Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 7.0.1, Avaya Aura® Session Manager 7.0.1, and Avaya Session Border Controller for Enterprise 7.1, with AT&T IP Flexible Reach - Enhanced Features Service using IPv6 – Issue 1.1

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 7.0.1, Avaya Aura® Session Manager 7.0.1, and Avaya Session Border Controller for Enterprise 7.1, with the AT&T IP Flexible Reach - Enhanced Features service, using IPv6 and AT&T's **AVPN** or **MIS/PNT** transport connections.

The AT&T Flexible Reach is one of the many SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features which are not part of IP Flexible Reach service.

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

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

Table of Contents

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 7.0.1 (IPv4 address), Avaya Aura® Session Manager 7.0.1 (IPv4 address), Avaya Aura® System Manager 7.0 (IPv4 address), and Avaya Session Border Controller for Enterprise 7.1 (IPv4/IPv6 address), with the AT&T IP Flexible Reach - Enhanced Features service (IPv6 address) using AVPN or MIS/PNT transport connections.

Avaya Aura® Communication Manager 7.0.1 (Communication Manager) is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya Aura® Session Manager 7.0.1 (Session Manager) is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® System Manager 7.0.1 (System Manager) is the provisioning and management application for Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 7.1 (Avaya SBCE) is the point of connection between Session Manager and the AT&T IP Flexible Reach - Enhanced Features (IPFR-EF) service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling and media for interoperability between IPv4 and IPv6.

The AT&T Flexible Reach service is one of the many SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features which are not part of IP Flexible Reach service. The AT&T IP Flexible Reach - Enhanced Features service utilizes AT&T's AVPN[1] or MIS/PNT[2] transport services.

2. General Test Approach and Test Results

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

The interoperability compliance testing focused on verifying inbound and outbound call flows between IPFR-EF and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, and Avaya SBCE (see **Section 3.2** for call flow examples). The test environment consisted of:

- A simulated enterprise with Communication Manager, Session Manager, System Manager (for Session Manager provisioning), Avaya SBCE, Avaya phones, and fax machines (Ventafax application). Avaya Aura® Messaging (Messaging) is used to provide voicemail capabilities for the CPE.

[1] AVPN supports compressed RTP (cRTP).
[2] MIS/PNT does not support cRTP.

- An IPFR-EF service test lab circuit, to which the simulated enterprise was connected via AVPN transport.

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

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

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

2.1. Interoperability Compliance Testing

Note – Documents used to provision the test environment are listed in **Section 10**. In the following sections, references to these documents are indicated by the notation **[x]**, where *x* is the document reference number.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPFR-EF network. Calls were made between the PSTN, via the IPFR-EF network, and the CPE.

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

- Incoming and outgoing voice calls between PSTN, the IPFR-EF service, Avaya SBCE, Session Manager, and Communication Manager. Avaya SIP telephones (desk and softphone), and H.323 telephones (desk) were used.
- Inbound/Outbound fax calls using T.38.
- Various outbound PSTN destinations were tested including long distance, international, and toll-free.
- Requests for privacy (i.e., caller anonymity) for Communication Manager outbound calls to the PSTN, as well as privacy requests for inbound calls from the PSTN to Communication Manager users.
- SIP OPTIONS messages used to monitor the health of the SIP trunks between the CPE and AT&T.
- Incoming and outgoing calls using the G.729(A & B) and G.711 ULAW codecs.
- Call redirection with Diversion Header.
- Operator assistance and 911 calls.
- Long duration calls.
- DTMF transmission (RFC 2833) for successful PSTN, Communication Manager, and voice mail menu navigation.

- Telephony features such as hold, transfer, and conference.
- Basic Communication Manager EC500 "mobility" calls.
- An Avaya Remote Worker endpoint (an Avaya 9621 SIP telephone) was used in the reference configuration. The Remote Worker endpoint resides on the public side of the Avaya SBCE (IPv4 via a TLS connection), and registers/communicates with Avaya Session Manager via Avaya SBCE as though it was an endpoint residing in the private CPE space.

Note – The configuration of the Remote Worker environment is beyond the scope of this document.

- AT&T IPFR-EF service features such as:
    - Simultaneous Ring
    - Sequential Ring
    - Call Forward – Always
    - Call Forward – Busy
    - Call Forward – Ring No Answer
    - "Blind" and Attended transfers utilizing Refer messaging.

2.2. Test Results

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

1) **IPFR-EF Simultaneous Ring and Sequential Ring - Loss of calling display information on Communication Manager stations**. If the Communication Manager station associated with these IPFR-EF "secondary" number answers the call, the phone may not display all the calling information. By default, Communication Manager expects a display update from the network in the PAI header. However, the subsequent network signaling does not contain a PAI header, and the From header must be used instead.
    a) The recommended workaround is described in **Section 6.8.1**, where Communication Manager will retrieve the display information using the *From* header.

2) **T.38/G.729 fax is limited to 9600bps when using the G4xx Media Gateways.** A G430 Media Gateway is used in the reference configuration. As a result T.38/G.729 fax was limited to 9600 bps. Also note that the sender and receiver of a T.38 fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3.

3) **IPFR-EF Call Forward Always (CFA/CFU) – No ringing heard for Ring Splash reminder**. When Call Forward is activated with the Ring Splash feature (ring reminder on call forward) through the IPFR-EF service, and a call is placed to the primary number, no indication is seen on the CPE endpoint. The c-line in the SDP of the Ring Splash SIP INVITE has a domain name "anonymous.invalid" instead of an IPv6 address, and this was not parsed correctly by the Avaya SBCE. This anomaly is currently under investigation by Avaya. A workaround is to include an Avaya SBCE Signaling Manipulation Rule to change the domain name to an IPv6 address (See **Section 7.3.3**). After the script is applied, the CPE endpoint's call appearance will flash briefly to indicate that the call has been forwarded, but the IPFR-EF service may send a CANCEL before the endpoint has had a chance to provide an audible ring tone.

4) **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 should be specified.

5) **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), Session Manager is provisioned to remove SIP headers not required by the AT&T IPFR-EF service (see **Section 5.3.2**). These headers are:
   a) AV-Correlation-ID, AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Location, Remote-Party-ID, Av-Secure-Indication.

6) **Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64, causing AT&T network issues**. Certain Avaya SIP endpoints (e.g., 9630, 9621, and 9608 models) may generate various Bandwidth headers depending on the call flow. It has been observed that sending these Bandwidth headers may cause issues with AT&T services. Therefore an Avaya SBCE Signaling Manipulation Rule is used to remove these headers (see **Section 7.3.3**).

7) **Alphanumeric characters in IPv6 address** – The Avaya SBCE Server Configuration IP address field is case sensitive. The AT&T IPv6 address needs to be entered using lowercase characters. The Avaya SBCE will not match the source address of incoming SIP packets from AT&T if the IPv6 address is entered using uppercase characters (See **Section 7.3.5**).

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

2.3. Support

For more information on the AT&T IP Flexible Reach service visit:
http://www.business.att.com/enterprise/Service/voice-services/null/sip-trunking/
AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

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

- Communication Manager 7.0.1, System Manager 7.0.1, Session Manager 7.0.1, and Avaya SBCE 7.1. Note that all of these Avaya components ran on a VMware (ESXi 5.5) platform.
- In the reference configuration System Manager provides a common administration interface for centralized management of Session Manager and Communication Manager.
- In the reference configuration, an Avaya G430 Media Gateway and Avaya Aura® Media Server are used. This solution is extensible to other Avaya Media Gateways.
- Avaya desk telephones used are Avaya 96x1 Series IP Telephones (H.323 and SIP), Avaya Equinox™ for Windows (SIP), as well as 2424 Digital Telephones. Avaya SIP endpoints register to Session Manager while Avaya H.323 endpoints register to Communication Manager.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPFR-EF IPv6 service and the enterprise internal IPv4 network.
- The IPFR-EF service Border Element (BE) uses IPv6 and SIP over UDP to communicate with enterprise edge SIP devices, (e.g., the Avaya SBCE in this sample configuration). Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements. In the reference configuration, Session Manager uses IPv4 and SIP over TLS to communicate with Avaya SBCE and with Communication Manager.
- Avaya Aura® Messaging was used in the reference configuration to provide voice mailbox capabilities. This solution is extensible to other messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Testing was performed using an IPFR-EF service test lab circuit.

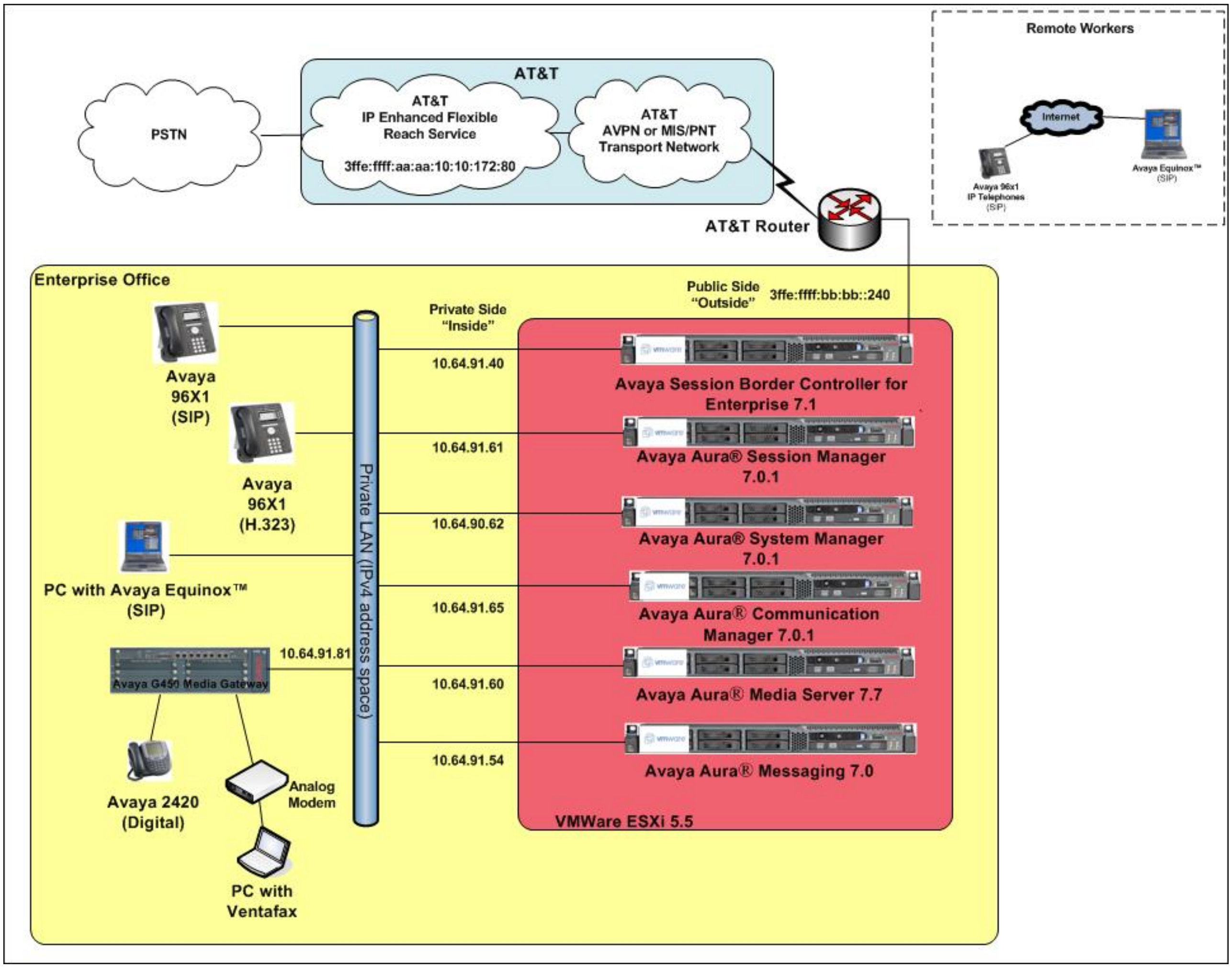


Figure 1: Reference configuration

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are for illustrative purposes only. Customers must obtain and use the specific values for their own configurations.

Note – The IPFR-EF service Border Element IP address and DID/DNIS digits are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DID/DNIS digits as part of the IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura® Session Manager	
IP Address	10.64.91.61
Avaya Aura® Communication Manager	
IP Address	10.64.91.65
Avaya Aura® System Manager	
IP Address	10.64.90.62
Avaya Aura® Messaging	
IP Address	10.64.91.54
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Inside (Private) Interface	10.64.91.40
IP Address of Outside (Public) Interface	3ffe:ffff:bb:bb::240 (see note below)
AT&T Border Element	
IP Address	3ffe:ffff:aa:aa:10:10:172:80

Table 1: Network Values Used in these Application Notes

Note – The Avaya SBCE Outside interface communicates with AT&T Border Elements (BEs) located in the AT&T IP Flexible Reach network. For security reasons, the actual IPv6 addresses of the Avaya SBCE and AT&T BE are not included in this document. However as placeholders in the following configuration sections, the IP address of **3ffe:ffff:bb:bb::240** (Avaya SBCE public interface) and **3ffe:ffff:aa:aa:10:10:172:80** (AT&T BE IPv6 address) are specified.

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

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

3.2.1. Inbound

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

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

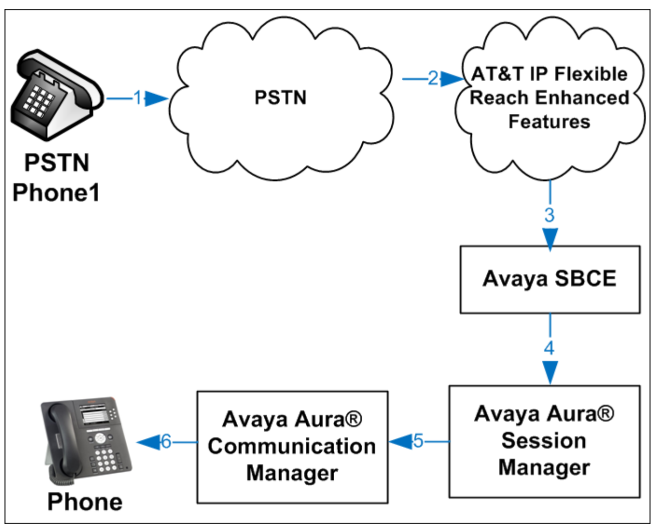


Figure 2: Inbound IPFR-EF Call

3.2.2. Outbound

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

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

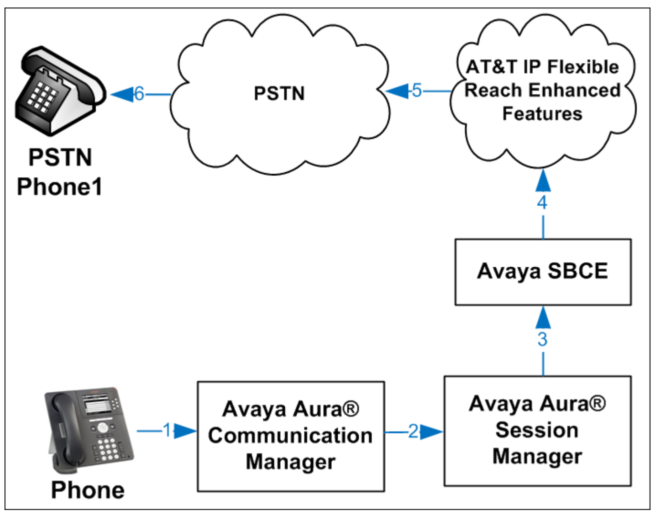


Figure 3: Outbound IPFR-EF Call

3.2.3. Call Forward Re-direction

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

Note – In cases where calls are forwarded to an alternate destination such as an 8xx numbers, the IPFR-EF service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 6.7**).

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager. Communication Manager routes the call to a station.
6. Because the Communication Manager phone has set Call Forward to another IPFR-EF service number, Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network.
7. The IPFR-EF service places a call to the alternate destination, and upon answering Communication Manager connects the calling party to the target party.

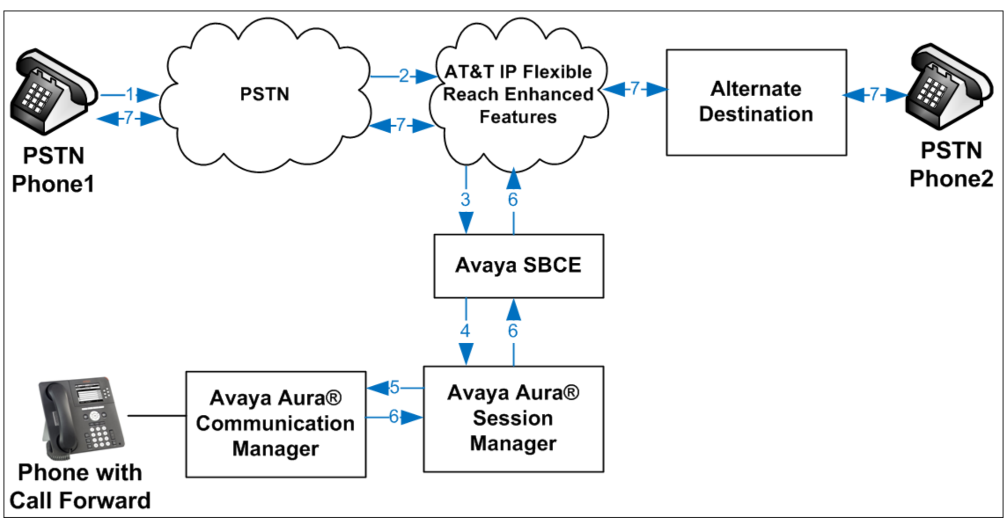


Figure 4: Station Re-directed (e.g., Call Forward) IPFR-EF Call

3.3. AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow

This section describes the call flow for IPFR-EF using SIP Refer to perform Network Based Blind Transfer. The Refer is generated by an inbound call to a Communication Manager Vector. The call scenario illustrated in **Figure 5** below is an inbound IPFR-EF call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a vector. The vector answers the call and, using Refer (*without the replaces parameter*), redirects the call back to the IPFR-EF service for routing to an alternate destination.

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Communication Manager routes the call to a VDN/Vector, which answers the call and plays an announcement, and attempts to redirect the call using a SIP Refer message. The SIP Refer message specifies the alternate destination, and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the IPFR-EF service.
7. IPFR-EF places a call to the alternate destination specified in the REFER, and upon answer, connects the calling party to the alternate party.
8. IPFR-EF clears the call on the redirecting/referring party (Communication Manager).

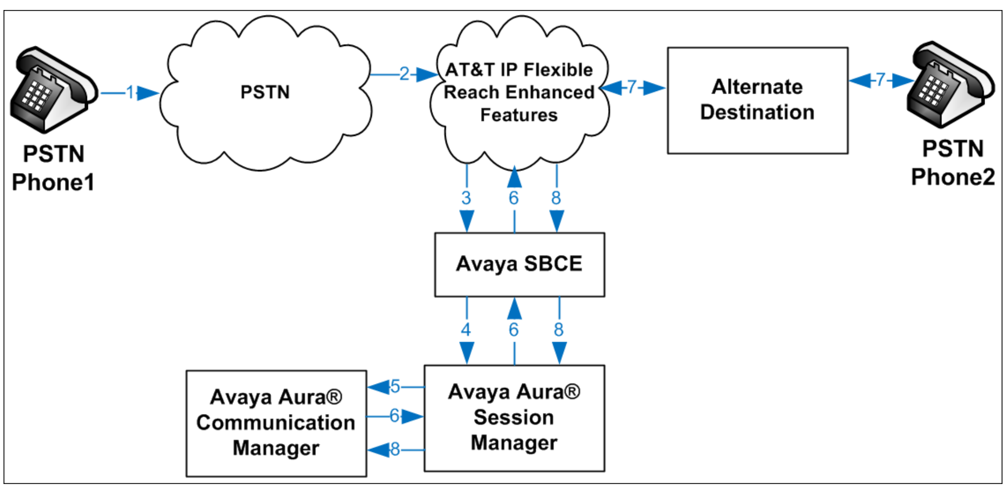


Figure 5: Network Based Blind Transfer Using Refer (Communication Manager Vector)

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

This section describes the call flow for IPFR-EF using SIP Refer to perform an Attended or Unattended Transfer. The call scenario illustrated in **Figure 6** below is an inbound IPFR-EF call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a station. The station answers the call and transfers it back out to a second PSTN destination. Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network. Communication Manager completes the transfer, using Refer (*with the replaces parameter*), to the IPFR-EF service to connect the two active calls together.

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager. Communication Manager routes the call to a station.
6. The station answers the call and then transfers it to a new PSTN destination. Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network. Communication Manager redirects the call using a SIP Refer message when the transfer is completed by the station. The SIP Refer message specifies the active call to replace, and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the IPFR-EF service.
7. IPFR-EF replaces the call with the alternate destination specified in the Refer and connects the calling party to the alternate party.
8. IPFR-EF clears the existing calls to Communication Manager.

