



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.2 with AT&T IP Toll Free SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager 7.1, Avaya Aura® Communication Manager 7.1, and the Avaya Session Border Controller for Enterprise 7.2 with the AT&T IP Toll Free service using AT&T's **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 7.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 7.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 7.2 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

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

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

TABLE OF CONTENTS

1	Introduction.....	5
2	General Test Approach and Test Results.....	5
2.1	Interoperability Compliance Testing.....	6
2.2	Test Results	6
2.3	Support	8
3	Reference Configuration	8
3.1	Illustrative Configuration Information	10
3.2	Call Flows	11
4	Equipment and Software Validated	12
5	Configure Avaya Aura® Session Manager	13
5.1	SIP Domain	14
5.2	Locations	15
5.2.1	Main Location	15
5.2.2	Common Location	16
5.3	Configure Adaptations	16
5.3.1	Adaptation for Avaya Aura® Communication Manager Extensions	17
5.3.2	Adaptation for the AT&T IP Toll Free Service	18
5.4	SIP Entities	19
5.4.1	Avaya Aura® Session Manager SIP Entity	19
5.4.2	Avaya Aura® Communication Manager SIP Entity – Public Trunk	20
5.4.3	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	22
5.4.4	Avaya Session Border Controller for Enterprise SIP Entity.....	23
5.5	Entity Links	24
5.5.1	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	24
5.5.2	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	25
5.5.3	Entity Link for the AT&T IP Toll Free Service via the Avaya SBCE	25
5.6	Time Ranges.....	26
5.7	Routing Policies	26
5.7.1	Routing Policy for AT&T Routing to Avaya Aura® Communication Manager	26
5.8	Dial Patterns	28
5.9	Verify TLS Certificates – Session Manager	29
6	Avaya Aura® Communication Manager	32
6.1	System-Parameters Customer-Options	32
6.2	System-Parameters Features	34
6.3	Dial Plan.....	34
6.4	IP Node Names.....	35
6.5	IP Interface for procr.....	35
6.6	IP Network Regions	35
6.6.1	IP Network Region 1 – Local CPE Region	36
6.6.2	IP Network Region 4 – SIP Trunk Region	38
6.7	IP Codec Parameters	38
6.7.1	Codecs for IP Network Region 1 (calls within the CPE)	39
6.7.2	Codecs for IP Network Region 4 (calls from AT&T)	40

6.7.3	Codecs for G.711 Pass-Through Fax	41
6.8	SIP Trunks.....	42
6.8.1	SIP Trunk for Inbound AT&T calls.....	42
6.8.2	Local SIP Trunk (Avaya SIP Telephone Access).....	45
6.9	Public Numbering	47
6.10	Private Numbering.....	48
6.11	Route Patterns for Local SIP Trunk	49
6.12	Automatic Alternate Routing (AAR) Dialing	49
6.13	Provisioning for Simulated Call Center Functionality	50
6.14	Avaya G450 Media Gateway Provisioning	52
6.15	Avaya Aura® Media Server Provisioning.....	53
6.16	Verify TLS Certificates – Communication Manager	54
6.17	Save Communication Manager Translations.....	55
7	Configure Avaya Session Border Controller for Enterprise	56
7.1	System Management – Status	57
7.2	TLS Management.....	58
7.2.1	Verify TLS Certificates – Avaya Session Border Controller for Enterprise	58
7.2.2	Server Profiles.....	59
7.2.3	Client Profiles	61
7.3	Global Profiles.....	62
7.3.1	Server Interworking – Avaya.....	62
7.3.2	Signaling Manipulation.....	65
7.3.3	Server Configuration – Session Manager	66
7.3.4	Server Configuration – AT&T.....	68
7.3.5	Routing – To Session Manager.....	69
7.3.6	Routing – To AT&T	69
7.3.7	Topology Hiding – Enterprise Side	70
7.3.8	Topology Hiding – AT&T Side.....	71
7.4	Domain Policies	72
7.4.1	Application Rules.....	72
7.4.2	Media Rules	73
7.4.3	Signaling Rules	74
7.4.4	Endpoint Policy Groups – Enterprise Connection	75
7.4.5	Endpoint Policy Groups – AT&T Connection.....	76
7.5	Device Specific Settings.....	77
7.5.1	Network Management.....	77
7.5.2	Advanced Options.....	78
7.5.3	Media Interfaces.....	79
7.5.4	Signaling Interface	80
7.5.5	Endpoint Flows – For Enterprise	81
7.5.6	Endpoint Flows – For AT&T.....	82
8	Verification Steps.....	83
8.1	AT&T IP Toll Free Service.....	83
8.2	Avaya Aura® Communication Manager	83

8.3	Avaya Aura® Session Manager Status	84
8.4	Avaya Session Border Controller for Enterprise Verification	86
8.4.1	Protocol Traces	86
9	Conclusion	88
10	References.....	89

1 Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager 7.1, Avaya Aura® Communication Manager 7.1, and the Avaya Session Border Controller for Enterprise 7.2 with the AT&T IP Toll Free service using AT&T Virtual Private Network (AVPN) or Managed Internet Service Private Network Transport (MIS/PNT) connections¹.

Avaya Aura® Session Manager 7.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 7.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 7.2 (Avaya SBCE) is the point of connection between Avaya Aura® Session Manager and the AT&T IP Toll Free service and is used to not only secure the SIP trunk, but also to adjust the SIP signaling for interoperability.

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.

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.

¹ MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does support cRTP.

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 and Alternate Destination Routing (ADR).
- Verify reception of IPTF SIP Multipart/NSS headers, including SDP and XML content.
- Long duration calls.

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 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, the Ring No Answer will be invoked.
2. **IP Toll Free ADR Call Redirection feature based on SIP error code response.** Upon receiving an error response, IPTF service can be configured to invoke ADR Call Redirection. The following error codes were producible by the reference configuration and tested successfully, 480 Temporarily Unavailable, 486 Busy Here, 503Service Unavailable, and 500 Server Internal Error. The following error codes are also supported by IPTF

service, but were not producible by the reference configuration, and thus not tested, 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 G450 Media Gateway is used in the reference configuration. As a result, T.38/G.729 fax was limited to 9600 bps. Also note that the sender and receiver of a T.38 fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3. Also note that inbound/outbound G.711 pass-through fax ran successfully at best line speed (rates of 14400 bps were observed).
5. **G.711 pass-through fax.** G.711 pass-through fax was tested in addition to T.38 fax. This was done by configuring a different Communication Manager **ip-codec-set** form (**Section 6.7.3**) to use **G.711 MU** codec as the first codec choice, and setting **Fax Mode** to **off**. The network region of the G450 Media Gateway hosting the fax machine was changed from the enterprise region, to one that utilized this ip-codec-set for IPTF service. Faxes using G.711 pass-through completed successfully during the test. It should be noted however, that 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.
6. **IP Toll Free service Landline/Mobility test cases could not be executed.** The AT&T supplied IP Toll Free test plan specifies test cases to verify the transmission of Landline/Mobility data by the IP Toll Free service. Due to network access issues, these test cases could not be executed.
7. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), Session Manager is provisioned to remove SIP headers not required by the AT&T IPTF service (see **Section 5.3.2**). These headers are:
 - AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, Av-Secure-Indication
8. **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues.** Certain Avaya SIP endpoints (e.g., 9641, 9621, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore, an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 7.3.2**).

9. **Enhanced CID – NSS feature.** The inbound calls to Communication Manager are not exercising the Enhanced CID feature. Although Communication Manager is accepting SIP Multipart/NSS headers, it is neither passing nor acting upon it. It is simply being ignored.
10. **The version of Communication Manager used during testing specified a ptime value of 20 in the SIP SDP when the codec set was configured for 30.** Although no issues were found during testing, AT&T recommends that for maximum customer bandwidth utilization, a ptime value of 30 milliseconds should be specified.

2.3 Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555.

Avaya customers may obtain documentation and support for Avaya products by visiting: <http://support.avaya.com>. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus. Customers may also use specific numbers (provided on <http://support.avaya.com>) 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 7.1 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 7.1 provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager 7.1 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 G450 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 desk telephones are represented with Avaya 96x1 Series IP Telephone (running H.323 firmware), a 96x1 Series IP Telephone (running SIP firmware), an Avaya 2420 Digital Telephone, as well as Avaya one-X® Agent soft phone (H323).
- The Avaya SBCE 7.2 provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPTF service and the enterprise internal network.

- Avaya Aura® Messaging was used in the reference configuration to provide voice mailbox capabilities. This solution is extensible to other Avaya messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- 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 and Communication Manager.
- Inbound calls were placed from the PSTN via the IPTF service, through the Avaya SBCE to the Session Manager, which routed the call to Communication Manager. Communication Manager terminated the calls to the appropriate Agent queue, Agent phone, or fax extension.

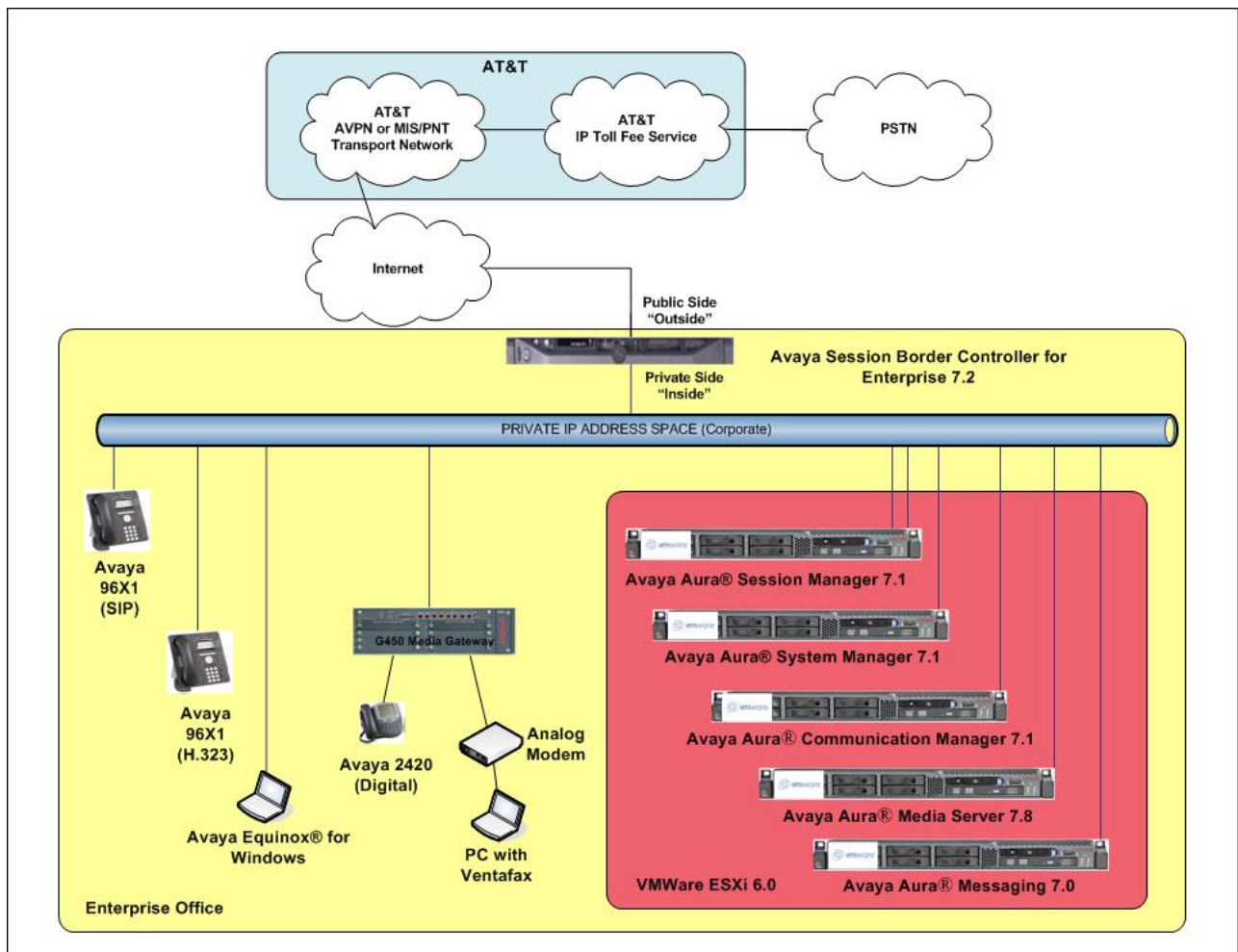


Figure 1: Reference configuration

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	10.64.90.12
Avaya Aura® Session Manager	
Management IP Address	10.64.90.11
Network IP Address	10.64.91.11
Avaya Aura® Communication Manager	
IP Address	10.64.91.65
Avaya Aura® Communication Manager extensions	14xxx = Stations 2xxxx = Agents 71xxx = Agent skill queue VDNs
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Inside (Private) Interface	10.64.91.41
IP Address of Outside (Public) Interface	192.168.80.43 (see note below)
AT&T IP Toll Free Border Element	
IP Address	192.168.225.210

Table 1: Illustrative Values Used in these Application Notes

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.

