



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 8.0.1 with AT&T IP Toll Free Service 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 the Avaya Session Border Controller for Enterprise 8.0.1 with the AT&T IP Toll Free service using IPv6 and AT&T's **AVPN** or **MIS/PNT** transport connections.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that this document do not include the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service, which are covered on separate Application Notes.

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	9
3.	Reference Configuration.....	10
3.1.	Illustrative Configuration Information	12
3.2.	Call Flows	13
4.	Equipment and Software Validated	14
5.	Configure Avaya Aura® Communication Manager.....	15
5.1.	System-Parameters Customer-Options	15
5.2.	System-Parameters Features	17
5.3.	Dial Plan.....	17
5.4.	Node Names	18
5.5.	Processor Ethernet.....	18
5.6.	IP Network Regions	19
5.6.1.	IP Network Region 1 – Local CPE Region	19
5.6.2.	IP Network Region 4 – AT&T Trunk Region	21
5.7.	IP Codec Sets	22
5.7.1.	Codecs for IP Network Region 1 (calls within the CPE).....	22
5.7.2.	Codecs for IP Network Region 4 (calls from AT&T)	23
5.8.	SIP Trunks.....	24
5.8.1.	SIP Trunk for Inbound AT&T calls.....	24
5.8.2.	Local SIP Trunk (Avaya SIP Telephones, Messaging Access).....	28
5.9.	Public Numbering	29
5.10.	Private Numbering.....	30
5.11.	Route Pattern for Local SIP Trunk	30
5.12.	Automatic Alternate Routing (AAR) Dialing	31
5.13.	Provisioning for Simulated Call Center Functionality	32
5.14.	Avaya G430 Media Gateway Provisioning	34
5.15.	Avaya Aura® Media Server Provisioning.....	35
5.16.	Save Translations.....	36
5.17.	Verify TLS Certificates – Communication Manager	37
6.	Configure Avaya Aura® Session Manager	38
6.1.	System Manager Login and Navigation.....	39
6.2.	SIP Domain	40
6.3.	Locations	41
6.3.1.	Main Location.....	41
6.3.2.	Common-SBCs Location	41
6.4.	Configure Adaptations	42
6.4.1.	Adaptation for Avaya Aura® Communication Manager Extensions	42
6.4.2.	Adaptation for the AT&T IP Toll Free Service	44
6.5.	SIP Entities.....	45
6.5.1.	Avaya Aura® Session Manager SIP Entity	45
6.5.2.	Avaya Aura® Communication Manager SIP Entity – Public Trunk	47

6.5.3.	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	48
6.5.4.	Avaya Session Border Controller for Enterprise SIP Entity.....	48
6.6.	Entity Links	49
6.6.1.	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	49
6.6.2.	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	50
6.6.3.	Entity Link for the AT&T IP Toll Free Service via the Avaya SBCE	50
6.7.	Time Ranges – (Optional)	51
6.8.	Routing Policies	51
6.8.1.	Routing Policy for AT&T Routing to Avaya Aura® Communication Manager	51
6.9.	Dial Patterns	53
6.9.1.	Dial Pattern for Inbound Calls to Communication Manager	53
6.10.	Verify TLS Certificates – Session Manager.....	55
7.	Configure Avaya Session Border Controller for Enterprise	57
7.1.	Device Management – Status	58
7.2.	TLS Management.....	60
7.2.1.	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	60
7.2.2.	Server Profiles.....	61
7.2.3.	Client Profiles	62
7.3.	Network Management	63
7.4.	Advanced Options	64
7.5.	Media Interfaces.....	65
7.6.	Signaling Interfaces.....	66
7.7.	Server Interworking Profiles	67
7.7.1.	Server Interworking Profile – Enterprise	67
7.7.2.	Server Interworking – AT&T	68
7.8.	Signaling Manipulation.....	70
7.9.	SIP Server Profiles	71
7.9.1.	SIP Server Profile – Session Manager	71
7.9.2.	SIP Server Profile – AT&T.....	73
7.10.	Routing Profiles.....	75
7.10.1.	Routing Profile – Session Manager.....	75
7.10.2.	Routing Profile – AT&T	76
7.11.	Topology Hiding Profiles	77
7.11.1.	Topology Hiding – Enterprise Side.....	77
7.11.2.	Topology Hiding – AT&T Side	78
7.12.	Application Rules	78
7.13.	Media Rules.....	79
7.13.1.	Enterprise – Media Rule.....	79
7.13.2.	AT&T – Media Rule	81
7.14.	Signaling Rules.....	82
7.14.1.	Signaling Rule – Enterprise.....	82
7.14.2.	Signaling Rule – AT&T	82
7.15.	Endpoint Policy Groups.....	83
7.15.1.	Endpoint Policy Group – Enterprise	83
7.15.2.	Endpoint Policy Group – AT&T.....	84
7.16.	Endpoint Flows – Server Flows	84

7.16.1.	Server Flows – Enterprise	84
7.16.2.	Server Flow – AT&T	85
8.	AT&T IP Toll Free Service Configuration	86
9.	Verification Steps.....	86
9.1.	AT&T IP Toll Free Service.....	86
9.2.	Avaya Aura® Communication Manager Verification	87
9.3.	Avaya Aura® Session Manager Verification.....	88
9.4.	Avaya Session Border Controller for Enterprise Verification	90
9.4.1.	Incidents	90
9.4.2.	Server Status	91
9.4.3.	Protocol Traces	92
10.	Conclusion	94
11.	References.....	95
12.	Appendix A – Configuration for G.711 Fax Testing.....	96

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 8.1 (IPv4 addresses), Avaya Aura® Session Manager 8.1 (IPv4 addresses) and Avaya Session Border Controller for Enterprise 8.0.1 (IPv4/IPv6 addresses) with the AT&T IP Toll Free service (IPv6 addresses) using AT&T Virtual Private Network (AVPN) or Managed Internet Service Private Network Transport (MIS/PNT) connections¹.

Avaya Aura® Communication Manager 8.1 (Communication Manager) is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 8.1 (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 8.0.1 (Avaya SBCE) is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service. It is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability. The Avaya SBCE also performs network address translations between the CPE private IPv4 network and the AT&T IP Toll Free IPv6 SIP trunk, at both the IP and SIP layers.

The AT&T IP Toll Free service, referred to in the remainder of this document as IPTF, is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT transport.

Note – These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. That solution is described in a separate document.

¹ MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does 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 IPTF and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager and the Avaya SBCE (see **Section 3.2** for call flow examples).

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 these Application Notes, the interface between Avaya systems and the AT&T Toll Free 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 IPTF network. Calls were made from the PSTN, across the IPTF network, to the CPE.

The following SIP trunking VoIP features were tested with the IPTF service:

- Inbound PSTN/IPTF calls to Communication Manager stations, Vector Directory Numbers (VDNs), Vectors, and Agents.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones/Agents via IPTF.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729A and G.711Mu codecs.
- T.38 fax calls via IPTF to Communication Manager fax endpoints.
- G.711 pass-through fax calls via IPTF to Communication Manager fax endpoints.
- DTMF tone transmission using RFC 2833/4733 between Communication Manager and IPTF automated access systems.
- Inbound IPTF service calls to Communication Manager that are routed to Agent queues or directly to Agents.
- IPTF network features such as Legacy Transfer Connect (inband) and Alternate Destination Routing (ADR).
- Long duration calls.

An Avaya Remote Worker SIP endpoint (Avaya IX™ Workplace Client for Windows) was used in the reference configuration. The Remote Worker 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.

2.2. Test Results

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

1. **IP Toll Free ADR Call Redirection feature in response to a ring-no-answer condition.**
There is an anomaly in the AT&T VIT lab where the Ring No Answer did not get triggered due to Lab restrictions. However, in production, if there is no answer for 20 seconds, ADR Call Redirection will be invoked.
2. **IP Toll Free ADR Call Redirection feature based on SIP error code response.** The IP Toll Free service can be configured to invoke the ADR Call Redirection feature upon receiving of an error response from the CPE.
 - The following error conditions were producible in the reference configuration and tested successfully: 480 Temporarily Unavailable, 486 Busy Here, 500 Server Internal Error and 503 Service Unavailable.
 - Even though the following error conditions were not producible in the reference configuration, the associated error codes were simulated via an Avaya SBCE signaling manipulation rule, and also tested successfully: 408 Request Timeout, 504 Server Timeout, and 600 Busy Everywhere.
3. **G.726-32 codec support.** While Communication Manager supports G.726-32, the IPTF implementation of G.726-32 results in poor audio quality. Therefore, G.726-32 codec is not supported between Communication Manager and the IPTF service.
4. **T.38/G.729 fax is limited to 9600bps when using the G4xx Media Gateways.** A G430 Media Gateway is used in the reference configuration. As a result, T.38/G.729 fax was limited to 9600 bps. Also note that the sender and receiver of a T.38 fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3.
5. **G.711 pass-through fax.** Inbound G.711 pass-through fax was tested in addition to T.38 fax. This was done by configuring a separate Communication Manager network region and ip-codec-set (**Section 12**). Faxes using G.711 pass-through completed successfully during the test. However, when the PSTN sender and CPE receiver both used SG3 fax devices, the results were erratic. Due to the unpredictability of pass-through techniques, which only work well on networks with very few hops and with limited end-to-end delay, G.711 fax pass-through is delivered in Communication Manager on a “best effort” basis; its success is not guaranteed, and it should be used at the customer’s discretion. T.38 should be the preferred method for faxing.
6. **DiffServ markings** – The IP header in RTP media and SIP signaling packets sent from the Avaya SBCE to AT&T do not contain the Quality of Service DSCP values configured on the Media and Signaling Rules under Domain policies (**Sections Error! Reference source not found.** and **Error! Reference source not found.**). This issue is restricted to Avaya SBCE interfaces configured with IPv6 addresses, and it is currently under investigation by Avaya.
7. **IP Toll Free services IP InfoPack and Landline/Mobility test cases could not be executed.** The AT&T supplied IP Toll Free test plan specifies test cases to verify the inbound transmission of INFOPAK and Landline/Mobility data by the IP Toll Free service. Due to network provisioning and lab support issues, these test cases could not be executed.

8. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), Session Manager is provisioned to remove SIP headers not required by the AT&T IPTF service (see **Section 6.4.2**). These headers are:
 - AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, Av-Secure-IndicationTo 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**.
9. **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues.** Certain Avaya SIP endpoints (e.g., 9641, 9621, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore, an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 7.8**).
10. **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 5.7.2**), it will send a ptime value of 20ms when it receives “a=ptime:20” from the Avaya SBCE. This causes the media packetization to be set to 20ms. No issues were found during testing due to this behavior.

2.3. Support

AT&T customers may obtain support information for the AT&T IP Toll Free service by visiting <https://www.business.att.com/products/ip-toll-free.html> or by calling (800) 325-5555.

Avaya customers may obtain documentation and support for Avaya products by visiting the Support page: <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers provided on the Support website to directly access specific support and consultation services based upon their Avaya support agreements.

3. Reference Configuration

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

- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya SIP endpoints register to Session Manager.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager provides the voice communication services for a particular enterprise site. Avaya H.323 endpoints register to Communication Manager.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G430 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya Aura® Media Server provides additional media resources for Communication Manager.
- Avaya Aura® Messaging (Messaging) is used in the reference configuration to provide voice mailbox capabilities. This solution is extensible to other Avaya messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Avaya desk telephones are represented with Avaya 96x1 Series IP Deskphones (running H.323 and SIP firmware), J100 Series IP Deskphones using the SIP software bundle Avaya 9408 Digital Deskphones, as well as Avaya IX Workplace™ for Windows softphones.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF IPv6 service and the enterprise internal IPv4 network.
- The IPTF service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya SBCE. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya SBCE (e.g., UDP, TCP, or TLS) and Communication Manager (e.g., TCP or TLS). In the reference configuration, Session Manager uses SIP over TLS to communicate with the Avaya SBCE, Messaging and Communication Manager.
- Inbound calls were placed from the PSTN via the IPTF service, through the Avaya SBCE to Session Manager, which routed the call to Communication Manager. Communication Manager terminated the calls to the appropriate Agent queue, Agent phone, or fax extension.

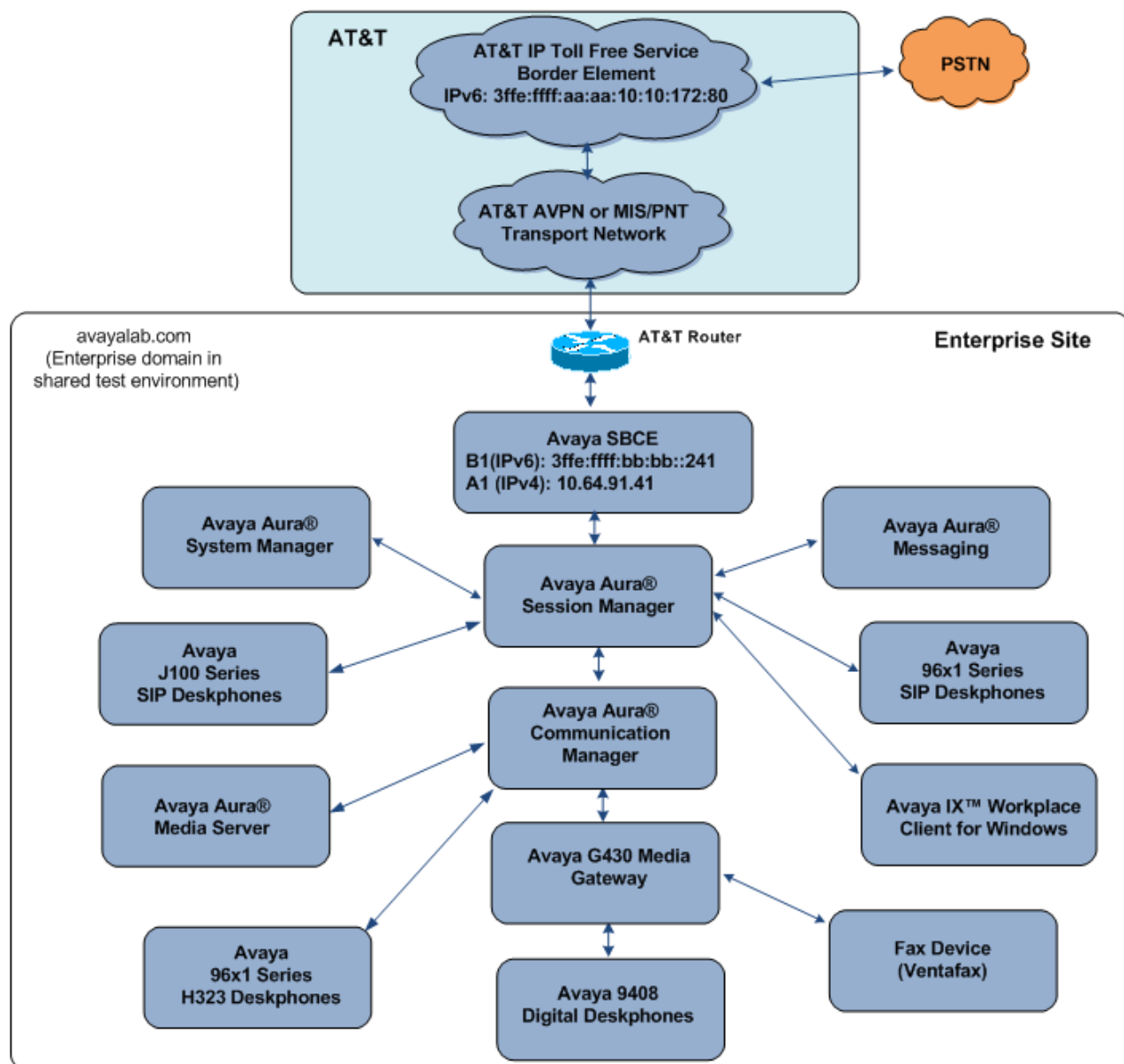


Figure 1: Reference configuration

Note – In the reference configuration, the IPTF service delivered 15 DNIS digits, with the format `00000xxxxxxxxxx`. These DNIS digits are used in the provisioning defined in the following sections, not the dialed digits. The DNIS digit length can vary depending on the customer's needs. Although during testing 15 digits were used, the total length supported by the IPTF service is 21 digits, including the five leading zeroes.