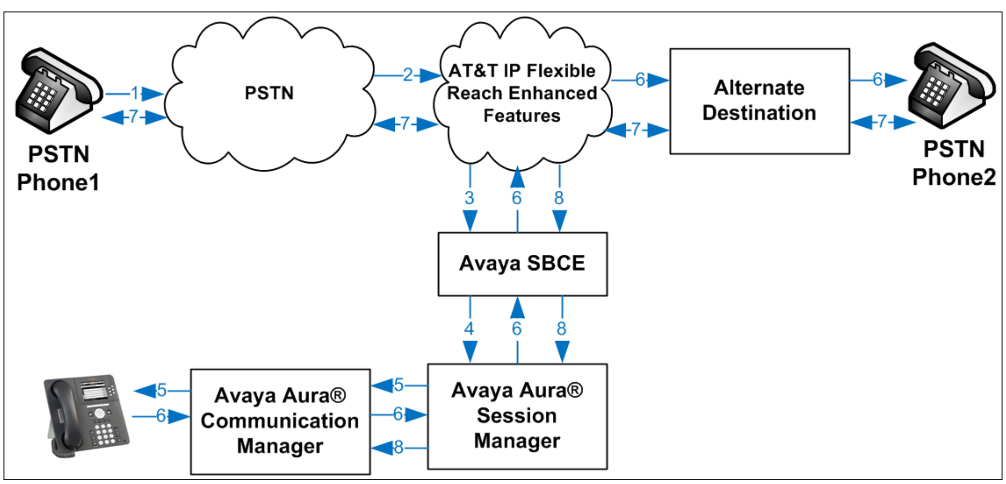


Figure 6: Attended/Unattended Transfer Using Refer (Communication Manager Station)

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
HP Proliant DL360 G7 server	VMware ESXi 5.5
• Avaya Aura® Session Manager	7.0.1.2.701230
• Avaya Aura® System Manager	7.0.1.2.086007
• Avaya Aura® Communication Manager	7.0.1.2.0-R017x.00.0.441.0 (23523)
• Avaya Session Border Controller for Enterprise	7.1.0.1-07-12368
• Avaya Aura® Messaging	7.0-00.0.441.0-017_0004 (SP 0)
• Avaya Aura® Media Server	7.7.0.236
Avaya G430 Media Gateway	g430_sw_37_41_0
Avaya 96x1 IP Telephone	H.323 = 6.6401 SIP = 7.0.1.4.6
Avaya Equinox™ for Windows (SIP)	3.0.0.147
Ventafax Home Version (Windows based Fax device)	7.8.253.611

Table 2: Equipment and Software Versions

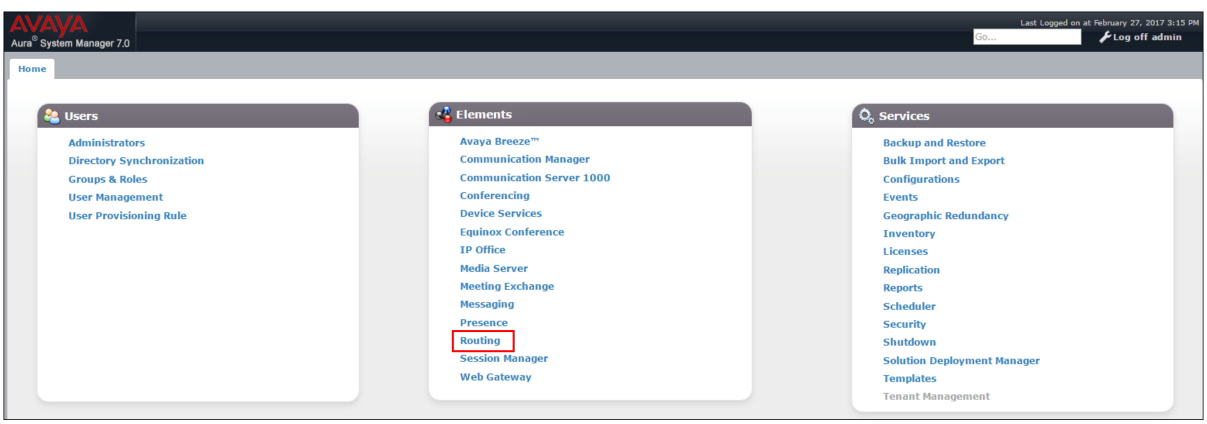
5. Configure Avaya Aura® Session Manager

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult **[1] - [4]** for further details.

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

- Define a SIP Domain.
- Define a Location for Customer Premises Equipment (CPE).
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Avaya SBCE, and Messaging.
- Define SIP Entities corresponding to Session Manager, Communication Manager, the Avaya SBCE, and Messaging.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, and Messaging, as well as the SIP trunks between the Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, Messaging, and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for inbound and outbound call routing.
- Verify TLS Certificates.

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



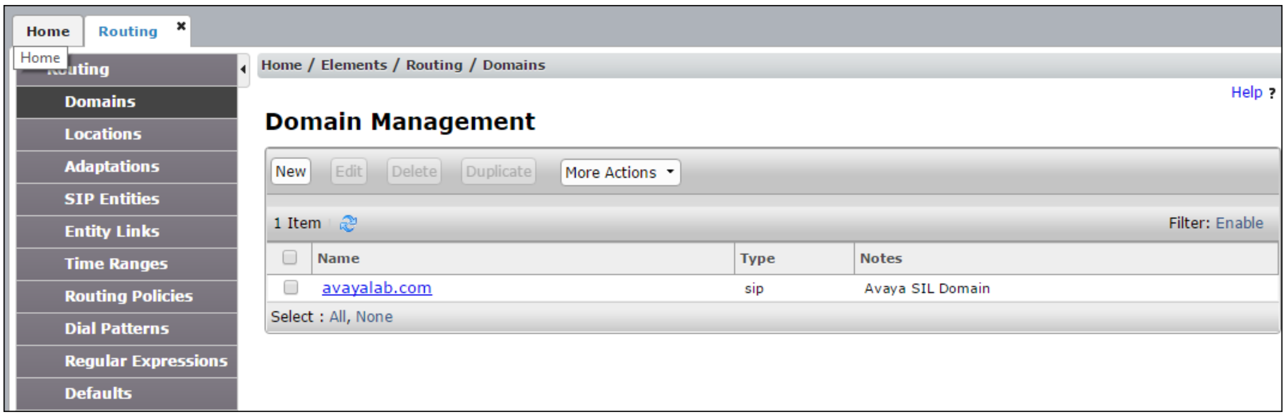
5.1. SIP Domain

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.



5.2. Locations

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

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

5.2.1. Main Location

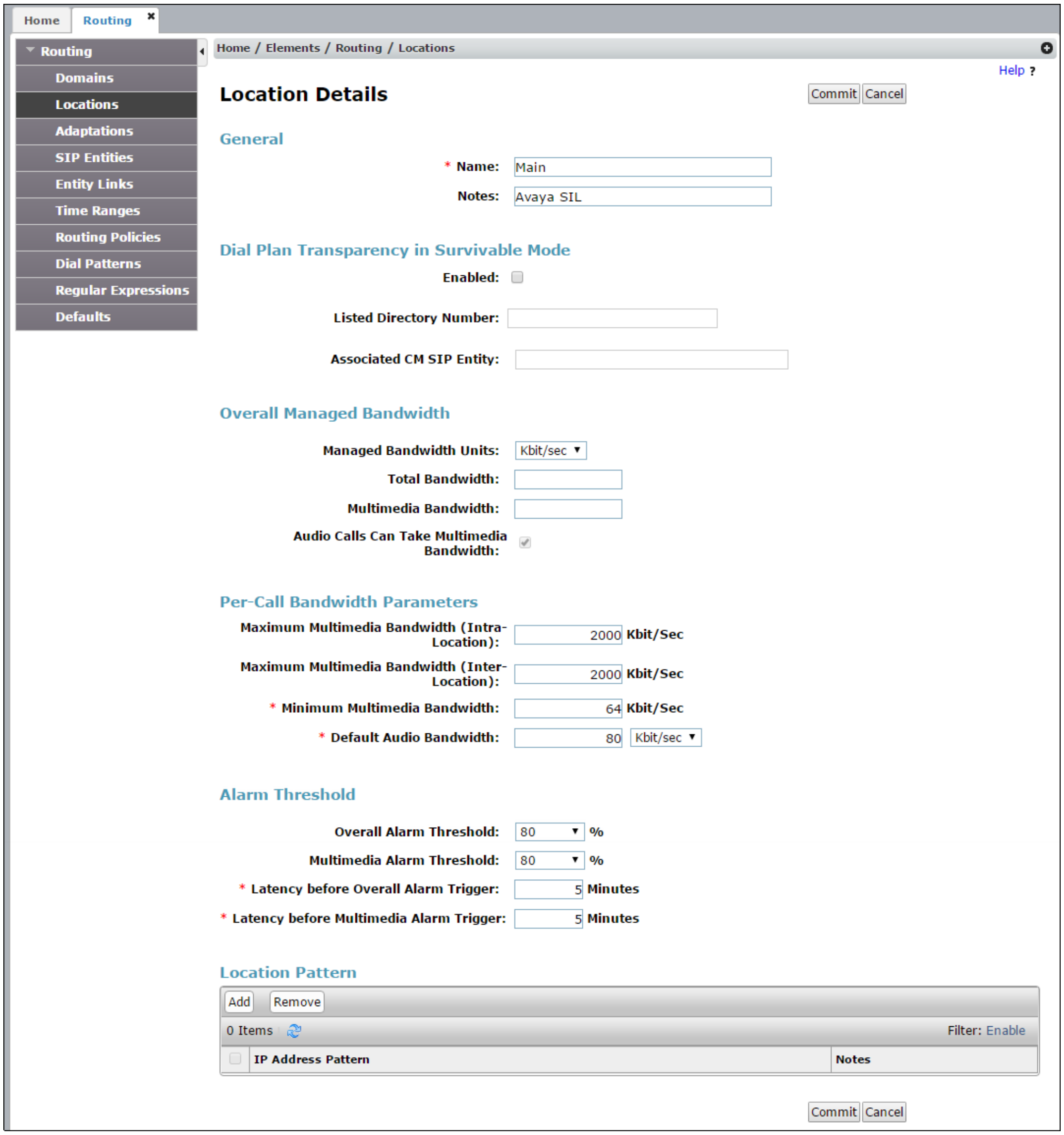
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

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

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern:** Leave blank.
- **Notes:** Add a brief description.

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



5.2.2. CM-TG-5 Location

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

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

5.2.3. Common Location

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

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

5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T. In the reference configuration the following Adaptations were used:

- Calls from AT&T (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager extensions.
    - The AT&T DNIS number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDN.
- Calls to AT&T (**Section 5.3.2**) - Modification of SIP messages sent by Communication Manager extensions.
    - The History-Info header is removed automatically by the **ATTAdapter**.
    - Avaya SIP headers not required by AT&T are removed (see **Section 2.2, Item 5)**).

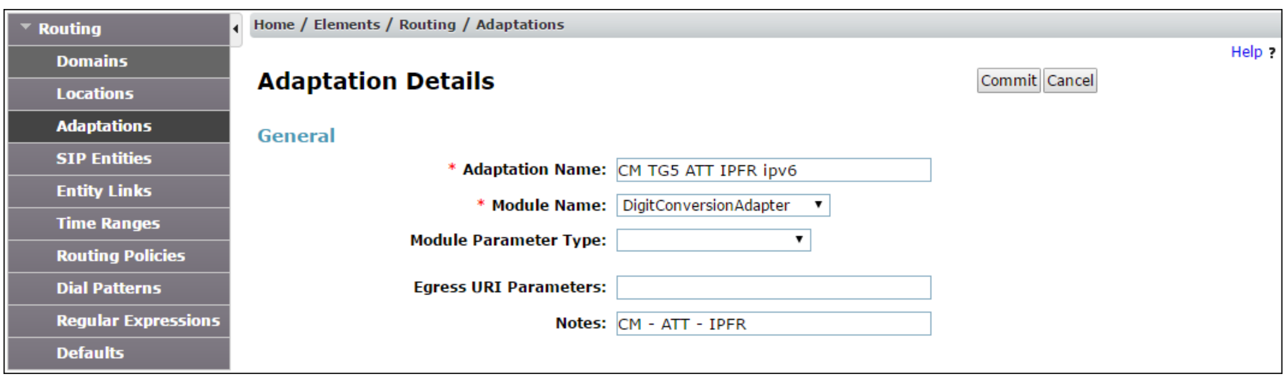
5.3.1. Adaptation for Avaya Aura® Communication Manager Extensions

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager extensions from AT&T.

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

Step 2 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **CM TG5 ATT IPFR ipv6**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).



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

1. **Example 1 – destination extension**: 7325552753 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension 19001.
    - Enter **7325552753** in the **Matching Pattern** column.
    - Enter **10** in the **Min/Max** columns.
    - Enter **10** in the **Delete Digits** column.
    - Enter **14008** in the **Insert Digits** column.

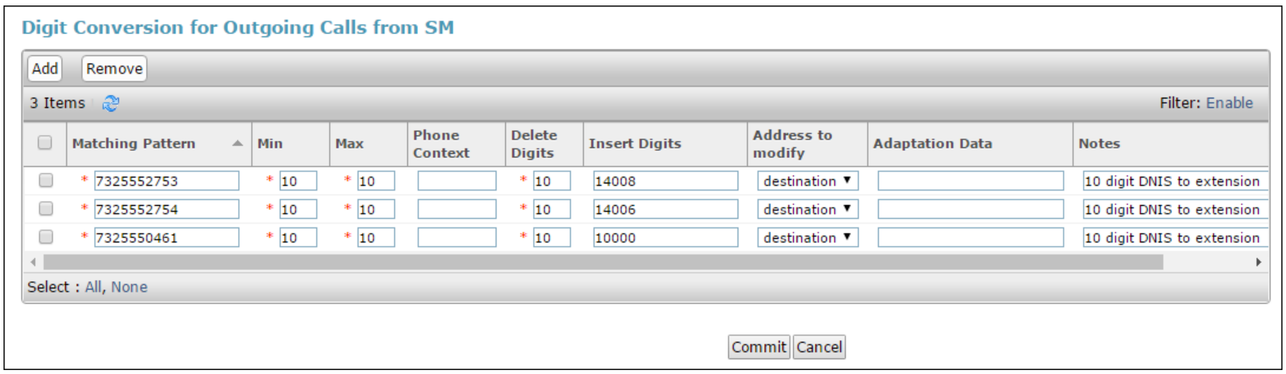
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 - Repeat **Step 3** for all additional AT&T DNIS numbers/Communication manager extensions.

Step 5 - Click on **Commit**.

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

Note – In the reference configuration, the AT&T IPFR-EF service delivered 10-digit DNIS numbers.



5.3.2. Adaptation for the AT&T IP Flexible Reach – Enhanced Features Service

The Adaptation administered in this section is used for modification of SIP messages from Communication Manager to AT&T. Repeat the steps in **Section 5.3.1** with the following changes.

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

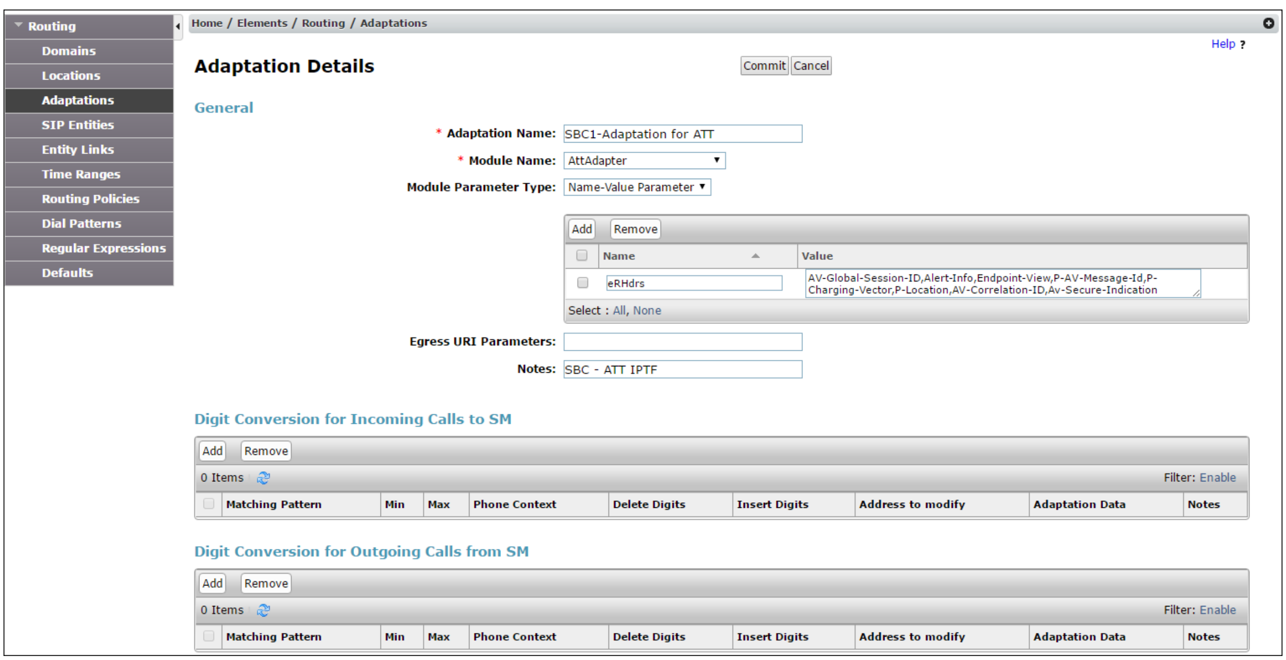
1. A descriptive **Name**, (e.g., **SBC1-Adaptation for ATT**).
2. Select **AttAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **AttAdapter**). The AttAdapter will automatically remove History-Info headers, (which the IPFR-EF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

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

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

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

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



5.4. SIP Entities

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

- Session Manager (**Section 5.4.1**).
- Communication Manager for AT&T trunk access (**Section 5.4.2**) – This entity, and its associated Entity Link (using TLS with port 5065), is for calls to/from AT&T and Communication Manager via the Avaya SBCE.
- Communication Manager for local trunk access (**Section 5.4.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager, as well as calls to Messaging.
- Avaya SBCE (**Section 5.4.4**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from the IPFR-EF service via the Avaya SBCE.
- Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Messaging.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5065), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the AT&T IPFR-EF service uses UDP/5060 per AT&T requirements.

5.4.1. Avaya Aura® Session Manager SIP Entity

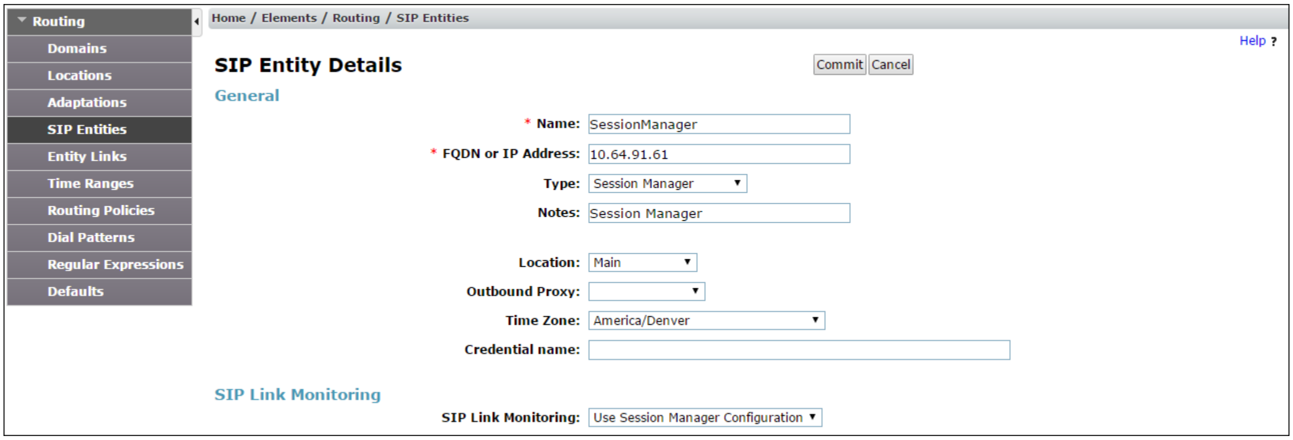
Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

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

- **Name –** Enter a descriptive name (e.g., **SessionManager**).
- **FQDN or IP Address –** Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.61**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 5.2.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.

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

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



Step 4 - Scrolling down to the **Listen Port** section of the **SIP Entity Details** page, 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**)

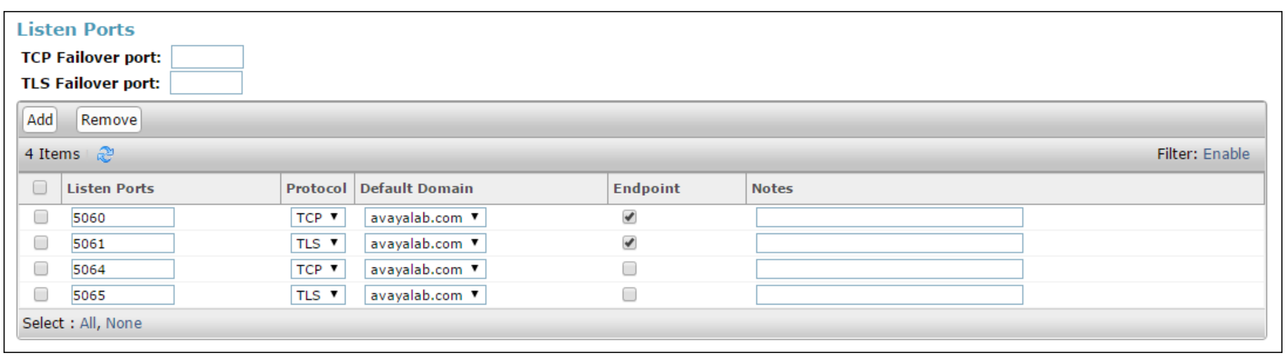
Step 5 - Repeat **Step 4** to provision entries for any other listening ports used by Session Manager, for example:

- **5060** for **Port** and **TCP** for **Protocol**
- **5064** for **Port** and **TCP** for **Protocol**
- **5065** for **Port** and **TLS** for **Protocol**

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

Step 7 - Click on **Commit**.

