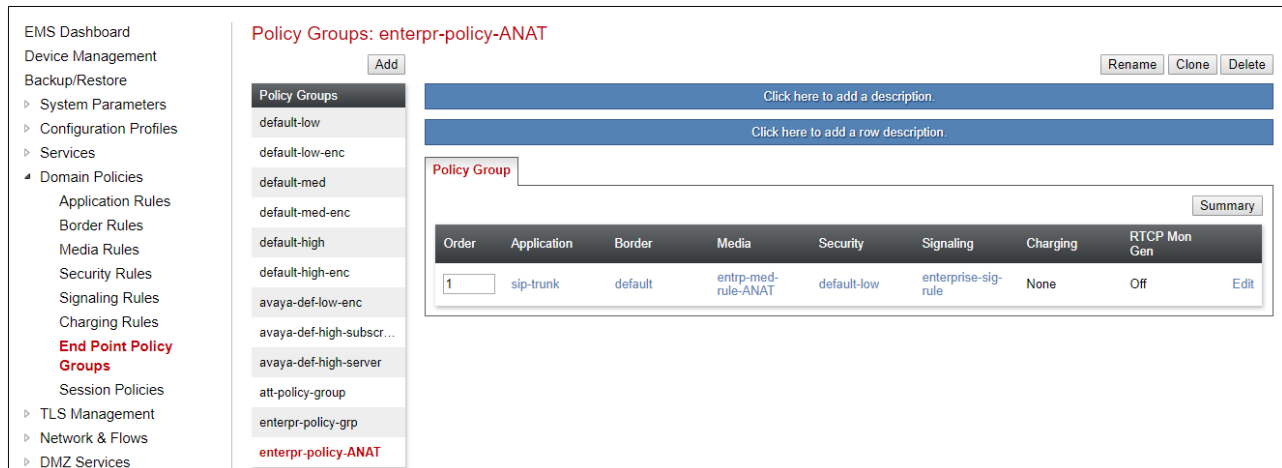


**Step 3** – On the **Policy Group** window (not shown), select the following.

- **Application Rule:** sip-trunk (created in **Section 7.12**).
- **Border Rule:** default.
- **Media Rule:** enterpr-med-rule-ANAT (created in **Section 7.13.1**).
- **Security Rule:** default-low.
- **Signaling Rule:** enterprise-sig-rule (created in **Section 7.14.1**).

**Step 4** - Select **Finish**.

The completed Policy Group **enterpr-policy-ANAT** is shown on the screen below.



## 7.15.2. Endpoint Policy Group – AT&T

**Step 1** - Repeat steps 1 through 4 from **Section 7.15.1** with the following changes:

- **Group Name:** att-policy-group
- **Media Rule:** att-med-rule (created in **Section 7.13.2**)
- **Signaling Rule:** att-sig-rule (created in **Section 7.14.2**)

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

The completed Policy Group **att-policy-grp** is shown on the screen below.

The screenshot displays the EMS Dashboard interface. On the left is a navigation menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups (highlighted in red), and Session Policies. The main area is titled 'Policy Groups: att-policy-group' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a list of policy groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, avaya-def-low-enc, avaya-def-high-subscri..., and avaya-def-high-server. The 'att-policy-group' is highlighted in red. To the right of the list is a table for the selected policy group. The table has columns: Order, Application, Border, Media, Security, Signaling, Charging, and RTP Mon Gen. The first row shows: Order 1, Application sip-trunk, Border default, Media att-med-rule, Security default-low, Signaling att-sig-rule, Charging None, and RTP Mon Gen Off. There are also buttons for 'Click here to add a description.', 'Click here to add a row description.', 'Summary', and 'Edit'.

Order	Application	Border	Media	Security	Signaling	Charging	RTP Mon Gen
1	sip-trunk	default	att-med-rule	default-low	att-sig-rule	None	Off

## 7.16. Endpoint Flows – Server Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow.

Create separate Server Flows for the enterprise and AT&T IPFR-EF service. These flows use the interfaces, polices, and profiles defined in previous sections.

### 7.16.1. Server Flows – Enterprise

**Step 1** - Select **Network and Flows** → **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:** Enter a name for the flow, e.g., **SM-IPv6 Flow IPFR**.
- **Server Configuration:** **SM8-IPv6** (Section 7.9.1).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** **Outside-Signaling-IPv6-FR** (Section 7.6).
- **Signaling Interface:** **Inside-A1-Sig\_IPv6-FR** (Section 7.6).
- **Media Interface:** **Inside-A1-Med-IPv6-FR** (Section 7.5).
- **Secondary Media Interface:** **Inside-Media** (Section 7.5).
- **End Point Policy Group:** **enterpr-policy-ANAT** (Section 7.15.1).
- **Routing Profile:** **To ATT IPv6** (Section 7.10.2).
- **Topology Hiding Profile:** **Enterprise-Topology** (Section 7.11.1).
- Let other fields at the default values.