Note – For security reasons, the actual IP addresses of the Avaya SBCE and AT&T BE are not included in this document. However, as placeholders in the following configuration sections, the IP address of **192.168.80.43** (Avaya SBCE public interface) and **192.168.225.210** (AT&T BE IP address) are specified.

3.2 Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled by the Avaya SBCE, Session Manager and Communication Manager, 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.

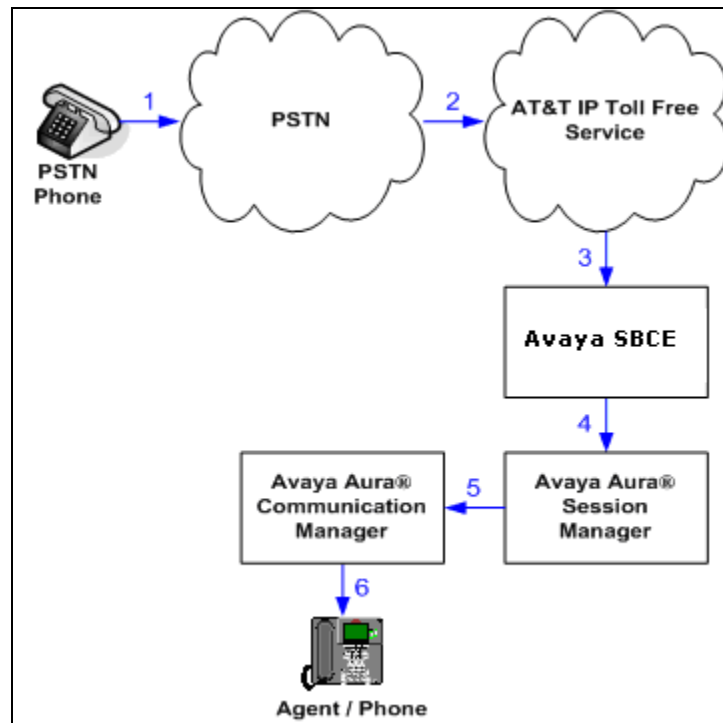


Figure 2: Inbound AT&T IP Toll Free Service Call to an Agent queue/telephone

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	<ul style="list-style-type: none">7.1.2.0.057353
Avaya Aura® Session Manager	<ul style="list-style-type: none">7.1.2.0.712004
Avaya Aura® Communication Manager	<ul style="list-style-type: none">7.1.2.0.0-R017x.01.0.532.0 (24182)
Avaya Aura® Media Server	<ul style="list-style-type: none">7.8.0.107.8.0.355
Avaya Aura® Messaging	<ul style="list-style-type: none">7.0-00.0.441.0-017_0004 (SP 0)
Avaya G450 Media Gateway	<ul style="list-style-type: none">38.21.0
Avaya Session Border Controller for Enterprise	<ul style="list-style-type: none">7.2.1.0-05-14222
Avaya 96x1 IP Telephones	<ul style="list-style-type: none">H.323 Version 6.6604SIP Version 7.1.1.0.9
Avaya one-X® Agent (H323)	<ul style="list-style-type: none">2.5.50022.65
Ventafax Home Version (Windows based Fax device)	<ul style="list-style-type: none">7.9.255.613

Table 2: Equipment and Software Versions

5 Configure Avaya Aura® Session Manager

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult documents [1] through [4] 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. In addition, provisioning for calls to Aura® Messaging are described.

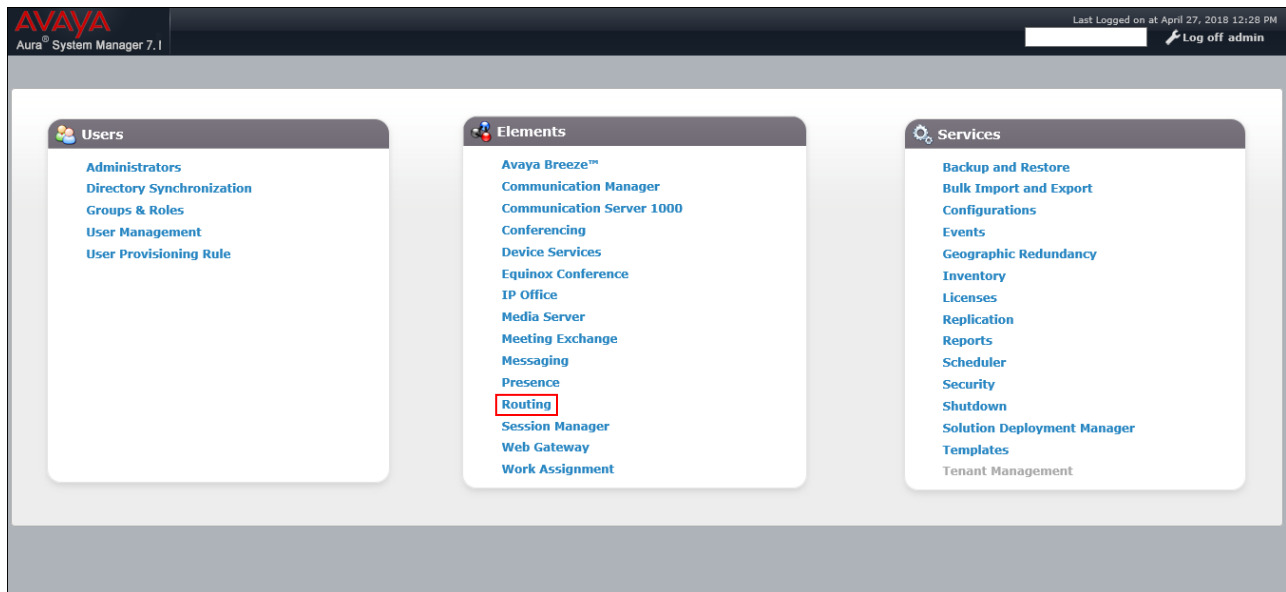
Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as 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 Locations
- Configure the Adaptation Modules that will be associated with digit manipulations for calls between the SIP Entities for Communication Manager, and the Avaya SBCE
- Define SIP Entities corresponding to Communication Manager, and the Avaya SBCE
- Define Entity Links describing the SIP trunk between Communication Manager and Session Manager, and the SIP Trunk between Session Manager and the Avaya SBCE
- Define Routing Policies associated with the Communication Manager, and the Avaya SBCE
- Define Dial Patterns, which govern which routing policy will be selected for call routing

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



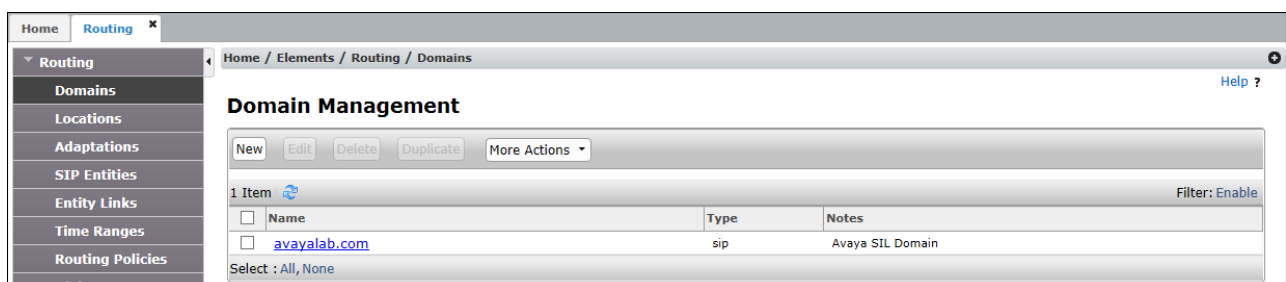
5.1 SIP Domain

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

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

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

Step 3 - Click **Commit** to save (not shown).



5.2 Locations

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

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager, the G450 Media Gateway, and telephones.
- **Common** – This site contains the Avaya SBCE.

5.2.1 Main Location

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

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

Step 2 - Click **Commit** to save.

The screenshot displays the 'Location Details' configuration page in the Avaya System Manager. The left-hand navigation pane shows the 'Locations' menu item selected under the 'Routing' category. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- Name:** Main
- Notes:** Avaya STL

The 'Dial Plan Transparency in Survivable Mode' section includes:

- Enabled:** ☐
- Listed Directory Number:** [Empty field]
- Associated CM SIP Entity:** [Empty field]

The 'Overall Managed Bandwidth' section includes:

- Managed Bandwidth Units:** Kbit/sec
- Total Bandwidth:** [Empty field]
- Multimedia Bandwidth:** [Empty field]
- Audio Calls Can Take Multimedia Bandwidth:** ☒

The 'Per-Call Bandwidth Parameters' section includes:

- Maximum Multimedia Bandwidth (Intra-Location):** 2000 Kbit/Sec
- Maximum Multimedia Bandwidth (Inter-Location):** 2000 Kbit/Sec
- * Minimum Multimedia Bandwidth:** 64 Kbit/Sec
- * Default Audio Bandwidth:** 80 Kbit/sec

The 'Alarm Threshold' section includes:

- Overall Alarm Threshold:** 80 %
- Multimedia Alarm Threshold:** 80 %
- * Latency before Overall Alarm Trigger:** 5 Minutes
- * Latency before Multimedia Alarm Trigger:** 5 Minutes

The 'Location Pattern' section includes:

- Add** button
- Remove** button
- 0 Items**
- Filter: Enable**
- IP Address Pattern** checkbox
- Notes** field

5.2.2 Common Location

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

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

The screenshot shows the 'Location Details' configuration page. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes a 'Commit' button. The 'General' section shows the 'Name' field set to 'Common' and the 'Notes' field set to 'SBC to PSTN'. 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', 'Multimedia Bandwidth', and a checked 'Audio Calls Can Take Multimedia Bandwidth' checkbox. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)' (2000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (2000 Kbit/Sec), 'Minimum Multimedia Bandwidth' (64 Kbit/Sec), and 'Default Audio Bandwidth' (80 Kbit/Sec). The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold' (80 %), 'Multimedia Alarm Threshold' (80 %), 'Latency before Overall Alarm Trigger' (5 Minutes), and 'Latency before Multimedia Alarm Trigger' (5 Minutes).

The screenshot shows the 'Location' list view. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, and Defaults. The main content area is titled 'Location' and includes a 'New' button, an 'Edit' button, a 'Delete' button, a 'Duplicate' button, and a 'More Actions' dropdown. Below the buttons is a table with 3 items. The table has columns for 'Name', 'Correlation', and 'Notes'. The 'Name' column contains the values 'Common', 'Main', and 'Main'. The 'Correlation' column contains the values 'SBC to PSTN' and 'Avaya SIL'. The 'Notes' column contains the values 'SBC to PSTN' and 'Avaya SIL'. The table is filtered by 'Filter: Enable'.

Name	Correlation	Notes
Common	SBC to PSTN	SBC to PSTN
Main	Avaya SIL	Avaya SIL

5.3 Configure Adaptations

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

- Calls from AT&T - Modification of SIP messages sent to Communication Manager extensions.
- 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.

5.3.1 Adaptation for Avaya Aura® Communication Manager Extensions

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:

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

Home / Elements / Routing / Adaptations

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

General

* Adaptation Name: CM-TG4-IPTF

* Module Name: DigitConversionAdapter

Module Parameter Type:

Egress URI Parameters:

Notes: CM - ATT - IPTF

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). 000001111171057 is a DNIS string sent in the Request URI by the IPTF service that is associated with Communication Manager Agent/VDN skill queue 71057.