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



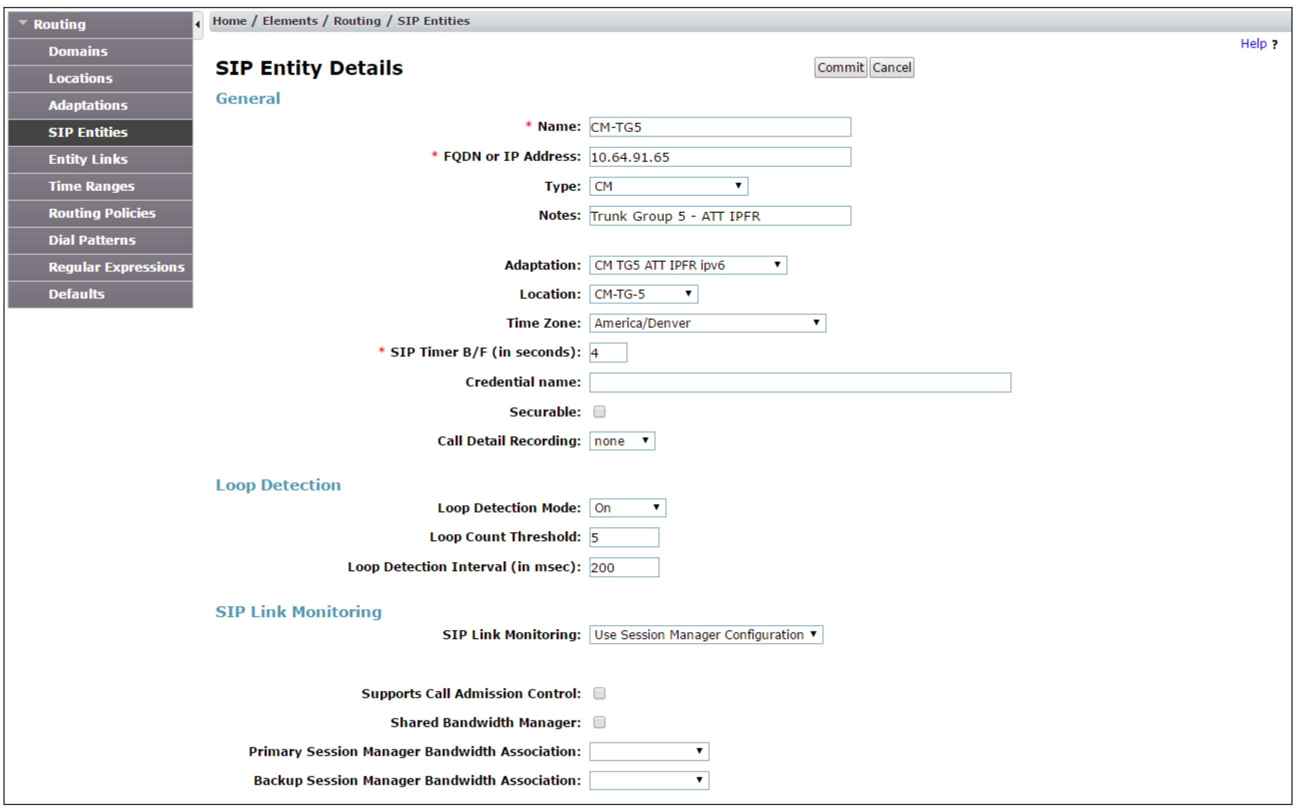
5.4.2. Avaya Aura® Communication Manager SIP Entity – Public Trunk

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

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

- **Name** – Enter a descriptive name (e.g., **CM-TG5**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 6.4** (e.g., **10.64.91.65**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM TG5 ATT IPFR ipv6** 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**.



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

5.4.4. Avaya Session Border Controller for Enterprise SIP Entity

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

- **Name –** Enter a descriptive name (e.g., **SBCE-ipv6**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.40**, see **Section 7.5.1**).
- **Type –** Select **SIP Trunk**.
- **Adaptations –** Select Adaptation **SBC1-Adaptation for ATT** (**Section 5.3.2**).

5.4.5. Avaya Aura® Messaging SIP Entity

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

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

5.5. Entity Links

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

- Session Manager to Communication Manager Public trunk (**Section 5.5.1**).
- Session Manager to Communication Manager Local trunk (**Section 5.5.2**).
- Session Manager to Avaya SBCE (**Section 5.5.3**).
- Session Manager to Messaging (**Section 5.5.4**).

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

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

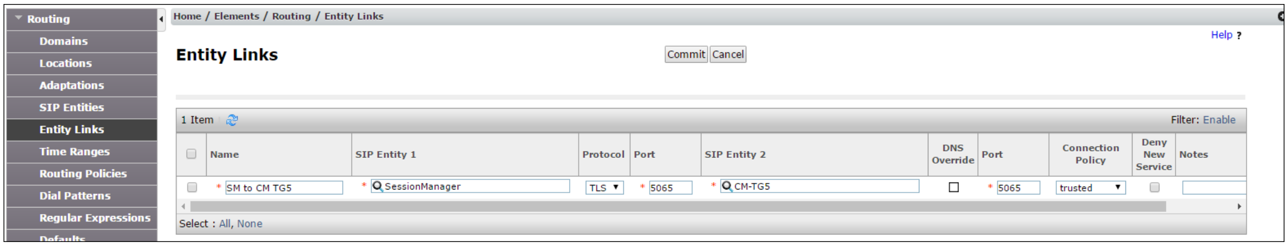
5.5.1. Entity Link to Avaya Aura® Communication Manager – Public Trunk

Step 1 - In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM-TG5**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager (e.g., **SessionManager**).
- **Protocol** – Select **TLS** (see **Section 6.8.1**).

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

Step 3 - Click on **Commit**.



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

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

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

5.5.3. Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE

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

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to SBCE-IPv6**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE entity (e.g., **SBCE-ipv6**).
- **SIP Entity 2 Port** – Enter **5061**.

5.5.4. Entity Link to Avaya Aura® Messaging

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

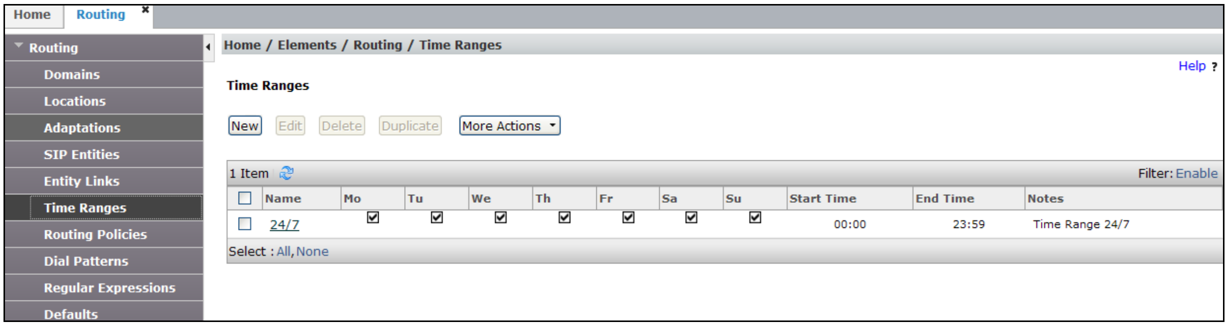
- **Name** – Enter a descriptive name for this link to Messaging (e.g., **SM to AAM**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.5** for the Aura® Messaging entity (e.g., **Aura Messaging**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 6.8.2**).

5.6. Time Ranges – (Optional)

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

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

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



5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (**Section 5.7.1**).
- Inbound calls to Aura® Messaging (**Section 5.7.2**).
- Outbound calls to AT&T/PSTN (**Section 5.7.3**).

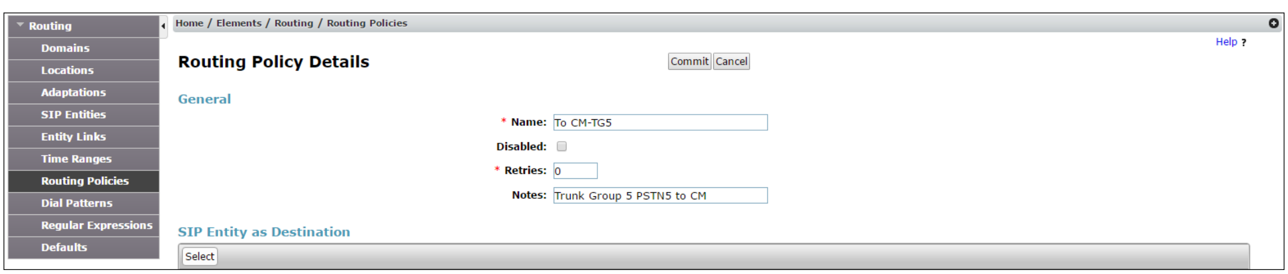
5.7.1. Routing Policy for AT&T Routing to Avaya Aura® Communication Manager

This Routing Policy is used for inbound calls from AT&T.

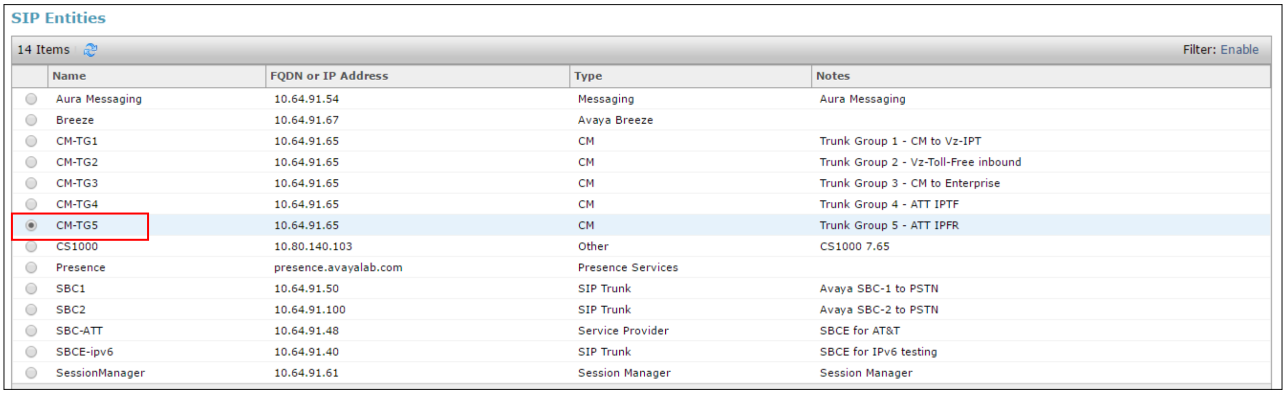
Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **To CM-TG5**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the **SIP Entities** list page will open.

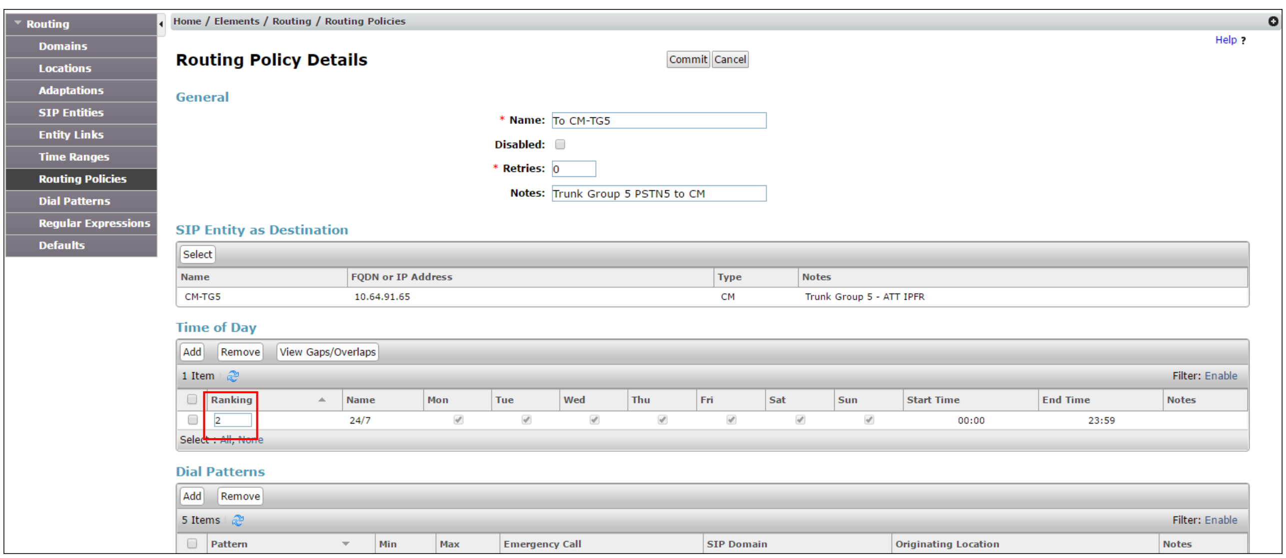


Step 4 - In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**CM-TG5**), and click on **Select**.



Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**.
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.
Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, enter a **Ranking** of **2**.
Step 8 - No **Regular Expressions** were used in the reference configuration.
Step 9 - Click on **Commit**.

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



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

This routing policy is for inbound calls to Aura® Messaging for message retrieval. Repeat the steps in **Section 5.7.1** with the following differences:

- Enter a descriptive **Name** (e.g., **To AAM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.5** for Aura® Messaging (e.g., **AAM**).

5.7.3. Routing Policy for Outbound Calls to AT&T

This Routing Policy is used for Outbound calls to AT&T. Repeat the steps in **Section 5.7.1** with the following differences:

- Enter a descriptive **Name** for routing calls to the AT&T IPFR-EF service via the Avaya SBCE (e.g., **To SBCE-IPv6**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE SIP Entity (e.g., **SBCE-ipv6**).

5.8. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:

- Inbound PSTN calls via the IPFR-EF service to Communication Manager (**Section 5.8.1**).
- Outbound calls to AT&T (**Section 5.8.2**).
- Inbound calls to Aura® Messaging (**Section 5.8.4**).

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

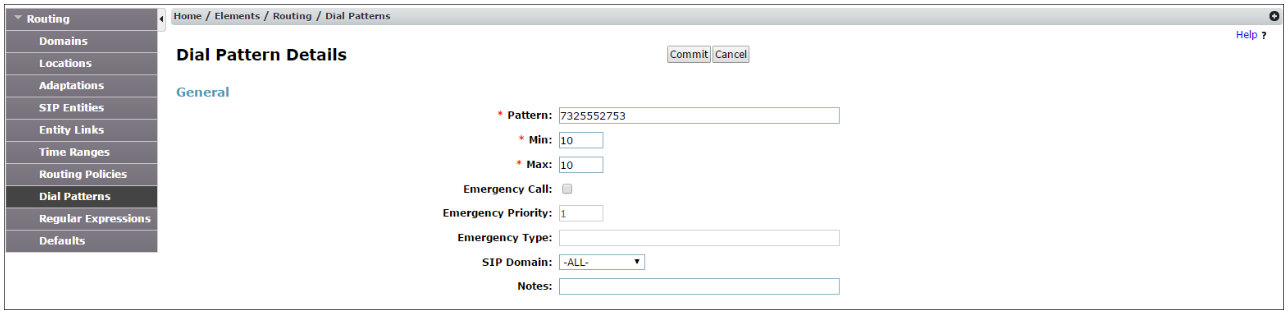
In the reference configuration inbound calls from the IPFR-EF service sent 10 DNIS digits in the SIP Request URI (for security purposes, these digits are represented in this document as 732**555**xxxx). The DNIS pattern must be matched for further call processing. Depending on customer deployments, the IPFR-EF service may send different DNIS digit lengths.

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

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

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

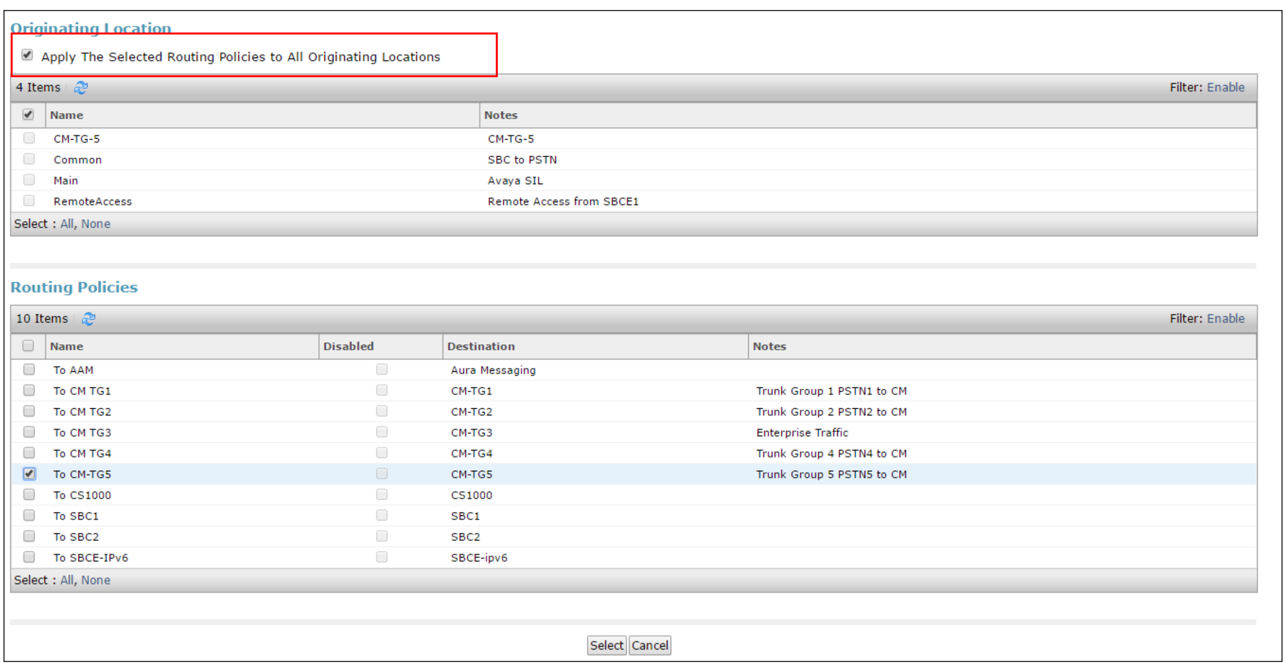
- **Pattern** – Enter **7325552753**. Note – The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 732-555-xxxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.



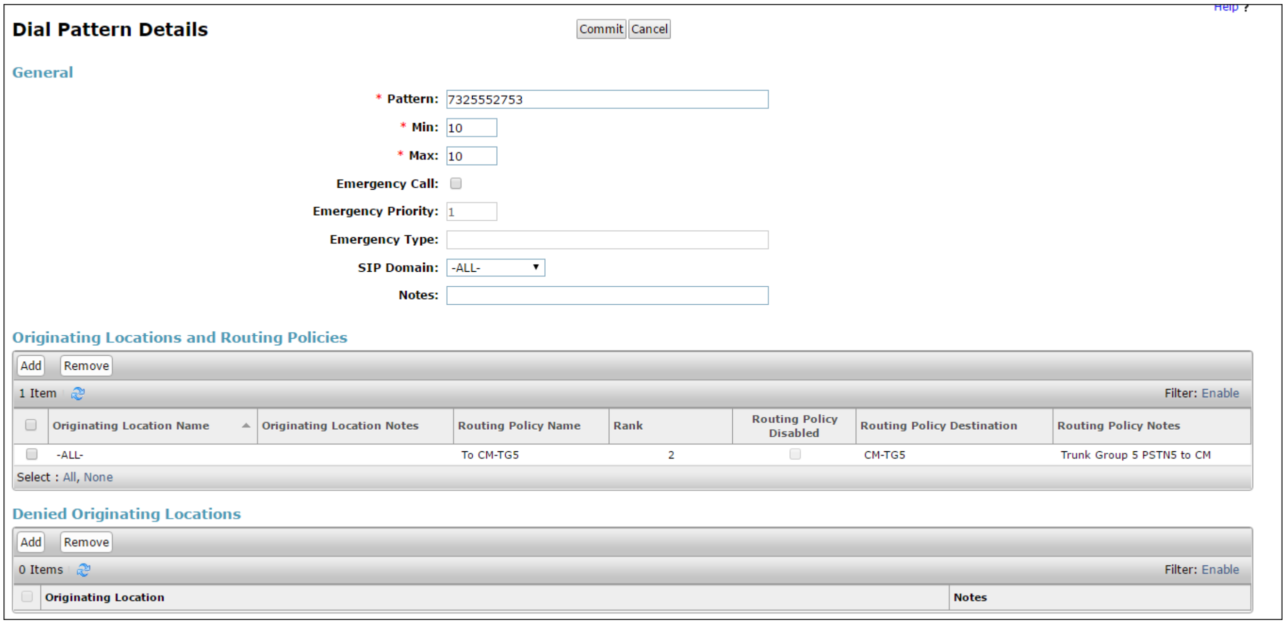
Step 3 - Scrolling down to the **Originating Location and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

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

Step 5 - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7.1** (e.g., **To CM-TG5**), and click on **Select**.