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

View Flow: SM8-IPv6 Flow IPFR		Profile	
Criteria			
Flow Name	SM8-IPv6 Flow IPFR	Signaling Interface	Inside-A1-Sig-IPv6-FR
Server Configuration	SM8-IPv6	Media Interface	Inside-A1-Med-IPv6-FR
URI Group	*	Secondary Media Interface	Inside-Media
Transport	*	End Point Policy Group	enterpr-policy-ANAT
Remote Subnet	*	Routing Profile	To ATT IPv6
Received Interface	Outside-Signaling-IPv6-FR	Topology Hiding Profile	Enterprise-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	<input type="checkbox"/>



## 7.16.2. Server Flow – AT&T

**Step 1** - Repeat steps 1 through 4 from **Section 7.16.1**, with the following changes:

- **Flow Name:** Enter a name for the flow, e.g., **ATT IPFR Full IPv6 Flow**.
- **Server Configuration:** **ATT-IPv6-trk-svr** (Section 7.9.2).
- **Received Interface:** **Inside-A1-Sig-IPv6-FR** (Section 7.6).
- **Signaling Interface:** **Outside-Signaling-IPv6-FR** (Section 7.6).
- **Media Interface:** **Outside-Media-IPv6-FR** (Section 7.5).
- **End Point Policy Group:** **att-policy-group** (Section 7.15.2).
- **Routing Profile:** **Route to SM8-IPv6** (Section 7.10.1).
- **Topology Hiding Profile:** **SIP-Trunk-Topology** (Section 7.11.2).

View Flow: ATT IPFR Full IPv6 Flow

Criteria

Flow Name	ATT IPFR Full IPv6 Flow
Server Configuration	ATT-IPv6-trk-svr
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-A1-Sig-IPv6-FR

Profile

Signaling Interface	Outside-Signaling-IPv6-FR
Media Interface	Outside-Media-IPv6-FR
Secondary Media Interface	None
End Point Policy Group	att-policy-group
Routing Profile	Route to SM8-IPv6
Topology Hiding Profile	SIP Trunk-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

## 8. AT&T IP Flexible Reach – Enhanced Features Configuration

Information regarding the AT&T IPFR-EF service offer can be obtained at <https://www.business.att.com/products/sip-trunking.html> or by contacting an AT&T sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. AT&T provided the IPFR-EF service border element IP addresses, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPFR-EF features, and their associated access numbers are also provisioned and assigned by AT&T.

## 9. Verification Steps

The following steps may be used to verify the configuration.

### 9.1. 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 and G.711 ULAW codecs.

## 9.2. Avaya Aura® Communication Manager Verification

This section illustrates verifications examples in Communication Manager.

The following edited Communication Manager *list trace tac* trace output shows an incoming call received on trunk group 7, member 1. The adaptation in Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 89321, before sending the INVITE to Communication Manager.

Note that the IPv6 addresses of the Avaya SBCE private interface (**fd22:305b:b390:14e6::1a**) and the Media Server (**fd22:305b:b390:14e6::7**) are included initially on the media path.

```
list trace tac *07                                     Page 1

LIST TRACE

time          data
09:02:14 TRACE STARTED 04/01/2020 CM Release String cold-01.0.890.0-26095
09:04:46 SIP<INVITE sips:89321@avayalab.com;user=phone SIP/2.0
09:04:46      Call-ID: 07778b5f6fa3a40ebfac2d1835a0c801
09:04:46      active trunk-group 7 member 1      cid 0x264
09:04:46 SIP>SIP/2.0 180 Ringing
09:04:46      Call-ID: 07778b5f6fa3a40ebfac2d1835a0c801
09:04:46      dial 89321
09:04:46      ring station      89321 cid 0x264
09:04:46      SIP-ANAT Offer Received on trunk-group 7.
09:04:46      09:04:46      Alerting party uses public-unknown-numbering
09:04:46      G729 ss:off ps:20
09:04:46      rgn:6 [fd22:305b:b390:14e6::1a]:16544
09:04:46      rgn:1 [fd22:305b:b390:14e6::7]:6088
09:04:46      G72264K ss:off ps:20
09:04:46      rgn:1 [10.5.5.211]:25048
09:04:46      rgn:1 [10.64.91.86]:6090
09:04:50 SIP>SIP/2.0 200 OK
09:04:50      Call-ID: 07778b5f6fa3a40ebfac2d1835a0c801
09:04:50      active station      89321 cid 0x264
09:04:50      Connected party uses public-unknown-numbering
```