- Enter **000001111171057** in the **Matching Pattern** column.
- Enter **15** in the **Min/Max** columns.
- Enter **15** in the **Delete Digits** column.
- Enter **71057** in the **Insert Digits** column.
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 - Repeat **Step 3** for all additional IPTF DNIS numbers.

Step 5 - Click on **Commit** (not shown).

Digit Conversion for Outgoing Calls from SM

[Add] [Remove]

5 Items [Filter: Enable]

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*00001111171057	*15	*15		*15	71057	destination		DNIS to VDN Conversion
<input type="checkbox"/>	*00000111118105	*15	*15		*15	71058	destination		DNIS to VDN Conversion
<input type="checkbox"/>	*00000111119105	*15	*15		*15	71059	destination		DNIS to VDN Conversion
<input type="checkbox"/>	*00000111116010	*15	*15		*15	71060	destination		DNIS to VDN Conversion
<input type="checkbox"/>	*00001111111061	*15	*15		*15	71061	destination		DNIS to VDN Conversion (ADR)

Select : All, None

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

5.3.2 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 5.3.1** with the following changes.

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

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

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

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

1. **Name** – Enter **eRHdrs**
2. **Value** – Enter the following Avaya headers to be removed by Session Manager. Note that each header name is separated by a comma 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-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, Adaptations (selected), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb 'Home / Elements / Routing / Adaptations' and a 'Help ?' link. The 'Adaptation Details' section includes a 'General' tab and a 'Commit' button. The configuration fields are: 'Adaptation Name' (SBC1-Adaptation for ATT), 'Module Name' (AttAdapter), and 'Module Parameter Type' (Name-Value Parameter). Below these is a table for Name-Value Parameters with columns 'Name' and 'Value'. One entry is shown: Name 'eRHdrs' and Value 'AV-Global-Session-ID,Alert-Info,Endpoint-View,P-AV-Message-Id,P-Charging-Vector,P-Location,Av-Secure-Indication'. There are 'Add' and 'Remove' buttons above the table. Below the table is a 'Select' dropdown set to 'All, None'. Further down are 'Egress URI Parameters' and 'Notes' (SBC - ATT IPTF). At the bottom, there are two sections for 'Digit Conversion'. The first, 'Digit Conversion for Incoming Calls to SM', shows '0 Items' and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The second, 'Digit Conversion for Outgoing Calls from SM', also shows '0 Items' and the same columns.

5.4 SIP Entities

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

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

- Session Manager (**Section 5.4.1**). Note that this Entity is normally created during Session Manager installation, but is shown here for completeness.
- Communication Manager for AT&T access (**Section 5.4.2**) – 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 5.4.3**) – 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 5.4.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls from the IPTF service via the Avaya SBCE.

5.4.1 Avaya Aura® Session Manager SIP Entity

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

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

- **Name** – Enter a descriptive name (e.g., **SessionManager**).
- **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.11**).
- **Type** – Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 5.2.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.
- **Minimum TLS Version** – Select **Use Global Setting**. In the reference configuration, the Session Manager Global Setting TLS version is 1.0 (not shown).

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

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

SIP Entity Details

General

* Name: SessionManager

* FQDN or IP Address: 10.64.91.11

Type: Session Manager

Notes: Session Manager

Location: Main

Outbound Proxy:

Time Zone: America/Denver

Minimum TLS Version: Use Global Setting

Credential name:

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Step 4 - Scrolling down to the **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 5.1** (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 5.5**.

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

Step 7 - Click on **Commit**.

Listen Ports

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avayalab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avayalab.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avayalab.com	<input checked="" type="checkbox"/>	

Select : All, None

5.4.2 Avaya Aura® Communication Manager SIP Entity – Public Trunk

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

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

- **Name** – Enter a descriptive name (e.g., **CM-TG4**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Sections 6.4** and **6.5** (e.g., **10.64.91.65**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM-TG4-IPTF** administered in **Section 5.3.1**.
- **Location** – Select a Location **Main** administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.

- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

CommitCancel

General

* Name:CM-TG4

* FQDN or IP Address:10.64.91.65

Type:CM

Notes:Trunk Group 4 - ATT IPTF

Adaptation:CM-TG4-IPTF

Location:Main

Time Zone:America/Denver

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

Minimum TLS Version:Use Global Setting

Credential name:

Securable:

Call Detail Recording:none

Loop Detection

Loop Detection Mode:On

Loop Count Threshold:5

Loop Detection Interval (in msec):200

Monitoring

SIP Link Monitoring:Use Session Manager Configuration

CRLF Keep Alive Monitoring:Use Session Manager Configuration

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

5.4.3 Avaya Aura® Communication Manager SIP Entity – Local Trunk

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

- **Name** – Enter a descriptive name (e.g., **CM-TG3**).
- Note that this Entity has no Adaptation defined.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: CM-TG3

* FQDN or IP Address: 10.64.91.65

Type: CM

Notes: Trunk Group 3 - CM to Enterprise

Adaptation:

Location: Main

Time Zone: America/Denver

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

5.4.4 Avaya Session Border Controller for Enterprise SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **SBCE-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 7.5.1**).
- **Type** – Verify **SIP Trunk** is selected.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for ATT** (**Section 5.3.2**).
- **Location** – Select location **Common** (**Section 5.2.2**).

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb navigation at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. A 'Help ?' link is in the top right. The 'General' tab is active. Fields include: 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), Time Zone (America/Denver), SIP Timer B/F (1), Minimum TLS Version (Use Global Setting), Credential name (empty), Securable (unchecked), Call Detail Recording (egress), Loop Detection Mode (On), Loop Count Threshold (5), Loop Detection Interval (200), SIP Link Monitoring (Use Session Manager Configuration), CRLF Keep Alive Monitoring (Use Session Manager Configuration), Supports Call Admission Control (unchecked), Shared Bandwidth Manager (unchecked), Primary Session Manager Bandwidth Association (empty), and Backup Session Manager Bandwidth Association (empty). The 'Loop Detection' and 'Monitoring' sections are also visible.

Home / Elements / Routing / SIP Entities

SIP Entity Details [Commit](#) [Cancel](#) [Help ?](#)

General

* 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

Time Zone: America/Denver

* SIP Timer B/F (in seconds): 1

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

5.5 Entity Links

In this section, Entity Links are administered between Session Manager and the following SIP Entities:

- Avaya Aura® Communication Manager – Public (**Section 5.5.1**).
- Avaya Aura® Communication Manager – Local (**Section 5.5.2**).
- Avaya SBCE (**Section 5.5.3**).

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

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

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

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

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

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG4**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g., **SessionManager**).
- **SIP Entity 1 Port** – Enter **5064**.
- **Protocol** – Select **TLS** (see **Section 6.8.1**). **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **CM-TG4**).
- **SIP Entity 2 Port** – Enter **5064** (see **Section 6.8.1**).
- **Connection Policy** – Select **trusted**.

Step 3 - Click on **Commit**.

Entity Links

Commit Cancel

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Not
<input type="checkbox"/>	* SM to CM TG4	* SessionManager	TLS	* 5064	* CM-TG4	<input type="checkbox"/>	* 5064	trusted	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None

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

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

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM TG3**).
- **Protocol** – Select **TLS**.
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local entity (e.g., **CM-TG3**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 6.8.2**).

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

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

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

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to SBCE-TollFree**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE entity (e.g., **SBCE-Toll Free**).

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

5.6 Time Ranges

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

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

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

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

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	Time Range 24/7

5.7 Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions.

5.7.1 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.

The screenshot shows the 'Routing Policy Details' configuration page. The left sidebar has 'Routing Policies' selected under the 'Routing' section. The main area shows the 'General' section with fields for 'Name' (To CM TG4), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (Trunk Group 4 PSTN4 to CM). There are 'Commit' and 'Cancel' buttons at the top right. The 'SIP Entity as Destination' section is visible at the bottom with a 'Select' button.

Routing Policy Details

General

* Name: To CM TG4

Disabled: ☐

* Retries: 0

Notes: Trunk Group 4 PSTN4 to CM

SIP Entity as Destination

Select

Step 4 - In the **SIP Entities List** page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**CM-TG4**), and click on **Select**.

Name	FQDN or IP Address	Type	Notes
<input type="radio"/> Aura Messaging	10.64.91.54	Modular Messaging	Aura Messaging
<input type="radio"/> CM-TG1	10.64.91.65	CM	Trunk Group 1 - ATT IPTF
<input type="radio"/> CM-TG2	10.64.91.65	CM	Trunk Group 2 - ATT IPTF
<input type="radio"/> CM-TG3	10.64.91.65	CM	Trunk Group 3 - CM to Enterprise
<input checked="" type="radio"/> CM-TG4	10.64.91.65	CM	Trunk Group 4 - ATT IPTF
<input type="radio"/> CS1000	10.80.140.103	Other	CS1000 7.65
<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

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

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

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

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

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

Step 10 - Click on **Commit**.

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM-TG4	10.64.91.65	CM	Trunk Group 4 - ATT IPTF

Time of Day

Add Remove View Gaps/Overlaps

1 Item

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

Select: All, None

Dial Patterns

Add Remove

2 Items

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input checked="" type="checkbox"/> 00000	15	15	<input type="checkbox"/>	-ALL-	Common	ATT Inbound

5.8 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. This pattern must be matched for further call processing.

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

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

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

- **Pattern** – In the reference configuration, AT&T sends a 15-digit number in the Request URI with the format 00000xxxxxxxxxx. Enter **00000**.

Note – The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 00000xxxxxxxxxx numbers into their corresponding Communication Manager extensions.

- **Min** and **Max** – Enter **15**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.

The screenshot shows the 'Dial Pattern Details' page with the following fields and values:

- Pattern:** 00000
- Min:** 15
- Max:** 15
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** -ALL- (dropdown menu)
- Notes:** ATT Inbound

At the bottom, the 'Originating Locations and Routing Policies' section includes an 'Add' button.


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

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

Step 5 - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7** (e.g., **To CM TG4**). Click on **Select** (not shown).

Originating Location


☒ Apply The Selected Routing Policies to All Originating Locations

3 Items  Filter: Enable

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

Select : All, None

Routing Policies


8 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 PSTN2 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 CS1000	<input type="checkbox"/>	CS1000	
<input type="checkbox"/>	To SBC1	<input type="checkbox"/>	SBC1	

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

Originating Locations and Routing Policies

Add Remove


1 Item  Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Common	SBC to PSTN	To CM TG4	2	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM

Select : All, None

Denied Originating Locations

Add Remove

0 Items  Filter: Enable

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

Commit Cancel

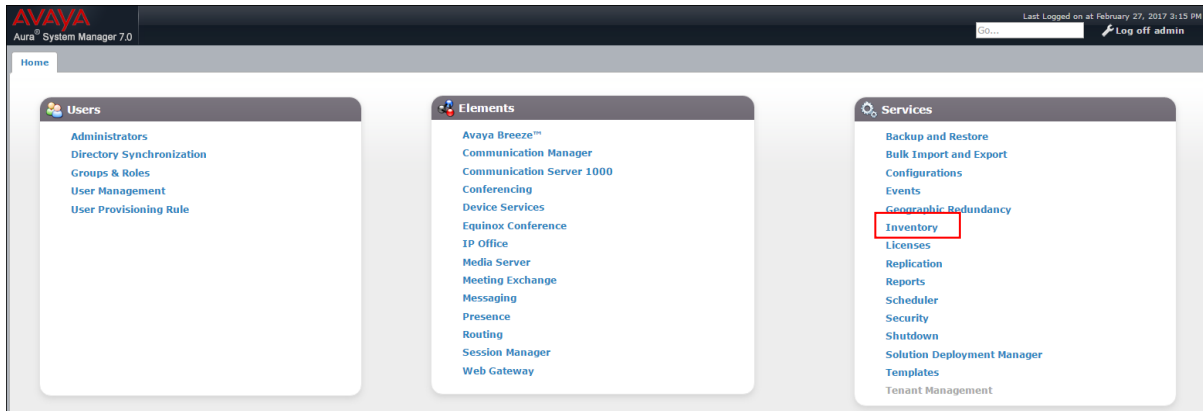
Step 7 - Repeat **Steps 1-6** for any additional inbound dial patterns from AT&T.