Step 6 - Returning to the Dial Pattern Details page click on **Commit**.
Step 7 - Repeat **Steps 1-6** for any additional inbound dial patterns from AT&T.

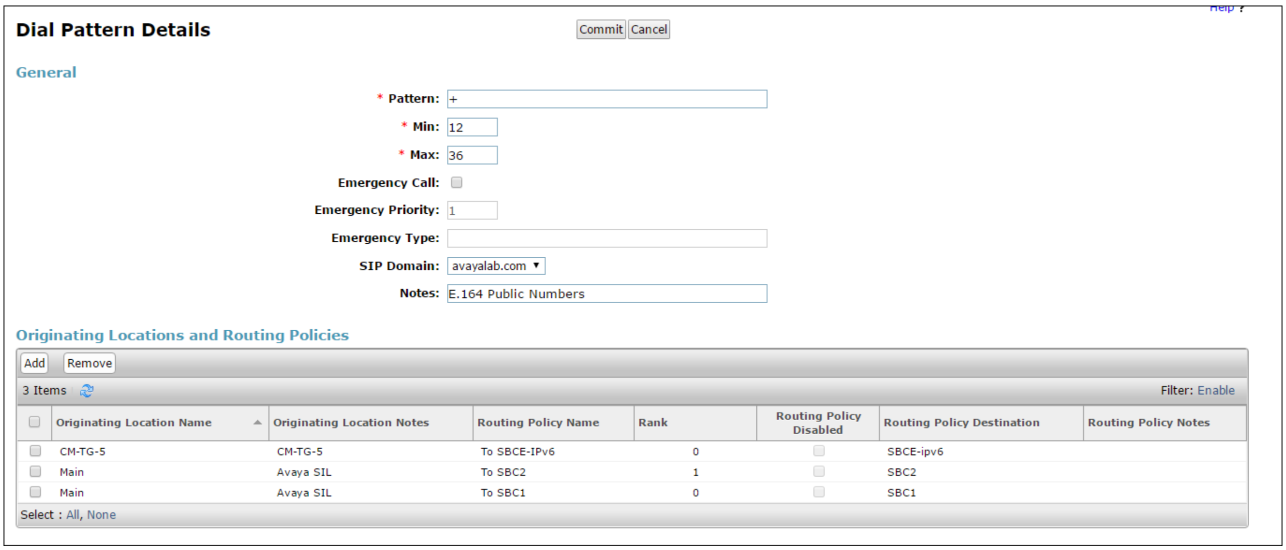


5.8.2. Matching Outbound Calls to AT&T

In this section, Dial Patterns are administered for all outbound calls to AT&T. In the reference configuration 1xxxyyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes ***7** and ***9** (e.g., *71yyyzzzxxxx & *91yyyzzzxxxx) are specified.

Step 1 - Repeat the steps shown in **Section 5.8.1**, with the following changes:

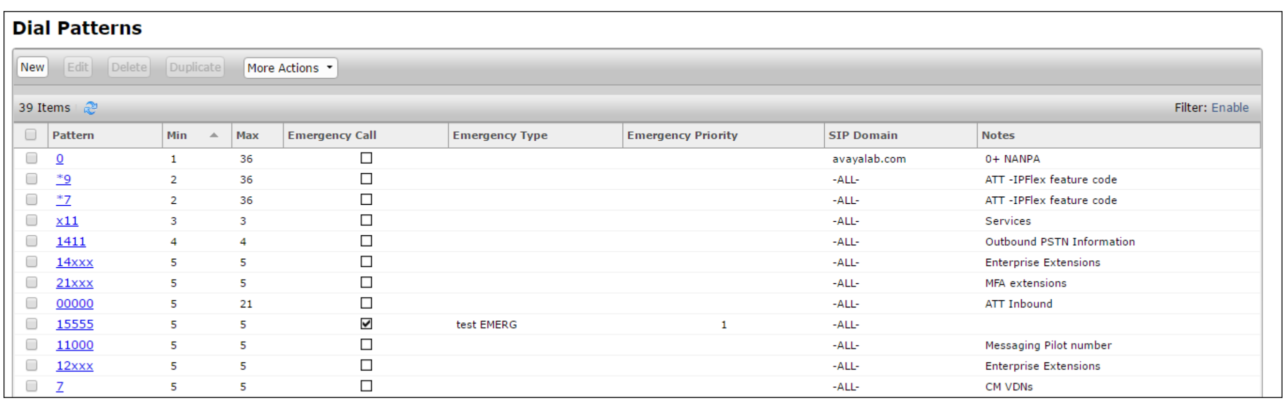
- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to AT&T/PSTN (e.g., +). This will match any outbound call prefixed with a plus sign (+), such as an E.164 formatted number.
- Enter a **Min** pattern of **12**.
- Enter a **Max** pattern of **36**.
- In the **Routing Policies** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to the Routing Policy administered for routing calls to AT&T in **Section 5.7.3** (e.g., **To SBCE-IPv6**).



	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	CM-TG-5	CM-TG-5	To SBCE-IPv6	0	☐	SBCE-ipv6	
☐	Main	Avaya SIL	To SBC2	1	☐	SBC2	
☐	Main	Avaya SIL	To SBC1	0	☐	SBC1	

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

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



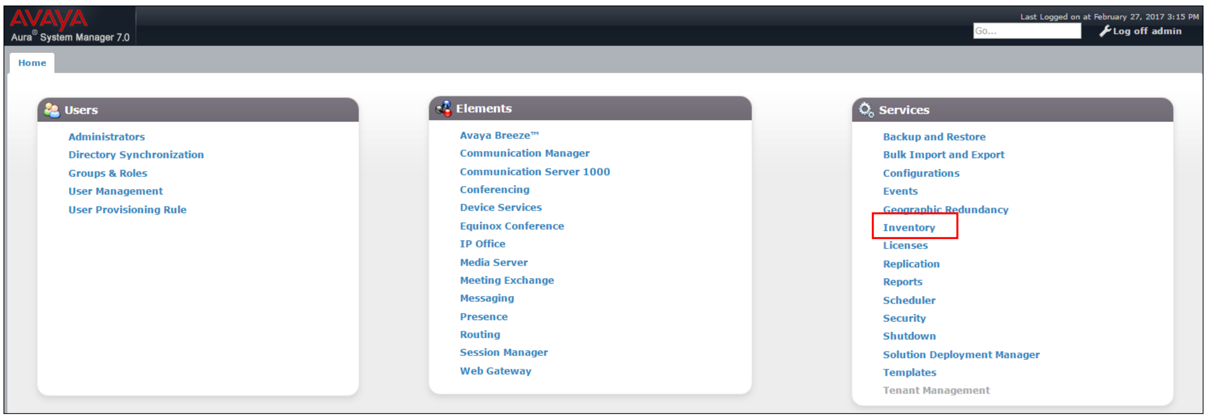
	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
☐	0	1	36	☐			avayalab.com	0+ NANPA
☐	*9	2	36	☐			-ALL-	ATT -IPFlex feature code
☐	*7	2	36	☐			-ALL-	ATT -IPFlex feature code
☐	x11	3	3	☐			-ALL-	Services
☐	1411	4	4	☐			-ALL-	Outbound PSTN Information
☐	14xxx	5	5	☐			-ALL-	Enterprise Extensions
☐	21xxx	5	5	☐			-ALL-	MFA extensions
☐	00000	5	21	☐			-ALL-	ATT Inbound
☐	15555	5	5	☑	test EMERG	1	-ALL-	
☐	11000	5	5	☐			-ALL-	Messaging Pilot number
☐	12xxx	5	5	☐			-ALL-	Enterprise Extensions
☐	7	5	5	☐			-ALL-	CM VDNs

5.9. Verify TLS Certificates – Session Manager

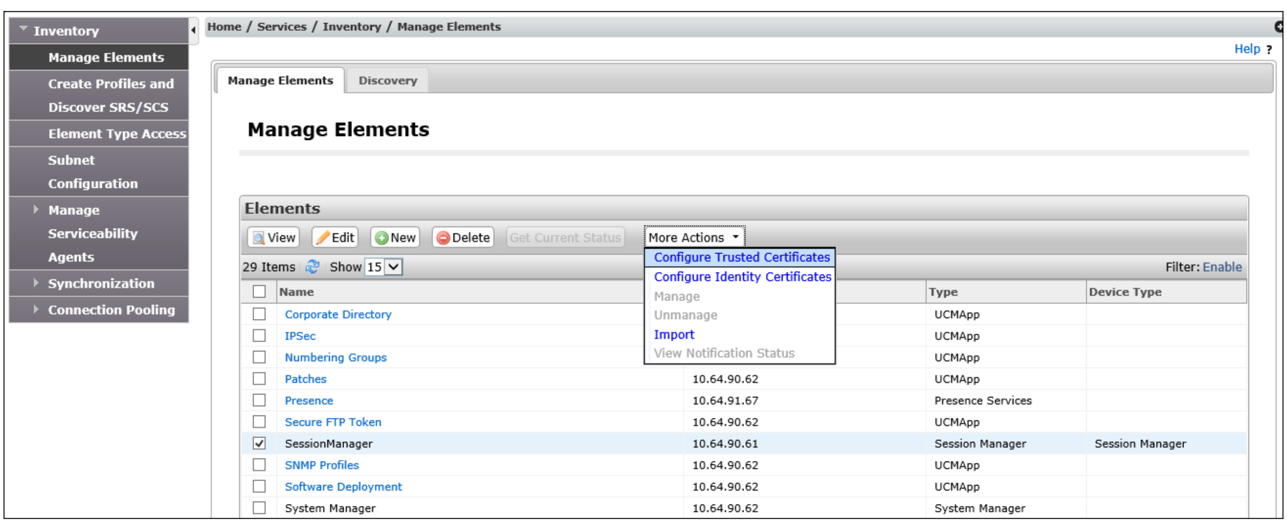
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

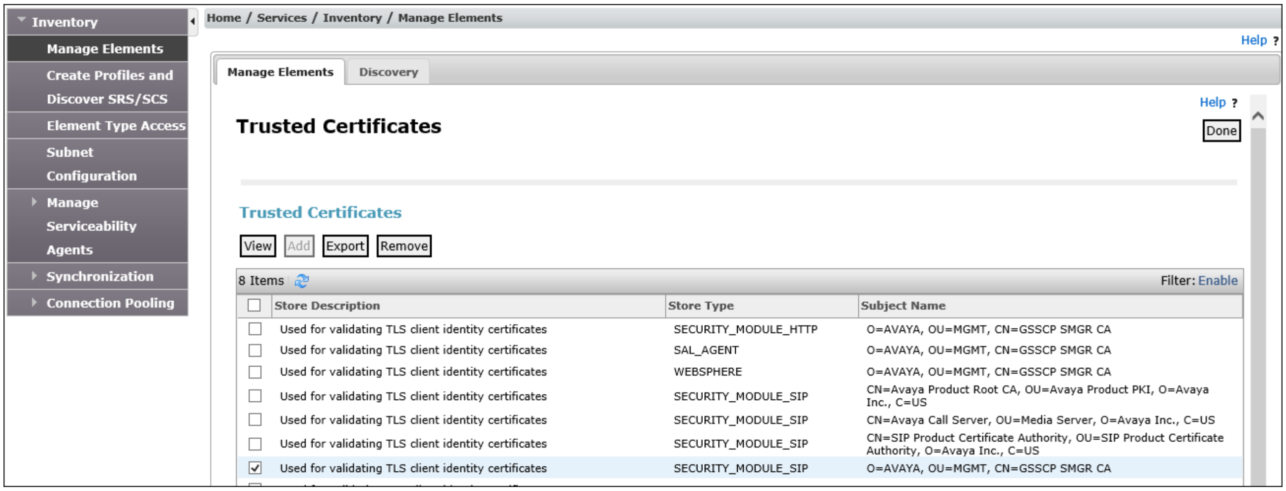
Step 1 - From the **Home** screen, under the **Services** heading in the right column, select **Inventory**.



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**.

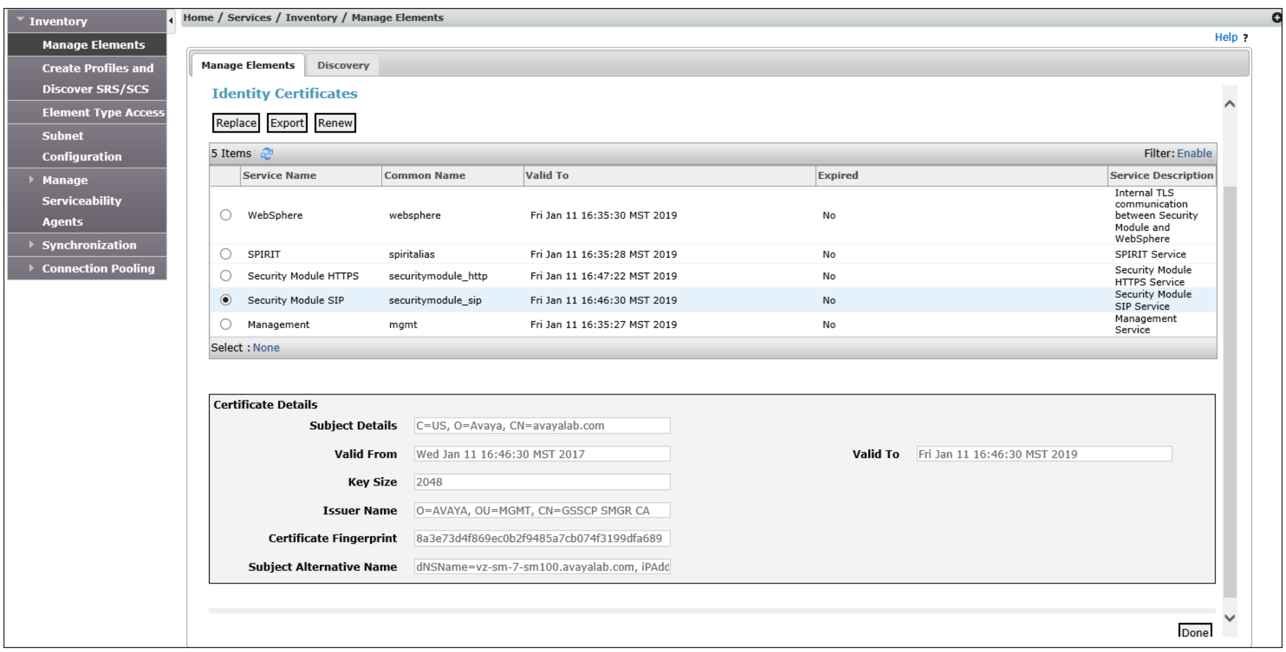


Step 3 - Verify the System Manager Certificate Authority certificate is listed in the trusted store, **SECURITY_MODULE_SIP**. Click **Done** to return to the previous screen.



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. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult **[5] - [7]** for more information.

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

6.1. Verify Communication Manager System Settings

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

6.1.1. System-Parameters Customer-Options

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

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

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

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  0
           Maximum Concurrently Registered IP Stations: 2400  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 6** of the form, verify that the **Processor Ethernet** field is set to **y**.

```
display system-parameters customer-options                      Page   6 of  12
                                OPTIONAL FEATURES

                Multinational Locations? n          Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                     Multiple Locations? n
                                            System Management Data Transfer? n
          Personal Station Access (PSA)? y             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   Total  Call       Dialed   Total  Call       Dialed   Total  Call
    String   Length Type       String   Length Type       String   Length 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
                                                        Allow H.248 Gateways? y
        Network Region: 1                               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., **Main**).
- 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                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                        IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      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 – AT&T Trunk Region

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

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

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

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

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

```
change ip-network-region 4                                      Page   4 of  20

 Source Region: 4     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst 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
```

6.7. IP Codec Parameters

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

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

```
change ip-codec-set 1                                           Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n         2        20
 2: G.729A             n         2        20
 3: G.729B             n         2        20
```

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

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

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

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

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

```
change ip-codec-set 4                                          Page   1 of   2

                          IP CODEC SET
    Codec Set: 4

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

change ip-codec-set 4                                          Page   2 of   2
                          IP CODEC SET
                              Allow Direct-IP Multimedia? n
                                                                     Packet
                          Mode                   Redundancy           Size(ms)
    FAX                   t.38-standard           0            ECM: y
    Modem                 off                     0
    TDD/TTY               US                      3
    H.323 Clear-channel   n                       0
    SIP 64K Data          n                       0                  20
```

6.8. SIP Trunks

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

- Inbound/outbound AT&T access – SIP Trunk 5
  - Note that this trunk will use TLS port 5065 as described in **Section 5.5.1**.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 1
  - Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

Note – Although TLS is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the IPFR-EF service. See the note in **Section 5.4** regarding the use of TLS transport protocols in the CPE.

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

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

6.8.1.1 Signaling Group 5

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The system will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.4** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5065**.
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 6.5.2**.
- **Far-end Domain** – Enter **avayalab.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **Initial IP-IP Direct Media** is set to **n**.
- **H.323 Station Outgoing Direct Media** is set to **n**.
- Use the default parameters on **page 2** of the form (not shown).


```
add signaling-group 5                                           Page   1 of   2
                                SIGNALING GROUP

 Group Number: 4              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                    Far-end Node Name: SM
 Near-end Listen Port: 5065                   Far-end Listen Port: 5065
                                           Far-end Network Region: 4

Far-end Domain: avayalab.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

6.8.1.2 Trunk Group 5

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

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

```
add trunk-group 5                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip          CDR Reports: y
  Group Name: ATT IPFR                    COR: 5        TN: 1        TAC: *05
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 5
                                                     Number of Members: 10
```

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

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

```
add trunk-group 4                                                Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                                   Digital Loss Group: 18
                     Preferred Minimum Session Refresh Interval(sec): 900

 Disconnect Supervision - In? y  Out? y

             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 1xC: station-extension
```

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

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

```
add trunk-group 4                                                Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

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

- Verify **Network Call Redirection** is set to **y**.
- Set **Send Diversion Header** to **y**. This is required for Communication Manager station Call Forward scenarios to IPFR-EF service.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPFR-EF service (e.g., **100**).
- Set **Identity for Calling Party Display** to **From**. Note that the display issue described in **Section 2.2**, **Item 1** may be resolved by setting the ***Identity for Calling Party Display:*** parameter to ***From***.

Note – The IPFR-EF service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, the History Info header is automatically removed from SIP signaling by Session Manager, as part of the AttAdapter (see **Section 5.3.2**). Alternatively, History Info may be disabled here.

```
add trunk-group 4                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? y
                              Telephone Event Payload Type: 100

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: From
            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
```

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

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

6.8.2.1 Signaling Group 3

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

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

Step 2 - Set the following parameters on page 1:

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

6.8.2.2 Trunk Group 3

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

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

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

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

- Same as **Section 6.8.1.2**

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

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

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

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

6.9. Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 6.8.1.2**), is used to convert Communication Manager local extensions to IPFR-EF DNIS numbers, for inclusion in any SIP headers directed to the IPFR-EF service via the public trunk.

Step 1 - Enter **change public-unknown-numbering 5 ext-digits xxxxx**, where xxxxx is the 5-digit extension number to change.

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

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter a Communication Manager extension (e.g., **14002**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **5**).
- **Private Prefix** – Enter the corresponding IPFR-EF DNIS number (e.g., 1**7325552753**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

```
change public-unknown-numbering 5 ext-digits 14006             Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext             Trk       CPN           CPN
Len Code            Grp(s)    Prefix        Len
                                                  Total Administered: 26
 5  14002           5         17325552753    11      Maximum Entries: 240
 5  14006           5         17325552754    11
 5  14008           5         17325552755    11   Note: If an entry applies to
                                                  a SIP connection to Avaya
                                                  Aura(R) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.