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 specific configurations.

Note - The AT&T IP Toll Free service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the AT&T Toll Free service) are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DNIS digits as part of the IP Toll Free provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura® System Manager	
IP Address	10.64.90.82
Avaya Aura® Session Manager	
IP Address	10.64.91.81
Avaya Aura® Communication Manager	
IP Address	10.64.91.75
Communication Manager dialplan	89xxx = Stations 2xxxx = Agents 71xxx = Agent skill queue VDNs
Avaya Aura® Messaging	
IP Address	10.64.91.84
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Private (A1) Interface	10.64.91.41
IP Address of Public (B1) Interface	3ffe:ffff:bb:bb::241 (see note below)
AT&T IP Toll Free Border Element	
IP Address	3ffe:ffff:aa:aa:10:10:172:80

Table 1: Illustrative Values Used in these Application Notes

Note – For security reasons, the actual 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 address of **3ffe:ffff:bb:bb::241** (Avaya SBCE public interface) and **3ffe:ffff:aa:aa:10:10:172:80** (AT&T BE IPv6 address) are specified.

3.2. Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled in the Avaya CPE environment, a general call flow is described below. In **Figure 2** an inbound IPTF service call arrives at the Avaya SBCE and is subsequently routed to Session Manager and to Communication Manager.

1. A PSTN telephone originates a call to an IPTF service number.
2. The PSTN routes the call to the IPTF service network.
3. The IPTF service 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 Routing Policies, determines 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 an Agent queue or telephone.

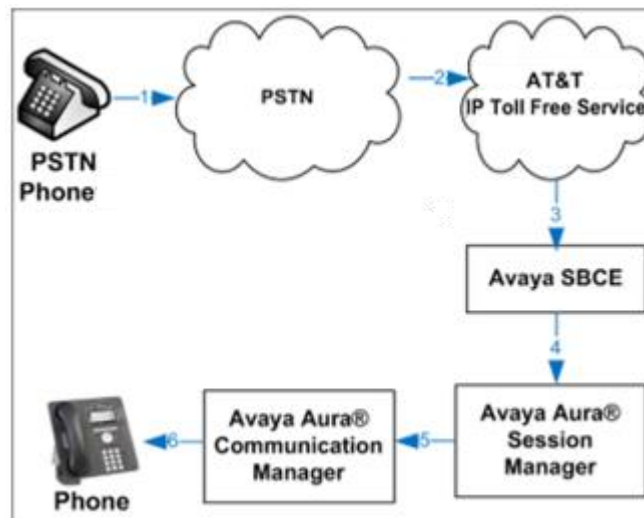


Figure 2: Inbound AT&T IP Toll Free Service Call to an Agent queue/telephone

Note: The IPTF service features such as Legacy Transfer Connect and Alternate Destination Routing utilize this call flow as well.

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	8.1.1.0.0310504 (Feature Pack 1)
Avaya Aura® Session Manager	8.1.1.0.811021
Avaya Aura® Communication Manager	8.1.1.0 (Feature Pack 1)
Avaya Session Border Controller for Enterprise	8.0.1.0-10-17555
Avaya Aura® Media Server	8.0.2.61
Avaya Aura® Messaging	7.1.Service Pack 2
Avaya G430 Media Gateway	41.16.0
Avaya 96x1 Series IP Deskphone (H.323)	6.8304
Avaya 96x1 Series IP Deskphone (SIP)	7.1.8.0.9
Avaya J129 IP Deskphone	4.0.3.1.4
Avaya IX™ Workplace Client for Windows	3.7.4.22.1
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 the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [5] and [6] in the References section for further details if necessary.

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. System-Parameters Customer-Options

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

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

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

display system-parameters customer-options			Page	2 of 12
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		4000	0	
Maximum Concurrently Registered IP Stations:		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	
Maximum Administered SIP Trunks:		4000	75	
Max Administered Ad-hoc Video Conferencing Ports:		4000	0	
Max Number of DS1 Boards with Echo Cancellation:		80	0	

Step 2 - On Page 5 of the form, verify that the Media Encryption Over IP field is set to y.

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

Step 3 - 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		
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

5.2. System-Parameters Features

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

change system-parameters features	Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
Self Station Display Enabled? y	
Trunk-to-Trunk Transfer: all	
Automatic Callback with Called Party Queuing? n	
Automatic Callback - No Answer Timeout Interval (rings): 3	
Call Park Timeout Interval (minutes): 10	
Off-Premises Tone Detect Timeout Interval (seconds): 20	
AAR/ARS Dial Tone Required? y	
Music (or Silence) on Transferred Trunk Calls? all	
DID/Tie/ISDN/SIP Intercept Treatment: attendant	
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred	
Automatic Circuit Assurance (ACA) Enabled? n	
Abbreviated Dial Programming by Assigned Lists? n	
Auto Abbreviated/Delayed Transition Interval (rings): 2	
Protocol for Caller ID Analog Terminals: Bellcore	
Display Calling Number for Room to Room Caller ID Calls? n	

5.3. Dial Plan

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

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

- 5-digit extensions with a **Call Type** of **ext** beginning with:
 - The digits **1, 5, 7** and **8** for Communication Manager extensions.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code ***xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 5.8**.

change dialplan analysis	Page 1 of 12							
DIAL PLAN ANALYSIS TABLE								
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						

5.4. Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used. Note that the Communication Manager procr name and IP address are entered during installation. The procr IP address was used to define the Communication Manager SIP Entities in **Section 6.5**.

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

- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.81**).
- Media Server (e.g., **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	
SM	10.64.91.81	
default	0.0.0.0	
procr	10.64.91.75	
procr6	::	

5.5. Processor Ethernet

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

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

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

5.6. 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 G430 Media Gateway and Avaya Media Server are in region 1. To provide testing flexibility, network region 4 was associated to components used specifically for the AT&T SIP trunk access.

5.6.1. IP Network Region 1 – Local CPE Region

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

- Enter a descriptive name (e.g., **Enterprise**).
- Enter the enterprise domain (e.g., **avayalab.com**) in the **Authoritative Domain** field (see **Section 6.2**).
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min**: – Set to **16384** (AT&T requirement).
- **UDP Port Max**: – Set to **32767** (AT&T requirement).

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: avayalab.com	
Name: Enterprise	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 16384	IP Audio Hairpinning? n	
UDP Port Max: 32767		
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		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y	RSVP Enabled? n	
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

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.

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

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

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

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

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **4** in the **dst rgn** column, enter **4** for the codec set (this means region 1 is permitted to talk to region 4 and it will use codec set 4 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		
dst	codec	direct	WAN-BW-limits		Video	Intervening		Dyn	A	G	
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	
1	1									L	
										e	
2	2	y	NoLimit						n	all	
3	1	y	NoLimit						n	t	
4	4	y	NoLimit						n	t	

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

Repeat the steps in **Section 5.6.1** with the following changes:

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

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

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

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

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

Note: An additional IP Network Region and IP Codec Set were created in the reference configuration, used to test G.711 pass-through fax. Details of this optional configuration can be found in **Section 122**.

5.7. 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.

Note – The IPTF service offers G.729A, G.726-32, and G.711MU codecs in their Invite SDP. G.726-32 codec is supported by Communication Manager, but testing found issues when G.726-32 codec is used (see **Section 2.2, item 3**). In addition, some calls could require support of G.729B (silence suppression). Therefore G.729B is also included in the codec lists.

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

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., **1**). On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, **G.729A**, and **G.729B** are included in the codec list. Note that the packet interval size will default to 20ms. Under **Media Encryption**, ensure **1-srtp-aescm128-hmac80** is included to support Secure Real-time Transport Protocol (SRTP).

change ip-codec-set 1				Page 1 of 2
IP CODEC SET				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711MU	n	2	20	
2: G.729A	n	2	20	
3: G.729B	n	2	20	
Media Encryption			Encrypted SRTP: enforce-unenc-srtp	
1: 1-srtp-aescm128-hmac80				
2: none				

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

change ip-codec-set 1				Page 2 of 2
IP CODEC SET				
Allow Direct-IP Multimedia? y				
Maximum Call Rate for Direct-IP Multimedia: 15360:Kbits				
Maximum Call Rate for Priority Direct-IP Multimedia: 15360:Kbits				
	Mode	Redundancy	Packet Size (ms)	
FAX	t.38-standard	0	ECM: y	
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0	20	

5.7.2. Codecs for IP Network Region 4 (calls from AT&T)

Step 1 - Repeat the steps in **Section 5.7.1** with the following changes.

- Provision the codecs in the order shown below. Note that the order of G.729A and G.729B codecs may be reversed as required.
- Set **Frames Per Pkt** to **3**. This will auto-populate **30** for the **Packet Size (ms)** field, and specify a PTIME value of 30 in the SDP (recommended by AT&T). See **Section 2.2, Item 10** for limitations with the packet size.

change ip-codec-set 4				Page 1 of 2
IP CODEC SET				
Codec Set: 4				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.729A	n	3	30	
2: G.729B	n	3	30	
3: G.711MU	n	3	30	
Media Encryption			Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80				
2: none				
change ip-codec-set 4				Page 2 of 2
IP CODEC SET				
Allow Direct-IP Multimedia? n				
FAX	Mode	Redundancy	ECM: y	Packet Size (ms)
Modem	t.38-standard	0		
TDD/TTY	off	0		
H.323 Clear-channel	US	3		
SIP 64K Data	n	0		20

Note: An additional IP Network Region and IP Codec Set were created in the reference configuration, used to test G.711 pass-through fax. Details of this optional configuration can be found in **Section 122**.

5.8. SIP Trunks

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

- Inbound IPTF access – SIP Trunk 4. This trunk will use TLS port 5064
- Internal CPE access (e.g., Avaya SIP telephones, etc.) – SIP Trunk 3. This trunk will use TLS port 5061.

Note that different ports are assigned to each trunk. This is necessary so Session Manager can distinguish the traffic on the service provider trunk, from the traffic on the trunk used for other enterprise SIP traffic.

Note – While TLS is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the IPTF service. See the note in **Section 6.5** regarding the use of TLS transport protocol in the CPE.

5.8.1. SIP Trunk for Inbound AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for inbound IPTF calls. This trunk corresponds to the **CM-TG4** SIP Entity defined in **Section 6.5.2**.

5.8.1.1 Signaling Group 4

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5064**.
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 5.6.2**.
- **Far-end Domain** – Enter **avayalab.com**. This is the domain provisioned for Session Manager in **Section 6.2**.
- **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.

add signaling-group 4		Page 1 of 2
SIGNALING GROUP		
Group Number: 4	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5064	Far-end Listen Port: 5064	
	Far-end Network Region: 4	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

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

5.8.1.2 Trunk Group 4

Step 1 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 4). 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 IPTF**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***04**).
- **Direction** – Set to **incoming**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Step 1** (e.g., 4).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **20**).

add trunk-group 4		Page 1 of 21
TRUNK GROUP		
Group Number: 4	Group Type: sip	CDR Reports: y
Group Name: ATT IPTF	COR: 1	TN: 1 TAC: *04
Direction: incoming	Outgoing Display? n	
Dial Access? n	Night Service:	
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 4	
	Number of Members: 20	

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

- Set the **Preferred Minimum Session Refresh Interval (sec):** to **900**.

add trunk-group 4	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 900	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n	
Caller ID for Service Link Call to H.323 1xC: station-extension	

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

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

add trunk-group 4	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: public	
	UII Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
Show ANSWERED BY on Display? y	

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

- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPTF service (e.g., **100**).

Note – The IPTF service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, any History Info headers sent by Communication Manager are automatically removed from SIP signaling by Session Manager, as part of the AttAdapter (see **Section 6.4.2**). Alternatively, History Info may be disabled here.

add trunk-group 4	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 100	
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	

5.8.2. Local SIP Trunk (Avaya SIP Telephones, Messaging Access)

This trunk corresponds to the **CM-TG3** SIP Entity defined in **Section 6.5.3**.

5.8.2.1 Signaling Group 3

Repeat the steps in **Section 5.8.1.1** with the following changes:

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

Step 2 - Set the following parameters on page 1:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 5.6.1**.

5.8.2.2 Trunk Group 3

Repeat the steps in **Section 5.8.1.2** with the following changes:

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

- **Group Name** – Enter a descriptive name (e.g., **SM Enterprise**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***03**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Section**
Error! Reference source not found. (e.g., **3**).

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

- Same as **Section 5.8.1.2**.

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

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

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

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

Use default values for all other settings.

5.9. Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 5.8.1**), is used to convert Communication Manager local extensions to IPTF DNIS numbers, for inclusion in any SIP headers directed to the IPTF 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 any Communication Manager Agent skill VDN extensions and their corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager extension (e.g., Skill VDN **71025**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **000008884571025**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **15**).

Step 3 - Add any Communication Manager station extensions and their corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager station extension (e.g., SIP phone **89324**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **000008884571028**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **15**).

Step 4 - Repeat **Steps 2** and **3** for all IPTF DNIS numbers and their corresponding Communication Manager station, Skill, or Agent extensions.

change public-unknown-numbering 5 ext-digits 71025					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	71025	4	000008884571025	15	Total Administered: 67
5	71026	4	000008884571026	15	Maximum Entries: 240
5	71027	4	000008884571027	15	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	89324	4	000008884571028	15	
					Communication Manager automatically inserts a '+' digit in this case.

5.10. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 5.8.2**), 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 Communication Manager extension patterns defined in the Dial Plan in **Section 5.3** (e.g., **20, 71, 89**).
- **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 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	12	3		5	Total Administered: 6
5	14	3		5	Maximum Entries: 540
5	20	3		5	
5	71	3		5	
5	89	3		5	

5.11. Route Pattern for Local SIP Trunk

Route Patterns are used to direct calls to the Local SIP trunk for access to SIP phones or other destinations in the CPE. This form specifies the local SIP trunk (e.g., 3), based on the route-pattern selected by the AAR table in **Section 5.12** (e.g., calls SIP phone extensions).

Note – As IPTF is an inbound only service, no outbound route patterns are defined for the public SIP trunk.

Step 1 - Enter the **change route-pattern 3** command and enter the following:

- In the **Grp No** column enter **3** for SIP trunk 3 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the **Numbering Format** column across from line **1**, enter **lev0-pvt**.

change route-pattern 3										Page 1 of 3			
Pattern Number: 3					Pattern Name: ToSM Enterprise								
SCCAN? n		Secure SIP? n		Used for SIP stations? y									
Primary SM: SM					Secondary SM:								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted				DCS/	IXC	
No		Mrk	Lmt	List	Del	Digits				QSIG			
										Dgts	Intw		
1:	3	0										n	user
2:											n	user	
3:											n	user	
BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature		PARM	Sub	Numbering	LAR	
0 1 2 M 4 W		Request								Dgts	Format		
1:	y	y	y	y	y	n	n	rest		lev0-pvt none			

5.12. Automatic Alternate Routing (AAR) Dialing

AAR is used to direct calls to the local SIP trunk for Avaya SIP telephones, using the route pattern defined in **Section 5.11**.