5.9 Verify TLS Certificates – Session Manager

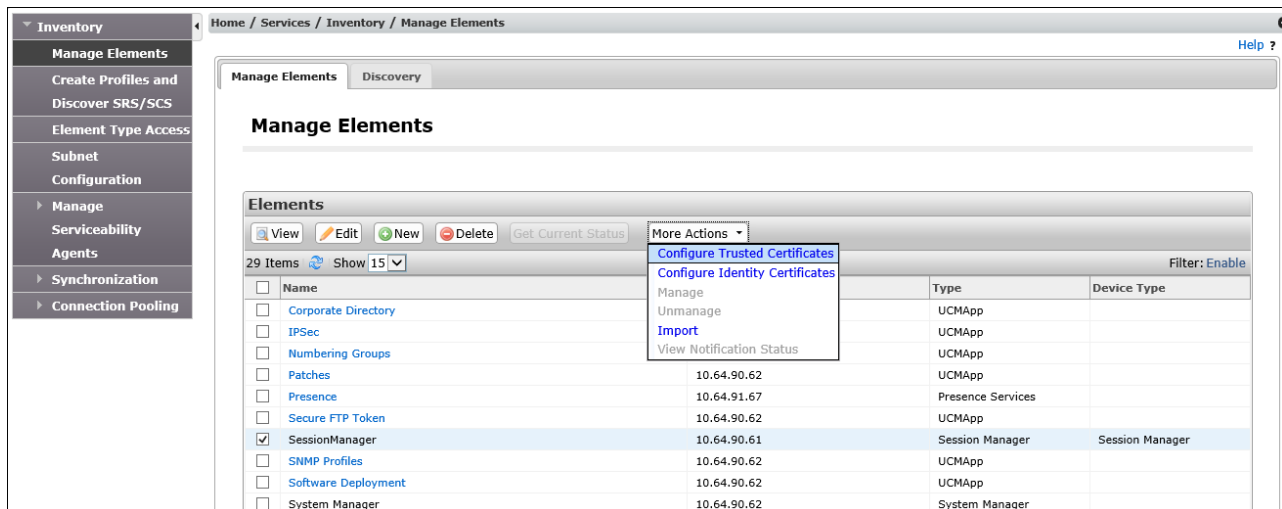
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

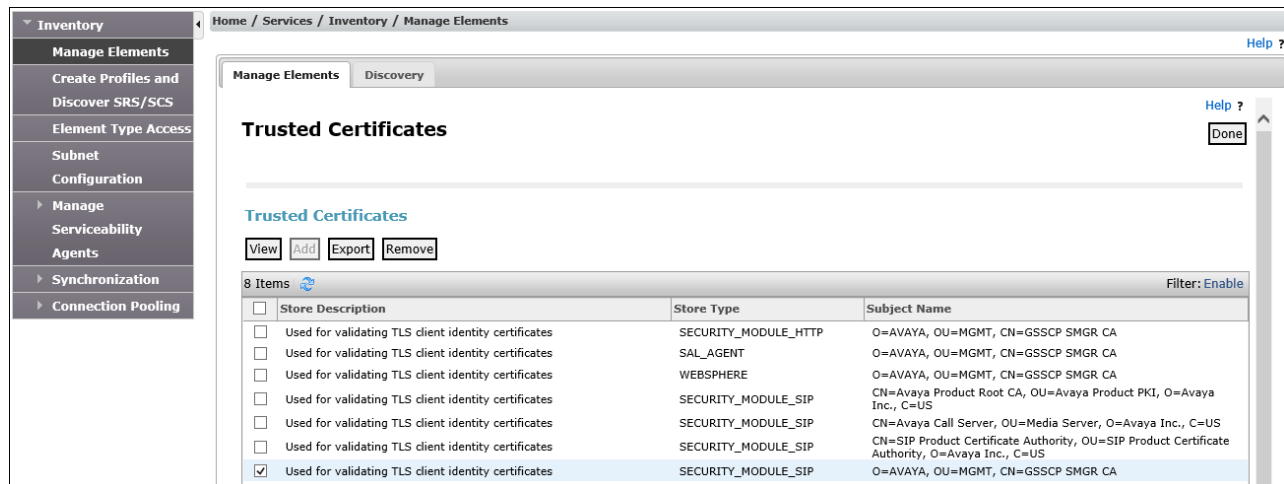
Step 1 - From the **Home** screen, under the **Services** heading in the right column, select **Inventory**.



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** → **Configure Trusted Certificates**.

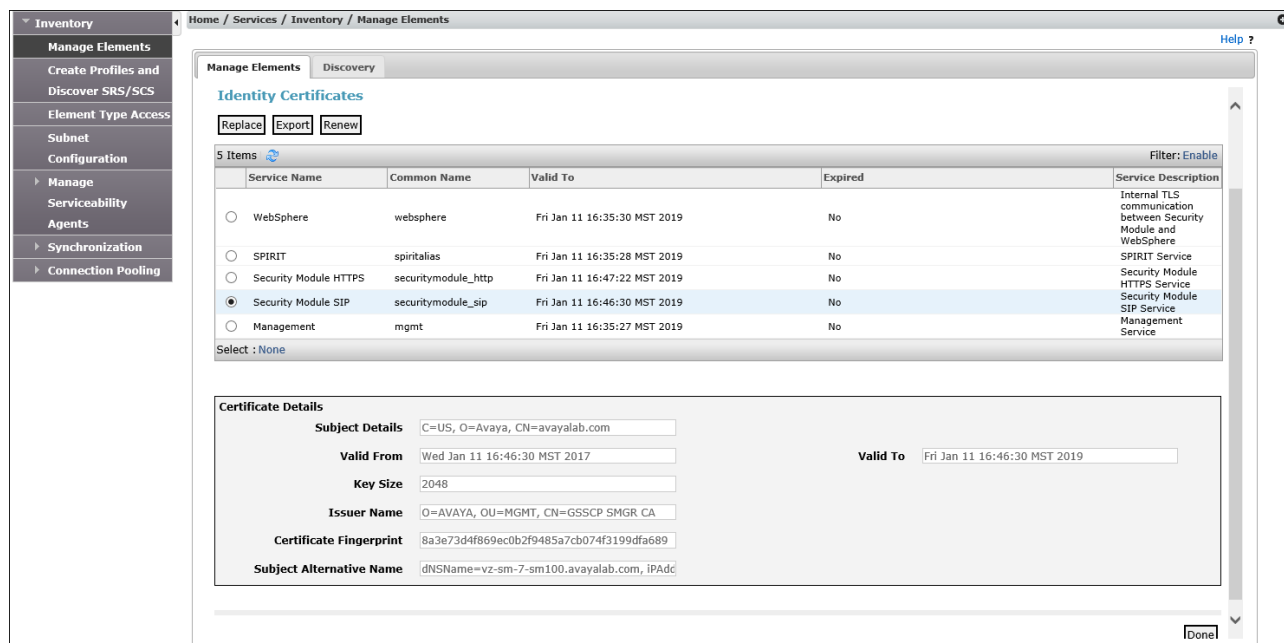


Step 3 - Verify the System Manager Certificate Authority certificate is listed in the trusted store, **SECURITY_MODULE_SIP**. Click **Done** to return to the previous screen.



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

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



6 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] 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.

6.1 System-Parameters Customer-Options

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

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

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	4000	0	
Maximum Concurrently Registered IP Stations:	2400	1	
Maximum Administered Remote Office Trunks:	4000	0	
Maximum Concurrently Registered Remote Office Stations:	2400	0	
Maximum Concurrently Registered IP eCons:	68	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	2400	3	
Maximum Video Capable IP Softphones:	2400	4	
Maximum Administered SIP Trunks:	4000	30	
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0	
Maximum 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	ISDN-BRI Trunks? y
Enterprise Survivable Server? n		ISDN-PRI? y
Enterprise Wide Licensing? n		Local Survivable Processor? n
ESS Administration? y		Malicious Call Trace? y
Extended Cvg/Fwd Admin? y		Media Encryption Over IP? y
External Device Alarm Admin? y	Mode Code for Centralized Voice Mail? n	
Five Port Networks Max Per MCC? n		
Flexible Billing? n		
Forced Entry of Account Codes? y		Multifrequency Signaling? y
Global Call Classification? y		Multimedia Call Handling (Basic)? y

Step 2 - On Page 6 of the form, verify that the Private Networking and Processor Ethernet fields are set to y.

display system-parameters customer-options		Page 6 of 12
OPTIONAL FEATURES		
Multinational Locations? n		Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n		Station as Virtual Extension? y
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	Tenant Partitioning? y
PNC Duplication? n		Terminal Trans. Init. (TTI)? y
Port Network Support? n		Time of Day Routing? y
Posted Messages? y	TN2501 VAL Maximum Capacity? y	Uniform Dialing Plan? y
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
Processor Ethernet? y		Wideband Switching? y
		Wireless? n
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		
(NOTE: You must logoff & login to effect the permission changes.)		

6.2 System-Parameters Features

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

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

6.3 Dial Plan

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

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

- 5-digit extensions with a **Call Type** of **ext** beginning with:
 - The digits **1, 2** and **7** for Communication Manager extensions.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code ***xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 6.8**.

change dialplan analysis	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						
7	5	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	3	fac						

6.4 IP Node Names

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

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

- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.61**).
- Media Server (e.g., **AMS** and **10.64.91.60**). 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	
AMS	10.64.91.60	
SM	10.64.91.61	
default	0.0.0.0	
procr	10.64.91.65	
procr6	::	

6.5 IP Interface for procr

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

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

display ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		Target socket load: 4800
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.64.91.65	
Subnet Mask: /24		

6.6 IP Network Regions

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

6.6.1 IP Network Region 1 – Local CPE Region

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

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

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

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		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 16384	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 32767	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

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

- Verify that **RTCP Reporting 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 t

dst codec direct WAN-BW-limits Video Intervening Dyn A G c

rgn set WAN Units Total Norm Prio Shr Regions CAC R L e

1 1 all

2 2 y NoLimit n t

3 1 y NoLimit n t

4 4 y NoLimit n t

6.6.2 IP Network Region 4 – SIP Trunk Region

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

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

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

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

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

change ip-network-region 4										Page	4	of	20
Source Region: 4		Inter Network Region Connection Management								I		M	
										G	A	t	
dst	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 – Region 3 was created to test G.711 pass-through fax (not shown), and is permitted to talk to region 4 using codec set 3.

6.7 IP Codec Parameters

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.

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

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., 1). On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, **G.729A**, and **G.729B** are included in the codec list. Note that the packet interval size will default to 20ms. 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 SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80					
2: none					

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

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

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

Step 1 - Repeat the steps in **Section 6.7.1** with the following changes.

- Provision the codecs in the order shown below. Note that the order of G.729A and G.729B codecs may be reversed as required.
- Set **Frames Per Pkt** to **3**. This will auto-populate **30** for the **Packet Size (ms)** field, and specify a PTIME value of 30 in the SDP (recommended by AT&T). See **Section 2.2, 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					
	Mode	Redundancy	ECM: y	Packet Size (ms)	
FAX	t.38-standard	0			
Modem	off	0			
TDD/TTY	US	3			
H.323 Clear-channel	n	0			
SIP 64K Data	n	0		20	

6.7.3 Codecs for G.711 Pass-Through Fax

During G.711 pass-through fax testing, the network region assigned to the G450 Media Gateway was changed from region 1 to region 3 (**Section 6.14**). This network region utilized **ip-codec-set 3** for calls between region 3 and region 4 (IPTF calls). This codec set 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. For this codec set, **G.711MU** is listed as the preferred codec, and on **Page 2**, the **Fax Mode** is set to **off**. Creating a dedicated network region and ip-codec-set for G.711 pass-through fax allowed for fax calls from this G450 Media Gateway to begin with 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 6.7.2**).

change ip-codec-set 3

Page 1 of 2

IP CODEC SET

Codec Set: 3

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

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1: 1-srtp-aescm128-hmac80

2: none

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	

6.8 SIP Trunks

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

- Inbound IPTF access – SIP Trunk 4
 - Note that this trunk will use TLS port 5064 as described in **Section 5.5.1**.
- Internal CPE access (e.g., Avaya SIP telephones, etc.) – SIP Trunk 3
 - Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

6.8.1 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 5.4.2**.