                                                  Communication Manager
                                                  automatically inserts
                                                  a '+' digit in this case.
```

6.10. Private Numbering

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

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

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 6.3** (e.g., **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

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

6.11.1. Route Pattern for National Calls to AT&T

This form defines the public SIP trunk, based on the route-pattern selected by the ARS table in **Section 6.12**. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks. In the reference configuration, route pattern 1 is used for national calls, route pattern 2 is used for international calls, and route pattern 4 is used for service calls and IPFR-EF Call Forward feature access codes.

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

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

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name: To PSTN SIP Trk
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 5    0       1                p                                     n   user
 2:                                                                     n   user
 3:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                                           none
```

6.11.2. Route Pattern for International Calls to AT&T

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

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

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

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2      Pattern Name: 011 to E.164
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 5    0                    3   p                                     n   user
 2:                                                                     n   user
 3:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                                          none
```

6.11.3. Route Pattern for Service Calls to AT&T

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

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

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

```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4      Pattern Name: Service Numbers
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 5    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                                          none
```

6.11.4. Route Pattern for Calls within the CPE

This form defines the Route pattern for the local SIP trunk, based on the route-pattern selected by the AAR table in **Section 6.13** (e.g., calls to Avaya SIP telephone extensions or Messaging).

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

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

```
change route-pattern 3                                          Page   1 of   3
                    Pattern Number: 3      Pattern Name: ToSM Enterprise
    SCCAN? n    Secure SIP? n     Used for SIP stations? y
    Primary SM: SM              Secondary SM:
    Grp FRL NPA Pfx Hop Toll No.  Inserted                           DCS/ IXC
    No          Mrk Lmt List Del  Digits                             QSIG
                             Dgts                                    Intw
 1: 3    0                                                            n   user
 2:                                                                   n   user
 3:                                                                   n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
1: y y y y y n  n            rest                                lev0-pvt  none
```

6.12. Automatic Route Selection (ARS) Dialing

The ARS table is selected based on the caller dialing the ARS access code (e.g., **9**) as defined in **Section 6.3**. The access code is removed and the ARS table matches the remaining outbound dialed digits and sends them to the designated route-pattern (see **Section 6.11**).

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

- In the **Dialed String** column enter a matching dial pattern (e.g., **1720**). Note that the best match will route first, that is 1720555xxxx will be selected before 17xxxxxxxxx.
- In the **Min** and **Max** columns enter the corresponding digit lengths, (e.g., **11** and **11**).
- In the Route Pattern column select a route-pattern to be used for these calls (e.g., **1**).
- In the **Call Type** column enter **fnpa** (selections other than **fnpa** may be appropriate, based on the digits defined here).

Step 2 - Repeat **Step 1** for all other outbound call strings. In addition, IPFR-EF Call Forward feature access codes ***7** and ***9** are defined here as well.

```
change ars analysis 1720                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all         Percent Full: 1

          Dialed           Total      Route     Call   Node   ANI
          String          Min  Max   Pattern    Type   Num    Reqd
    1720                  11   11     1         fnpa          n
    18                    11   11     1         fnpa          n
    19                    11   11     1         fnpa          n
    1900                  11   11     deny      fnpa          n
    1900555               11   11     deny      fnpa          n
    1xxx976               11   11     deny      fnpa          n
    *7                    3    16     4         svcl          n
    *9                    3    16     4         svcl          n
    311                   3    3      4         svcl          n
    011                   10   18     2         intl          n
    411                   3    3      4         svcl          n
    5                     10   10     1         fnpa          n
    511                   3    3      4         svcl          n
    555                   7    7      deny      hnpa          n
    5551212               7    7      1         svcl          n
```

6.13. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

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

- **Dialed String -** In the reference configuration all SIP telephones used extensions in the range 14xxx, therefore enter **14**.
- **Min** & **Max** – Enter **5**
- **Route Pattern** – Enter **3**
- **Call Type** – Enter **lev0**

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

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed            Total      Route     Call   Node  ANI
          String           Min  Max  Pattern    Type   Num   Reqd
    14                     5    5     3         lev0          n
```

6.14. Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateway is provisioned. The G430 is located in the Main site and is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. For additional information on G430 provisioning, see **[7]**.

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

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

Step 3 - Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.64.91.65**, see **Section 6.4**).

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

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

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

- Set **Type** = **g430**
- Set **Name** = a descriptive name (e.g., **G430-1**)
- Set **Serial Number** = the serial number copied from **Step 2** (e.g., **11N509736520**)
- Set the **Link Encryption Type** parameter as desired (**any-ptls/tls** was used in the reference configuration)
- Set **Network Region** = 1

Wait a few minutes for the G430 to register to Communication Manager. When the Media Gateway registers, the G430 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., ***G430-001(super)#***).

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

```
display media-gateway 1                                            Page   1 of   2
                             MEDIA GATEWAY 10

                    Type: g430
                    Name: G430-1
               Serial No: 11N509736520
    Link Encryption Type: any-ptls/tls       Enable CF? n
          Network Region: 1                   Location: 1
         Use for IP Sync? y                  Site Data:
           Recovery Rule: 1

              Registered?  y
   FW Version/HW Vintage: 37 .41 .0  /1
       MGP IPV4 Address: 10.64.19.61
       MGP IPV6 Address:
   Controller IP Address: 10.64.91.65
            MAC Address: b4:b0:17:8f:3a:49

   Mutual Authentication? optional
```

6.15. Avaya Aura® Media Server Provisioning

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

Note – Only the Media Server provisioning associated with Communication Manager is shown below. See **[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** and **Far-end Listen Port** – Set to **5060**.

- **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: 5060                Far-end Listen Port: 5060
                                        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. Save Translations

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

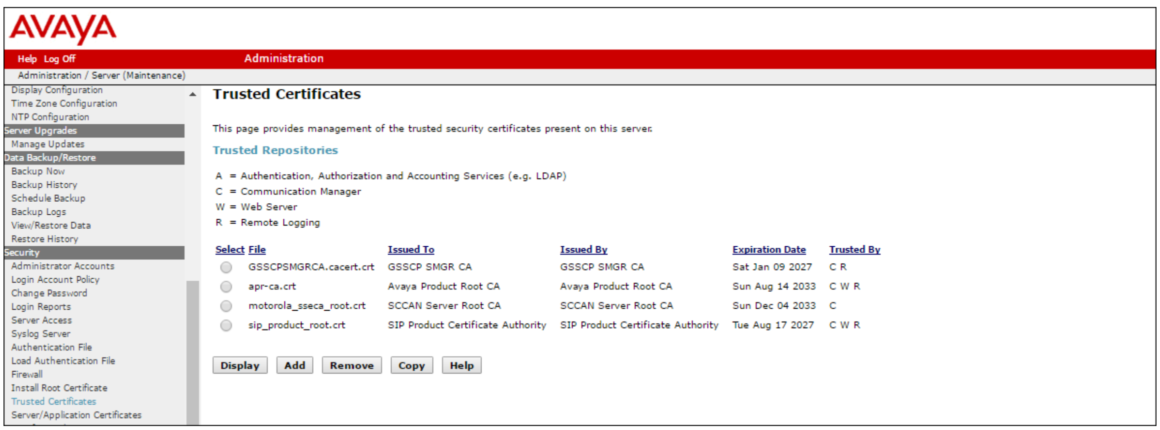
6.17. Verify TLS Certificates – Communication Manager

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

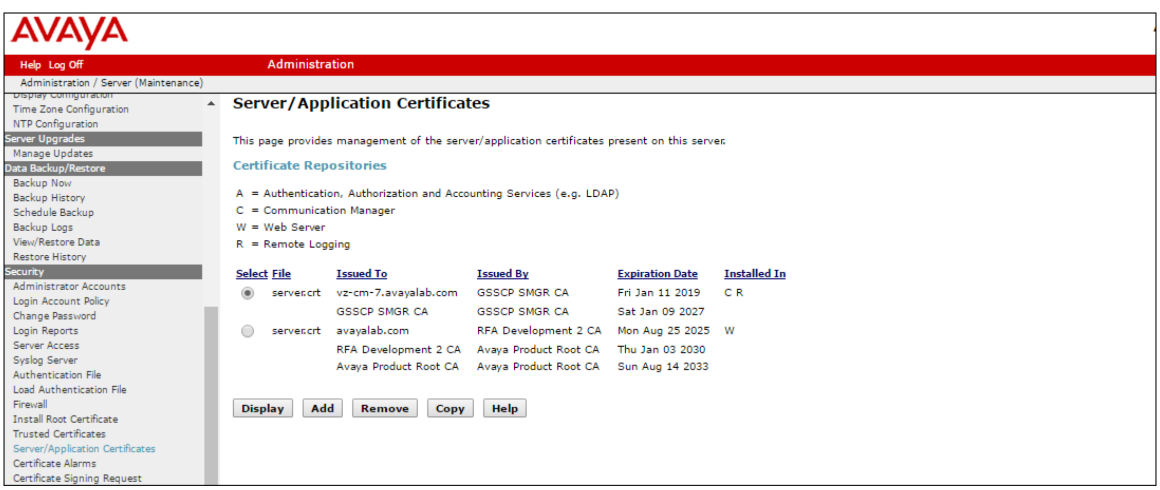
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. The following procedures show how to verify the certificates used by Communication Manager.

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

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



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



7. Configure Avaya Session Border Controller for Enterprise

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

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to **[10** and **11]** for additional information.

Note: The Avaya SBCE supports a Remote Worker configuration whereby Communication Manager SIP endpoints residing on the public side of the Avaya SBCE, can securely register/operate as a "local" Communication Manager station in the private CPE. While Remote Worker functionality was tested in the reference configuration, Remote Worker provisioning is beyond the scope of this document.

As described in **Section 3**, the reference configuration places the private interface A1 (IP address 10.64.91.40) of the Avaya SBCE in the Common site with access to the Main site. The connection to AT&T uses the Avaya SBCE public interface B1 (IPv6 address 3ffe:ffff:bb:bb::240).

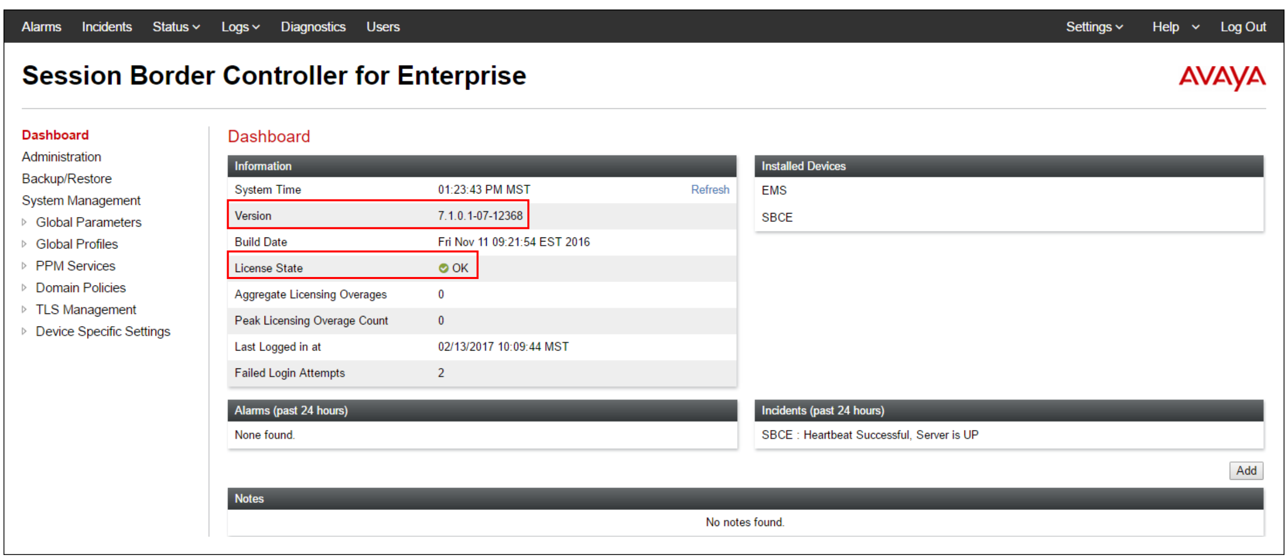
The following provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

Step 1 - Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).
Step 2 - Enter the **Username** and click on **Continue**.

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

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.

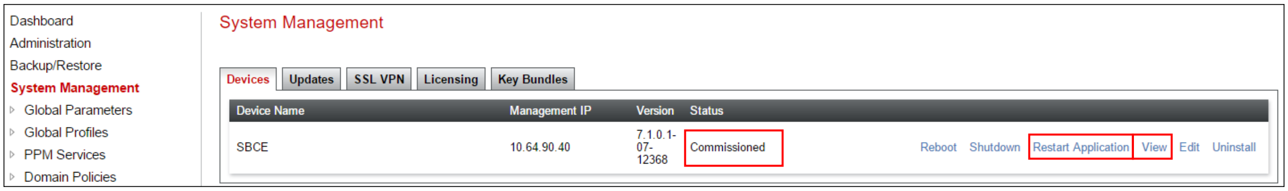
Note – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.



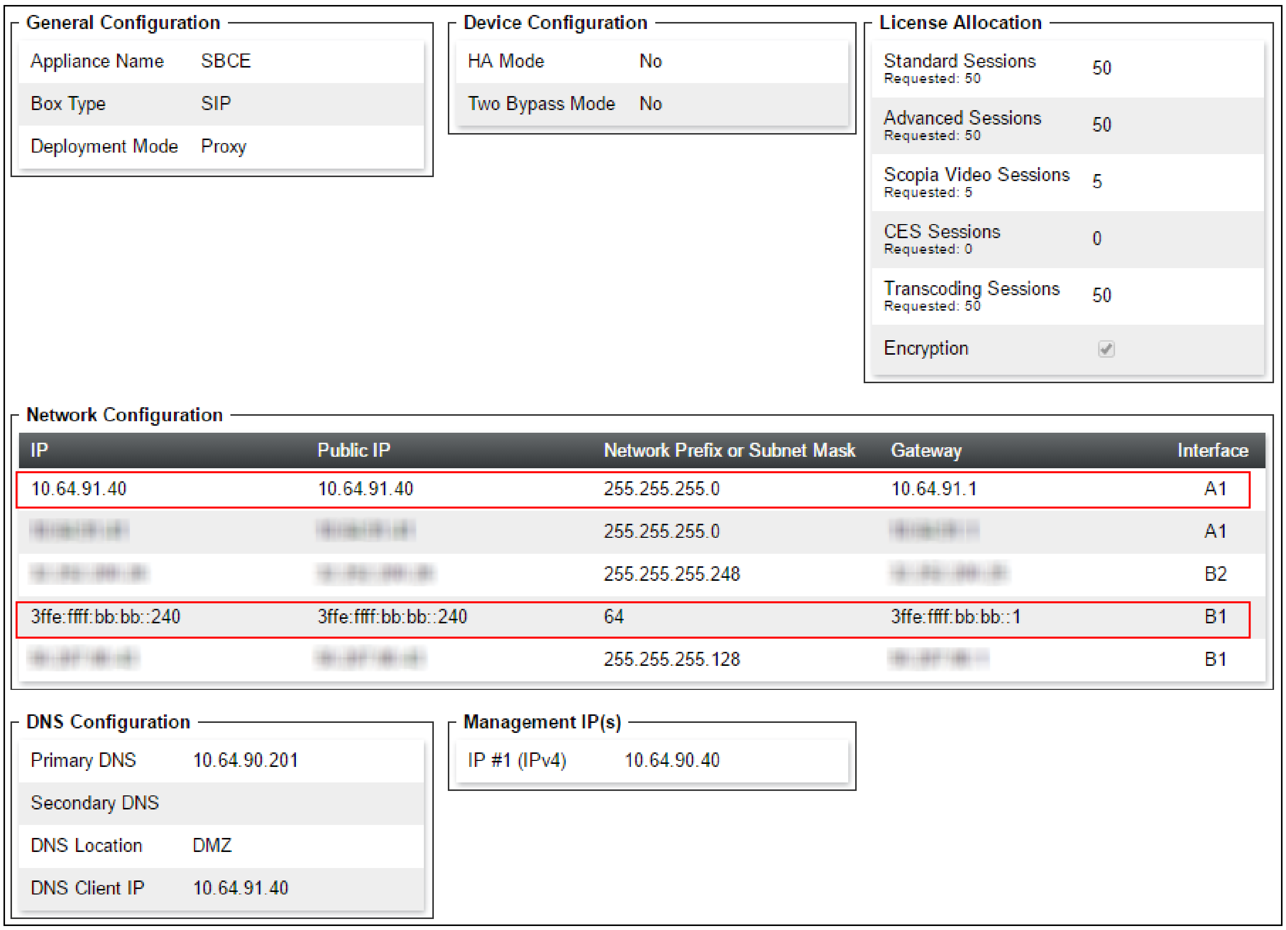
7.1. System Management – Status

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

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



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



7.2. TLS Management

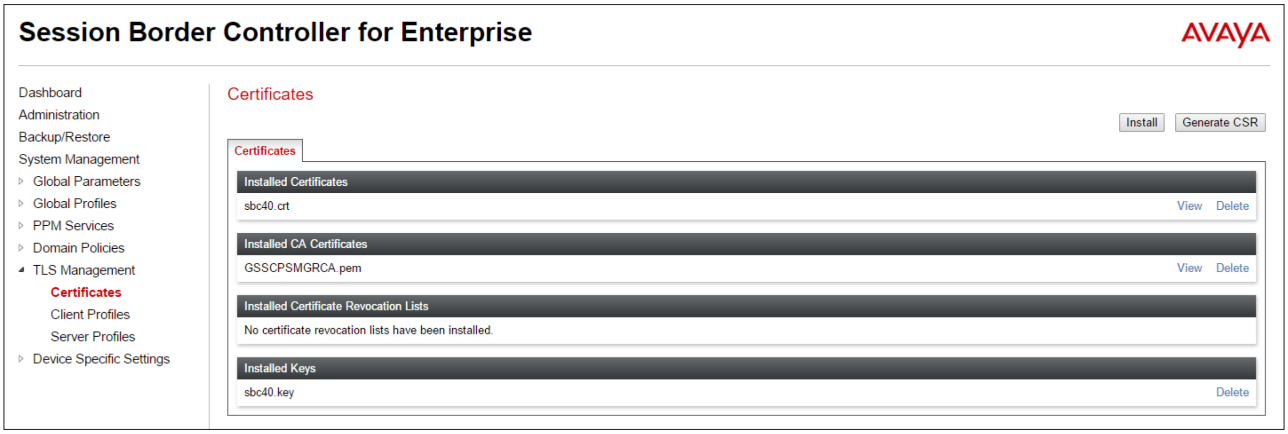
Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

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.

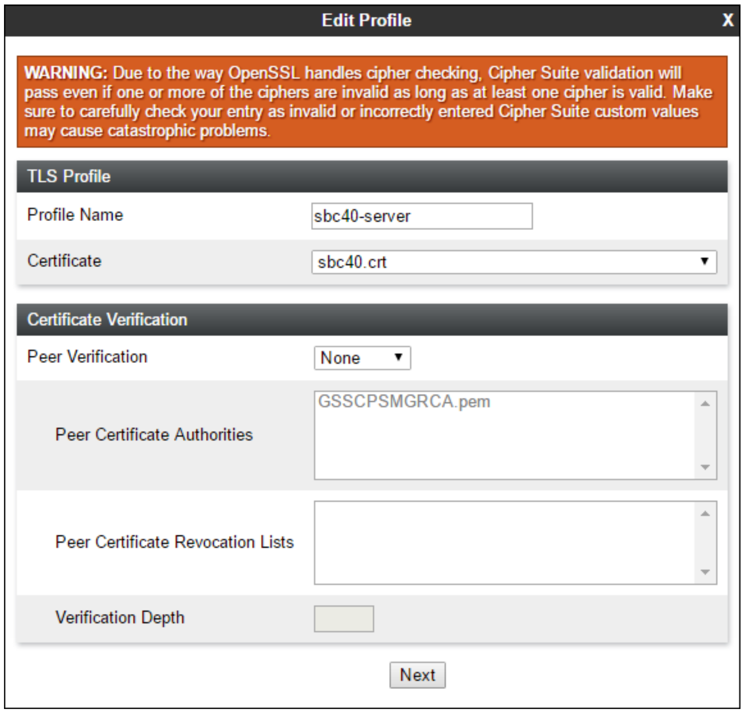


7.2.2. Server Profiles

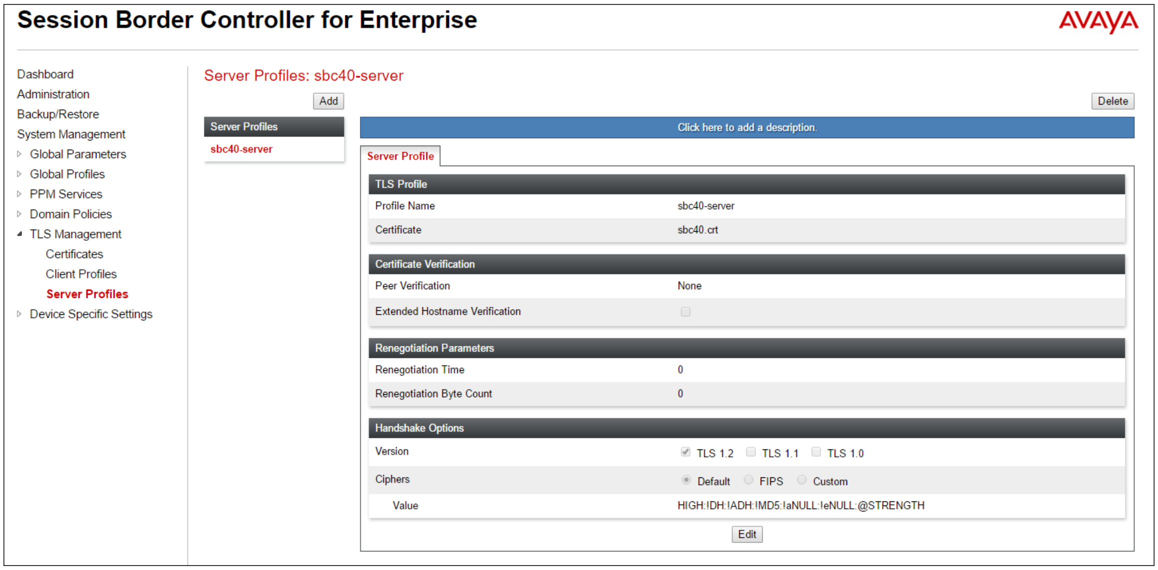
Step 1 - Select **TLS Management → Server Profiles**, and click on **Add**. Enter the following:

- **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**.