Step 1 - Enter the following:

- **Dialed String** - In the reference configuration all SIP telephones used extensions in the range 89xxx, therefore enter **89**.
- **Min & Max** - Enter **5**.
- **Route Pattern** - Enter **3**.
- **Call Type** - Enter **lev0**.

change aar analysis 0								Page 1 of 2
AAR DIGIT ANALYSIS TABLE								
Location: all								Percent Full: 1
Dialed String		Total		Route	Call	Node	ANI	
		Min	Max	Pattern	Type	Num	Reqd	
20		5	5	3	lev0		n	
89		5	5	3	lev0		n	

5.13. Provisioning for Simulated Call Center Functionality

In the reference configuration, a Call Center environment (skill queues and Agents) was simulated on Communication Manager. The administration of Communication Manager Call Center type elements – Agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult [6] and [10] in the References section for further details. The samples that follow are provided for reference purposes only.

- Agent form – **Page 1**

display agent-loginID 20001		Page	1 of 2
AGENT LOGINID			
Login ID: 20001	AAS? n		
Name: Agent 1	AUDIX? n		
TN: 1	Check skill TNs to match agent TN? n		
COR: 2			
Coverage Path: 1	LWC Reception: spe		
Security Code:	LWC Log External Calls? n		
Attribute:	AUDIX Name for Messaging:		
LoginID for ISDN/SIP Display? n			
Password:			
Password (enter again):			
Auto Answer: acd			
AUX Agent Remains in LOA Queue: system	MIA Across Skills: system		
AUX Agent Considered Idle (MIA): system	ACW Agent Considered Idle: system		
Work Mode on Login: system	Aux Work Reason Code Type: system		
Logout Reason Code Type: system			
Maximum time agent in ACW before logout (sec): system			
Forced Agent Logout Time: :			
WARNING: Agent must log in again before changes take effect			

- Agent form – **Page 2**

display agent-loginID 20001		Page	2 of 2
AGENT LOGINID			
Direct Agent Skill:	Service Objective? n		
Call Handling Preference: skill-level	Local Call Preference? n		
SN	RL SL	SN	RL SL
1: 1	1	16:	

- Skill 1 Hunt Group form – Page 1

display hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1		ACD? y
Group Name: Agent Group		Queue? y
Group Extension: 19991		Vector? y
Group Type: ucd-mia		
TN: 1		
COR: 1		MM Early Answer? n
Security Code:		Local Agent Preference? n
ISDN/SIP Caller Display: grp-name		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

- Skill 1 VDN form – Page 1

display vdn 71041		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 71041		
Name*: ATT Toll-Free 1		
Destination: Vector Number	4	
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		

- Skill 1 Vector form – Page 1

display vector 4		Page 1 of 6
CALL VECTOR		
Number: 4	Name: Call Center	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
01 #	Wait hearing ringback	BSR? y
02 wait-time	2 secs hearing ringback	Holidays? y
03 #	Play greeting and collect 1 digit	
04 collect	1 digits after announcement	11001 for none
05 goto step	7 if digits	= 1
06 stop		
07 #	Simple queue to skill with recurring announcement until available	
08 queue-to	skill 1	pri m
09 announcement	11004	
10 wait-time	30 secs hearing music	
11 goto step	8 if unconditionally	
12 stop		

5.14. Avaya G430 Media Gateway Provisioning

In the reference configuration, an Avaya G430 Media Gateway is provisioned. The G430 is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. For additional information for the provisioning of the Medias Gateway see **Error! Reference source not found.** in the References section.

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

Step 2 - Enter the **show system** command and copy down the G430 serial number.

Step 3 - Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.64.91.75**, see **Section 5.5**).

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

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

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

- Set **Type** = **g430**.
- Set **Name** = a descriptive name (e.g., **G430-1**).
- 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 G430 to register to Communication Manager. When the Media Gateway registers, the G430 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., *G430-001(super)#*).

Step 7 - Enter the **display media-gateway 1** command and verify that the G430 has registered.

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

      Type: g430
      Name: G430-1
      Serial No: 11IS31439520
Link Encryption Type: any-ptls/tls      Enable CF? n
      Network Region: 1                  Location: 1
      Use for IP Sync? n                 Site Data:
      Recovery Rule: none

      Registered? y
FW Version/HW Vintage: 41 .16 .0 /1
      MGP IPv4 Address: 10.64.91.91
      MGP IPv6 Address:
Controller IP Address: 10.64.91.75
      MAC Address: 00:1b:4f:53:37:69

Mutual Authentication? optional
```

5.15. Avaya Aura® Media Server Provisioning

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

Note – Only the Media Server provisioning associated with Communication Manager is shown below. See Error! Reference source not found. and Error! Reference source not found. in the References section for additional information.

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

Step 2 - On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP → Node and Routes** and add the Communication Manager Procr interface IP address (e.g., **10.64.91.75**, see **Section 5.4**) as a trusted node (not shown).

Step 3 - On Communication Manager, enter the **add signaling-group x** command where x is an unused signaling group (e.g., **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 5.4**.
- **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 5.4** (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 5.6.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

add signaling-group 80Page 1 of 2

SIGNALING GROUP

Group Number: 80Group Type: sip

Transport Method: tls

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

- **Signaling Group** – Enter the signaling group previously configured for Media Server (e.g., 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
```

5.16. Save Translations

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

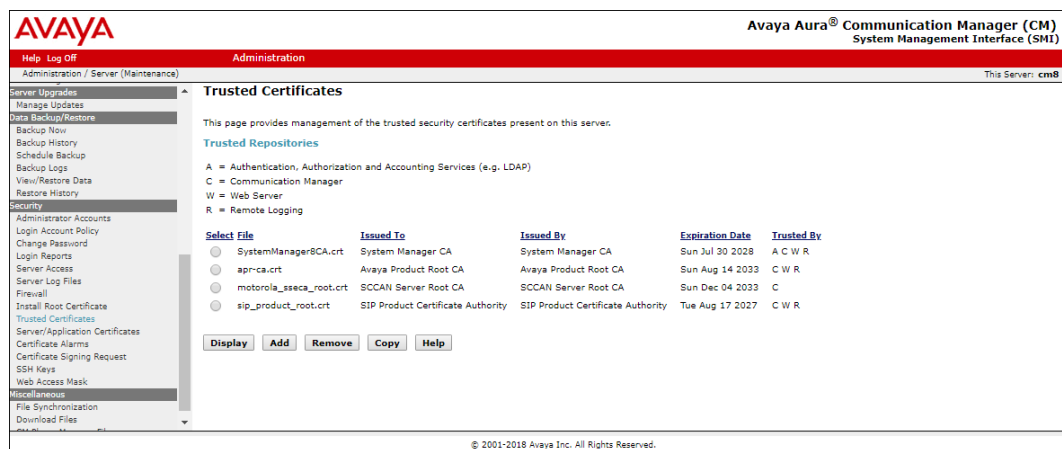
5.17. Verify TLS Certificates – Communication Manager

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

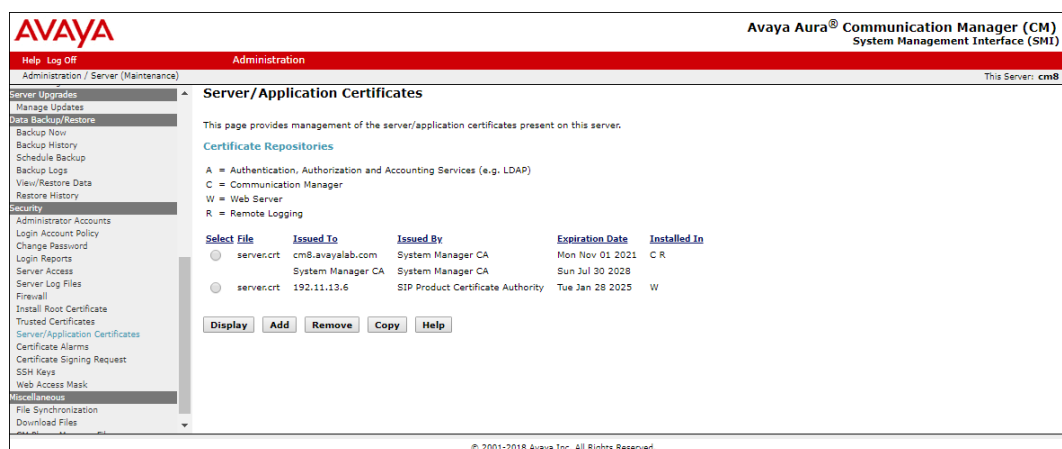
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. The following procedures show how to verify the certificates used by Communication Manager.

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

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



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



6. Configure Avaya Aura® Session Manager

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult documents [1] through [4] in the References section for further details if necessary.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Avaya SBCE.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented as Entity Links.

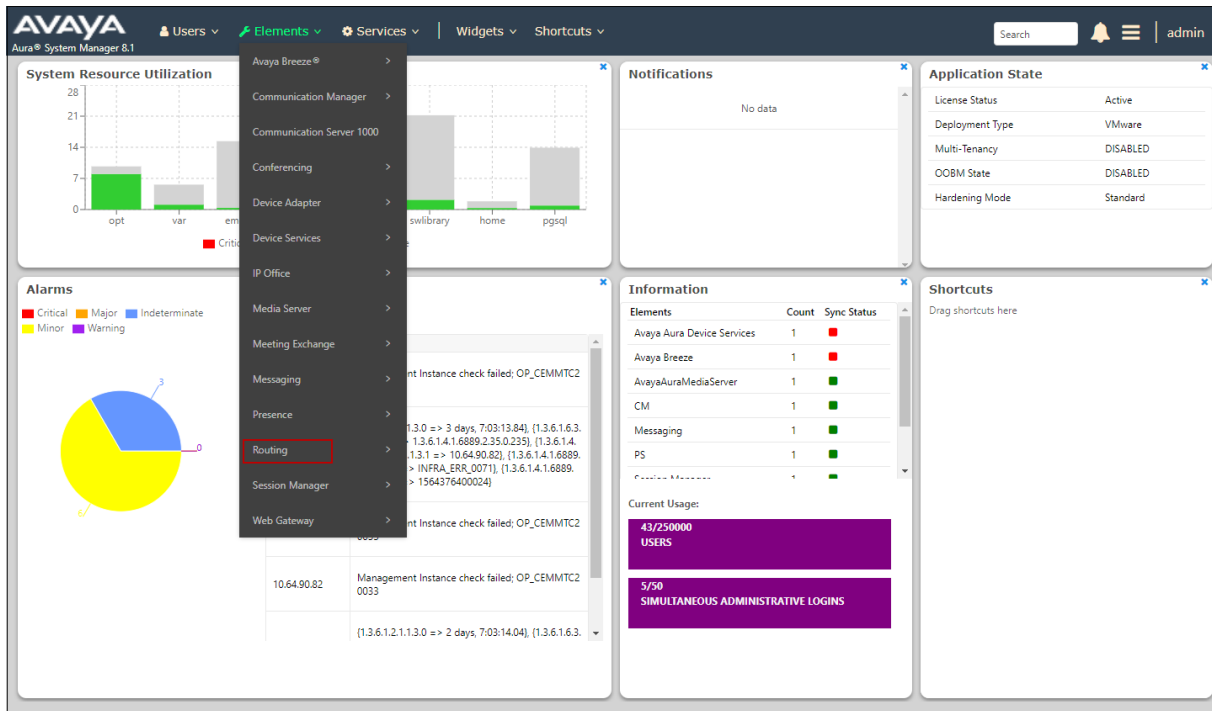
When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as Adaptations, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of normalizing the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed Dial Patterns and determines the destination SIP Entities based on Routing Policies specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

The following administration activities will be described:

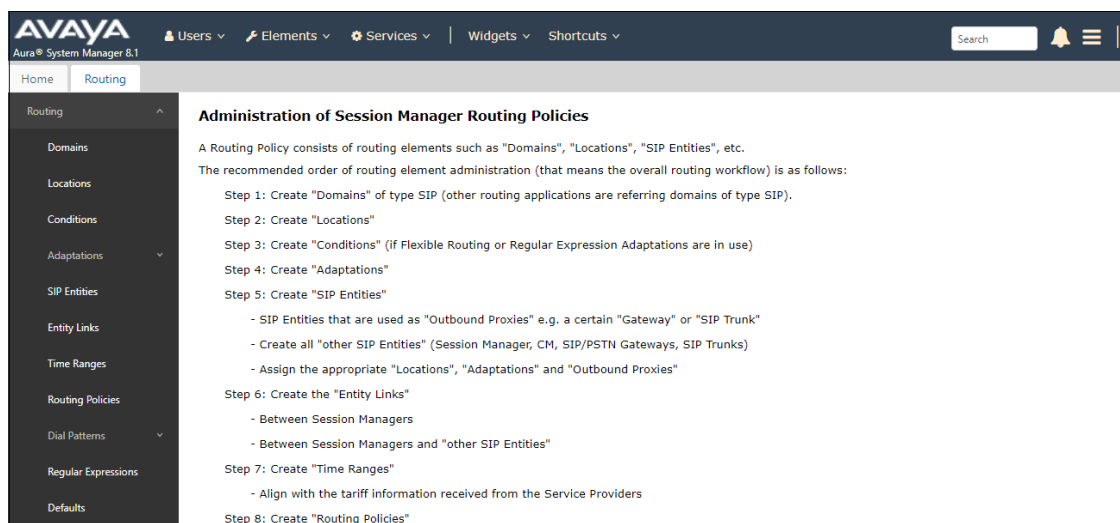
- Define a SIP Domain.
- Define a Location for Customer Premises Equipment (CPE).
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager and the Avaya SBCE.
- Define SIP Entities corresponding to Session Manager, Communication Manager and the Avaya SBCE.
- Define Entity Links describing the SIP trunks between Communication Manager and Session Manager, as well as the SIP trunks between the 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.
- 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. From the **Home** screen, under the **Elements** heading, 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 this section will be located under the **Routing** element shown below.



6.2. SIP Domain

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

Step 2 - Click **New**. 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 (not shown).

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' section expanded, with 'Domains' selected. The main content area is titled 'Domain Management' and contains a table with one item: 'avayalab.com' of type 'sip'. Above the table are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A 'Filter: Enable' link is on the right.

Name	Type	Notes
avayalab.com	sip	

6.3. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager, SIP endpoints, etc.
- **Common SBCs**– This site contains the Avaya SBCE.

6.3.1. 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 shows the 'Locations' menu item selected. The main content area is titled 'Location Details' and includes a 'Commit' button. The 'General' section contains fields for 'Name' (set to 'Main') and 'Notes' (set to 'Avaya SIL'). Below this, 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', along with a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section contains fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth' (set to '64 Kbit/Sec'), and 'Default Audio Bandwidth' (set to '80 Kbit/sec'). The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' (both set to '80 %'), and checkboxes for 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' (both set to '5 Minutes'). At the bottom, there is a 'Location Pattern' section with an 'Add' button and a table with columns for 'IP Address Pattern' and 'Notes'.

6.3.2. Common-SBCs Location

To configure the Avaya SBCE Location, follow the steps from **Section 6.3.1** with the following changes (not shown):

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

6.4. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T to Communication Manager.

- Inbound messages - Modification of SIP messages sent to Communication Manager extensions. (**Section 6.4.1**)
 - The AT&T called number digit string in the Request URI is replaced with the associated Communication Manager extensions defined for Agent skill queue VDNs/telephones.
- Outbound messages - Modification of SIP messages sent by Communication Manager extensions. (**Section 6.4.2**)
 - The History-Info header is removed automatically by the **AttAdapter**.
 - Avaya SIP headers not required by AT&T are removed.

6.4.1. 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-TG4-IPTF**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).

The screenshot shows the 'Adaptation Details' configuration page. On the left, a navigation pane under 'Routing' has 'Adaptations' selected. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The form contains the following fields: 'Adaptation Name' with the value 'CM-TG4-IPTF', 'Module Name' with a dropdown menu showing 'DigitConversionAdapter', 'Module Parameter Type' with a dropdown arrow, 'Egress URI Parameters' with an empty text box, and 'Notes' with the text 'CM - ATT - IPTF'. At the top right of the form are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

Step 3 - Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the inbound digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager). 00000888457102 in the example below are the first 14 digits of the 15 DNIS strings sent in the Request URI by the IPTF service, associated with Communication Manager Agent/VDN skills 71025 to 71029.