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

The following screen shows **Page 2** of the output of the **status trunk 7/x** command (where x is the trunk group member active on the call, **1** in the example) pertaining to this same call. Note that Communication Manager uses **procr6** as the **Near-end** node (**fd22:305b:b390:14e6::5**) for the signaling to Session Manager (**fd22:305b:b390:14e6::6**), using port **5067**. Also note that since the IP telephone used as the endpoint in this example uses an IPv4 address, after “shuffling” is completed the media is “ip-direct” from the IP Telephone (**10.5.5.211**) to the secondary (IPv4) inside Media Interface of Avaya SBCE (**10.64.91.40**), releasing the media resources in the Media Server.

```

status trunk 7/1                                     Page 2 of 3
                                     CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR6
  Signaling   IP Address                               Port
  Near-end:   fd22:305b:b390:14e6::5                   : 5067
  Far-end:    fd22:305b:b390:14e6::6                   : 5067
H.245 Near:
H.245 Far:
  H.245 Signaling Loc:                               H.245 Tunneled in Q.931? no

Audio Connection Type: ip-direct      Authentication Type: None
Near-end Audio Loc:                               Codec Type: G.729
  Audio       IP Address                               Port
  Near-end:   10.5.5.211                             : 25048
  Far-end:    10.64.91.40                             : 16820

```

The screen below shows **Page 3** of the output of the **status trunk 7/1** command pertaining to this same call. Note that G729 and SRTP are used.

```

status trunk 7/1                                     Page 3 of 3
                                     SRC PORT TO DEST PORT TALKPATH

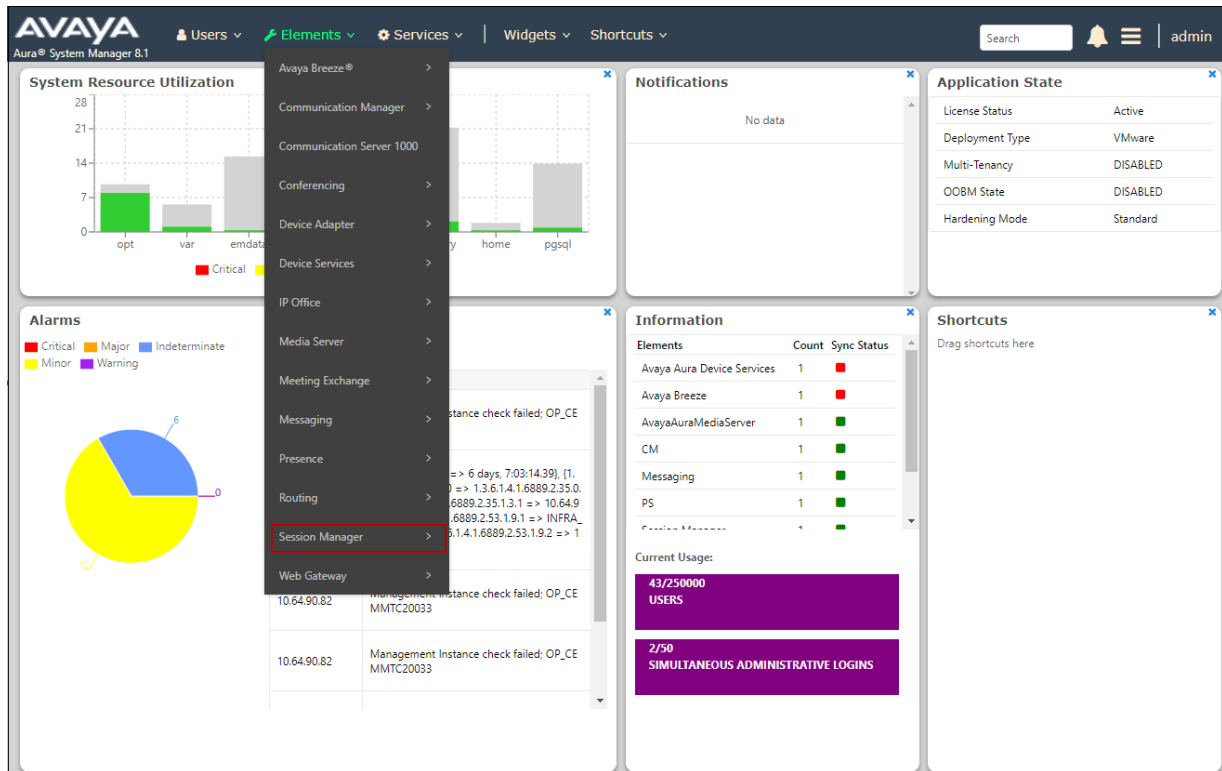
src port: T000089
T000089:TX:10.64.91.40:16820/g729/20ms/1-srtp-aescm128-hmac80
S000009:RX:10.5.5.211:25048/g729a/20ms/1-srtp-aescm128-hmac80