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 6.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.4** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5064**.
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 6.6.2**.
- **Far-end Domain** – Enter **avayalab.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **OPTIONAL**: If desired, set **Initial IP-IP Direct Media** to **y**. Otherwise leave it disable (default).

Note - Enabling the **Initial IP-IP Direct Media** parameter allows Communication Manager to signal the IP address of Avaya SIP telephones during the initial setup of a call. This permits the Avaya SIP telephone and the AT&T caller to exchange media directly, without allocating Communication Manager media resources. However, unless network routing permits direct IP access between the Avaya SIP telephone and the “inside” interface of the Avaya SBCE, a loss of audio can occur when this option is enabled. In addition, when this option is enabled, Communication Manager will not send SDP in 180 messages, and will not send 183 messages (if enabled).

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

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	
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? y	
	Alternate Route Timer(sec): 6	

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 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	Night Service:
Dial Access? n		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 4	
	Number of Members: 20	

Step 3 - 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 4 - 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		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Hold/Unhold Notifications? y		
Show ANSWERED BY on Display? y		

Step 5 - 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 5.3.2**). Alternatively, History Info may be disabled here.

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

6.8.2 Local SIP Trunk (Avaya SIP Telephone Access)

This trunk corresponds to the **CM-TG3** SIP Entity defined in **Section 5.4.3**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **3**), and repeat the steps in **Section 6.8.1** with the following changes:

- **Transport Method** – Set to **tls**.
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.6.1**.
- **Initial IP-IP Direct Media** – Set to **y**.

add signaling-group 3		Page 1 of 2
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
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? y	
	Alternate Route Timer(sec): 6	

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 3). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.8.1** with the following changes:

- **Group Name** – Enter a descriptive name (e.g., **To 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 **Step 1** (e.g., 3).

add trunk-group 3		Page 1 of 21
TRUNK GROUP		
Group Number: 3	Group Type: sip	CDR Reports: y
Group Name: To SM Enterprise	COR: 1	TN: 1 TAC: *03
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 3	
	Number of Members: 10	

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

- Same as **Section 6.8.1**.

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

- Same as **Section 6.8.1**.
- **Step 5** - On **Page 4** of the **Trunk Group** form:

- Use default values for all settings.

add trunk-group 3	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: 101 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	

6.9 Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 6.8.1**), 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 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 **14006**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **000001111101061**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **15**).

Step 3 - 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 **71057**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding IPTF DNIS number (e.g., **000001111171057**).
- **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 14006					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	Len	
5	14006	4	000001111101061	15	Total Administered: 20
5	71057	4	000001111171057	15	Maximum Entries: 240
5	71058	4	000001111181058	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	71059	4	000001111191059	15	
5	71060	4	000001111101060	15	
					Communication Manager automatically inserts a '+' digit in this case.

6.10 Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 6.8.2**), is used to send Communication Manager local extension numbers to Session Manager, for inclusion in any SIP headers directed to SIP endpoints and Messaging.

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

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code** – Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 6.3** (e.g., **14** and **20**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).

Total Len - Enter the total number of digits after the digit conversion (e.g., **5**).

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	10	3		5	Total Administered: 6
5	11	3		5	Maximum Entries: 540
5	12	3		5	
5	14	3		5	
5	20	3		5	

6.11 Route Patterns 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 6.12** (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					
															Intw					
1: 3 0															n user					
2:															n user					
3:															n user					
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub															Numbering LAR					
0 1 2 M 4 W Request															Dgts Format					
1: y y y y y n n rest															lev0-pvt none					

6.12 Automatic 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 6.11**.

Step 1 - Enter the following:

- **Dialed String** - In the reference configuration all SIP telephones used extensions in the range 14xxx, therefore enter **14**.
- **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 Min Max		Route Pattern		Call Type		Node Num		ANI Req'd	
14		5 5		3		lev0				n	
20		5 5		3		lev0				n	

6.13 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] 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 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
		BSR? y
		Holidays? y
01 #	Wait hearing ringback	
02 wait-time	2 secs hearing ringback	
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		

- Skill 1 VDN form – **Page 1**

display vdn 71057	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 71057	
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	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	

6.14 Avaya G450 Media Gateway Provisioning

In the reference configuration, a G450 Media Gateway is provisioned. The G450 is located in the Main site and is used for local DSP resources, announcements, etc.

Note – Only the Media Gateway provisioning associated with the G450 registration to Communication Manager is shown below. See [7] for additional information.

- Step 1** - SSH to the G450 (not shown). Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., **G450-???(*super*)#**).
- Step 2** - Enter the **show system** command and note the G450 serial number (e.g., **08IS38199678**).
- 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., **10.64.91.65**, see **Section 6.4**).
- Step 4** - Enter the **copy running-config startup-config** command to save the G450 configuration.
- Step 5** - On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown). Enter the following parameters:
- Set **Type** = **g450**
 - Set **Name** = Enter a descriptive name (e.g., **G450**)
 - Set **Serial Number** = Enter the serial number copied from **Step 2** (e.g., **08IS38199678**).
 - Set the **Link Encryption Type** parameter as desired (**any-ptls/tls** was used in the reference configuration).
 - Set **Network Region** = **1**

When the Media Gateway registers, the SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., *G450-001(super)#*).

Step 6 - Enter the **display media-gateway 1** command, and verify that the G450 has registered.

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

                                MEDIA GATEWAY 1

                                Type: g450
                                Name: G450-1
                                Serial No: 08IS38199678
                                Link Encryption Type: any-ptls/tls      Enable CF? n
                                Network Region: 1                        Location: 1
                                                                Site Data:

                                Recovery Rule: 1

                                Registered? y
                                FW Version/HW Vintage: 37 .41 .0 /1
                                MGP IPV4 Address: 10.64.19.81
                                MGP IPV6 Address:
                                Controller IP Address: 10.64.91.65
```

6.15 Avaya Aura® Media Server Provisioning

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

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

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

Step 2 - On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP → Node and Routes** and add the Communication Manager Procr interface IP address (e.g., **10.64.91.65**, see **Section 6.4**) as a trusted node (not shown).

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

- **Group Type** – Set to **sip**
- **Transport Method** – Set to **tls**
- Verify that **Peer Detection Enabled?** – Set to **n**
- **Peer Server** to **AMS**
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.4**.
- **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 6.4** (e.g., **AMS**).
- **Near-end Listen Port** – Set to **9061**
- **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 6.6.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

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

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

Peer Detection Enabled? n Peer Server: AMS

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

Far-end Domain: 10.64.91.60
```

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

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

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

Media Server ID: 1

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

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

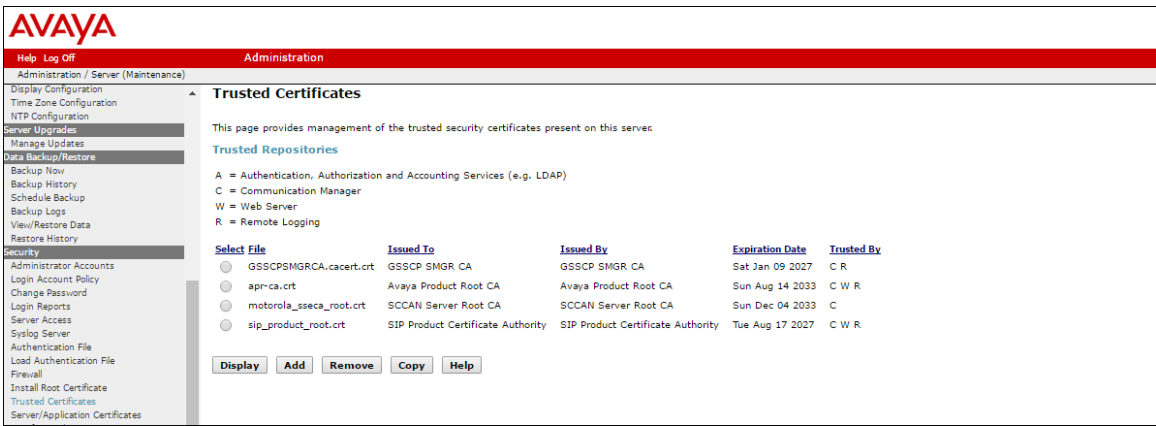
6.16 Verify TLS Certificates – Communication Manager

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.

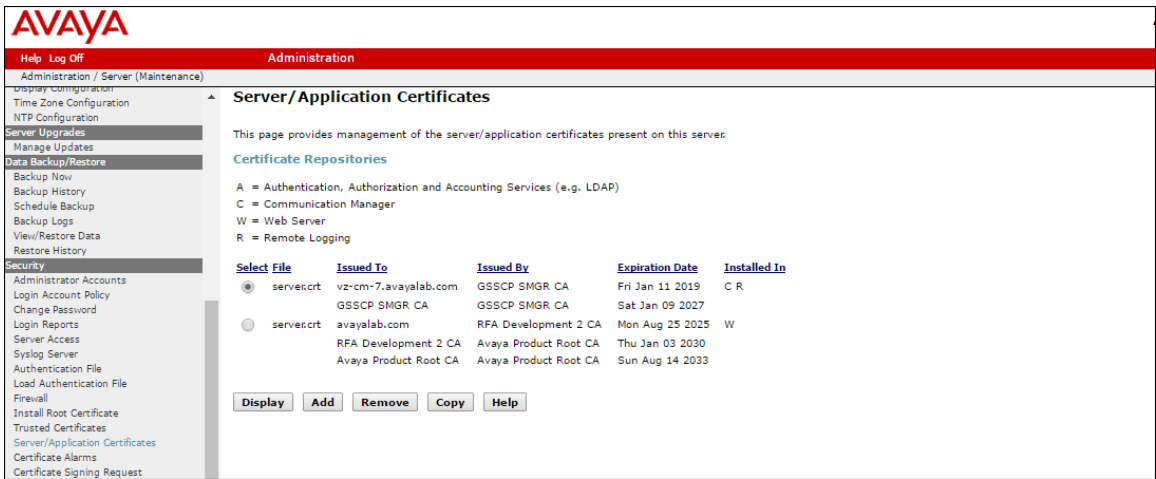
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. The following procedures show how to verify the certificates used by Communication Manager.

Step 1 - From a web browser, type in “https:// x.x.x.x”, where x.x.x.x 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.



6.17 Save Communication Manager Translations

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

7 Configure Avaya Session Border Controller for Enterprise

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


Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [11] and [12] for additional information.

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (IP address 10.64.91.41), with access to the Main site. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 192.168.80.43). The following provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection.

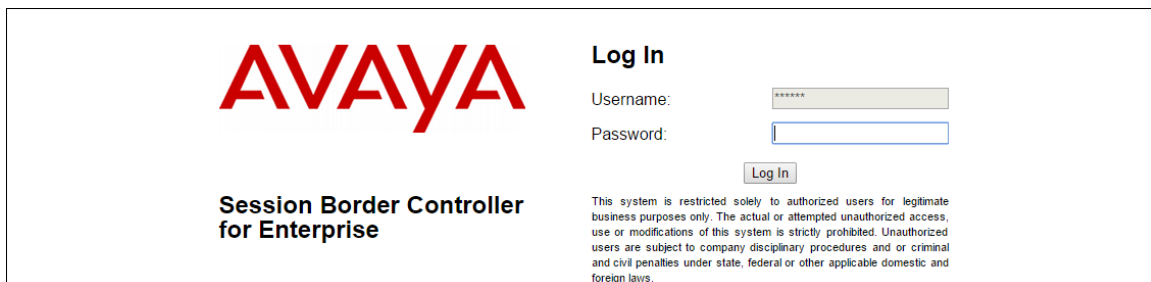
Step 1 - Access the web interface by typing “**https://x.x.x.x**”, where x.x.x.x is the management IP address of the Avaya SBCE.

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. At the bottom right, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." and "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials."

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field containing "*****". Below the input field is a "Password:" label followed by a text input field. Below the input field is a "Log In" button. At the bottom right, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." and "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials."

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

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

Session Border Controller for Enterprise

Dashboard

Information

System Time	12:10:33 PM MDT	Refresh
Version	7.2.1.0-05-14222	
Build Date	Tue Oct 31 00:06:46 UTC 2017	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	06/04/2018 12:08:05 MDT	
Failed Login Attempts	0	

Installed Devices

EMS
SBCE

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

Notes

No notes found.