- Enter **00000888457102** in the **Matching Pattern** column.
- Enter **15** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column. With this setting, the first 10 digits of the DNIS string are deleted, and the remaining 5 digits, corresponding to the Vector Directory Numbers (VDNs) in Communication Manager are left untouched.
- Specify that this digit conversion should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 – In the screen below, 000008884571030 is the DNIS associated with Communication Manager extension 89324. Repeat **Step 3** above with the following changes:

- Enter **000008884571030** in the **Matching Pattern** column.
- Enter **15** in the **Delete Digits** column.
- Enter **89324** in the **Inserted Digits** column. With these settings, all 15 digits of the DNIS string are deleted, and replaced with the 5 digit Communication Manager extension number.

Step 5 – Create entries for all additional IPTF DNIS numbers/Communication Manager VDNs and extensions.

Step 6 - Click on **Commit**.

Digit Conversion for Outgoing Calls from SM
Add Remove
2 Items Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*00000888457102	*15	*15		*10		destination ▼		15 digit DNIS to VDN Conversion
<input type="checkbox"/>	*000008884571030	*15	*15		*15	89324	destination ▼		15 digit to 5 digit extension

Select : All, None

Commit Cancel

Note – No **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

6.4.2. Adaptation for the AT&T IP Toll Free 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 6.4.1** with the following changes.

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

- A descriptive **Name**, (e.g., **SBC1-Adaptation for ATT**).
- 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 IPTF service does not support), sent by Communication Manager (see **Section 5.8.1**).

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

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

- **Name** – Enter **eRHdrs**
- **Value** – Enter the following Avaya headers to be removed by Session Manager. Note that each header name is separated by a comma with no spaces in between. If spaces are used after the comma, the string needs to be enclosed in quotes:
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: Routing, Domains, Locations, Conditions, Adaptations (selected), Regular Expression..., SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Adaptation Name' is 'SBC1-Adaptation for ATT', the 'Module Name' is 'AttAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this is a table for Name-Value Parameters with columns 'Name' and 'Value'. One entry is visible: 'eRHdrs' with a long list of Avaya headers to be removed. Below the table is a 'Select' dropdown set to 'All, None'. Further down, there are fields for 'Egress URI Parameters' and 'Notes' (containing 'SBC - ATT IPTF'). At the bottom, there are two sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM', each with a table for configuration. Both tables currently show '0 Items'.

6.5. SIP Entities

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

- Session Manager (**Section 6.5.1**). Note that this Entity is normally created during Session Manager installation but is shown here for completeness.
- Communication Manager for AT&T access (**Section 6.5.2**) – This entity, and its associated Entity Link (using TLS with port 5064, is for calls from the IPTF service to Communication Manager via the Avaya SBCE.
- Communication Manager for local access (**Section 6.5.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily used for traffic between Avaya SIP telephones and Communication Manager.
- Avaya SBCE (**Section 6.5.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls from the IPTF service via the Avaya SBCE.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5064), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the AT&T IPTF service uses UDP/5060 per AT&T requirements.

6.5.1. 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**).
- **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.81**).
- **Type** – Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 6.3.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.
- **Minimum TLS Version** – Select 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.

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

- **Port** – Enter **5061**
- **Protocol** – Select **TLS**
- **Default Domain** – Select a SIP domain administered in **Section 6.2** (e.g., **avayalab.com**)

Step 5 - Repeat **Step 4** to provision entries for any other listening ports used by Session Manager for SIP telephones. These are separate from the ports defined for the Entity Links in **Section 6.6**.

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

Step 7 - Click on **Commit**.

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

Note – The **Entity Links** section of these forms (not shown) will be automatically populated when the Entity Links are defined in **Section 6.6**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

6.5.2. 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-TG4**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Sections 5.4 and 5.5** (e.g., **10.64.91.75**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM-TG4-IPTF** administered in **Section 6.4.1**.
- **Location** – Select a Location **Main** administered in **Section 6.3.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field and use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

SIP Entity Details Commit Cancel

General

* Name:

* FQDN or IP 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:

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

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **CM-TG3**).
- **Adaptations** – Leave this field blank.
- **Location** – Select Location **Main** administered in **Section Error! Reference source not found.**

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** CM-TG3
- FQDN or IP Address:** 10.64.91.75
- Type:** CM
- Notes:** Trunk Group 3 - CM to Enterprise
- Adaptation:** (empty)
- Location:** Main
- Time Zone:** America/Denver
- * SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☒
- Call Detail Recording:** none

6.5.4. Avaya Session Border Controller for Enterprise SIP Entity

Repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **SBCE-Toll Free**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.41**), see **Section 7.3**.
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for ATT** (**Section 6.4.2**).
- **Location** – Select Location **Common-SBCs** administered in **Section 6.3.2**.

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** SBCE-Toll Free
- FQDN or IP Address:** 10.64.91.41
- Type:** SIP Trunk
- Notes:** SBCE for IPTF testing
- Adaptation:** SBC1-Adaptation for ATT
- Location:** Common-SBCs
- Time Zone:** America/Denver
- * SIP Timer B/F (in seconds):** 1
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** egress

6.6. Entity Links

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

- Session Manager to Communication Manager Public trunk (**Section 6.6.1**).
- Session Manager to Communication Manager Local trunk (**Section 6.6.2**).
- Session Manager to Avaya SBCE (**Section 6.6.3**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.5**.

Note – See the information in **Section 6.5** regarding the transport protocols and ports used in the reference configuration.

6.6.1. 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 TG4**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.5.1** for Session Manager (e.g., **Session Manager**).
- **SIP Entity 1 Port** – Enter **5064**.
- **Protocol** – Select **TLS** (see **Section 5.8.1**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public entity (e.g., **CM-TG4**).
- **SIP Entity 2 Port** – Enter **5064** (see **Section 5.8.1**).
- **Connection Policy** – Select **trusted**.

Step 3 - Click on **Commit**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
SM to CM TG4	Session Manager	TLS	5064	CM-TG4	5064	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

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

To configure this Entity Link, repeat the steps in **Section 6.6.1**, 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 6.5.3** for the Communication Manager local entity (e.g., **CM-TG3**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 5.8.2**).

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
* SM to CM TG3	* Session Manager	TLS	* 5061	* CM-TG3	* 5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>

6.6.3. Entity Link for the AT&T IP Toll Free Service via the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to SBCE-TollFree**).
- **SIP Entity 1 Port** – Enter **5061**
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE entity (e.g., **SBCE-Toll Free**).
- **SIP Entity 2 Port** – Enter **5061**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
* SM to SBCE-TollFree	* Session Manager	TLS	* 5061	* SBCE-Toll Free	* 5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>

6.7. 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	

6.8. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (Section 6.8.1).

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

This Routing Policy is used for inbound calls from IPTF.

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 TG4**), 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 Entity list page will open.

Name	FQDN or IP Address	Type	Notes
<			

Step 4 - In the **SIP Entities List** page, select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public SIP Entity (**CM-TG4**), and click on **Select**.

SIP Entities				
13 Items				
	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	Aura Messaging	10.64.91.84	Messaging	Aura Messaging
<input type="radio"/>	Breeze	10.64.91.18	Avaya Breeze	
<input type="radio"/>	CM-TG1	10.64.91.75	CM	Trunk Group 1 - CM to Vz-IPT
<input type="radio"/>	CM-TG2	10.64.91.75	CM	Trunk Group 2 - Vz-Toll-Free inbound
<input type="radio"/>	CM-TG3	10.64.91.75	CM	Trunk Group 3 - CM to Enterprise
<input checked="" type="radio"/>	CM-TG4	10.64.91.75	CM	Trunk Group 4 - ATT IPTF
<input type="radio"/>	CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR
<input type="radio"/>	IP500	10.64.19.70	Other	IP Office
<input type="radio"/>	Presence	10.64.91.18	Presence Services	
<input type="radio"/>	SBC1	10.64.91.50	SIP Trunk	Avaya SBC-1 to PSTN
<input type="radio"/>	SBC2	10.64.91.100	SIP Trunk	Avaya SBC-2 to PSTN
<input type="radio"/>	SBCE-ATT	10.64.91.40	SIP Trunk	SBCE for AT&T testing
<input type="radio"/>	SBCE-Toll Free	10.64.91.41	SIP Trunk	SBCE for IPTF testing
Select : None				

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

Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 6.7**, 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 6.9**) they will appear in the **Dial Pattern** section of this form.

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

Routing Policy Details

Commit Cancel

Help ?

General

* Name: To CM TG4

Disabled: ☐

* Retries: 0

Notes: Trunk Group 4 PSTN4 to CM

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM-TG4	10.64.91.75	CM	Trunk Group 4 - ATT IPTF

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. Dial Patterns

In this section, Dial Patterns are administered to match inbound PSTN calls via the IPTF service to Communication Manager. In the reference configuration, inbound calls from the IPTF service sent 15 digits in the SIP Request URI. The DNIS digit length can vary depending on the customer's needs. Although during testing 15 digits were used, the total length supported by the IPTF service is 21 digits. This pattern must be matched for further call processing.

6.9.1. Dial Pattern for Inbound Calls to Communication Manager

Note – In the reference configuration inbound calls from the IPTF service sent 15 DNIS digits in the SIP Request URI. Be sure to match on the digit string specified in the AT&T Request URI, not the digit string of the number dialed. They may be different.

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

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

- **Pattern** – In the reference configuration, AT&T sends a 10-digit number in the Request URI with the format 00000xxxxx. Enter **00000**.
- **Min** – Enter **6**.
- **Max** – Enter **21**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

Note – The Adaptation defined for Communication Manager in **Section 6.4.1** will convert the various 00000xxxxxx numbers into their corresponding Communication Manager extensions.

Dial Pattern Details [Commit] [Cancel] Help ?

General

* **Pattern:** 00000

* **Min:** 6

* **Max:** 21

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: ATT TF Inbound

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

[Add] [Remove]

1 Item

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
Common-SBCs	SBC to PSTN			To CM TG4	0	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM

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

Step 4 - In the **Originating Location** section of the **Originating Locations, Origination Dial Pattern Sets and Routing Policies** page, check the checkbox corresponding to the location assigned to the Avaya SBCE in **Section 6.3.2**, e.g., **Common-SBCs**.

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 6.8.1** (e.g., **To CM TG4**). Click on **Select** (not shown).

Originating Location

Select

Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

5 Items

Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5
<input checked="" 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

Select : All, None

Origination Dial Pattern Sets

1 Item

Filter: Enable

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

Select : None

Routing Policies

13 Items

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AAM	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 PSTN1 to CM
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 VzIPCC to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input checked="" 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 TG7	<input type="checkbox"/>	CM-TG7	Incoming calls from Masergy
<input type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	ExperiencePortal	

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

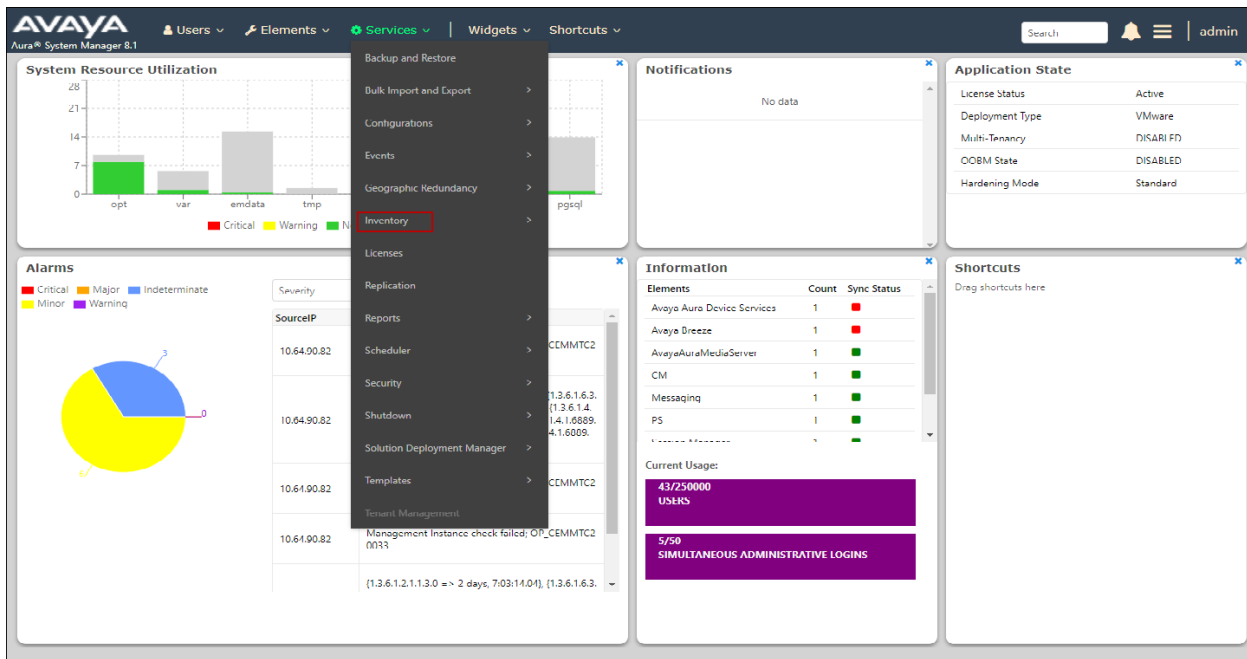
Step 7 - Repeat **Steps 1-6** for any additional inbound dial patterns from AT&T to Communication Manager.

6.10. Verify TLS Certificates – Session Manager

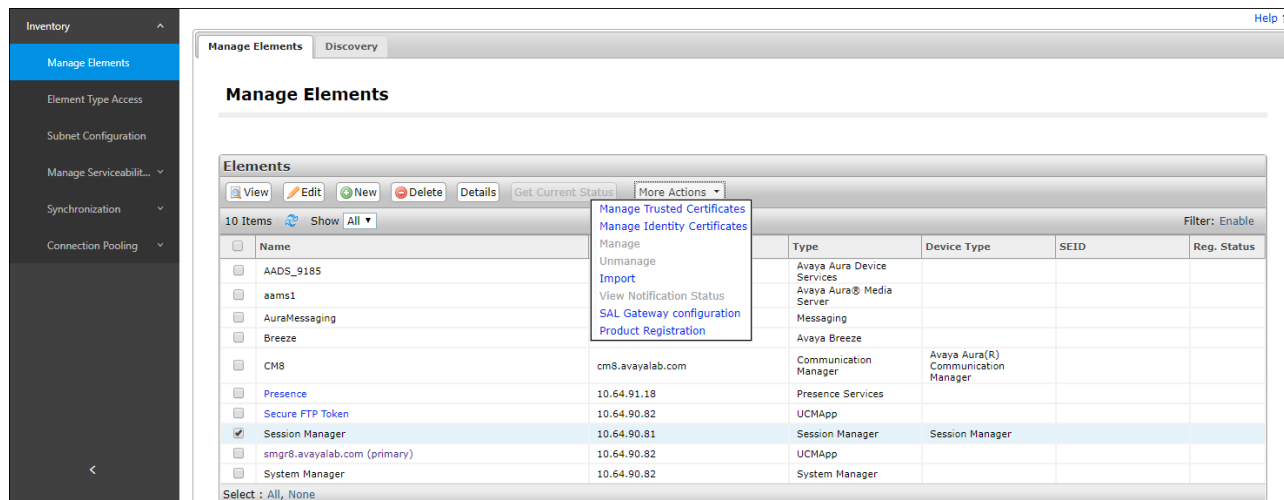
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

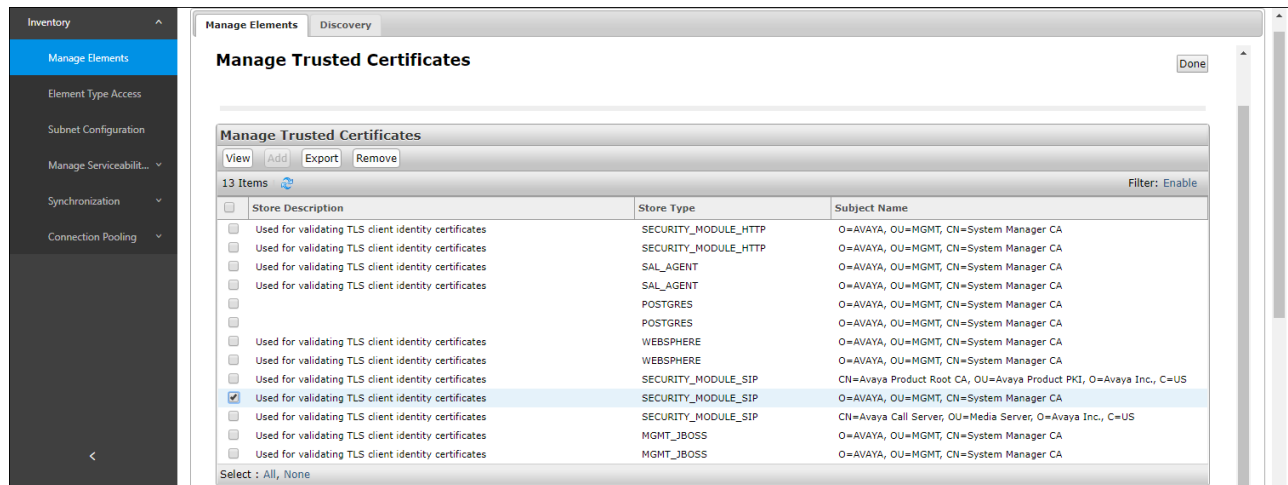
Step 1 - From the **Home** screen, under the **Services** heading, select **Inventory**.