```

### 9.3. Avaya Aura® Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



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

Session Manager

Dashboard

Session Manager Admin...

Global Settings

Communication Profile ...

Network Configuration

Device and Location ...

Application Configur...

System Status

Help ?

## 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

Clear Logs

As of 9:32 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"/>	<a href="#">Session Manager</a>	Core	✓	0/0/0	Up	Accept New Service	3/19	0	2/2	✓	✓	Normal	Enabled	8.1.2.0.812033

Select : All, None

In the example, the entry **3/19** under the **Entity Monitoring** column shows that there are alarms on 3 out of the 19 Entities being monitored by Session Manager. Clicking the entry under the **Entity Monitoring** column brings up the **Session Manager Entity Link Connection Status** page. Verify that the state of the Session Manager links of interest, to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

**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

19 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
	<a href="#">CM-TG1</a>	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG2</a>	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG9</a>	IPv4	10.64.91.75	5069	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG7</a>	IPv6	fd22:305b:b390:14e6::5	5067	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG6</a>	IPv6	fd22:305b:b390:14e6::5	5066	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG5</a>	IPv4	10.64.91.75	5065	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG4</a>	IPv4	10.64.91.75	5064	TLS	FALSE	UP	200 OK	UP
	<a href="#">SBCE-ATT</a>	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
	<a href="#">SBCE-Toll Free</a>	IPv4	10.64.91.41	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
	<a href="#">SBC1</a>	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
	<a href="#">CM-TG3</a>	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP
	<a href="#">Aura Messaging</a>	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
	<a href="#">ExperiencePortal</a>	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
	<a href="#">SBCE-ATT-IPFR-IPv6</a>	IPv6	fd22:305b:b390:14e6::1a	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
	<a href="#">SBCE ATT IPTF IPv6</a>	IPv6	fd22:305b:b390:14e6::8	5061	TLS	FALSE	UP	405 Method Not Allowed	UP

Select : None Page 1 of 2

**Note** – On the **SBCE-ATT-IPFR-IPv6** 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 forwards the Session Manager generated OPTIONS on to the AT&T IPFR-EF Border Element, it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends the response back to Session Manager.

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

## 9.4. Avaya Session Border Controller for Enterprise Verification

This section provides verification steps that may be performed with the Avaya SBCE.

### 9.4.1. Incidents

The Incident Viewer can be accessed from the Avaya top navigation menu as highlighted in the screenshot below.

**Device: SBCE8-70** | Alarms | **Incidents** | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

### Session Border Controller for Enterprise

**EMS Dashboard**  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Services  
Domain Policies  
TLS Management  
Network & Flows  
DMZ Services  
Monitoring & Logging

**Dashboard**  
GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

Information	
System Time	09:44:29 AM MDT <a href="#">Refresh</a>
Version	8.1.0.0-14-18490
GUI Version	8.1.0.0-18490
Build Date	Mon Feb 03 17:23:09 UTC 2020
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	04/01/2020 09:02:25 MDT
Failed Login Attempts	0

**Active Alarms (past 24 hours)**  
None found.

**Installed Devices**  
EMS  
SBCE8-70

**Incidents (past 24 hours)**  
SBCE8-70: Call Audit Cleanup  
SBCE8-70: Heartbeat Successful, Server is UP  
SBCE8-70: Heartbeat Failed, Server is Down

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures. Further Information can be obtained by clicking on an incident in the Incident Viewer screen.