7.1 System Management – Status

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

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

System Management

Devices | Updates | SSL VPN | Licensing | Key Bundles

Device Name	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
SBCE	10.64.90.40	7.2.1.0-05-14222	Commissioned						

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

System Information: SBCE

General Configuration

Appliance Name

SBCE

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 50

50

Advanced Sessions

Requested: 50

50

Scopia Video Sessions

Requested: 5

5

CES Sessions

Requested: 0

0

Transcoding Sessions

Requested: 50

50

Encryption

☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
				A1
10.64.91.41	10.64.91.41	255.255.255.0	10.64.91.1	A1
				B2
				B1
				B1
192.168.80.43	192.168.80.43	255.255.255.128	192.168.80.1	B1

DNS Configuration

Primary DNS

10.64.90.201

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.64.91.40

Management IP(s)

IP #1 (IPv4)

10.64.90.40

7.2 TLS Management

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

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

7.2.1 Verify TLS Certificates – Avaya Session Border Controller for Enterprise

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

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



7.2.2 Server Profiles

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

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

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

Edit Profile
X

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.

TLS Profile

Profile Name

Certificate sbc40.crt ▼

Certificate Verification

Peer Verification None ▼

Peer Certificate Authorities
▲ ▼

GSSCPSMGRCA.pem

Peer Certificate Revocation Lists
▲ ▼

Verification Depth

Next

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Profiles, PPM Services, Domain Policies, TLS Management (expanded), Certificates, Client Profiles, **Server Profiles** (highlighted), and Device Specific Settings. The main content area is titled 'Server Profiles: sbc40-server' and includes an 'Add' button. Below this, a list of server profiles shows 'sbc40-server' selected. The 'Server Profile' form is displayed with the following sections and values:

- TLS Profile**
 - Profile Name: sbc40-server
 - Certificate: sbc40.crt
- Certificate Verification**
 - Peer Verification: None
 - Extended Hostname Verification: ☐
- Renegotiation Parameters**
 - Renegotiation Time: 0
 - Renegotiation Byte Count: 0
- Handshake Options**
 - Version: ☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0
 - Ciphers: ☒ Default ☐ FIPS ☐ Custom
 - Value: HIGH:DH:1ADH:1MD5:1aNULL:1eNULL:@STRENGTH

An 'Edit' button is located at the bottom of the form.

7.2.3 Client Profiles

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

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

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

Edit Profile [X]

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.

TLS Profile

Profile Name: sbc40-client

Certificate: sbc40.crt

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: GSSCPSMGRCA.pem

Peer Certificate Revocation Lists:

Verification Depth: 1

Extended Hostname Verification: ☐

Custom Hostname Override:

Next

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (selected), Certificates, Client Profiles (highlighted), Server Profiles, and Device Specific Settings. The main area is titled 'Client Profiles: sbc40-client' and contains a 'Delete' button. Below this is a 'Client Profile' tab with a 'Click here to add a description' link. The profile configuration is divided into several sections: 'TLS Profile' (Profile Name: sbc40-client, Certificate: sbc40.crt), 'Certificate Verification' (Peer Verification: Required, Peer Certificate Authorities: GSSCP5MGRCA.pem, Peer Certificate Revocation Lists: ---, Verification Depth: 1, Extended Hostname Verification: unchecked), 'Renegotiation Parameters' (Renegotiation Time: 0, Renegotiation Byte Count: 0), and 'Handshake Options' (Version: TLS 1.2 selected, Ciphers: Default selected, Value: HIGH:DH:ADH:MD5:1eNULL:1eNULL:@STRENGTH). An 'Edit' button is at the bottom right of the form.

7.3 Global Profiles

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

7.3.1 Server Interworking – Avaya

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

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

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

The screenshot shows the 'Interworking Profiles: avaya-ru' screen. The left navigation menu is the same as in the previous screenshot, with 'Server Interworking' highlighted. The main area shows a list of interworking profiles: 'cs2100', 'avaya-ru' (highlighted with a red box), 'OCS-Edge-Server', 'disco-ccm', and 'cups'. A 'Clone' button is highlighted with a red box in the top right corner. Below the list is a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' There are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table with the following data:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None

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

Clone Profile X

Profile Name
avaya-ru

Clone Name

Enterprise Interwork

Finish

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

Rename

Clone

Delete

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

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

Edit

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

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

The screenshot shows a dialog box titled "Editing Profile: Enterprise Interwork" with a close button (X) in the top right corner. The "General" tab is selected. The following options are visible:

- Hold Support:** Radio buttons for ☒ None, ☐ RFC2543 - c=0.0.0.0, and ☐ RFC3264 - a=sendonly.
- 180 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 181 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 182 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 183 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- Refer Handling:** ☐
- URI Group:** A dropdown menu showing "None".
- Send Hold:** ☐
- Delayed Offer:** ☐
- 3xx Handling:** ☐
- Diversion Header Support:** ☐
- Delayed SDP Handling:** ☐
- Re-Invite Handling:** ☐
- Prack Handling:** ☐
- Allow 18X SDP:** ☐
- T.38 Support:** ☒ (This checkbox is highlighted with a red border in the original image).
- URI Scheme:** Radio buttons for ☒ SIP, ☐ TEL, and ☐ ANY.
- Via Header Format:** Radio buttons for ☒ RFC3261 and ☐ RFC2543.

A "Finish" button is located at the bottom center of the dialog box.

Step 6 - Select the **Advanced** tab, accept the default values, and click **Finish**.

Editing Profile: Enterprise Interwork

Record Routes: ☒ None, ☐ Single Side, ☒ Both Sides, ☐ Dialog-Initiate Only (Single Side), ☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup: ☐

Extensions: Avaya

Diversion Manipulation: ☐

Diversion Condition: None

Diversion Header URI:

Has Remote SBC: ☒

Route Response on Via Port: ☐

DTMF: ☒ None, ☐ SIP NOTIFY, ☐ SIP INFO

Finish

7.3.2 Signaling Manipulation

Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages.

In the reference configuration, one signaling manipulation script is used.

Note – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 7.4.3**) does not meet the desired result. Refer to [11] for information on the Avaya SBCE scripting language.

Step 1 - As described in **Section 2.2, Item 7**, Avaya SIP endpoints may send requests with Endpoint-View headers containing private network information. These are removed in **Section 5.3.2**. However, an “epv” parameter is also inserted into the Contact header of these requests. This parameter also contains private network information. The following signaling manipulation is used to remove this “epv” parameter from the Contact header, along with the “gsid” parameter. The “gsid” parameter was removed to further reduce packet size.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.

4. Enter a name for the script in the **Title** box (e.g., **contact_param_bandwidth**). The following script is defined:

Title contact_param_bandwidth Save

```
1 within session "ALL"
2 {
3     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4     {
5
6         //Remove gsid and epv parameters from Contact header to hide internal topology
7         remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
8         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
9     }
10 }
```

Step 2 - As described in **Section 2.2, Item 8**, some Avaya SIP endpoints may send Bandwidth headers that may cause issues with the AT&T network. The following signaling manipulation script is added to the script defined in **Step 1** above, to remove these Bandwidth headers.

1. The following script is added:

Title contact_param_bandwidth Save

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

Step 3 - Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the AT&T Server Configuration in **Section 7.3.4, Step 3**.

7.3.3 Server Configuration – Session Manager

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

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

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

Add Server Configuration Profile X

Profile Name

EnterpriseCallServer

Next

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

- Select **Server Type: Call Server**.

- **IP Address/FQDN: 10.64.91.61** (Session Manager network IP Address)
- **Port: 5061.**
- Select **Transport: TLS.**
- **TLS Client Profile: sbc40-client.**
- Select **Next.**

Edit Server Configuration Profile - General

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

Server Type: Call Server

SIP Domain:

TLS Client Profile: sbc40-client

Add

IP Address / FQDN	Port	Transport
10.64.91.61	5061	TLS

Delete

Finish

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

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

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

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

Edit Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☒

Interworking Profile: Enterprise Interwork

Signaling Manipulation Script: None

Securable: ☐

Enable FGDN: ☐

TCP Failover Port:

TLS Failover Port:

Finish

7.3.4 Server Configuration – 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. See **Addendum 1** for information on configuring two IPTF Border Elements (Primary & Secondary).

Repeat the steps in **Section 7.3.3**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

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

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

- Select **Server Type: Trunk Server**
- **IP Address/FQDN: 192.168.225.210** (AT&T Border Element IP address)
- **Port: 5060**
- Select **Transport: UDP**
- Select **Next** until the **Advanced** tab is reached

The screenshot shows the 'Server Configuration: ATT-TollFree-trk-svr' window with the 'General' tab selected. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main area shows the 'General' tab with the following configuration:

IP Address / FQDN	Port	Transport
192.168.225.210	5060	UDP

Buttons for 'Add', 'Rename', 'Clone', and 'Delete' are visible at the top right. An 'Edit' button is located below the table.

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

- For the **Signaling Manipulation Script** select the **contact_param_bandwidth** script defined in **Section 7.3.2**.
- Select **Finish** (not shown).

The screenshot shows the 'Server Configuration: ATT-TollFree-trk-svr' window with the 'Advanced' tab selected. The left sidebar is the same as the previous screenshot. The main area shows the 'Advanced' tab with the following configuration:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ATT-Interworking
Signaling Manipulation Script	contact_param_bandwidth
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None

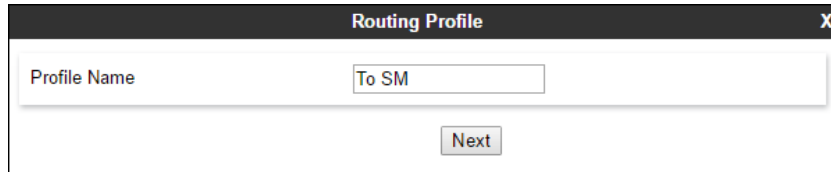
Buttons for 'Add', 'Rename', 'Clone', and 'Delete' are visible at the top right. An 'Edit' button is located at the bottom right.

7.3.5 Routing – To Session Manager

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

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

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

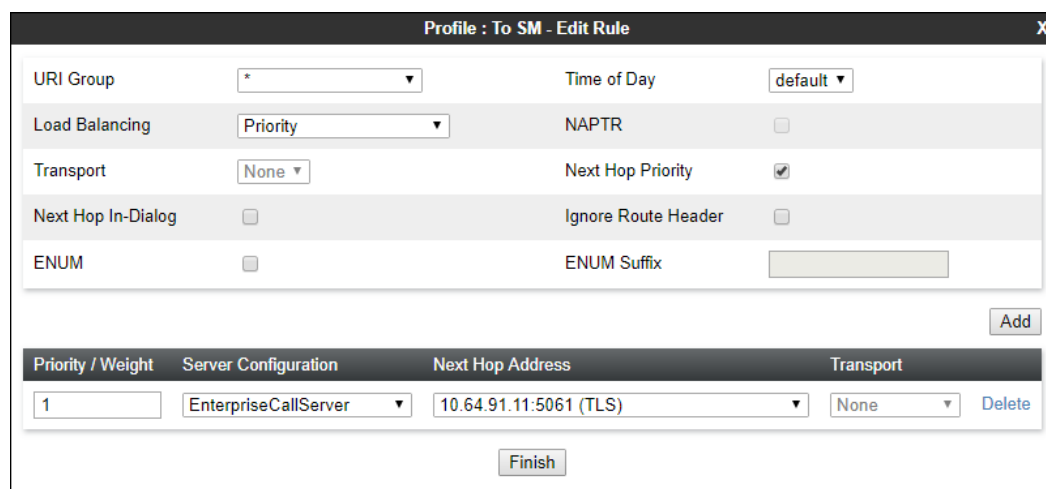


The image shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "To SM". Below the input field is a button labeled "Next".

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

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

- **Priority/Weight = 1**
- **Server Configuration = EnterpriseCallServer** (from **Section 7.3.3**).
- **Next Hop Address:** Verify that the **10.64.91.11:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** fields are grayed out.
- Click on **Finish**.



The image shows a window titled "Profile : To SM - Edit Rule" with a close button (X) in the top right corner. The window contains several configuration fields and a table of rules.