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

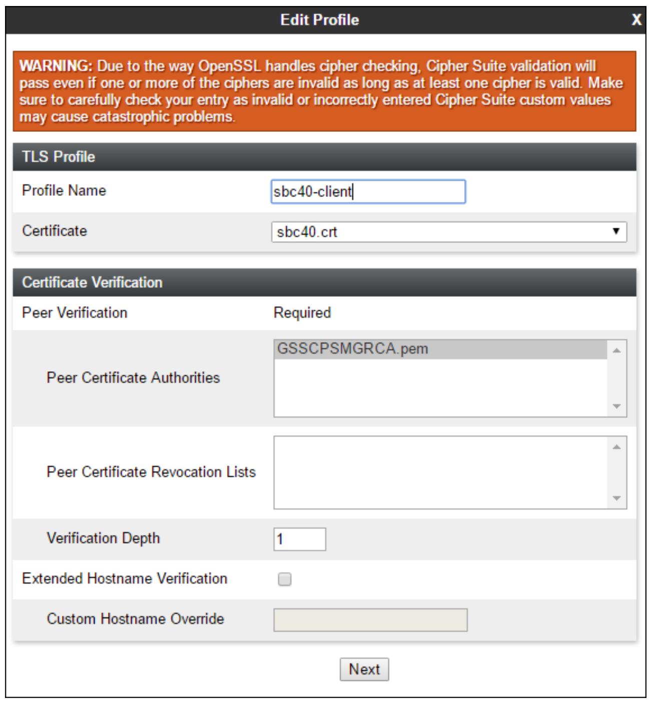


7.2.3. Client Profiles

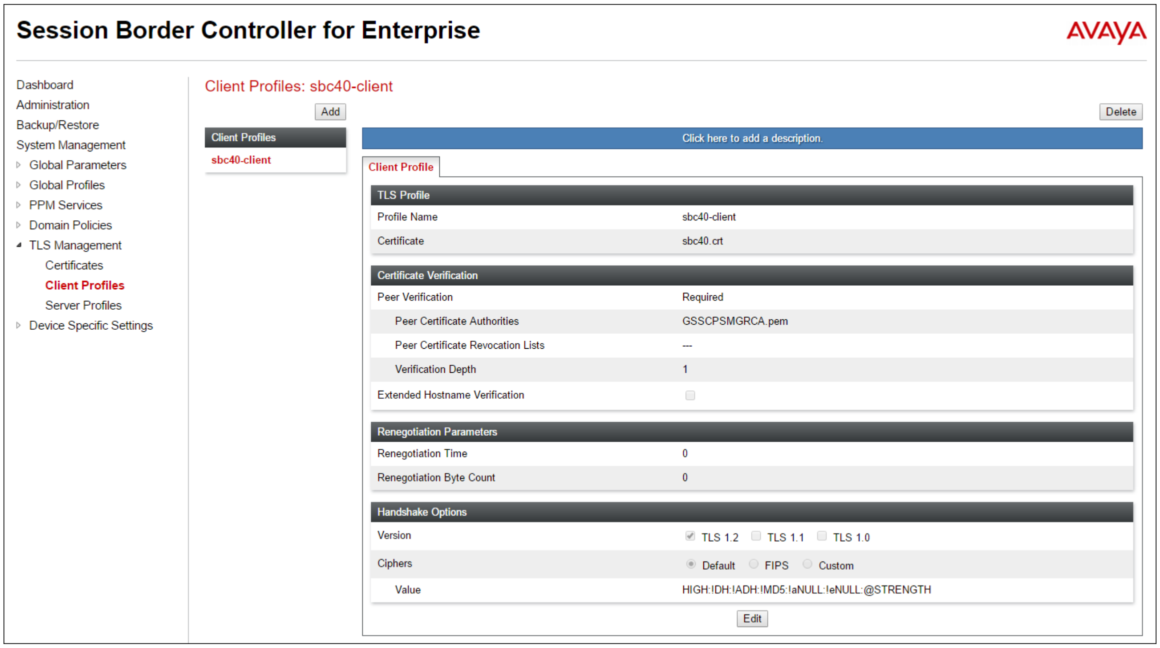
Step 1 - Select **TLS Management → Server Profiles**, and click on **Add**. Enter the following:

- **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**.



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



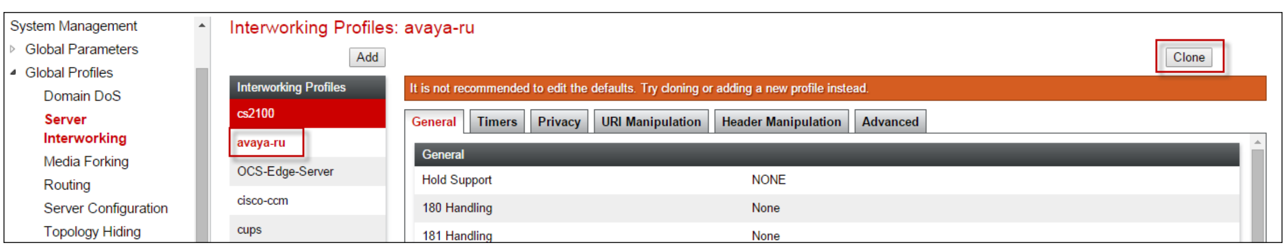
7.3. Global Profiles

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

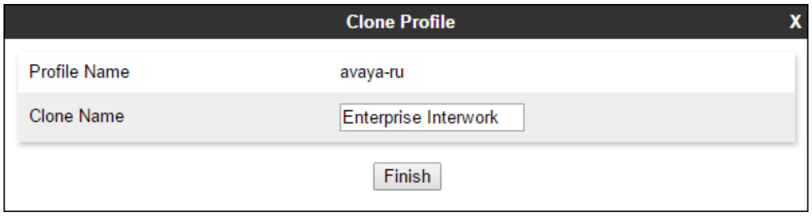
7.3.1. Server Interworking – Avaya

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.

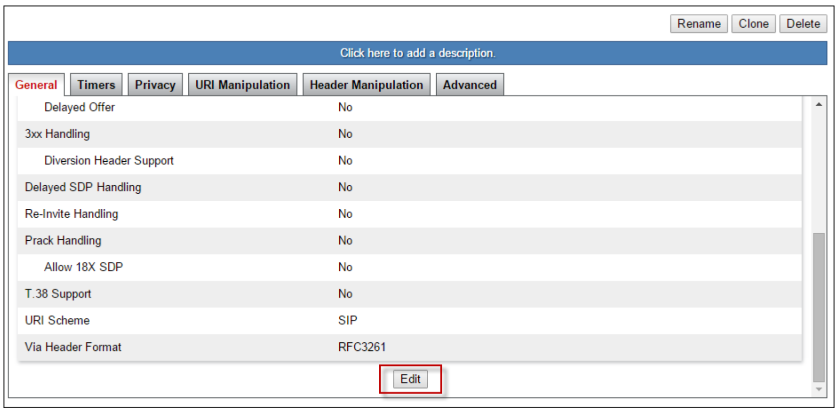
Step 1 - Select **Global Profiles → Server Interworking** from the left-hand menu.
Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.



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

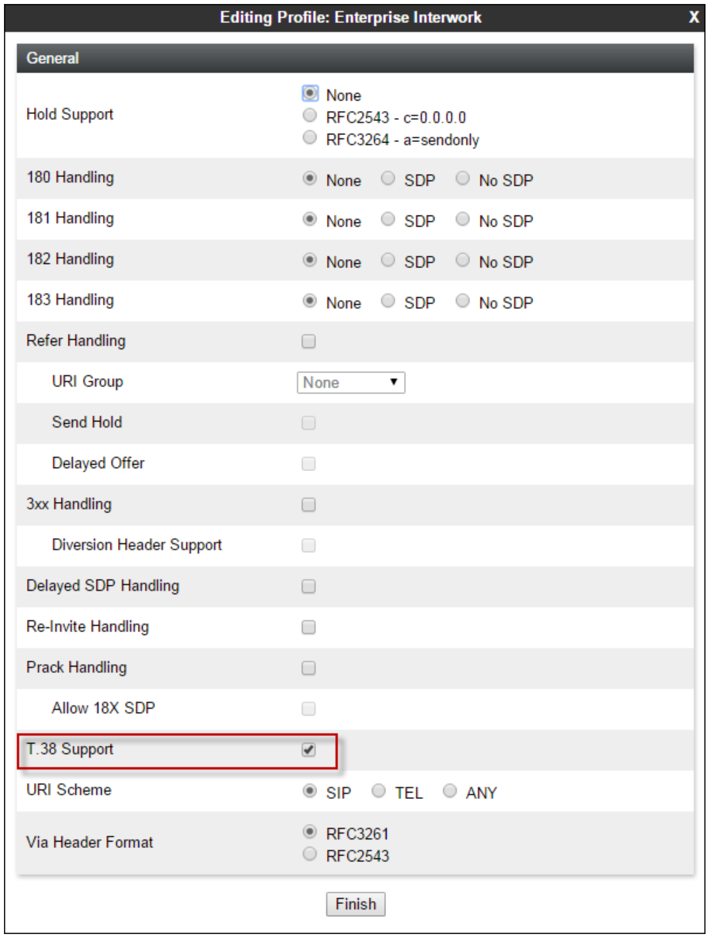


Step 4 - The new Enterprise Interwork profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.

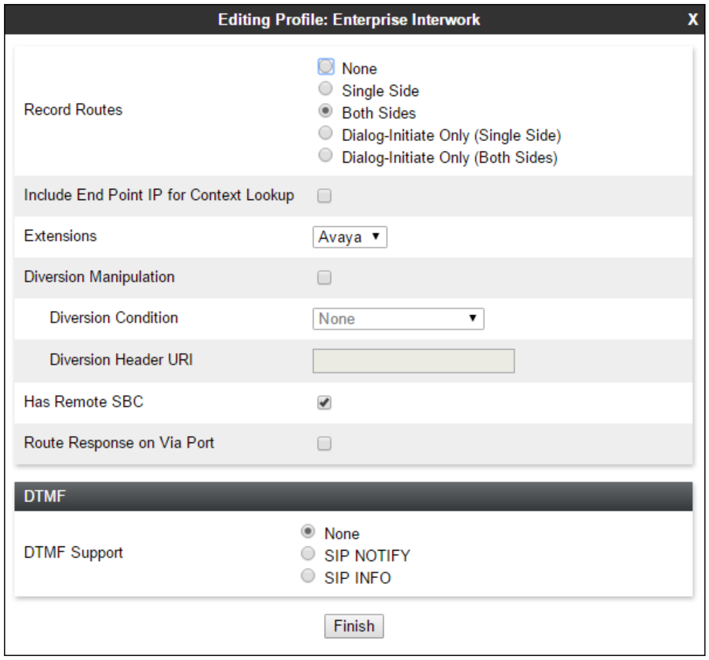


Step 5 - The **General** screen will open.

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



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



7.3.2. Server Interworking – AT&T

Repeat the steps shown in **Section 7.3.1** to add an Interworking Profile for the connection to AT&T via the public network, with the following changes:

Step 1 - Select **Add Profile** (not shown) and enter a profile name: (e.g., **ATT-Interworking**) and click **Next** (not shown).

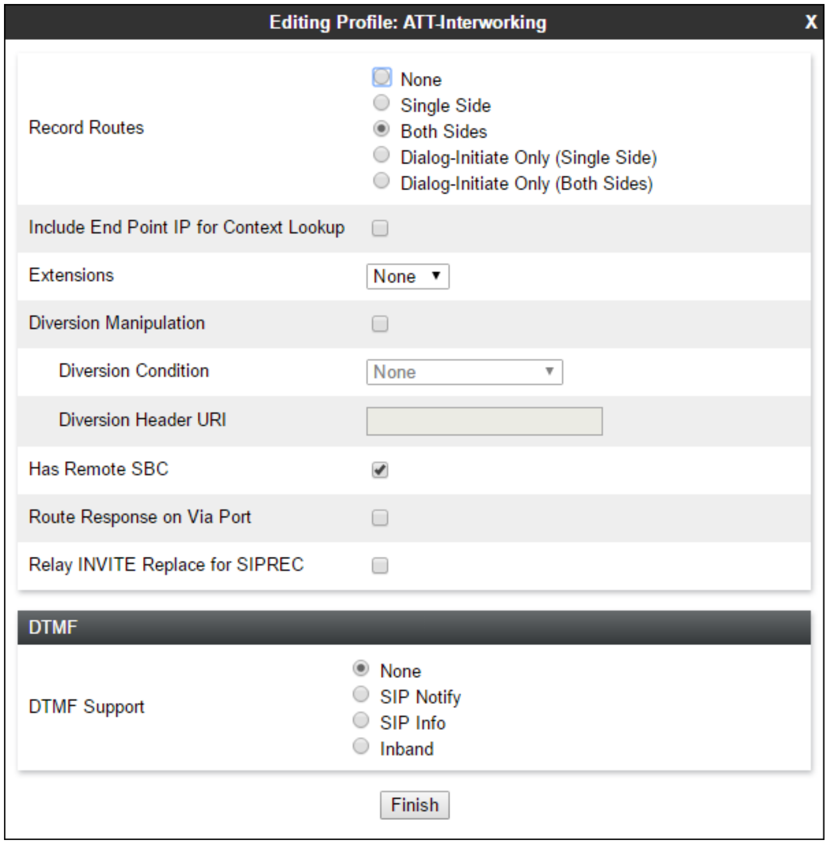
Step 2 - The **General** screen will open (not shown):

- Check **T38 Support**.
- All other options can be left as default.
- Click **Next**.

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

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

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



7.3.3. Signaling Manipulation

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

Note – Use of the Signaling Manipulation scripts require higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 8.4.3**) does not meet the desired result. Refer to **[10]** for information on the Avaya SBCE scripting language.

Step 1 - As described in **Section 2.2, Item 5)**, 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

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

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

Step 2 - As described in **Section 2.2**, **Item 6)**, 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

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

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

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

Step 3 - As described in **Section 2.2**, **Item 3)**, the Avaya SBCE was not able to parse the domain name presented in the Ring Splash INVITE. The following signaling manipulation script is added to the script defined in **Step 1** above, to convert the domain name to an IPv6 address.

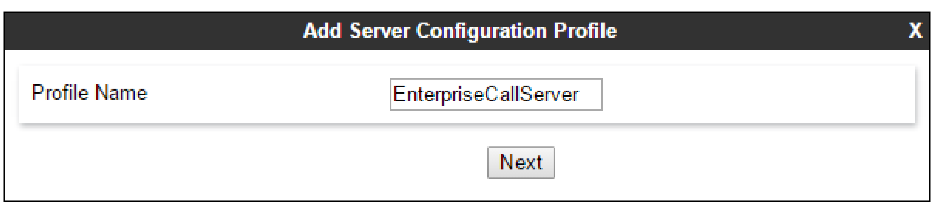
1. The following script is added:

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

7.3.4. Server Configuration – Session Manager

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

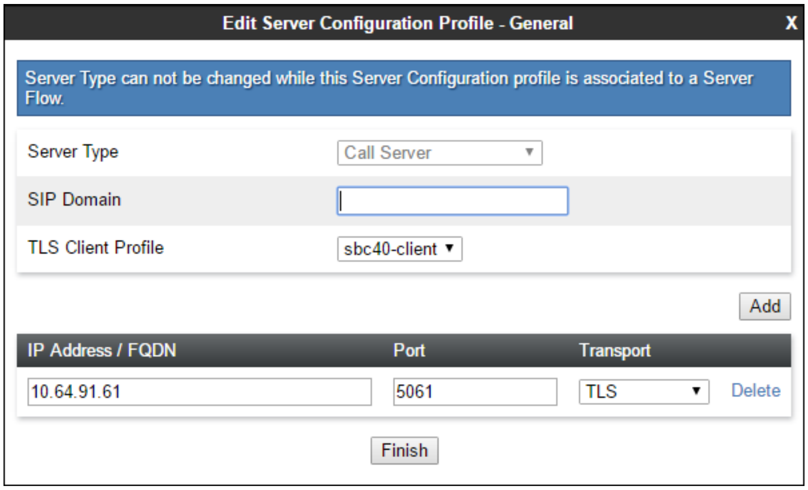
Step 1 - Select **Global Profiles → Server Configuration** from the left-hand menu.
Step 2 - Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **EnterpriseCallServer**) and click **Next**.



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

- Select **Server Type**: **Call Server**
- **SIP Domain**: Leave blank (default)
- **TLS Client Profile**: Select the profile create in **Section 8.2.3** (e.g., **sbc40-client**)
- **IP Address**: **10.64.91.61** (Session Manager network IP address)

- **Transport**: Select **TLS**
- **Port**: **5061**
- Select **Next**



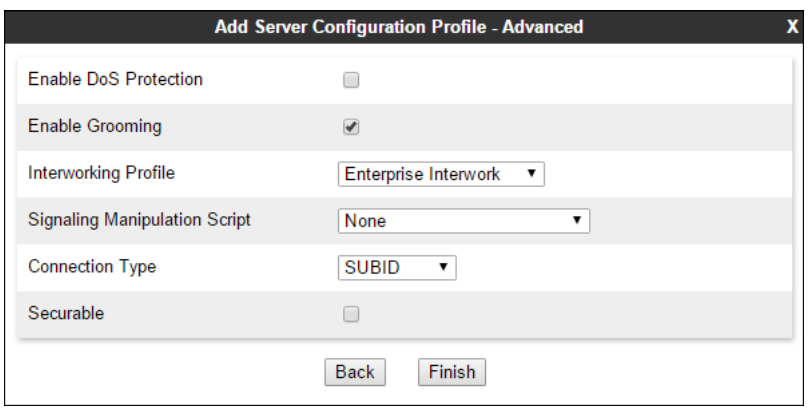
Step 4 - The **Authentication** and **Heartbeat** windows will open (not shown).

- Select **Next** to accept default values

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

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

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



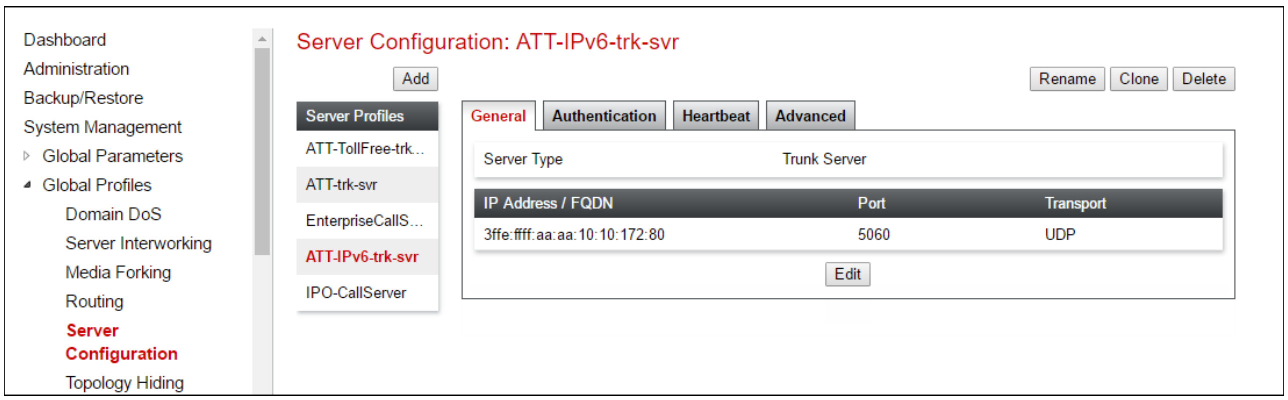
7.3.5. Server Configuration – AT&T

Repeat the steps in **Section 7.3.4**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

Step 1 - Select **Add** and enter a Profile Name (e.g., **ATT-IPv6-trk-svr**) and select **Next** (not shown).
Step 2 - On the **General** window, enter the following.

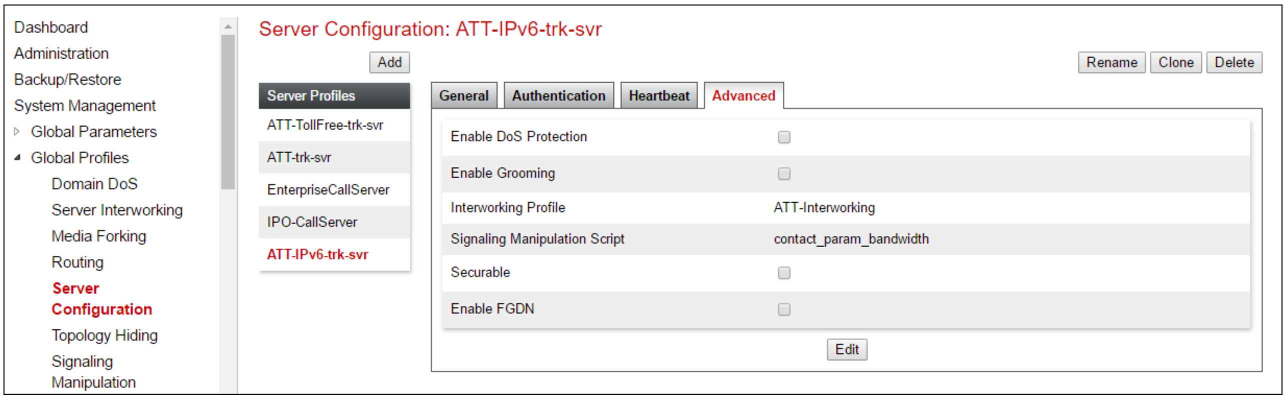
- **Server Type:** Select **Trunk Server**
- **IP Address: 3ffe:ffff:aa:aa:10:10:172:80** (AT&T Border Element IPv6 address)
- **Transport**: Select **UDP**
- **Port: 5060**
- Select **Next** until the Advanced tab is reached

> **Note** – The IPv6 address needs to be entered using lowercase characters. See **Section 2.2, Item 7)** for limitations in entering an IPv6 address.