### Incident Viewer

Device: All | Category: All | [Clear Filters](#) | [Refresh](#) | [Generate Report](#)

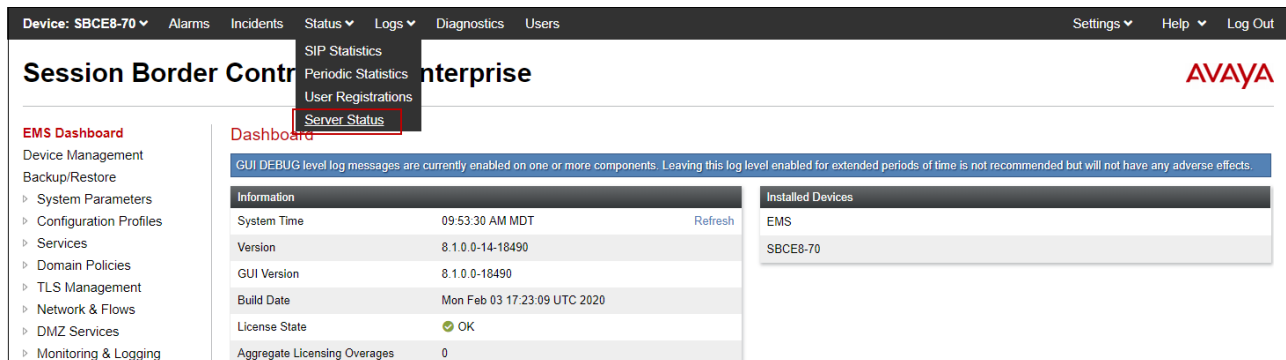
Displaying results 1 to 15 out of 2000.

ID	Device	Date & Time	Category	Type	Cause
792877126053160	SBCE8-70	Apr 1, 2020, 9:17:32 AM	Media Anomaly Detection	Media Inactivity Detected From Both Parties	Call Audit Cleanup
792868302014208	SBCE8-70	Apr 1, 2020, 4:23:24 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
792868274981833	SBCE8-70	Apr 1, 2020, 4:22:29 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
792862092930638	SBCE8-70	Apr 1, 2020, 12:56:25 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
792862065147670	SBCE8-70	Apr 1, 2020, 12:55:30 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
792844515897834	SBCE8-70	Mar 31, 2020, 3:10:31 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
792844493365703	SBCE8-70	Mar 31, 2020, 3:09:46 PM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
792833169490669	SBCE8-70	Mar 31, 2020, 8:52:18 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
792832985778633	SBCE8-70	Mar 31, 2020, 8:46:11 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP

<< < 1 2 3 4 5 > >>

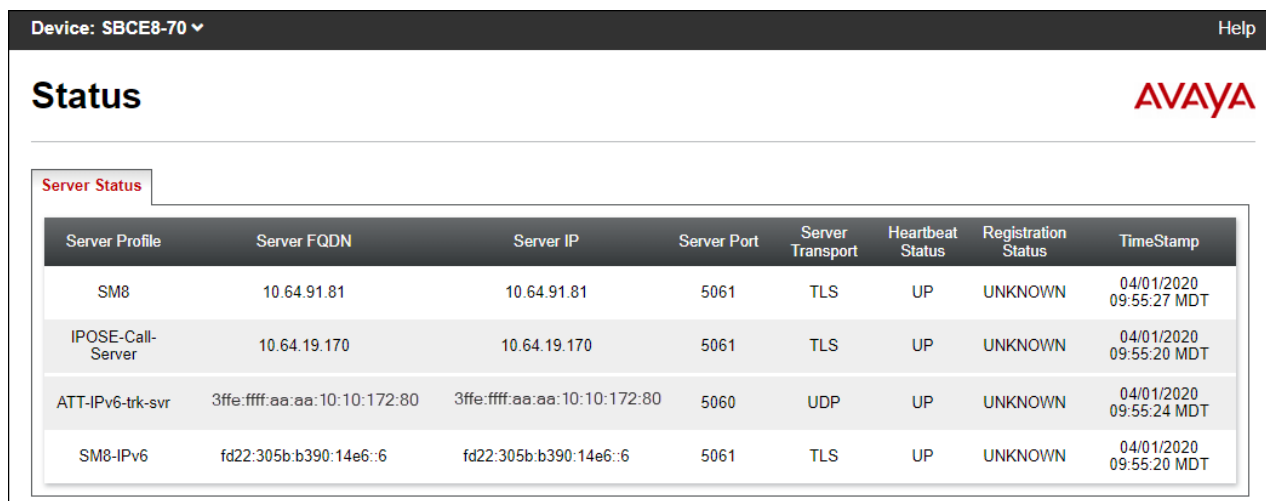
## 9.4.2. Server Status

The **Server Status** can be accessed from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**.