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**.

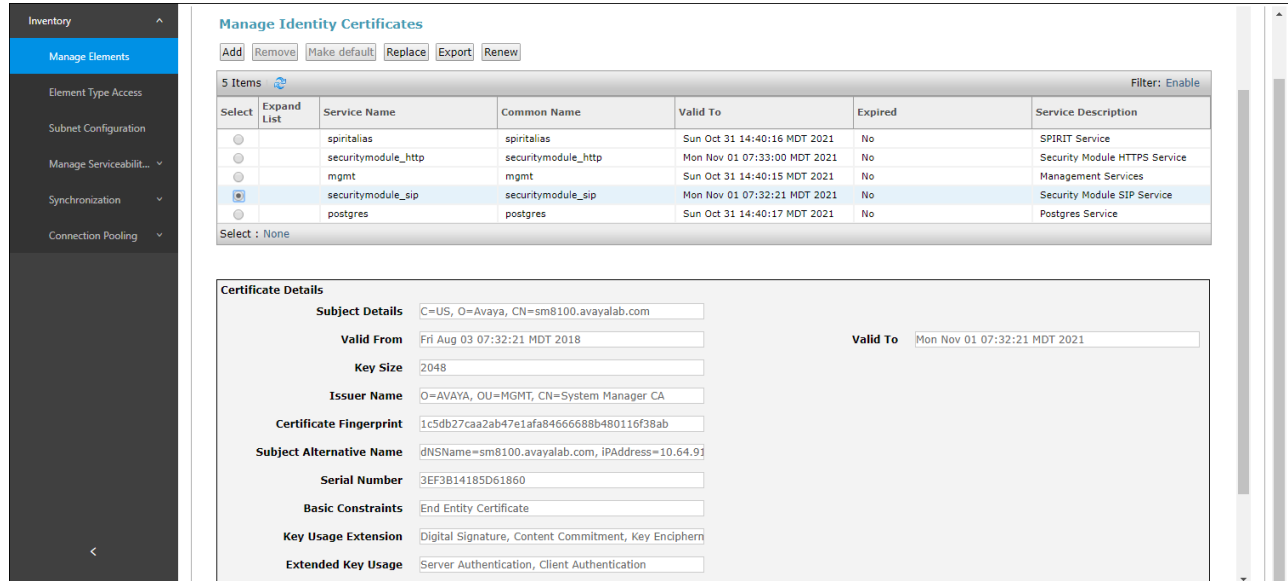


Step 3 - Verify the System Manager Certificate Authority certificate is listed in the trusted store, **SECURITY_MODULE_SIP**. Click **Done** to return to the previous screen.



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 login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there are input 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 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." and a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 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 EMS Dashboard for the Session Border Controller for Enterprise. The left-hand menu includes: EMS Dashboard, 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	09:09:09 AM MDT	Refresh
Version	8.0.1.0-10-17555	
Build Date	Tue Jul 30 22:53:51 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	10/14/2019 06:28:47 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 EMS Dashboard with the **Device Management** section selected. The left-hand menu is the same as in the previous screenshot. The main content area is titled 'Device Management' and contains a tabbed interface with the following tabs: Devices, Updates, SSL VPN, Licensing, and Key Bundles. The **Devices** tab is selected, showing a table of installed devices:

Device Name	Management IP	Version	Status						
SBCE8-70	10.64.90.70	8.0.1.0-10-17555	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 Name

SBCE8-70

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

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
3ffe:ffff:bb:bb::241	3ffe:ffff:bb:bb::241	64	3ffe:ffff:bb:bb::1	B1
				B1
				B2

DNS Configuration

Primary DNS

10.64.19.201

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.64.91.40

Management IP(s)

IP #1 (IPv4)

10.64.90.70

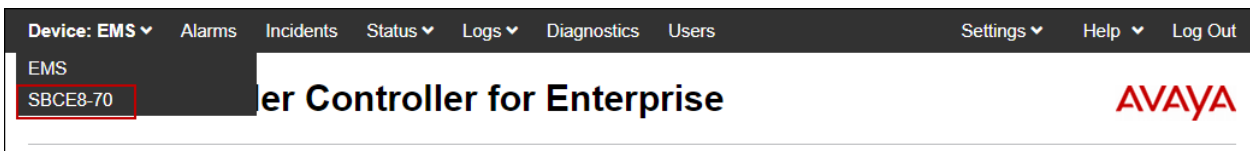
7.2. TLS Management

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.

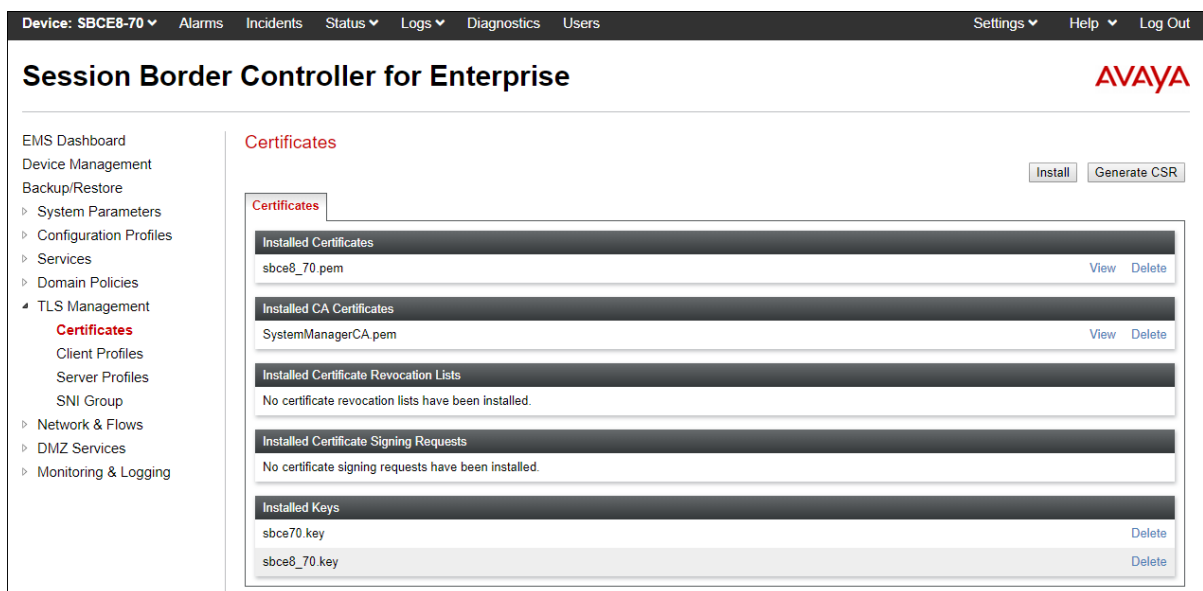
7.2.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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 contains a warning message at the top: "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 includes 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 shows the 'Server Profiles' section. The profile 'sbce8_70Server' is selected. The 'Server Profile' details are as follows: 'Profile Name' is sbce8_70Server, 'Certificate' is sbce8_70.pem, and 'SNI Options' is None. Under 'Certificate Verification', 'Peer Verification' is None, 'Extended Hostname Verification' is unchecked, and 'Verification Depth' is 0. Under 'Renegotiation Parameters', 'Renegotiation Time' and 'Renegotiation Byte Count' are both 0. Under 'Handshake Options', 'Version' is set to TLS 1.2, 'Ciphers' is set to Default, and the 'Value' is HIGH:IDH:ADH:IMD5:1aNULL:1eNULL:@STRENGTH. An 'Edit' button is at the bottom right.

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. It includes a warning about OpenSSL cipher checking, a 'TLS Profile' section with fields for Profile Name (sbce8_70Client), Certificate (sbce8_70.pem), and SNI (Enabled). The 'Certificate Verification' section shows Peer Verification set to Required, Peer Certificate Authorities set to SystemManagerCA.pem, Peer Certificate Revocation Lists as empty, Verification Depth set to 1, and Extended Hostname Verification as disabled. A 'Server Hostname' field is also present. A 'Next' button is at the bottom.

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

The 'Session Border Controller for Enterprise' interface displays the 'Client Profiles' section. A list of profiles shows 'sbce8_70Client' as the selected profile. The 'Client Profile' details are shown on the right, including the TLS Profile configuration (Profile Name: sbce8_70Client, Certificate: sbce8_70.pem, SNI: Enabled), Certificate Verification (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 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**.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Network Management' section active. The 'Interfaces' tab is selected, displaying a table of network interfaces. The table has three columns: 'Interface Name', 'VLAN Tag', and 'Status'. The interfaces listed are A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Enabled). There is an 'Add VLAN' button in the top right corner of the table area.

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

Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. The following Avaya SBCE IP addresses and associated interfaces were used in the sample configuration:

- **A1: 10.64.91.41** – IPv4 address configured for AT&T IPTF toward Session Manager.
- **B1: 3ffe:ffff:bb:bb::241** – IPv6 address configured for the AT&T IPTF service. This address is known to AT&T. See **Section 3**.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Network Management' section active. The 'Networks' tab is selected, displaying a table of network configurations. The table has five columns: 'Name', 'Gateway', 'Subnet Mask / Prefix Length', 'Interface', and 'IP Address'. The configurations listed are Inside-A1, Outside-B1, Outside-B1-IPv6, and Outside-B2. Each row has 'Edit' and 'Delete' links. There is an 'Add' button in the top right corner of the table area.

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
Outside-B1	10.64.91.1	255.255.255.0	B1	10.64.91.41
Outside-B1-IPv6	3ffe:ffff:bb:bb::1	64	B1	3ffe:ffff:bb:bb::241
Outside-B2	10.64.91.1	255.255.255.0	B2	10.64.91.41

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 features several tabs: Periodic Statistics, Feature Control, SIP Options, Network Options, Port Ranges (which is selected), RTP Monitoring, and Load Monitoring. A warning banner 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 contains four rows of input fields: '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.

7.5. Media Interfaces

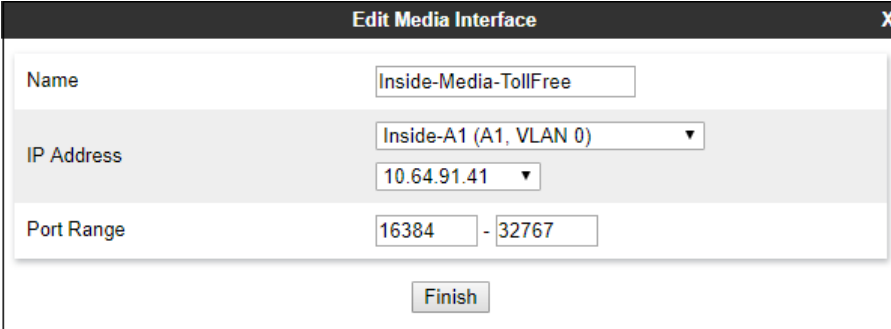
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Note that 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.

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-Media-TollFree**
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.41**
- **Port Range:** **16384 – 32767**

Step 3 - Click **Finish**.



The screenshot shows the 'Edit Media Interface' window with the following configuration:

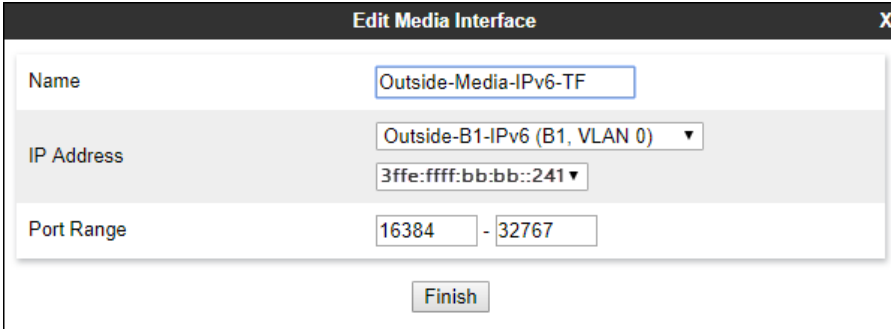
Field	Value
Name	Inside-Media-TollFree
IP Address	Inside-A1 (A1, VLAN 0) 10.64.91.41
Port Range	16384 - 32767

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

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

- **Name:** **Outside-Media-IPv6-TF**
- **IP Address:** Select **Outside-B1 (B1, VLAN0)** and **33fe:fff:bb:bb::241**
- **Port Range:** **16384 – 32767**

Step 5 - Click **Finish**



The screenshot shows the 'Edit Media Interface' window with the following configuration:

Field	Value
Name	Outside-Media-IPv6-TF
IP Address	Outside-B1-IPv6 (B1, VLAN 0) 3ffe:ffff:bb:bb::241
Port Range	16384 - 32767

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

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-Sig-TollFree-41
- **IP Address:** Select **Inside-A1 (A1, VLAN0)** and **10.64.91.41**
- **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' window. The 'Name' field is 'Inside-Sig-TollFree-41'. The 'IP Address' dropdown is set to 'Inside-A1 (A1, VLAN 0)' and the 'IP Address' text field shows '10.64.91.41'. The 'TCP Port' field is empty with the hint 'Leave blank to disable'. The 'UDP Port' field is empty with the hint 'Leave blank to disable'. The 'TLS Port' field is '5061' with the hint 'Leave blank to disable'. The 'TLS Profile' dropdown is set to 'sbce8_70Server'. The 'Enable Shared Control' checkbox is unchecked. The 'Shared Control Port' field is empty. A 'Finish' button is at the bottom right.