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

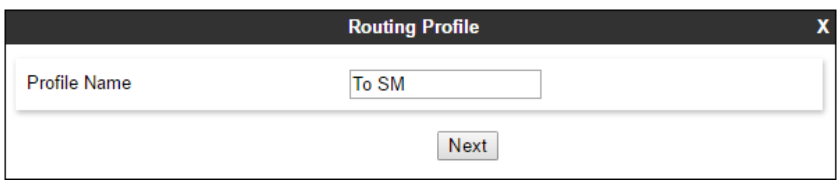
- Select **ATT-Interworking** (created in **Section 7.3.2**), for **Interworking Profile**.
- Select **contact_param_bandwidth** (created in **Section 7.3.3**) for **Signaling Manipulation Script**.
- Select **Finish** (not shown)



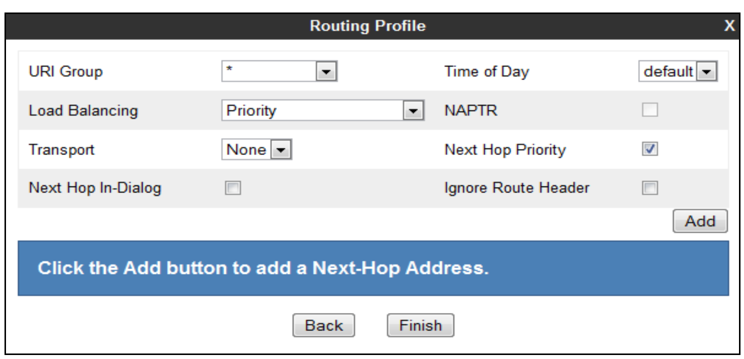
7.3.6. Routing – To Session Manager

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

Step 1 - Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown)
Step 2 - Enter a **Profile Name**: (e.g., **To SM**) and click **Next**.



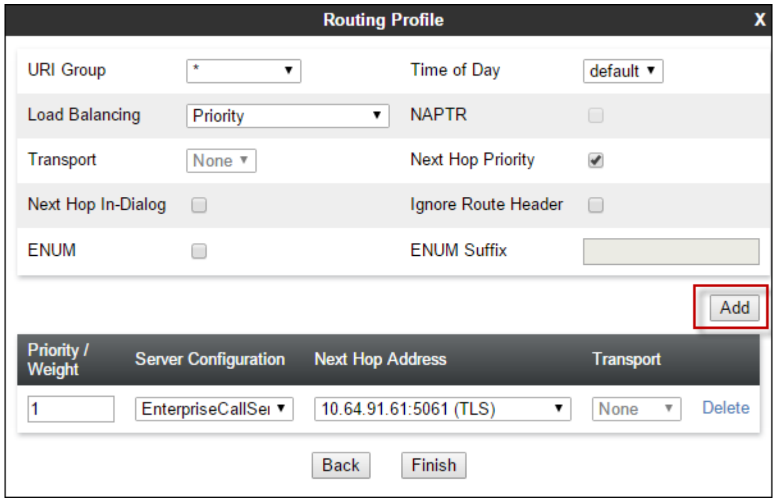
Step 3 - The Routing Profile window will open. Using the default values shown, click on **Add**.



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

- **Priority/Weight** = **1**
- **Server Configuration** = **EnterpriseCallServer** (from **Section7.3.4**).

- **Next Hop Address:** Verify that the **10.64.91.61:5061 (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**.



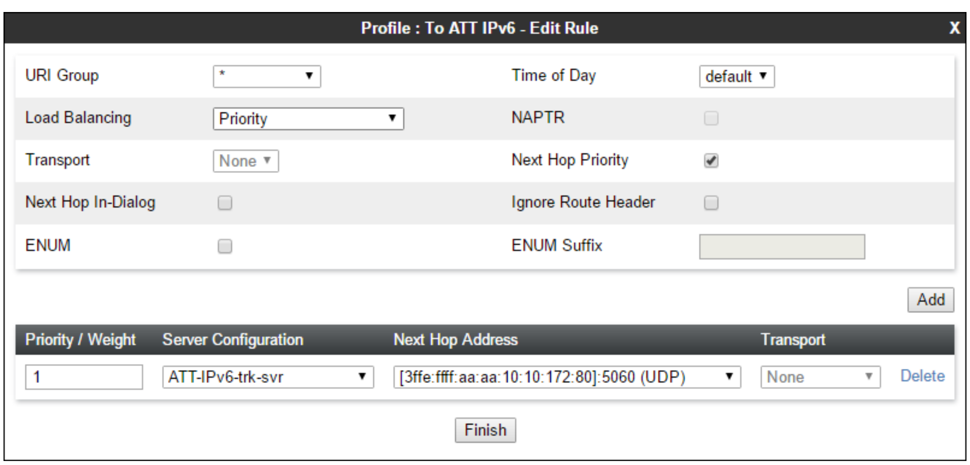
7.3.7. Routing – To AT&T

Repeat the steps in **Section 7.3.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

Step 1 - On the **Global Profiles → Routing Profile** window, enter a Profile Name: (e.g., **To ATT IPv6**).
Step 2 - On the **Next-Hop Address** window, populate the following fields:

- **Priority/Weight** = **1**
- **Server Configuration** = **ATT-IPv6-trk-svr** (**from Section 7.3.5**).
- **Next Hop Address:** select **[3ffe:ffff:aa:aa:10:10:172:80]:5060 (UDP)**.

Step 3 - Click **Finish**.



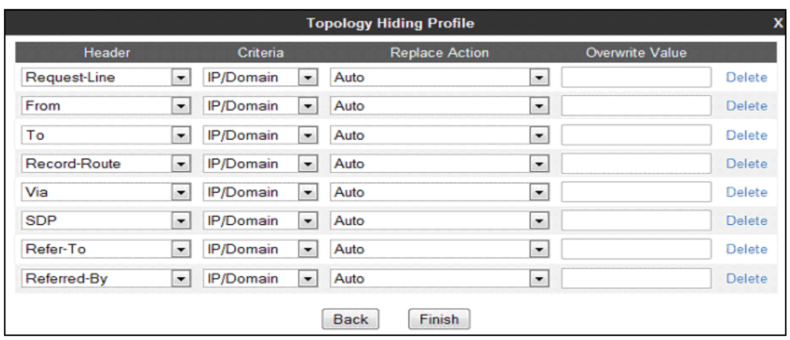
7.3.8. Topology Hiding – Enterprise Side

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

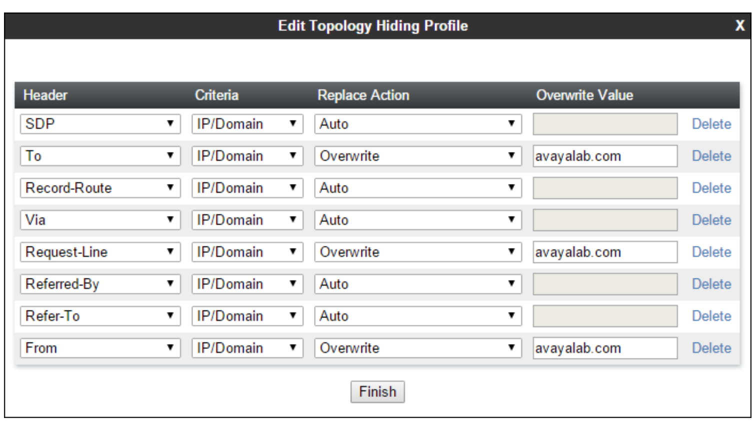
Step 1 - Select **Global Profiles → Topology Hiding** from the left-hand side menu.

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

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.



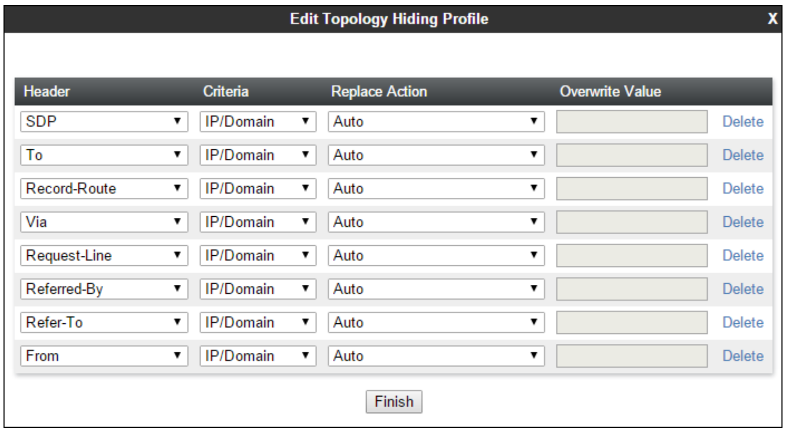
Step 4 - Populate the fields as shown below, and click **Finish**. Note that **avayalab.com** is the domain used by the CPE (see **Sections 5.1**, **6.5**, and **6.7**).



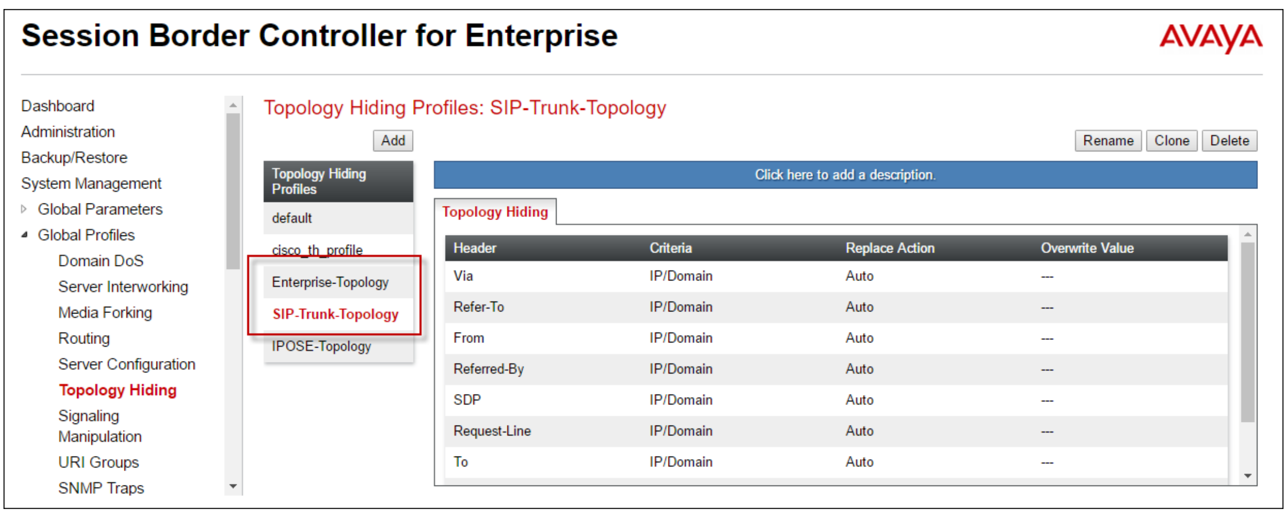
7.3.9. Topology Hiding – AT&T Side

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

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



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



7.4. Domain Policies

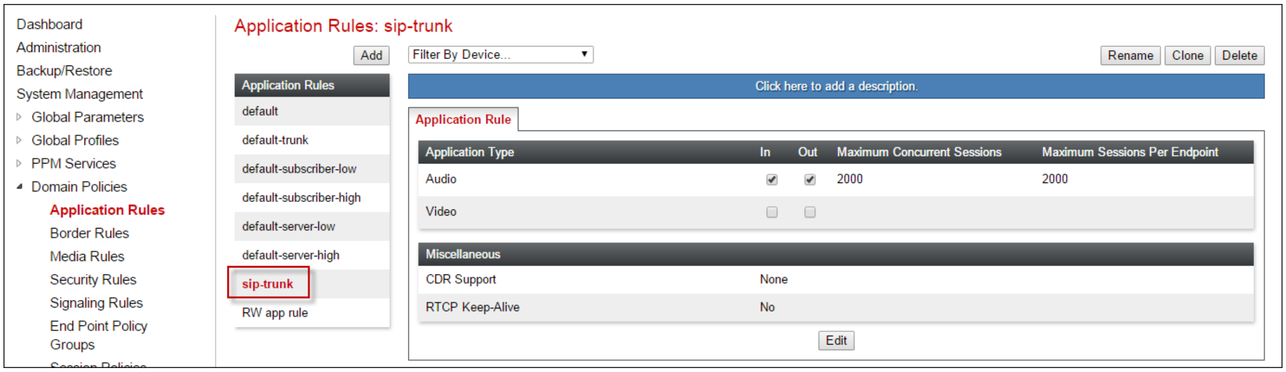
The Domain Policies feature allows users to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

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.



7.4.2. Media Rules

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

7.4.2.1 Enterprise – Media Rule

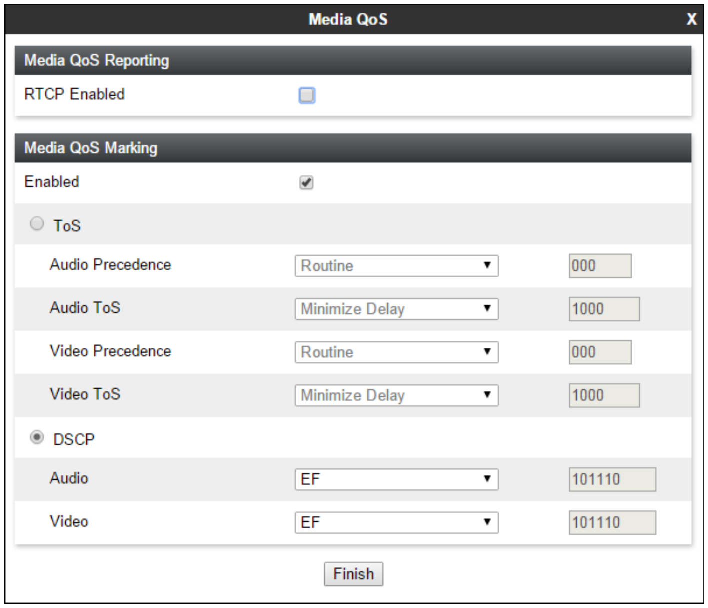
Step 1 - Select **Domain Policies → Media Rules** from the left-hand side menu (not shown).
Step 2 - From the Media Rules menu, select the **default-low-med** rule.
Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

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

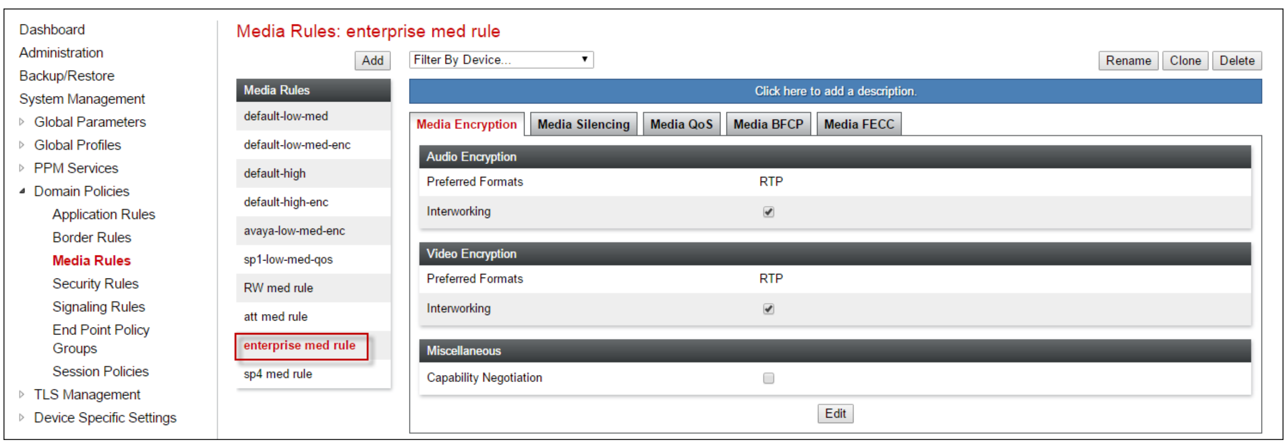
Step 4 - Highlight the **enterprise med rule** just created (not shown):

- Select the **Media QoS** tab (not shown).
- Click the **Edit** button and the **Media QoS** window will open.
- In the **Media QOS Marking** section, check **Enabled**.
- Select the **DSCP** box.
- **Audio**: Select **EF** from the drop-down.
- **Video**: Select **EF** from the drop-down.

Step 5 - Click **Finish**.



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

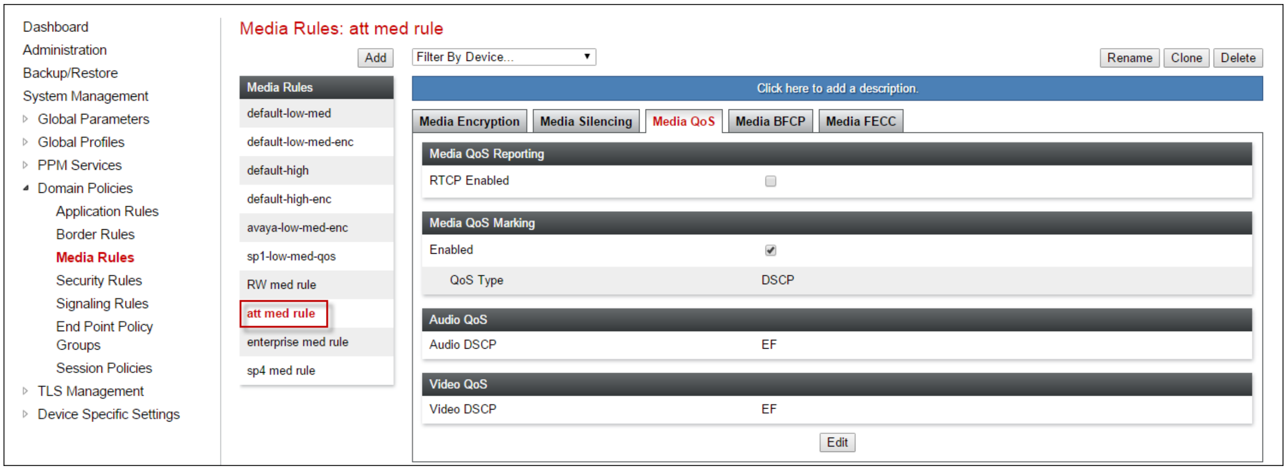


7.4.2.2 AT&T – Media Rule

Repeat the steps in **Section 7.3.2.1**, with the following changes, to create a Media Rule for AT&T.

1. In the **Clone Name** field enter **att med rule**

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



7.4.3. Signaling Rules

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

7.4.3.1 Enterprise – Signaling Rules

Step 1 - Select **Domain Policies → Signaling Rules** from the left-hand side menu (not shown).
Step 2 - The **Signaling Rules** window will open (not shown). From the Signaling Rules menu, select the **default** rule.
Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

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

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

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

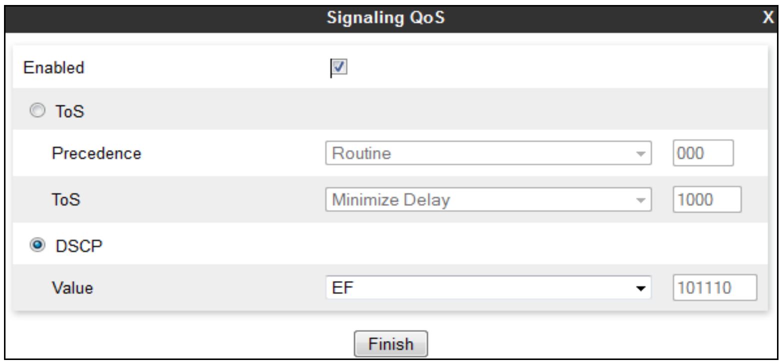
Step 5 - Click **Finish**.