The screenshot shows the Avaya SBCE top navigation bar. The 'Status' menu is open, and 'Server Status' is highlighted. The main content area shows the 'Session Border Controller Enterprise' dashboard with various sections like 'Information', 'Installed Devices', and 'GUI DEBUG level log messages'.

The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.99**.



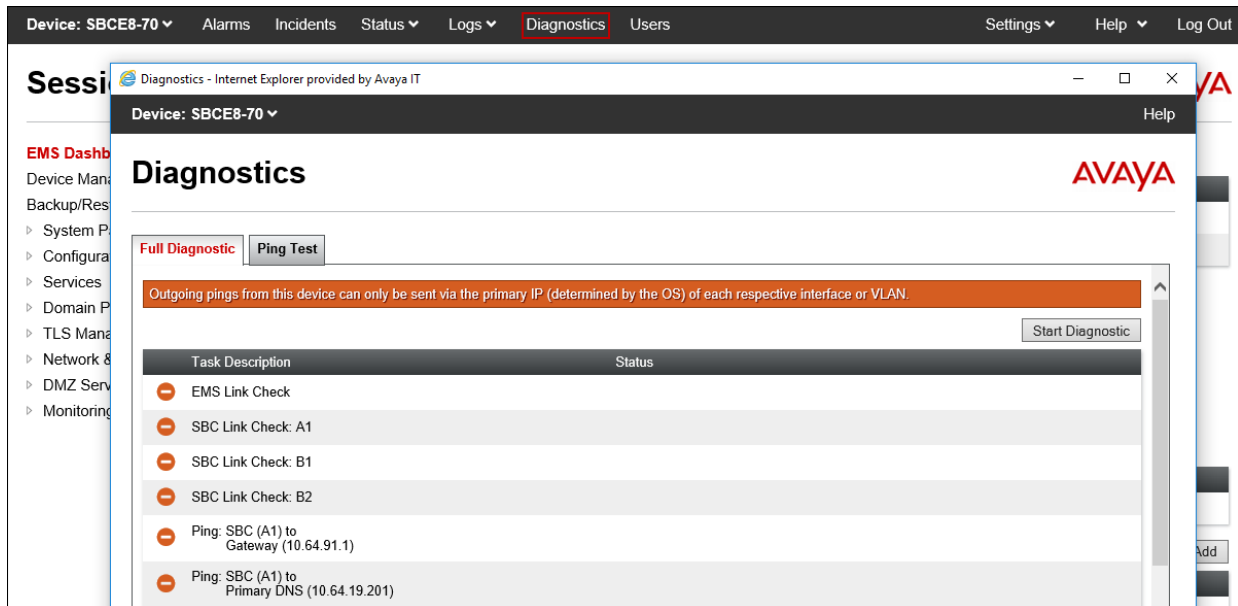
The screenshot shows the 'Status' page in the Avaya SBCE interface. The 'Server Status' tab is selected, displaying a table of connected SIP servers. The table includes columns for Server Profile, Server FQDN, Server IP, Server Port, Server Transport, Heartbeat Status, Registration Status, and TimeStamp.

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
SM8	10.64.91.81	10.64.91.81	5061	TLS	UP	UNKNOWN	04/01/2020 09:55:27 MDT
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	04/01/2020 09:55:20 MDT
ATT-IPv6-trk-svr	3ffe:ffff:aa:aa:10:10:172:80	3ffe:ffff:aa:aa:10:10:172:80	5060	UDP	UP	UNKNOWN	04/01/2020 09:55:24 MDT
SM8-IPv6	fd22:305b:b390:14e6::6	fd22:305b:b390:14e6::6	5061	TLS	UP	UNKNOWN	04/01/2020 09:55:20 MDT