Configuration fields:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐
- ENUM: ☐
- ENUM Suffix:

Buttons: Add, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	EnterpriseCallServer	10.64.91.11:5061 (TLS)	None

Buttons: Delete, Finish

7.3.6 Routing – To AT&T

Repeat the steps in **Section 7.3.5**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

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

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

- **Priority/Weight = 1**
- **Server Configuration = ATT-TollFree-trk-svr** (from **Section 7.3.4**).

- **Next Hop Address:** Verify that the **192.168.225.210:5060 (UDP)** entry from the drop down menu is selected (AT&T Border Element IP address).
- Use default values for the rest of the parameters.

Step 4 - Click **Finish**.

Profile : To ATT IPTF - Edit Rule

URI Group: *
 Load Balancing: Priority
 Transport: None
 Next Hop In-Dialog: ☐
 ENUM: ☐
 Time of Day: default
 NAPTR: ☐
 Next Hop Priority: ☒
 Ignore Route Header: ☐
 ENUM Suffix:
 Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ATT-TollFree-trk-svr	192.168.225.210:5060 (UDP)	None

Delete Finish

7.3.7 Topology Hiding – Enterprise Side

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

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

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

Topology Hiding Profile

Profile Name: Enterprise-Topology
 Next

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

Topology Hiding Profile

Add Header

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

Delete Back Finish

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

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

Finish

7.3.8 Topology Hiding – AT&T Side

Repeat the steps in **Section 7.3.7**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

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

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

Finish

The following screen shows the completed **Topology Hiding Profile** forms in the shared test environment.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration, **Topology Hiding**, Signaling Manipulation, URI Groups, and SNMP Traps. The main area is titled 'Topology Hiding Profiles: SIP-Trunk-Topology'. It features a list of profiles on the left: 'default', 'cisco_th_profile', 'Enterprise-Topology', 'SIP-Trunk-Topology' (highlighted with a red box), and 'IPOSE-Topology'. An 'Add' button is above this list. On the right, there's a 'Click here to add a description.' link and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a table titled 'Topology Hiding' with columns: Header, Criteria, Replace Action, and Overwrite Value.

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

7.4 Domain Policies

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

7.4.1 Application Rules

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

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

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

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

The screenshot shows the 'Application Rules: sip-trunk' configuration page. The left navigation menu is similar to the previous screenshot, with 'Domain Policies' expanded and 'Application Rules' selected. The main area has a title 'Application Rules: sip-trunk' and buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below the title is a 'Click here to add a description.' link. The main content area is titled 'Application Rule' and contains a table with columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint.

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"/>		

Below the table is a 'Miscellaneous' section with two rows: 'CDR Support' with value 'None' and 'RTCP Keep-Alive' with value 'No'. An 'Edit' button is at the bottom right of this section.

7.4.2 Media Rules

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

7.4.2.1 Enterprise – Media Rule

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

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

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

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

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

- Select the **Encryption** tab.
- Click the **Edit** button and the **Media Encryption** window will open (not shown).
- **Preferred Format #2**: Select **RTP** from the drop-down.
- Select the **Capability Negotiation** box.

Step 5 - Click **Finish**.

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

The screenshot displays the 'Media Rules: enterprise med rule' configuration page. On the left is a navigation menu with categories like Dashboard, Administration, System Management, and Domain Policies. The 'Media Rules' section under 'Domain Policies' is expanded, showing a list of rules including 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'ipv6-anat-media', 'att med rule', and 'enterprise med rule' (highlighted in red). The main area shows the configuration for the selected rule. At the top, there are buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below this is a tabbed interface with 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS' tabs. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Under 'Audio Encryption', 'Preferred Formats' is set to 'SRTP_AES_CM_128_HMAC_SHA1_80 RTP', 'Encrypted RTCP' is unchecked, 'MKI' is unchecked, 'Lifetime' is 'Any', and 'Interworking' is checked. Under 'Video Encryption', 'Preferred Formats' is 'RTP' and 'Interworking' is checked. A 'Miscellaneous' section at the bottom has 'Capability Negotiation' checked. An 'Edit' button is located at the bottom right of the configuration area.

7.4.2.2 AT&T – Media Rule

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

1. From the Media Rules menu, select the **default-low-med** rule.
2. In the **Clone Name** field enter **att med rule**.
3. Use default values for all settings.

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 Dashboard, Administration, System Management, and Domain Policies. The 'Media Rules' section is expanded, showing a list of rules: default-low-med, default-low-med-enc, default-high, default-high-enc, avaya-low-med-enc, ipv6-anat-media, **att med rule** (highlighted in red), and enterprise med rule. The main area displays the configuration for the selected rule. It includes a header with 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' buttons. Below the header is a description field with the placeholder 'Click here to add a description.' and tabs for 'Encryption', 'Codec Prioritization', 'Advanced', and 'QoS'. The 'QoS' tab is active, showing 'Media QoS Marking' settings: 'Enabled' is checked, 'QoS Type' is 'DSCP'. Below this are 'Audio QoS' settings with 'Audio DSCP' set to 'EF', and 'Video QoS' settings with 'Video DSCP' set to 'EF'. An 'Edit' button is at the bottom right of the configuration area.

7.4.3 Signaling Rules

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

7.4.3.1 Enterprise – Signaling Rules

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

Step 2 - The **Signaling Rules** window will open (not shown). From the Signaling Rules menu, select the **default** rule.

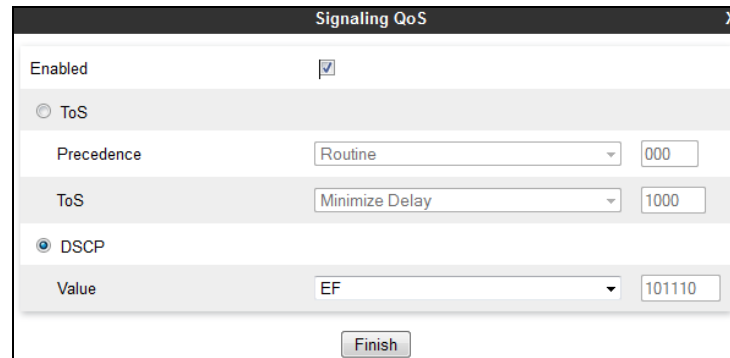
Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

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

Step 4 - Highlight **enterprise sig rule**, select the **Signaling QoS** tab and enter the following:

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

Step 5 - Click **Finish**.



The screenshot shows the 'Signaling QoS' configuration window. It has a title bar with 'Signaling QoS' and a close button 'X'. Inside, there is a section for 'Enabled' with a checked checkbox. Below this, there are two radio buttons: 'ToS' (unselected) and 'DSCP' (selected). Under 'ToS', there are fields for 'Precedence' (set to 'Routine') and 'ToS' (set to 'Minimize Delay'). Under 'DSCP', there is a 'Value' field set to 'EF'. At the bottom right, there is a 'Finish' button.

7.4.3.2 AT&T – Signaling Rule

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

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

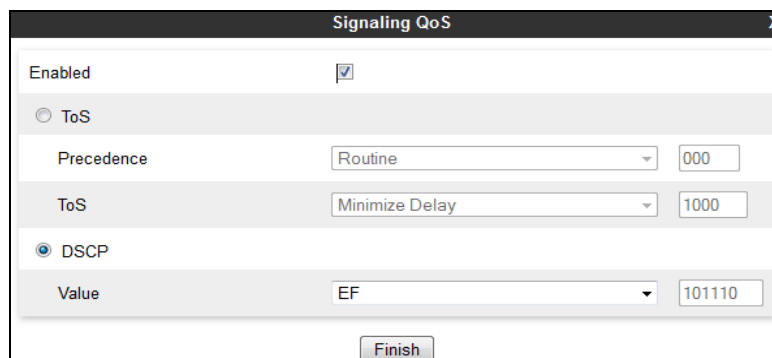
Step 3 - From the Signaling Rules menu, select the **default** rule.

Step 4 - Select **Clone Rule** button.

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

Step 5 - Click **Finish**.

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



This screenshot is identical to the one above, showing the 'Signaling QoS' configuration window with 'DSCP' selected and 'Value' set to 'EF'.

7.4.4 Endpoint Policy Groups – Enterprise Connection

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

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

Step 3 - Select **Add**.

- **Name:** enterprise policy.

- **Application Rule: sip-trunk** (created in Section 7.4.1).
- **Border Rule: default.**
- **Media Rule: enterprise med rule** (created in Section 7.4.2.1).
- **Security Rule: default-low.**
- **Signaling Rule: enterprise sig rule** (created in Section 7.4.3.1).

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

The screenshot shows the 'Policy Groups: enterprise policy' interface. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area displays a list of policy groups, with 'enterprise policy' selected and highlighted in red. Below the list, a 'Policy Group' summary table is shown.

Order	Application	Border	Media	Security	Signaling	
1	sip-trunk	default	enterprise med rule	default-low	enterprise sig rule	Edit

7.4.5 Endpoint Policy Groups – AT&T Connection

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

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

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

The screenshot shows the 'Policy Groups: att-policy-group' interface. The navigation menu on the left has 'att-policy-group' highlighted in red. The main area displays a list of policy groups, with 'att-policy-group' selected and highlighted in red. Below the list, a 'Policy Group' summary table is shown.

Order	Application	Border	Media	Security	Signaling	
1	sip-trunk	default	att med rule	default-low	att sig rule	Edit

7.5 Device Specific Settings

7.5.1 Network Management

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

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

The screenshot shows the 'Network Management: SBCE' page. On the left is a sidebar menu with 'Network Management' selected. The main content area has two tabs: 'Interfaces' (active) and 'Networks'. The 'Interfaces' tab displays a table with the following data:

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

An 'Add VLAN' button is located in the top right corner of the table.

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

The screenshot shows the 'Network Management: SBCE' page with the 'Networks' tab selected. The table displays IP provisioning details for interfaces A1 and B1:

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Inside-A1	10.64.91.1	255.255.255.0	A1	10.64.91.40, 10.64.91.41	Edit	Delete
Outside-B1	192.168.80.1	255.255.255.128	B1	192.168.80.43	Edit	Delete

An 'Add' button is located in the top right corner of the table.

7.5.2 Advanced Options

In **Section 7.5.3**, the media UDP port ranges required by AT&T are configured (**16384 – 32767**). However, by default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be defined in **Section 7.5.3**.

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

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

Step 3 - In the **Signaling Port Range** row, change the range to **12000 – 16380**

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

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

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

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

Advanced Options: SBCE

Devices
SBCE

CDR Listing | Feature Control | SIP Options | Network Options | **Port Ranges** | RTP Monitoring | Load Monitoring

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

Port Range Configuration

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

Save

7.5.3 Media Interfaces

As mentioned in **Section 7.4.2**, the IPTF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the IPTF service.

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

Step 2 - Select **Media Interface**.

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

- **Name:** **Inside-Media-TollFree**.
- **IP Address:** **10.64.91.41** (Avaya SBCE A1 IP address).
- **Port Range:** **16384 – 32767**.

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

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

- **Name:** **Outside-Media**.
- **IP Address:** **192.168.80.43** (Avaya SBCE B1 IP address).
- **Port Range:** **16384 – 32767**.

Step 6 - Click **Finish** (not shown). Note that changes to these values require an application restart (see **Section 7.1**). The completed **Media Interface** screen in the shared test environment is shown below.

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ PPM Services
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
  Network Management
  Media Interface
  Signaling Interface
  End Point Flows
  Session Flows
  ‣ DMZ Services
  TURN/STUN Service
  SNMP
  Syslog Management
  Advanced Options

Media Interface: SBCE

Devices
SBCE

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP Network	Port Range	Edit	Delete
Inside-Media-TollFree	10.64.91.41 Inside-A1 (A1, VLAN 0)	16384 - 32767	Edit	Delete
Outside-Media	192.168.80.43 Outside-B1 (B1, VLAN 0)	16384 - 32767	Edit	Delete

7.5.4 Signaling Interface

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

Step 2 - Select **Signaling Interface**.

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

- **Name:** Inside-Sig-TollFree-41.
- **IP Address:** 10.64.91.41 (Avaya SBCE A1 IP address).
- **TLS Port:** 5061.
- **TLS Profile:** sbc40-server.