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

- **Name:** Outside-Signaling-IPv6-TF
- **IP Address:** Select **Outside-B1 (B1, VLAN0)** and **33fe:fff:bb:bb::241**
- **UDP Port:** 5060. Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' window. The 'Name' field is 'Outside-Signaling-IPv6-TF'. The 'IP Address' dropdown is set to 'Outside-B1-IPv6 (B1, VLAN 0)' and the 'IP Address' text field shows '33fe:fff:bb:bb::241'. The 'TCP Port' field is empty with the hint 'Leave blank to disable'. The 'UDP Port' field is '5060' with the hint 'Leave blank to disable'. The 'TLS Port' field is empty with the hint 'Leave blank to disable'. The 'TLS Profile' dropdown is set to 'None'. The 'Enable Shared Control' checkbox is unchecked. The 'Shared Control Port' field is empty. A 'Finish' button is at the bottom right.

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 IPTF service.

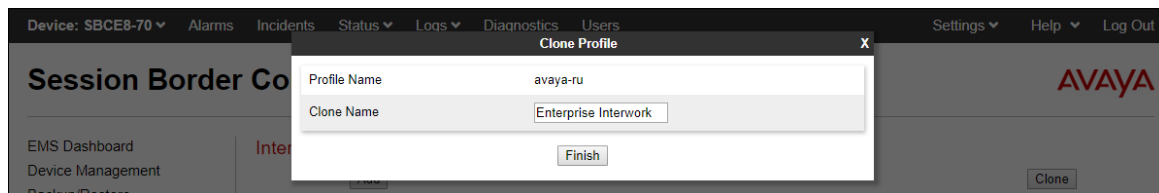
7.7.1. Server Interworking Profile – Enterprise

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.

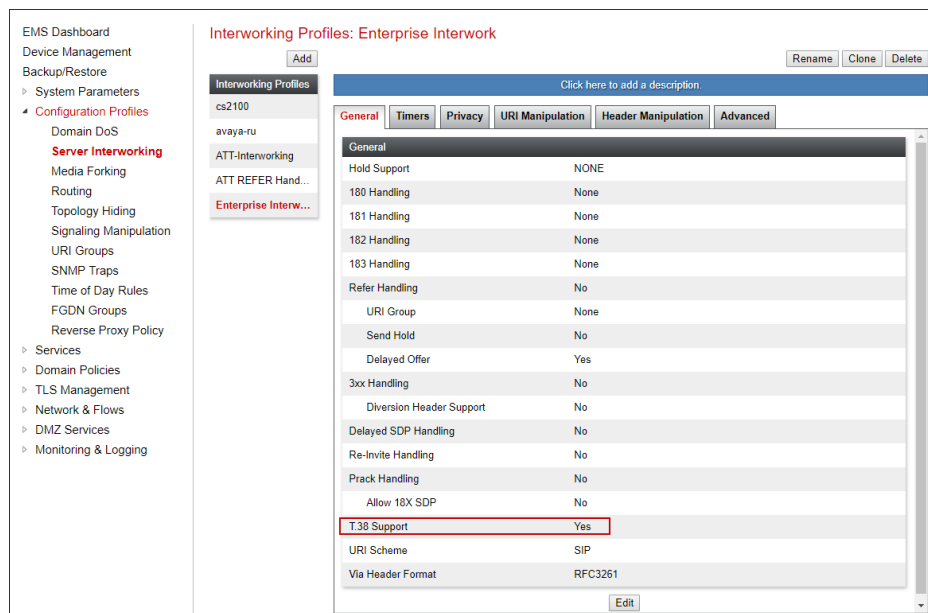
Step 3 - Enter profile name: (e.g., **Enterprise Interwork**), and click **Finish** to continue.



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.

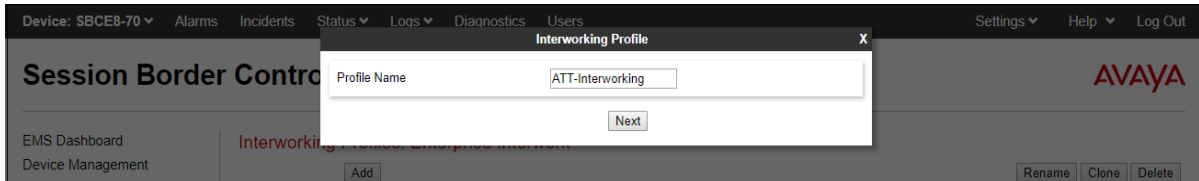
- Check **T38 Support**.
- All other options can be left with default values. Click **Finish** (not shown).



7.7.2. Server Interworking – AT&T

Repeat the steps shown in **Section 7.7.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

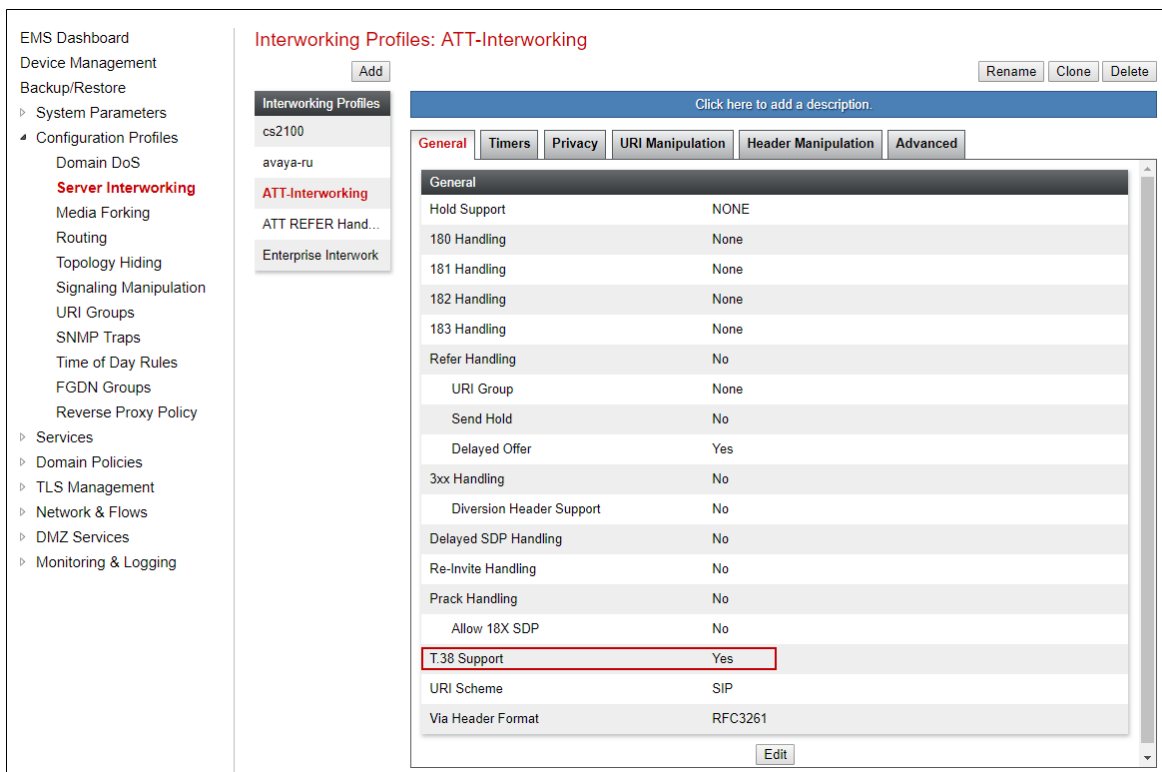
Step 1 - Select **Add Profile** and enter a profile name: (e.g., **ATT-Interworking**) and click **Next**.



The screenshot shows the 'Session Border Controller' configuration page. A modal dialog titled 'Interworking Profile' is open, with a text input field for 'Profile Name' containing 'ATT-Interworking' and a 'Next' button. The background interface includes a top navigation bar with 'Device: SBCE8-70', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar shows 'EMS Dashboard' and 'Device Management'. The main area has a header 'Session Border Control' and a sub-header 'Interworking Profiles'. Below the dialog, there are buttons for 'Add', 'Rename', 'Clone', and 'Delete'.

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

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



The screenshot displays the 'Interworking Profiles: ATT-Interworking' configuration page. The left sidebar contains a tree view with categories like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The 'Server Interworking' category is expanded, showing 'Domain DoS', 'Media Forking', 'Routing', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', and 'Reverse Proxy Policy'. The main area shows the 'Interworking Profiles' list with 'ATT-Interworking' selected. The 'General' tab is active, displaying a table of settings. The 'T.38 Support' setting is highlighted with a red box and set to 'Yes'.

Setting	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
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Step 3 – On the **Timers** tab, the **Trans Expire** timer is set to the allotted time the Avaya SBCE will try the first primary server before trying the secondary server, if one exists.

The screenshot shows the 'Interworking Profiles: ATT-Interworking' configuration page. On the left, a sidebar lists 'Interworking Profiles' with options: 'cs2100', 'avaya-ru', 'ATT-Interworking' (highlighted in red), 'ATT REFER Handl...', and 'Enterprise Interwork'. The main area has tabs for 'General', 'Timers' (active), 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. Below the tabs is a table titled 'SIP Timers' with the following data:

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	4 seconds
Invite Expire	---
Retry After	---

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

Step 4 - Click **Next** to accept default parameters for the **Privacy**, **URI Manipulation**, and **Header Manipulation** tabs (not shown).

Step 5 – 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).

The screenshot shows the 'Interworking Profiles: ATT-Interworking' configuration page with the 'Advanced' tab selected. The sidebar is the same as in Step 3. The main area has tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (active). Below the tabs is a table with the following data:

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

Below this table is a section titled 'DTMF' with a single row:

DTMF	
DTMF Support	None

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

7.8. Signaling Manipulation

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

Note – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Server Interworking Profiles (**Section 7.7**) or Signaling Rules (**Section 7.14**) do not meet the desired result. Refer to References [11] for information on the Avaya SBCE scripting language.


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

- Remove the gsid and epv parameters from outbound Contact headers. (**Section 2.2, Item 8**).
- Remove the Bandwidth headers sent by some Avaya SIP endpoints. (**Section 2.2, Item 9**).

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 IPTF-CM**).



Step 3 - Copy and paste the script below in the editor window.

```
-----
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", "");

    }
}
-----
```

Step 4 - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the AT&T SIP Server profile in **Section 7.9.2**.

7.9. SIP Server Profiles

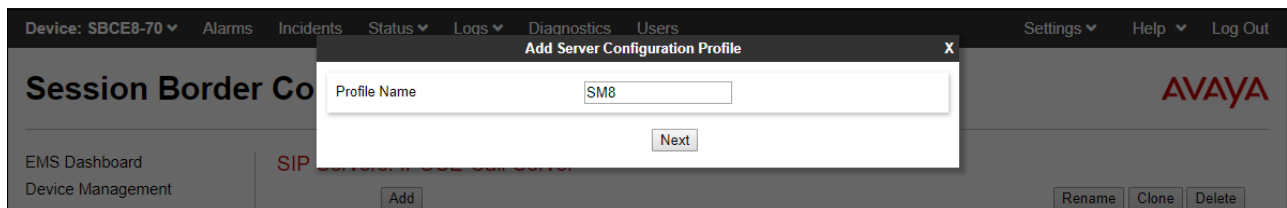
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

7.9.1. SIP Server Profile – Session Manager

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

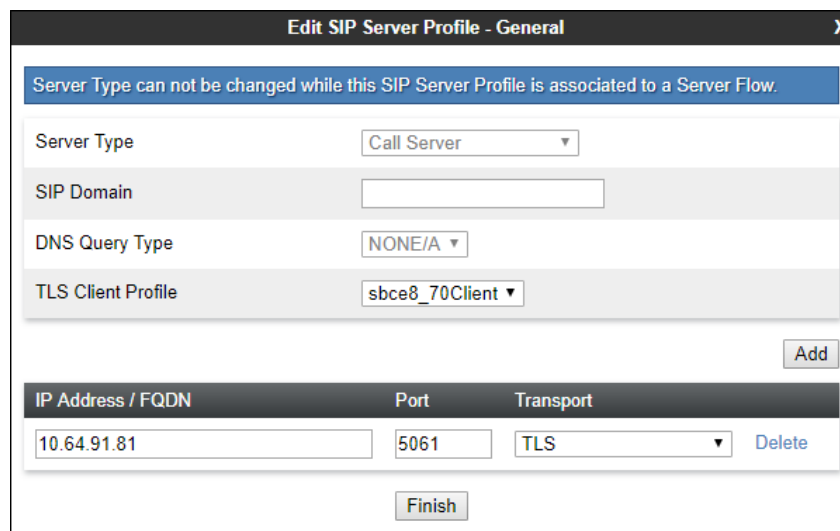
Step 1 - Select **Services** → **SIP Servers** from the left-hand menu.

Step 2 - Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM8**) 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**: **10.64.91.81** (Session Manager Security Module IP 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
10.64.91.81	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	sm@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.
- In the **Signaling Manipulation Script** field select **none**.
- 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 type="checkbox"/>
URI Group	None

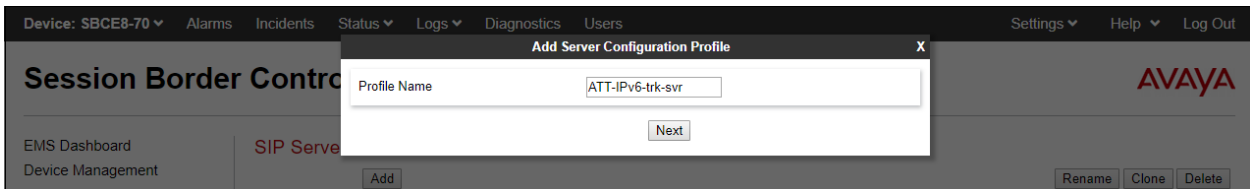
A 'Finish' button is located at the bottom right of the form.

7.9.2. SIP Server Profile – AT&T

Note – The AT&T IPTF service may provide a Primary and Secondary Border Element. This section describes the connection to a single (Primary) Border Element.

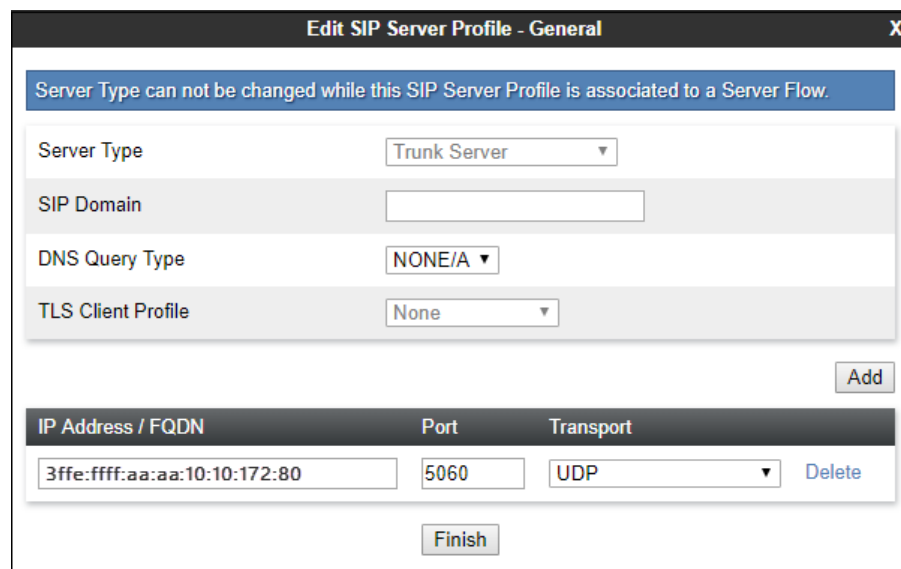
Repeat the steps in **Section 7.9.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to AT&T.

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.