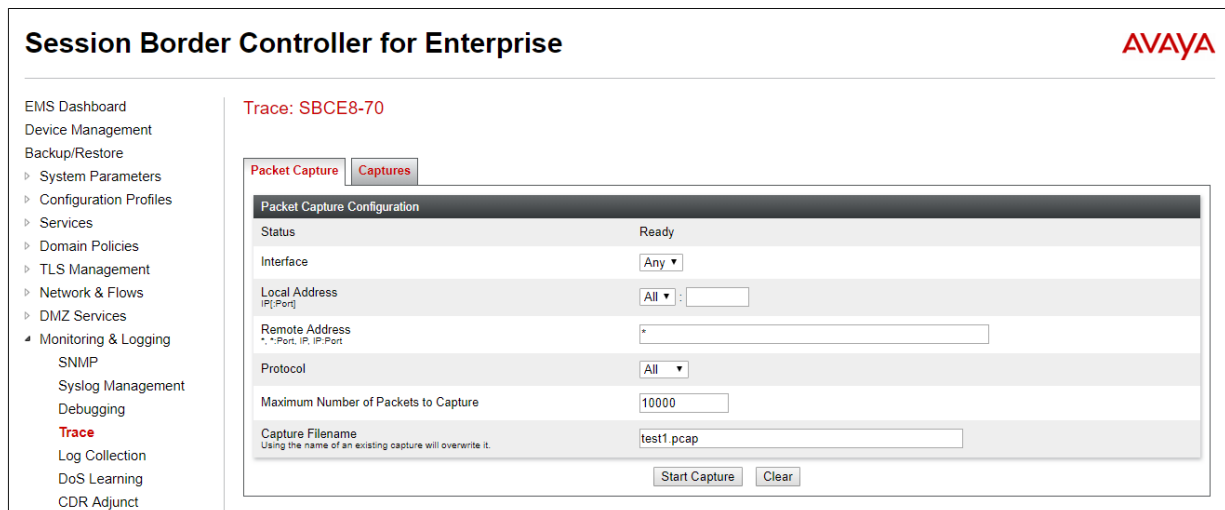
### 9.4.3. Diagnostic

This screen provides a **Full Diagnostics** tool to verify the link of each interface and ping the configured next-hop gateways and DNS servers. The **Ping Test** tool can be used to ping specific devices from any Avaya SBCE interface.



### 9.4.4. Protocol Traces

To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

SNMP

Syslog Management

Debugging

Trace

Log Collection

DoS Learning

CDR Adjunct

Trace: SBCE8-70

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 <small>(IP:Port)</small>	All
Remote Address <small>* -Port, IP, IP:Port</small>	
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test1.pcap

Stop Capture

Select the **Captures** tab to view the files created during the packet capture.

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

SNMP

Syslog Management

Debugging

Trace

Trace: SBCE8-70

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
test1_20200401103500.pcap	327,680	April 1, 2020 at 10:35:33 AM MDT	Delete

The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like Wireshark.

## 10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and the Avaya Session Border Controller for Enterprise 8.1 can be configured to interoperate successfully with the AT&T IP Flexible Reach – Enhanced Features service using IPv6, 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.

## 11. 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 8.1.x, Issue 3, March 2020
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 3, March 2020
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2020
- [4] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 5, March 2020

### **Avaya Aura® Communication Manager**

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2020
- [6] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020
- [7] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 6, March 2020
- [8] *Administering Avaya G450 Branch Gateway*, Release 8.1.x, Issue 3, March 2020
- [9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.2, Issue 9, December 2019
- [10] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, Issue 1.1, June 2018

### **Avaya Session Border Controller for Enterprise**

- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 1, February 2020
- [12] *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*, Release 8.1, Issue 1, February 2020
- [13] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 8.1, Issue 1, February 2020

### **AT&T IP Flexible Reach - Enhanced Features Service:**

- [14] *AT&T IP Flexible Reach – Product Description*  
<https://www.business.att.com/content/dam/attbusiness/briefs/voice-and-collaboration-ip-flex-reach-product-brief.pdf>

## 12. Appendix A – Configuration for Fax Testing

As previously mentioned in **Section 2.2, item 3**, during fax testing it was observed that the Avaya SBCE rejected the T.38 re-INVITEs from Communication Manager or AT&T when ANAT was enabled on the SBCE, and faxes failed. This issue is currently under investigation by Avaya. Inbound and outbound faxes using T.38 and G.711 pass-through were tested successfully, using the alternate configuration described below.

In this alternate configuration, ANAT is disabled on the Avaya SBCE Media Rule for the enterprise. Since ANAT is used to achieve media level interworking on the enterprise network between IPv4 and IPv6 devices, by making this change the implication is that Avaya SBCE will not continue to allow the use of IPv4 and IPv6 addresses simultaneously for the media on the private network. Fax was successfully tested with ANAT disabled on the Avaya SBCE, using IPv4 only or IPv6 addresses only for the media on the private network.

Since some of the media gateways and endpoints in the reference configuration only use IPv4 addresses, the steps below show the changes needed to support fax by setting up the media to use IPv4 addresses on the enterprise.