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

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

- **Name:** Outside-Signaling.
- **IP Address:** 192.168.80.43 (Avaya SBCE B1 IP address).
- **UDP Port:** 5060.

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

The screenshot shows the 'Signaling Interface: SBCE' configuration page. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The 'Signaling Interface' option is highlighted. The main content area has a tab for 'Signaling Interface' and a warning message: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table with columns: Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, TLS Profile, and Edit/Delete links. The table contains two entries: 'Inside-Sig-TollFree-41' with IP 10.64.91.41 and TLS Port 5061, and 'Outside-Signaling' with IP 192.168.80.43 and UDP Port 5060.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Inside-Sig-TollFree-41	10.64.91.41 Inside-A1 (A1, VLAN 0)	---	---	5061	sbc40-server	Edit	Delete
Outside-Signaling	192.168.80.43 Outside-B1 (B1, VLAN 0)	---	5060	---	None	Edit	Delete

7.5.5 Endpoint Flows – For Enterprise

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

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

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

- **Name:** SM Flow Toll Free
- **Server Configuration:** EnterpriseCallServer (Section 7.3.3)
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Outside-Signaling (Section 7.5.4)
- **Signaling Interface:** Inside-Sig-TollFree-41 (Section 7.5.4)
- **Media Interface:** Inside-Media-TollFree (Section 7.5.3)
- **End Point Policy Group:** enterprise policy (Section 7.4.4)
- **Routing Profile:** To ATT IPTF (Section 7.3.6)
- **Topology Hiding Profile:** Enterprise-Topology (Section 7.3.7)
- Let other values default

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

View Flow: SM Flow Toll Free

Criteria	
Flow Name	SM Flow Toll Free
Server Configuration	EnterpriseCallServer
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside-Signaling

Profile	
Signaling Interface	Inside-Sig-TollFree-41
Media Interface	Inside-Media-TollFree
Secondary Media Interface	None
End Point Policy Group	enterprise policy
Routing Profile	To ATT IPTF
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any

7.5.6 Endpoint Flows – For AT&T

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

- **Name:** ATT-IPTF
- **Server Configuration:** ATT-TollFree-trk-svr (Section 7.3.4)
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Inside-Sig-TollFree-41 (Section 7.5.4)
- **Signaling Interface:** Outside-Signaling (Section 7.5.4)
- **Media Interface:** Outside-Media (Section 7.5.3)
- **End Point Policy Group:** att-policy-group (Section 7.4.5)
- **Routing Profile:** To SM (Section 7.3.5)
- **Topology Hiding Profile:** SIP-Trunk-Topology (Section 7.3.8)

View Flow: ATT IPTF			
Criteria		Profile	
Flow Name	ATT IPTF	Signaling Interface	Outside-Signaling
Server Configuration	ATT-TollFree-trk-svr	Media Interface	Outside-Media
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	att-policy-group
Remote Subnet	*	Routing Profile	To SM
Received Interface	Inside-Sig-TollFree-41	Topology Hiding Profile	SIP-Trunk-Topology
		Signaling Manipulation Script	None
		Remote Branch Office	Any

8 Verification Steps

The following steps may be used to verify the configuration:

8.1 AT&T IP Toll Free 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.

8.2 Avaya Aura® Communication Manager

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

- Tracing a SIP trunk.
 - a. From the Communication Manager console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., 602). Note that in the trace shown below, Session Manager has previously converted the IPTF DNIS number included in the Request URI, to the Communication Manager VDN 71060, before sending the INVITE to Communication Manager.

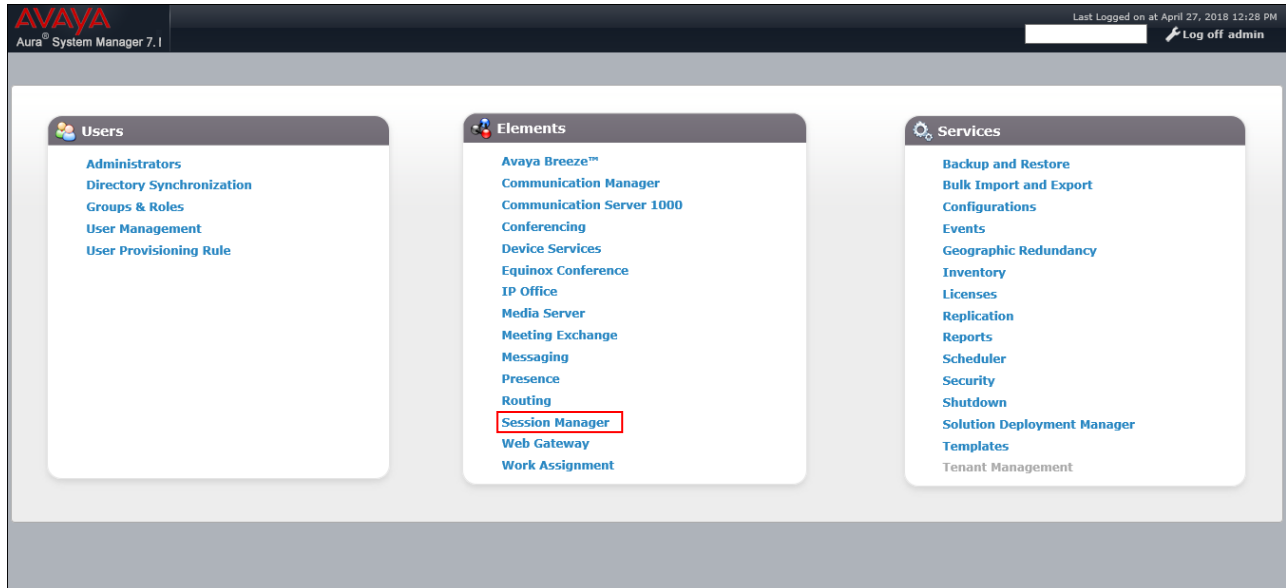
```
list trace tac *04                                     Page 1
LIST TRACE
time          data
10:07:02 TRACE STARTED 04/10/2017 CM Release String cold-00.0.441.0-23523
10:07:27 SIP<INVITE sip:71060@avayalab.com SIP/2.0
10:07:27      Call-ID: 2c36d935b7113b662d50240d11ec4e78
10:07:27      active trunk-group 4 member 1      cid 0xc90
10:07:27      0 0 ENTERING TRACE cid 3216
10:07:27      60 1 vdn e71060 bsr appl 0 strategy 1st-found override n
10:07:27      60 1 wait 2 secs hearing ringback
10:07:27 SIP>SIP/2.0 180 Ringing
10:07:27      Call-ID: 2c36d935b7113b662d50240d11ec4e78
10:07:27      dial 71060
10:07:27      ring vector 60      cid 0xc90
10:07:27      G729 ss:off ps:30
10:07:27      rgn:4 [10.64.91.41]:16580
10:07:27      rgn:1 [10.64.91.60]:6128
10:07:29      60 2 collect 1 digits after annnc 11001 for none
```

- 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***.

8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

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



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

In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **8** Entities defined in the shared test environment.

The screenshot displays the Session Manager Dashboard. The left sidebar contains a navigation menu with options like Dashboard, Session Manager Administration, Global Settings, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, and System Tools. The main content area shows the 'Session Manager Dashboard' with a sub-header 'This page provides the overall status and health summary of each administered Session Manager.' Below this is a section titled 'Session Manager Instances' with filters for Service State, Shutdown System, and EASG. A table lists the instances, with one instance 'SessionManager' highlighted. The table columns include checkboxes, Name, 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.

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
<input type="checkbox"/>	SessionManager	Core	✓	0/0/0	Up	Accept New Service	2/14	0	5/6	⚠	✓	Normal	Enabled	7.1.2.0.712004

Step 3 - Clicking on the **2/14** entry (shown above) in the **Entity Monitoring** column, results in the following display:

Home / Elements / Session Manager / Dashboard									
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: SessionManager									
Summary View									
14 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	10.64.91.54	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Breeze	IPv4	10.64.91.17	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG1	IPv4	10.64.91.65	5081	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG2	IPv4	10.64.91.65	5071	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG3	IPv4	10.64.91.65	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG4	IPv4	10.64.91.65	5064	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG5	IPv4	10.64.91.65	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CS1000	IPv4	10.80.140.103	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
<input type="radio"/>	IP500	IPv4	10.64.19.70	5061	TLS	FALSE	DOWN	408 Request Timeout	DOWN
<input type="radio"/>	Presence	IPv4	10.64.91.17	5061	TLS	FALSE	UP	200 OK	UP
<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"/>	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 – 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.

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

8.4 Avaya Session Border Controller for Enterprise Verification

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

The screenshot displays the Avaya SBCE dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo. A left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is divided into several sections: 'Information' (System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (EMS, SBCE), 'Active Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (highlighted with a red box, showing three incidents), and 'Notes' (No notes found).

Information	
System Time	02:00:42 PM MDT
Version	7.2.1.0-05-14222
Build Date	Tue Oct 31 00:06:46 UTC 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	06/04/2018 13:23:05 MDT
Failed Login Attempts	0

Installed Devices	
EMS	
SBCE	

Incidents (past 24 hours)	
SBCE	Heartbeat Successful, Server is UP
SBCE	Heartbeat Failed, Server is Down
SBCE	Heartbeat Failed, Server is Down

8.4.1 Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

Step 1 - Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**.

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

- Select the desired **Interface** from the drop-down menu (e.g., **All**).
- Specify the **Maximum Number of Packets to Capture** (e.g., **10000**).
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
- Click **Start Capture** to begin the trace.

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

Trace: SBCE

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

Devices

SBCE

Packet Capture

Captures

Packet Capture Configuration

Status

Ready

Interface

B1

Local Address
IP[:Port]

All

Remote Address
,,Port, IP, IP:Port

*

Protocol

All

Maximum Number of Packets to Capture

10000

Capture Filename
Using the name of an existing capture will overwrite it.

TEST.pcap

Start Capture

Clear

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

Trace: SBCE

Devices

SBCE

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

B1

Local Address
IP[:Port]

All

Remote Address
,,Port, IP, IP:Port

*

Protocol

All

Maximum Number of Packets to Capture

10000

Capture Filename
Using the name of an existing capture will overwrite it.

TEST.pcap

Stop Capture

Step 3 - Run the test.

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

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

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

Trace: SBCE

Devices

SBCE

Packet Capture

Captures

Last Modified

Descending

Sort

Reset

Refresh

File Name	File Size (bytes)	Last Modified	
TEST_20180604140526.pcap	200,704	June 4, 2018 2:07:23 PM MDT	Delete

DDT; Reviewed:
SPOC 7/9/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

87 of 90
CM71SM71SBC72TF

9 Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1, and the Avaya Session Border Controller for Enterprise 7.2, can be configured to interoperate successfully with the AT&T IP Toll Free service, 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.

10 References

The Avaya product documentation is available at <http://support.avaya.com> unless otherwise noted.

Avaya Aura® Session Manager/System Manager

- [1] Deploying Avaya Aura® Session Manager, Release 7.1.2, Issue 4, December 2017
- [2] Administering Avaya Aura® Session Manager, Release 7.1.2, Issue 4, March 2018
- [3] Deploying Avaya Aura® System Manager, Release 7.1.2, Issue 6, March 2018
- [4] Administering Avaya Aura® System Manager for Release 7.1.2, Issue 11, March 2018

Avaya Aura® Communication Manager

- [5] Deploying Avaya Aura® Communication Manager, Release 7.1.2, Issue 3, December 2017
- [6] Administering Avaya Aura® Communication Manager, Release 7.1.2, Issue 5, February 2018
- [7] Administering Avaya G450 Branch Gateway, Release 7.1.2, Issue 2, December 2017
- [8] Deploying and Updating Avaya Aura® Media Server Appliance, Release 7.8, Issue 4, December 2017
- [9] Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager, August 2015
- [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 7.2.2, Issue 9, April 2018
- [12] Deploying Avaya Session Border Controller for Enterprise, Release 7.2.2, Issue 7, April 2018

AT&T IP Toll Free Service:

- AT&T IP Toll Free Service description - <http://www.business.att.com/enterprise/Service/voice-services/null/ip-toll-free/>
- AT&T IP Toll Free service support: (800) 325-5555.

©2018 Avaya Inc. All Rights Reserved.

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

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