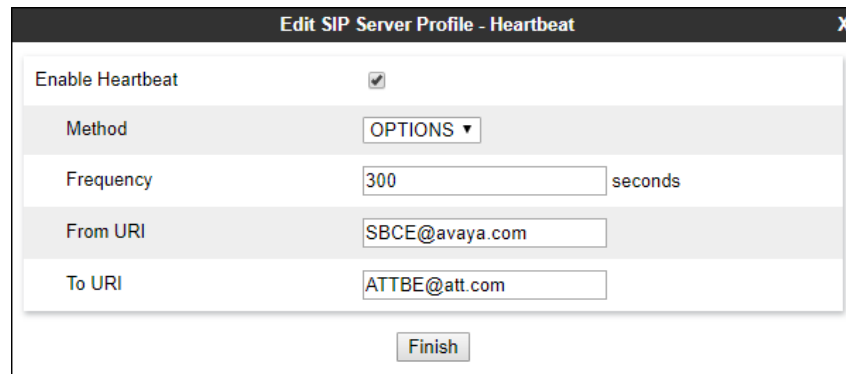
- Select **Server Type: Trunk Server**
- **IP Address/FQDN: 3ffe:ffff:aa:aa:10:10:172:80** (AT&T Border Element IPv6 address)
- **Port: 5060**
- Select **Transport: UDP**
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



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.

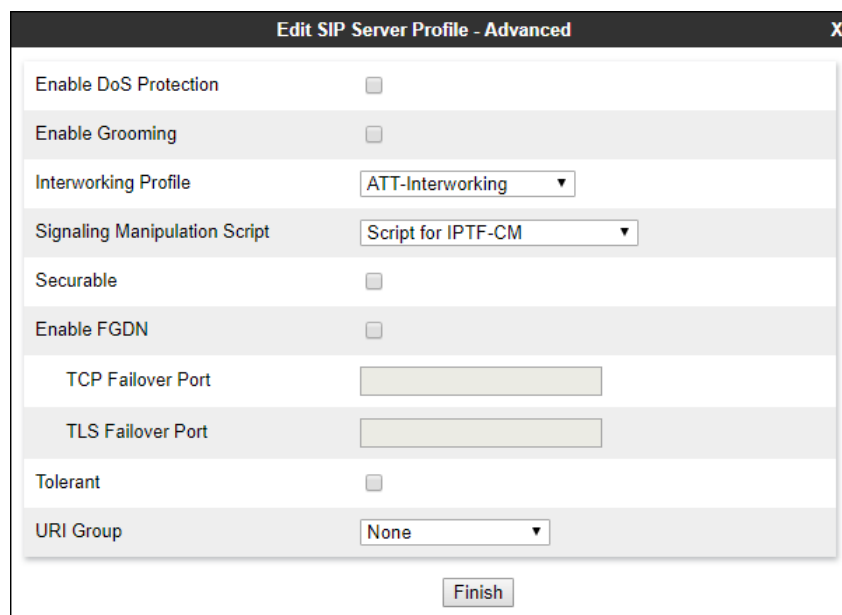
- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward AT&T.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.



Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▼
Frequency	300 seconds
From URI	SBCE@avaya.com
To URI	ATTBE@att.com
<button>Finish</button>	

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 7.7.2**), for **Interworking Profile**.
- Select the **Script for IPTF-CM** (created in **Section 7.8**) for **Signaling Manipulation Script**.
- Select **Finish**



Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT-Interworking ▼
Signaling Manipulation Script	Script for IPTF-CM ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None ▼
<button>Finish</button>	

7.10. Routing Profiles

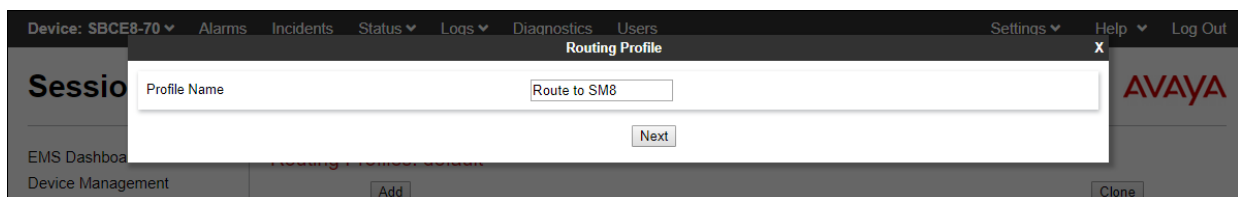
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and determine which security features will be applied to those packets. Parameters defined by Routing Profiles include load balancing, packet transport settings, name server addresses and resolution methods and next hop routing information. 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**.

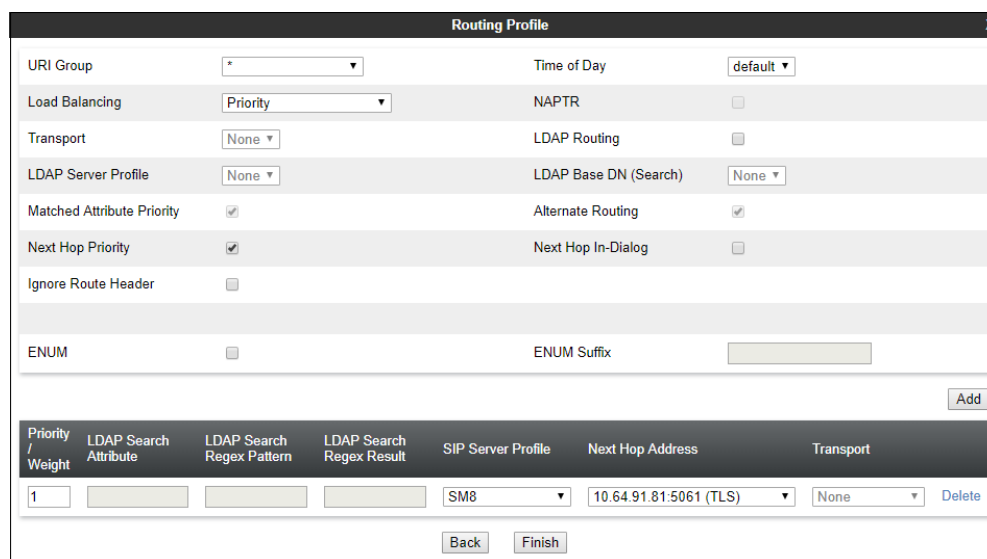
Step 2 - Enter a **Profile Name**: (e.g., **Route to SM8**) and click **Next**.

The screenshot shows the 'Routing Profile' configuration window. At the top, there's a navigation bar with 'Device: SBCE8-70' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main area has a 'Session Manager' sidebar on the left. The central form has a 'Profile Name' field containing 'Route to SM8' and a 'Next' button. The bottom of the window shows 'EMS Dashboard' and 'Device Management' sections with 'Add' and 'Clone' buttons respectively. The Avaya logo is in the top right corner.

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** (from **Section 7.9.1**).
- **Next Hop Address:** Verify that the **10.64.91.81:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out. Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window with various settings. The 'URI Group' is set to '*'. 'Time of Day' is 'default'. 'Load Balancing' is 'Priority'. 'Transport' is 'None'. 'LDAP Server Profile' is 'None'. 'LDAP Base DN (Search)' is 'None'. 'Matched Attribute Priority' is checked. 'Alternate Routing' is checked. 'Next Hop Priority' is checked. 'Next Hop In-Dialog' is unchecked. 'Ignore Route Header' is unchecked. 'ENUM' is unchecked. 'ENUM Suffix' is empty. The 'Add' button is at the bottom right. Below the main form is a table with columns: 'Priority / Weight', 'LDAP Search Attribute', 'LDAP Search Regex Pattern', 'LDAP Search Regex Result', 'SIP Server Profile', 'Next Hop Address', and 'Transport'. The first row has values: '1', empty, empty, empty, 'SM8', '10.64.91.81:5061 (TLS)', and 'None'. The 'Delete' button is at the bottom right of the table. 'Back' and 'Finish' buttons are at the bottom of the window.

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 7.9.2).**
- **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	Delete
1				ATT-IPv6-trk-svr	[3ffe:ffff:aa:aa:10:10:172:80]:5	None	Delete

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.

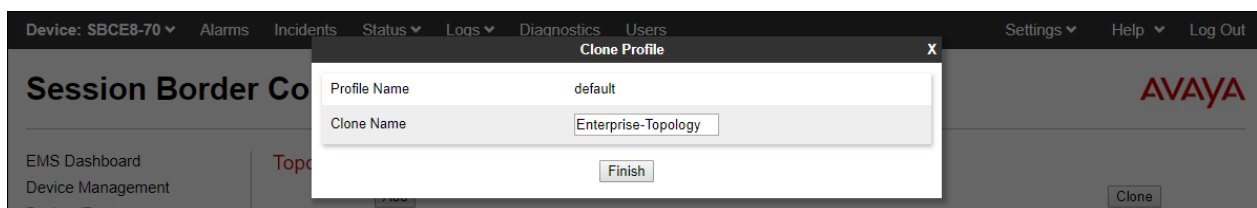
7.11.1. Topology Hiding – Enterprise Side

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 Side

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 media encryption and QoS parameters. Separate media rules are created for the enterprise and AT&T.

7.13.1. Enterprise – Media Rule

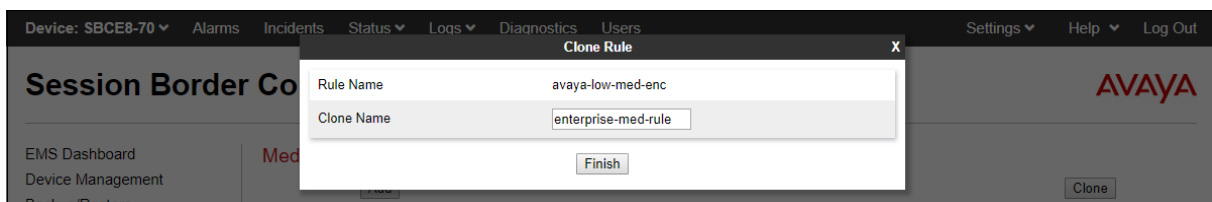
In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

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., **enterprise-med-rule**)
- Click **Finish**. The newly created rule will be displayed.



Step 4 - On the **enterprise med 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**.

Step 5 - Click **Finish**.

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	2h
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	2h
Interworking	<input checked="" type="checkbox"/>

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

The completed **enterprise-med-rule** 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: enterprise-med-rule

Add

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- att-med-rule
- enterprise-med-rule**

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input 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
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

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

Edit

MAA: Reviewed
SPOC 3/22/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

80 of 99
Au81SBCE8IP6-TF

7.13.2. AT&T – Media Rule

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**)

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

The screenshot shows the 'Media Rules: att-med-rule' configuration page. 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 (highlighted), Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, TLS Management, Network & Flows, and DMZ Services. The main content area has a title 'Media Rules: att-med-rule' and an 'Add' button. Below the title is a list of media rules: default-low-med, default-low-med-enc, default-high, default-high-enc, avaya-low-med-enc, att-med-rule (highlighted), and enterprise-med-rule. The configuration area for 'att-med-rule' has tabs for Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing sections for Audio Encryption, Video Encryption, and Miscellaneous. Audio Encryption has Preferred Formats set to RTP and Interworking checked. Video Encryption also has Preferred Formats set to RTP and Interworking checked. Miscellaneous has Capability Negotiation unchecked. There are 'Rename', 'Clone', and 'Delete' buttons at the top right, and an 'Edit' button at the bottom right.

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

This screenshot shows the 'QoS' tab of the 'Media Rules: att-med-rule' configuration page. The 'QoS' tab is active, showing sections for Media QoS Marking, Audio QoS, and Video QoS. Media QoS Marking has 'Enabled' checked and 'QoS Type' set to DSCP. Audio QoS has 'Audio DSCP' set to EF. Video QoS has 'Video DSCP' set to EF. The 'Edit' button is at the bottom right. The left navigation menu is the same as in the previous screenshot.

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. Below this is a list of signaling rules: 'default', 'No-Content-Type-Ch...', 'att-sig-rule', 'enterprise-sig-rule' (selected), and 'ATT-TF-408-test-sig'. The configuration for 'enterprise-sig-rule' is shown 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'. There is also a 'Content-Type Policy' section with 'Enable Content-Type Checks' checked and 'Action' set to 'Allow'. An 'Exception List' is also present.

7.14.2. Signaling Rule – AT&T

Signaling rule **att sig rule** was also cloned from the default rule and used for AT&T. The DSCP value **AF41** for assured forwarding (default value) was set for **Signaling QoS**. See **Section 2.2, item 6** for current limitations.

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. Below this is a list of signaling rules: 'default', 'No-Content-Type-Ch...', 'att-sig-rule' (selected), 'enterprise-sig-rule', and 'ATT-TF-408-test-sig'. The configuration for 'att-sig-rule' is shown 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' value set to 'AF41'. An 'Exception List' is also present.

7.15. Endpoint Policy Groups

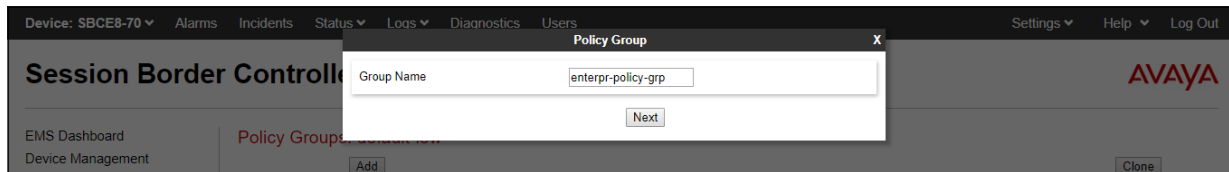
The rules created within the Domain Policies are assigned to an End Point Policy Group. The End Point Policy Group is then applied to a Server Flow in **Section 7.16**.

7.15.1. Endpoint 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-grp**)
- Click **Next**.

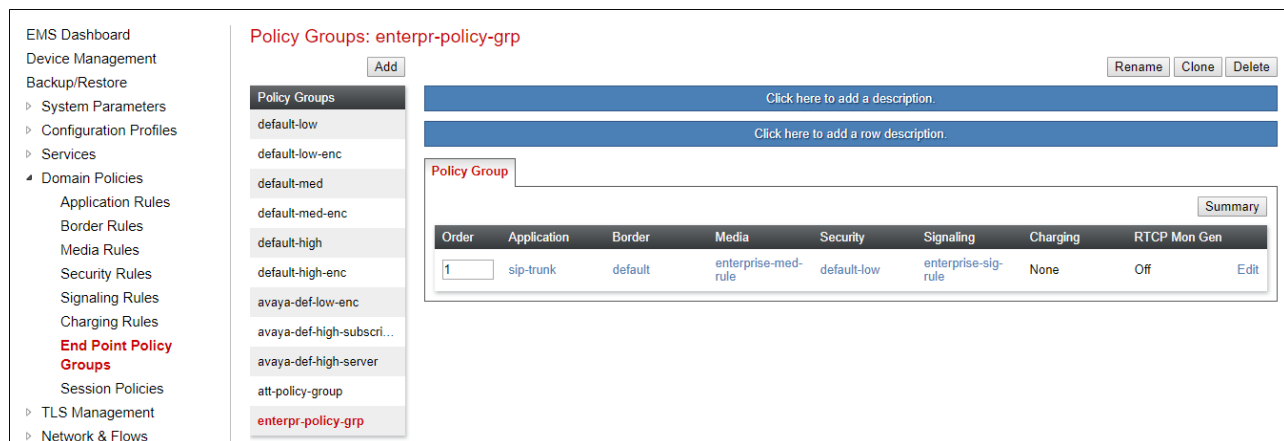


Step 3 – On the **Policy Group** window (not shown), select the following.

- **Application Rule:** sip-trunk (created in **Section 7.127.12**).
- **Border Rule:** default.
- **Media Rule:** enterprise-med-rule (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-grp** is shown on the screen below.



Policy Groups: enterpr-policy-grp

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

Click here to add a row description.

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

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. 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 with columns: Order, Application, Border, Media, Security, Signaling, Charging, and RTP Mon Gen. The table contains one row with the following values: 1, sip-trunk, default, att-med-rule, default-low, att-sig-rule, None, and Off. There are also buttons for 'Rename', 'Clone', and 'Delete' at the top right of the main area.