### 12.1. Configuration Changes for T.38 Fax

**Step 1** – In Communication Manager, enter the **change ip-codec-set 6** command, as shown in **Section 5.9.2**. Under **Media Connection IP Address Type Preferences**, enter **IPv4** as the first preference. Leave the second preference blank.

change ip-codec-set 6

Page 2 of 2

IP MEDIA PARAMETERS

Allow Direct-IP Multimedia? n

	Mode	Redun- dancy	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

Media Connection IP Address Type Preferences

1: IPv4

2:

**Step 2** – On the Avaya SBCE, on the Media Rule for the enterprise (**Section 7.13.1**), uncheck **ANAT Enabled** under the **Advanced** tab (not shown).

**Step 3** – On the Avaya SBCE, on the Server Flow for the enterprise (**Section 7.16.1**) make the following changes:

- **Media Interface:** select **Inside Media** (**Section 7.5**).
- **Secondary Media Interface:** leave this field blank.

Edit Flow: SM8-IPv6 Flow IPFR	
Flow Name	SM8-IPv6 Flow IPFR
SIP Server Profile	SM8-IPv6
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-Signaling-IPv6-FR
Signaling Interface	Inside-A1-Sig-IPv6-FR
Media Interface	Inside-Media
Secondary Media Interface	None
End Point Policy Group	enterpr-policy-ANAT
Routing Profile	To ATT IPv6
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
<b>Finish</b>	

## 12.2. Configuration Changes for G.711 Fax

During the compliance test, in order to perform G.711 pass-through fax testing, the network region assigned to the G450 Media Gateway where the fax machine was connected was changed from region 1 (**Section 5.16**) to region 3. This network region utilized IP Codec Set 3 for calls between region 3 and region 6 (IPFR calls). Creating a dedicated network region and ip-codec-set for G.711 pass-through fax allowed for fax calls from this G450 Media Gateway to begin with codec G.711MU, while voice calls to other Media Gateways, Media Servers, and IP endpoints belonging to region 1, will continue to request G.729A as the first codec choice. (**Section 5.9.1**).

This configuration shown here is for completeness and is only needed if G.711 pass-through is preferred to T.38 fax.

To create the IP Network Region 3 used for G.711 fax testing, repeat the steps in **Section 5.8.1** with the following changes:

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

- Enter a descriptive name (e.g., **G711 Fax**).
- Enter **3** for the **Codec Set** parameter.

**Step 2** - On **Page 2** of the form, leave **ANAT enabled** with the default value **n**.

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

- Set codec set **3** for **dst rgn 6**.
- Note that **dst rgn 3** is pre-populated with codec set **3** (from page 1 provisioning).

change ip-network-region 3										Page	4	of	20
Source Region: 3		Inter Network Region Connection Management								I	S	M	
										G	A	y	t
dst	codec	direct	WAN-BW-limits		Video		Intervening		Dyn	A	G	n	c
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	c	e
1	1	y	NoLimit							n		y	t
2	2	y	NoLimit							n		y	t
3	3										all		
4	3	y	NoLimit							n		y	t
5													
6	3	y	NoLimit							n		y	t
7													

Repeat the steps in **Section 5.9.1** to create IP Codec Set 3 with the following changes:

**Step 1 - On Page 1 of the form**

- Provision the codecs in the order shown below. Note that **G.711MU** is listed as the preferred codec.
- 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.

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

- Set the **Fax Mode** to **off**.
- Under **Media Connection IP Address Type Preferences**, enter **IPv4** as the first preference. Leave the second preference blank.

change ip-codec-set 3

Page 1 of 2

IP CODEC SET

Codec Set: 3

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

Media Encryption

1: 1-srtp-aescm128-hmac80

2: none

Encrypted SRTCP: enforce-unenc-srtcp

change ip-codec-set 3

Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size (ms)
<b>FAX</b>	<b>off</b>	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Media Connection IP Address Type Preferences

1: IPv4

2:

On the Avaya SBCE, repeat **Step 2** (Media Rule) and **Step 3** (Server Flow), previously shown in **Section 12.1**.



## 13. Appendix B – Avaya SBCE – SigMa Script File

Details of the Signaling Manipulation script used in the configuration of the Avaya SBCE, in Section 7.8.

```
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {

//Remove gsid and epv parameters from Contact header to hide internal topology
        remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
        remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

//Remove Bandwidth from SDP
        %BODY[1].regex_replace("b=(TIAS|AS|CT):(\d+)\r\n","");

// fix call-fwd
        %HEADERS["Diversion"][1].regex_replace("sips","sip");
    }
}
within session "ALL"
{
    act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
    {
// RingSplash Fix
        %BODY[1].regex_replace("anonymous.invalid","::");
    }
}
```

---

**©2020 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>TM</sup> and <sup>®</sup> 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](mailto:devconnect@avaya.com).