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 IPTF 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 Flow Toll Free IPv6**
- **Server Configuration:** **SM8** (Section 7.9.1).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** **Outside-Signaling-IPv6-TF** (Section 7.6).
- **Signaling Interface:** **Inside-Sig-TollFree-41** (Section 7.6).
- **Media Interface:** **Inside-Media-TollFree** (Section 7.5).

- **End Point Policy Group:** enterpr-policy-grp (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: SM Flow Toll Free IPv6	
Criteria	
Flow Name	SM Flow Toll Free IPv6
Server Configuration	SM8
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-Signaling-IPv6-TF
Profile	
Signaling Interface	Inside-Sig-TollFree-41
Media Interface	Inside-Media-TollFree
Secondary Media Interface	None
End Point Policy Group	enterpr-policy-grp
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"/>

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-IPv6 Toll Free Flow**.
- **Server Configuration:** ATT-IPv6-trk-svr (Section 7.9.2).
- **Received Interface:** Inside-Sig-TollFree-41 (Section Error! Reference source not found.).
- **Signaling Interface:** Outside-Signaling-IPv6-TF (Section Error! Reference source not found.).
- **Media Interface:** Outside-Media-IPv6-TF (Section Error! Reference source not found.).
- **End Point Policy Group:** att-policy-group (Section 7.15.2).
- **Routing Profile:** Route to SM8 (Section 7.10.1).
- **Topology Hiding Profile:** SIP-Trunk-Topology (Section 7.11.2).

View Flow: ATT-IPv6 Toll Free Flow

X

Criteria

Flow Name	ATT-IPv6 Toll Free Flow
Server Configuration	ATT-IPv6-trk-svr
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-Sig-TollFree-41

Profile

Signaling Interface	Outside-Signaling-IPv6-TF
Media Interface	Outside-Media-IPv6-TF
Secondary Media Interface	None
End Point Policy Group	att-policy-group
Routing Profile	Route to SM8
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 Toll Free Service Configuration

AT&T provides the IPTF service border element IP address, the access DID numbers, and the associated DNIS digits used in the reference configuration. In addition, the AT&T IPTF features, and their associated access numbers, are also assigned by AT&T. AT&T requires that the Avaya SBCE public (B1) IP address be provided to the IPTF service, as part of the provisioning process. For more information, consult reference [13].

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. AT&T IP Toll Free Service

The following scenarios may be executed to verify functionality with the AT&T IPTF service:

1. Place an inbound call, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.
4. Using the appropriate IPTF access numbers and DTMF codes, verify that the following IPTF features are successful:
 - a. Legacy Transfer Connect DTMF triggered Agent Hold, Conference and Transfer capabilities
 - b. Alternate Destination Routing call redirection capabilities based on Busy, Ring-No-Answer, and other SIP error codes.
5. Inbound fax using T.38 or G.711. See **Section 2.2** for limitations.
6. SIP OPTIONS monitoring of the health of the SIP trunk.

9.2. Avaya Aura® Communication Manager Verification

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

- Tracing a SIP trunk.
 1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., *04). Note that in the trace shown below, Session Manager has previously converted the IPTF DNIS number included in the Request URI, to the Communication Manager VDN 71025, before sending the INVITE to Communication Manager.

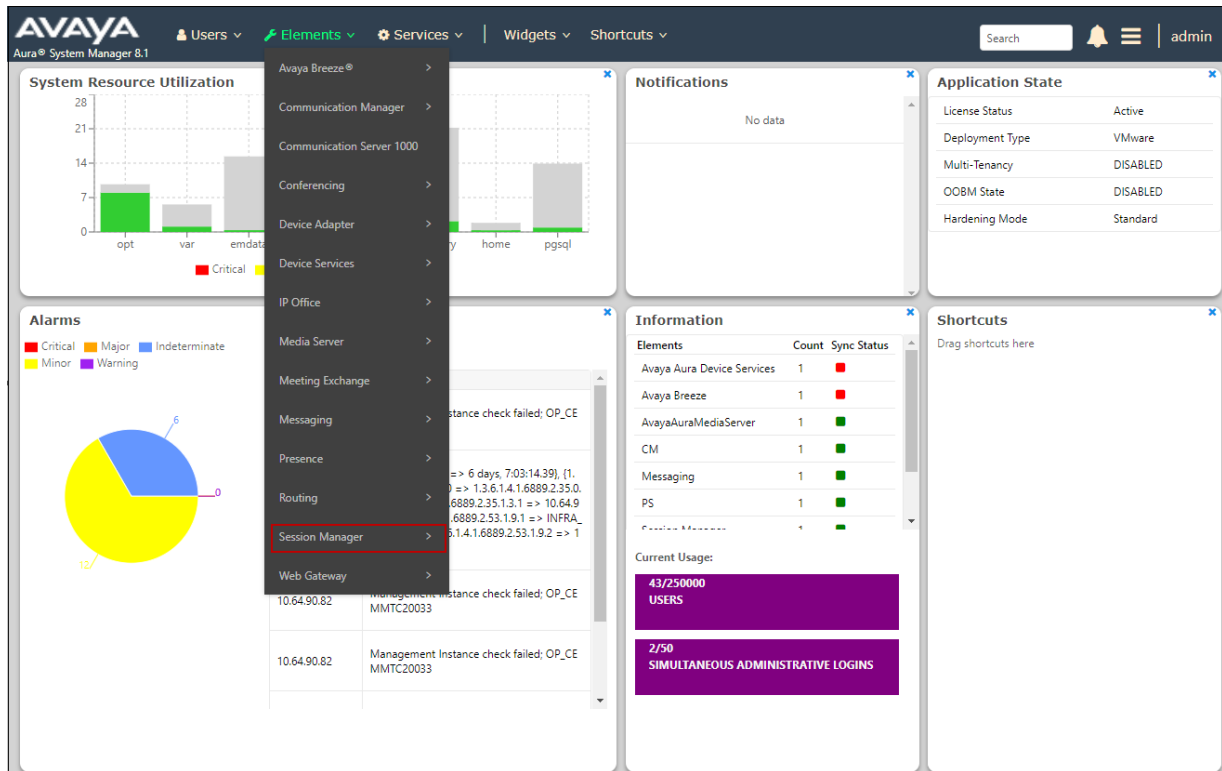
```
list trace tac *04                                     Page 1
LIST TRACE
time          data
13:35:53 TRACE STARTED 11/06/2019 CM Release String cold-01.0.890.0-25763
13:36:04 SIP<INVITE sips:71025@avayalab.com SIP/2.0
13:36:04      Call-ID: 31ebc87eee7ec97b24e184164efeeae18
13:36:04      active trunk-group 4 member 1      cid 0xf6b
13:36:04      0 0 ENTERING TRACE cid 3947
13:36:04      4 1 vdn e71025 bsr appl 0 strategy 1st-found override n
13:36:04      4 1 AVDN: 71025 AVRDN:
13:36:04      4 1 # Wait hearing ringback...
13:36:04      4 2 wait 2 secs hearing ringback
13:36:04 SIP>SIP/2.0 180 Ringing
13:36:04      Call-ID: 31ebc87eee7ec97b24e184164efeeae18
13:36:04      dial 71025
13:36:04      ring vector 4      cid 0xf6b
13:36:04      G729 ss:off ps:20
13:36:04      rgn:4 [10.64.91.41]:16924
13:36:04      rgn:1 [10.64.91.91]:16394
13:36:04      xoip options: fax:T38 modem:off tty:US uid:0x50001f
13:36:04      xoip ip: [10.64.91.91]:16394
13:36:06      4 3 # Play greeting and collect 1 d...
13:36:06      4 4 collect 1 digits after annnc 11001 for none
13:36:06 SIP>SIP/2.0 200 OK
```

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

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. Verify that the **Tests Pass**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status.

The screenshot shows the Session Manager Dashboard. The dashboard displays the overall status and health summary of each administered Session Manager. The 'Session Manager Instances' table is shown, with columns for 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, and Version. The 'Session Manager' instance is highlighted, showing 'Tests Pass' as 'Up', 'Alarms' as '0/0/0', 'Service State' as 'Accept New Service', and 'Data Replication' as 'Green'.

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
Session Manager	Core	Up	0/0/0	Up	Accept New Service	2/15	0	2/2	Green	Green	Normal	Enabled	8.1.1.0.811021

In the example, the entry **2/15** under the **Entity Monitoring** column shows that there are alarms on 2 out of the 15 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

15 Items Filter: Enable

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	Aura Messaging	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Breeze	IPv4	10.64.91.18	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	CM-TG1	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG2	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG3	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG4	IPv4	10.64.91.75	5064	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG5	IPv4	10.64.91.75	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG7	IPv4	10.64.91.75	5067	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	ExperiencePortal	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Presence	IPv4	10.64.91.18	5061	TLS	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	SBC1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBC2	IPv4	10.64.91.100	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBC2-101	IPv4	10.64.91.101	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBCE-ATT	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
<input type="radio"/>	SBCE-Toll Free	IPv4	10.64.91.41	5061	TLS	FALSE	UP	405 Method Not Allowed	UP

Select : None

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

The screenshot shows the Avaya Session Border Controller for Enterprise dashboard. The top navigation bar includes links for Alarms, Incidents (highlighted), Status, Logs, Diagnostics, and Users. The main content area is divided into several sections: EMS Dashboard, Information, Installed Devices, Active Alarms (past 24 hours), and Incidents (past 24 hours). The Information section displays system details such as System Time, Version, Build Date, License State, and Aggregate Licensing Overages. The Installed Devices section lists the EMS and SBCE8-70. The Active Alarms section shows 'None found'. The Incidents section lists '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.

The screenshot shows the Avaya Incident Viewer interface. It includes a search bar with filters for Device (All) and Category (All), a Clear Filters button, and buttons for Refresh and Generate Report. Below the search bar, it indicates 'Displaying results 1 to 15 out of 2000'. The main table lists incidents with the following columns: ID, Device, Date & Time, Category, Type, and Cause. The table contains 10 rows of incident data.

ID	Device	Date & Time	Category	Type	Cause
791023071146010	SBCE8-70	Feb 18, 2020 10:15:42 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
790809156821219	SBCE8-70	Feb 13, 2020 11:25:13 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
790809040313698	SBCE8-70	Feb 13, 2020 11:21:20 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
790808739097947	SBCE8-70	Feb 13, 2020 11:11:18 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
790808739087889	SBCE8-70	Feb 13, 2020 11:11:18 AM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
790808706819505	SBCE8-70	Feb 13, 2020 11:10:13 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
790808706819273	SBCE8-70	Feb 13, 2020 11:10:13 AM	Policy	Server Heartbeat	Heartbeat Failed, Server is Down
790511920768118	SBCE8-70	Feb 6, 2020 2:17:21 PM	Protocol Discrepancy	BYE Message Out of Dialog	General Method not allowed Out-Of-Dialog
790511625763287	SBCE8-70	Feb 6, 2020 2:07:31 PM	Protocol Discrepancy	BYE Message Out of Dialog	General Method not allowed Out-Of-Dialog

9.4.2. Server Status

The **Server Status** screen 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 interface. The top navigation bar includes "Device: SBCE8-70", "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". The left sidebar shows the "Session Border Controller Enterprise" menu with options like "SIP Statistics", "Periodic Statistics", "User Registrations", and "Server Status". The main content area displays the "Server Status" dashboard. It includes a "Dashboard" section with "Information" and "Installed Devices". The "Information" section shows system time, version, build date, license state, and aggregate licensing overages. The "Installed Devices" section shows the EMS and SBCE8-70.

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 7.9**.

The screenshot shows the "Status" screen with the "Server Status" tab selected. The table below lists the server profiles and their status.

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	12/16/2019 08:00:20 MST
IPOSE-Call-Server	10.64.19.170	10.64.19.170	5061	TLS	UP	UNKNOWN	12/16/2019 08:00:52 MST
ATT-TollFree-trk-svr	10.64.19.170	10.64.19.170	5060	UDP	UP	UNKNOWN	12/16/2019 07:57:10 MST
ATT-IPv6-trk-svr	10.64.19.170	10.64.19.170	5060	UDP	UP	UNKNOWN	12/16/2019 07:59:11 MST
ATT-trk-svr	10.64.19.170	10.64.19.170	5060	UDP	UP	UNKNOWN	12/16/2019 08:00:56 MST
ATT-trk-svr	10.64.19.170	10.64.19.170	5060	UDP	UP	UNKNOWN	12/16/2019 08:00:56 MST

9.4.3. Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces. 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.

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**

Packet Capture Configuration

Status	Ready
Interface	Any ▾
Local Address <small>[IP:Port]</small>	All ▾ : <input type="text"/>
Remote Address <small>*: *Port, IP, IP:Port</small>	<input type="text"/>
Protocol	All ▾
Maximum Number of Packets to Capture	<input type="text" value="10000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input type="text" value="test1.pcap"/>

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

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 ▾ : <input type="text"/>
Remote Address <small>*: *Port, IP, IP:Port</small>	<input type="text"/>
Protocol	All ▾
Maximum Number of Packets to Capture	<input type="text" value="10000"/>
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	<input type="text" value="test1.pcap"/>

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. On the left is a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging (which includes SNMP, Syslog Management, Debugging, and Trace). The main area is titled 'Trace: SBCE8-70' and contains two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active, showing a table with one entry: 'test1_20190724082944.pcap' with a file size of 696,320 bytes and a last modified date of July 24, 2019 8:30:26 AM MDT. A 'Delete' link is next to the file name. A 'Refresh' button is in the top right of the table area.

File Name	File Size (bytes)	Last Modified
test1_20190724082944.pcap	696,320	July 24, 2019 8:30:26 AM MDT

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 8.0.1, can be configured to interoperate successfully with the AT&T IP Toll Free service using IPv6, within the constraints described in **Section 2.2**.

Testing was performed on a simulated AT&T IP Toll Free 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 2, December 2019
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1.1, Issue 2, October 2019
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 4, October 2019
- [4] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 4, October 2019

Avaya Aura® Communication Manager

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 3, October 2019
- [6] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 5, November 2019
- [7] *Administering Avaya G430 Branch Gateway*, Release 8.1.x, Issue 2, October 2019
- [8] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.2, Issue 9, December 2019
- [9] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, Issue 1.1, June 2018
- [10] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya Session Border Controller for Enterprise

- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0.x, Issue 4, August 2019
- [12] *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*, Release 8.0.x, Issue 4, August 2019

AT&T IP Toll Free Service

- [13] *AT&T IP Toll Free Service – Product Description*
<https://www.business.att.com/products/ip-toll-free.html>

12. Appendix A – Configuration for G.711 Fax Testing

During the compliance test, in order to perform G.711 pass-through fax testing, the network region assigned to the G430 Media Gateway where the fax machine was connected was changed from region 1 (**Section 5.14**) to region 3. This network region utilized IP Codec Set 3 for calls between region 3 and region 4 (IPTF calls). Creating a dedicated network region and ip-codec-set for G.711 pass-through fax allowed for fax calls from this G430 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 5.7.2**).

This configuration is shown here for completeness and is only needed if G.711 pass-through is preferred to T.38 fax. See **Section 2.2** for limitations.

To create the IP Network Region 3 used for G.711 fax testing, repeat the steps in **Section 5.6.1** 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 4** of the form:

- Set codec set **3** for **dst rgn 4**.
- 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	M	
										G	A	
dst	codec	direct	WAN-BW-limits		Video	Intervening			Dyn	A	G	c
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	e
1	1	y	NoLimit							n		t
2	2	y	NoLimit							n		t
3	3										all	
4	3	y	NoLimit							n		t

Repeat the steps in **Section 5.7.1** 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**.

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)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	

©2020 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by TM and [®] are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect program at devconnect@avaya.com.