7.4.3.2 AT&T – Signaling Rule

Step 1 - Select **Domain Policies** from the menu on the left-hand side menu (not shown).
Step 2 - Select **Signaling Rules** (not shown).
Step 3 - From the Signaling Rules menu, select the **default** rule.
Step 4 - Select **Clone Rule** button

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

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

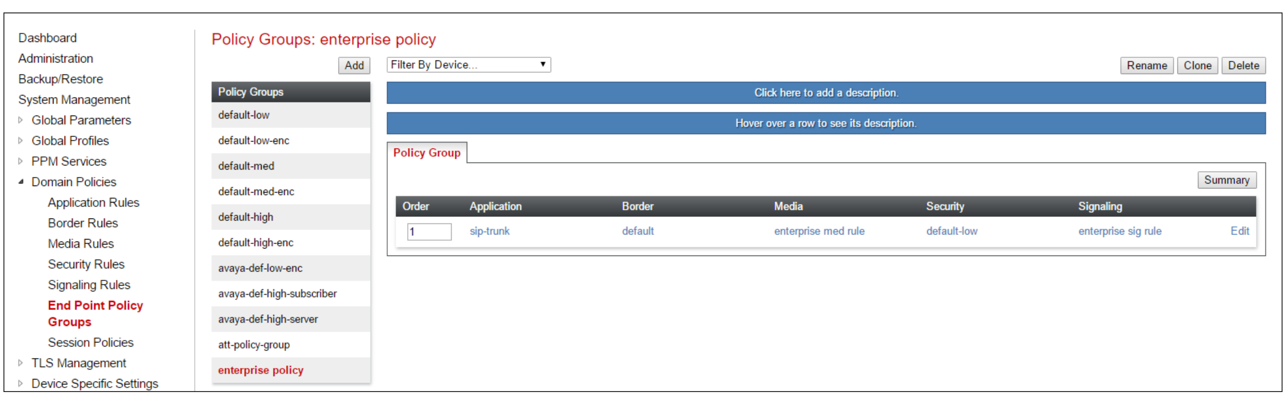


7.4.4. Endpoint Policy Groups – Enterprise Connection

Step 1 - Select **Domain Policies** from the menu on the left-hand side.
Step 2 - Select **End Point Policy Groups**.
Step 3 - Select **Add**.

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

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

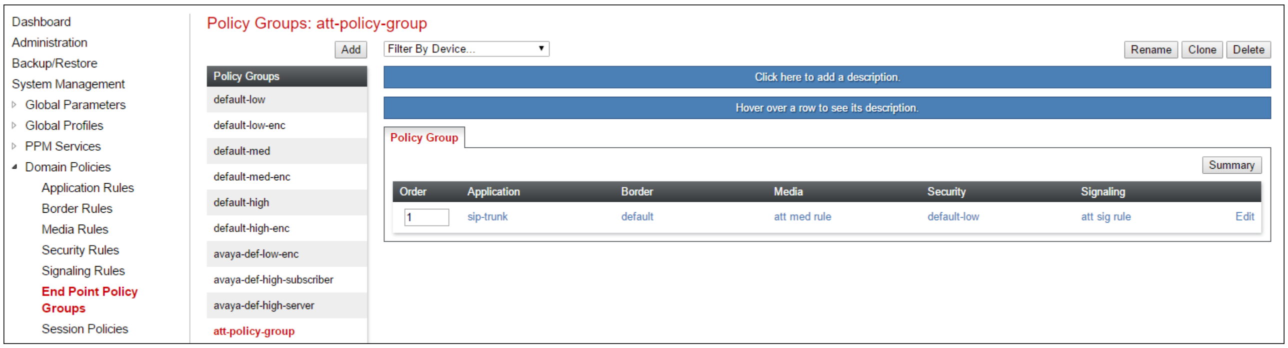


7.4.5. Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps **1** through **4** from **Section 7.3.4** with the following changes:

- **Group Name**: **att-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).

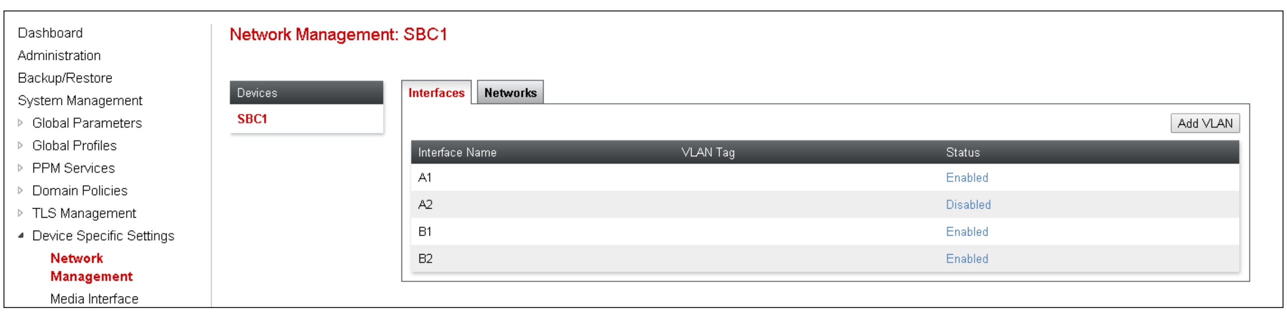


7.5. Device Specific Settings

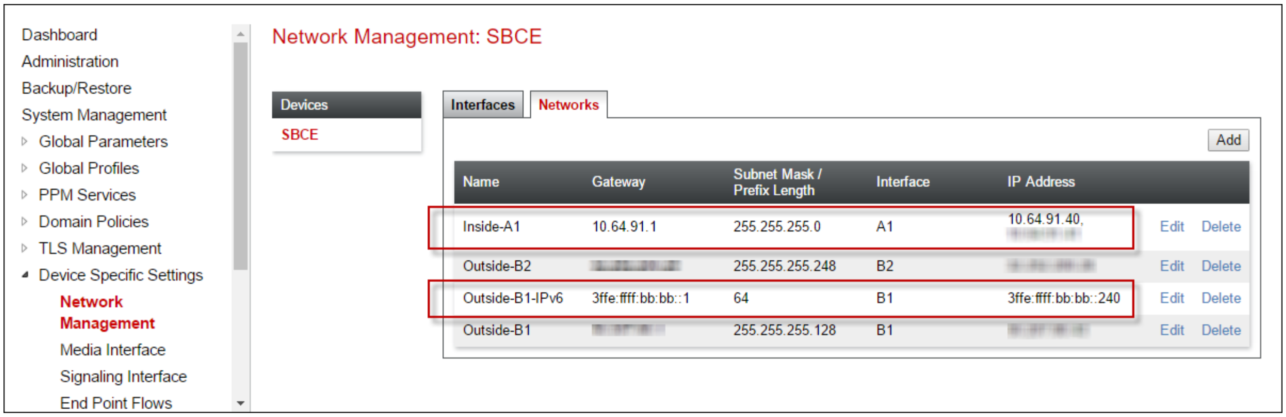
7.5.1. Network Management

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.



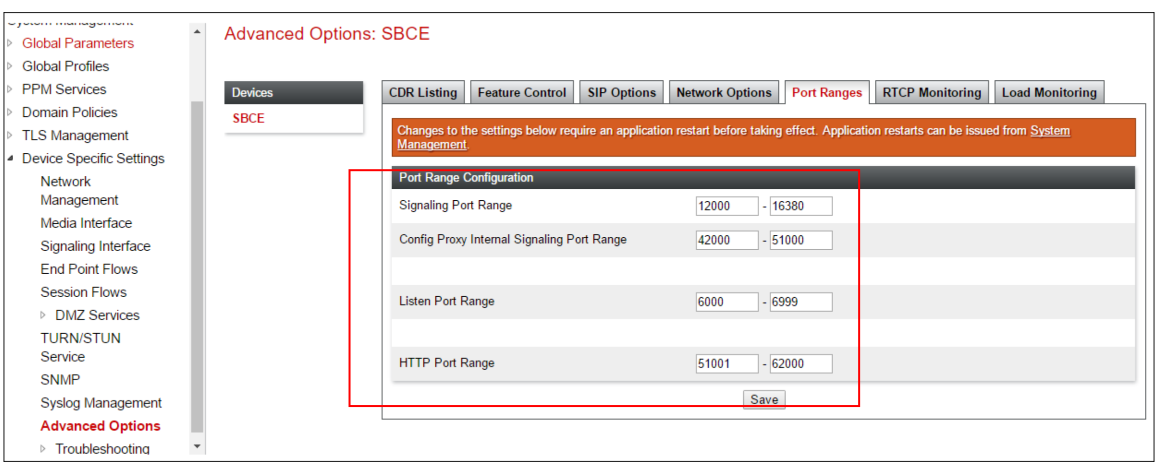
Step 3 - Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.



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**).



7.5.3. Media Interfaces

As mentioned in **Section 7.5.2**, the AT&T IPFR-EF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, though only the outside port range is required by the AT&T IPFR-EF service.

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side (not shown).
Step 2 - Select **Media Interface**.
Step 3 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

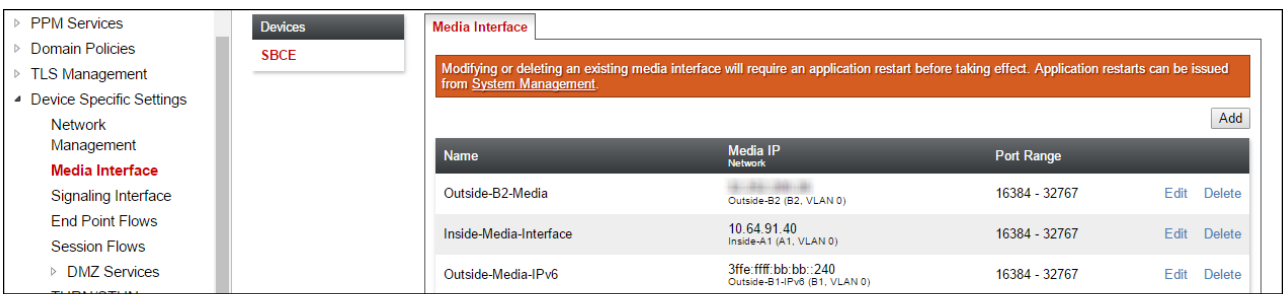
- **Name**: **Inside-Media-Interface**
- **IP Address**: Select **Inside- (A1,VLAN0)** and **10.64.91.40**
- **Port Range**: **16384 – 32767**

Step 4 - Click **Finish** (not shown).
Step 5 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: **Outside-Media-IPv6**
- **IP Address**: Select **Outside-B1-IPv6 (B1,VLAN0)** and **3ffe:ffff:bb:bb::240**
- **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.



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:

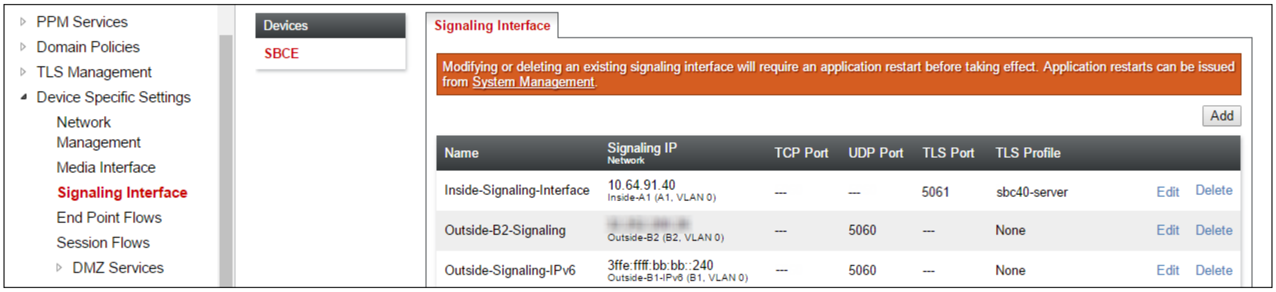
- **Name**: **Inside-Signaling-Interface**
- **IP Address**: Select **Inside-A1 (A1,VLAN0)** and **10.64.91.40**
- **TLS Port**: **5061**
- **TLS Profile**: Select the TLS server profile created in **Section 7.2.2** (e.g., **sbc40-server**)

Step 4 - Click **Finish** (not shown).
Step 5 - Select **Add** again, and enter the following:

- **Name**: **Outside-Signaling-IPv6**

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

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



7.5.5. Server Flows – For Session Manager

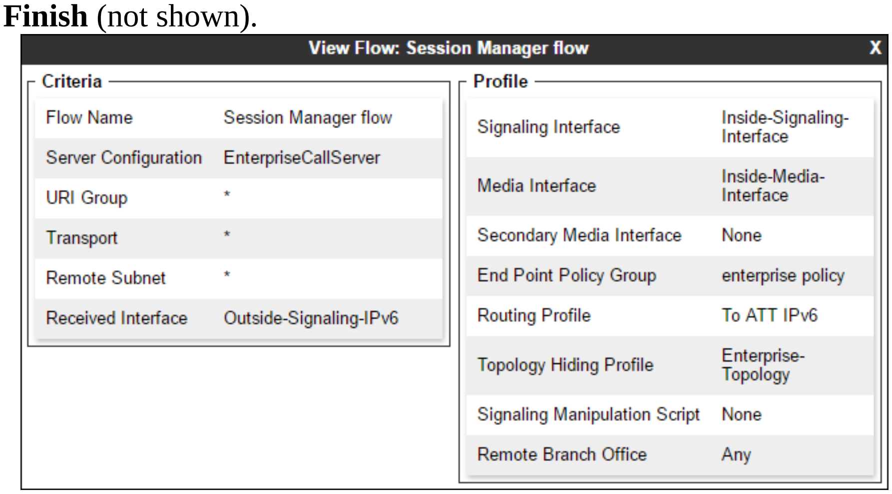
Step 1 - Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).

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

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

- **Flow Name**: **SM_Trunk**.
- **Server Configuration**: **SM_Trunk_SC** (**Section 7.3.4**).
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Outside-Signaling-IPv6** (**Section 7.5.4**).
- **Signaling Interface**: **Inside-Signaling-Interface** (**Section 7.5.4**).
- **Media Interface**: **Inside-Media-Interface** (**Section 7.5.3**).
- **End Point Policy Group**: **enterprise policy** (**Section 7.4.4**).
- **Routing Profile**: **to ATT IPv6** (**Section 7.3.7**).
- **Topology Hiding Profile**: **Enterprise-Topology** (**Section 7.3.8**).
- Let other values default.

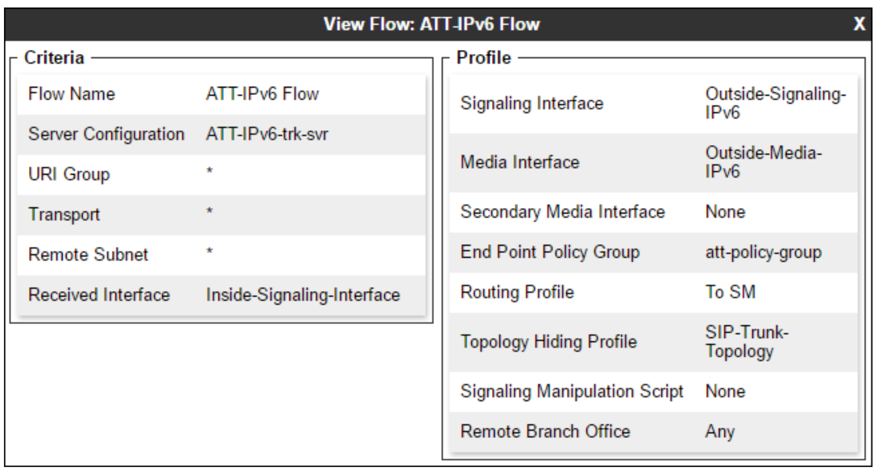
Step 4 - Click **Finish** (not shown).



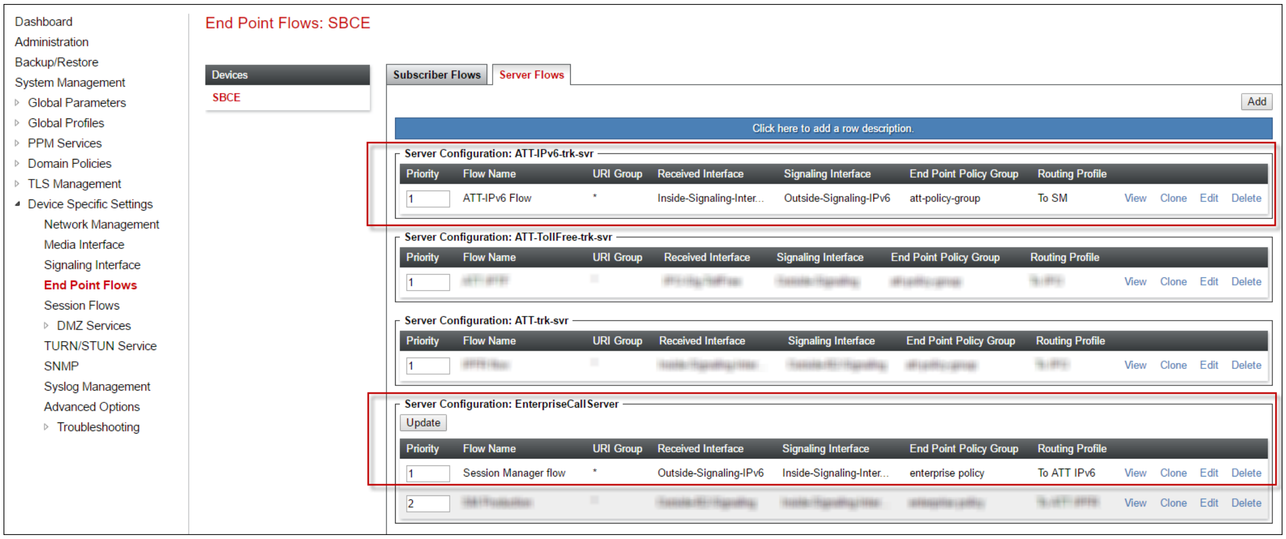
7.5.6. Server Flows – For AT&T

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

- **Flow Name**: **ATT**.
- **Server Configuration**: **ATT_SC** (**Section 7.3.5**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Inside-Signaling-Interface** (**Section 7.5.4**).
- **Signaling Interface**: **Outside-Signaling-IPv6 (Section 7.5.4**).
- **Media Interface**: **Outside-Media-IPv6** (**Section 7.5.3**).
- **End Point Policy Group**: **att-policy-group** (**Section 7.4.5**).
- **Routing Profile**: **To SM** (**Section 7.3.6**).
- **Topology Hiding Profile**: **SIP-Trunk-Topology** (**Section 7.3.9**).



The completed **End Point Flows** screen in the shared test environment is shown below.



8. Verification Steps

The following steps may be used to verify the configuration:

8.1. AT&T IP Flexible Reach – Enhanced Features

The following scenarios may be executed to verify Communication Manager, Session Manager, Avaya SBCE, and the AT&T IPFR-EF service interoperability:

- Place inbound and outbound calls, answer the calls, and verify that two-way talk path exists.
- Verify that calls remain stable and disconnect properly.
- Verify basic call functions such as hold, transfer, and conference.
- Verify the use of DTMF signaling.
- Place an inbound call to a telephone, but do not answer the call. Verify that the call covers to voicemail (e.g., Aura® Messaging). Retrieve voicemail messages either locally or from PSTN.
- Using the appropriate IPFR-EF access numbers and codes, verify that the following features are successful:
  - Network based Simultaneous Ring – The “primary” and “secondary” endpoints ring, and either may be answered.
  - Network based Sequential Ring (Locate Me) – Verify that after the “primary” endpoint rings for the designated time, the “secondary” endpoint rings and may be answered.
  - Network based Call Forwarding Always (CFA/CFU), Network based Call Forwarding Ring No Answer (CF-RNA), Network based Call Forwarding Busy (CF-Busy), Network based Call Forwarding Not Reachable (CF-NR) – Verify that based on each feature criteria, calls are successfully redirected and may be answered.
- Inbound / Outbound T.38 fax.
- SIP OPTIONS monitoring of the health of the SIP trunk.
- Incoming and outgoing calls using the G.729 (A or B) and G.711 ULAW codecs.

8.2. Avaya Aura® Communication Manager

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

- Tracing a SIP trunk.
  1. From the Communication Manager Element Cut-Through command line interface or console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., *05). Note that in the trace shown below, Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 14008, before sending the INVITE to Communication Manager.

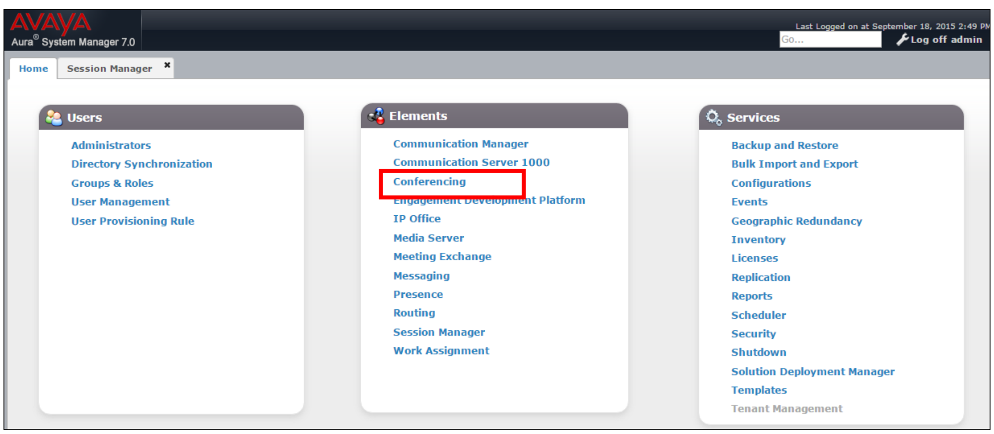
```
list trace tac *05                                                    Page    1
                                LIST TRACE
time            data
14:01:34 TRACE STARTED 03/06/2017 CM Release String cold-00.0.441.0-23523
14:01:42 SIP<INVITE sips:14008@avayalab.com;user=phone SIP/2.0
14:01:42     Call-ID: dcb15c538755192a2208d41f5ec50f0e
14:01:42     active trunk-group 5 member 1    cid 0x481
14:01:42     dial 14008
14:01:42     term station      14008 cid 0x481
14:01:42     Called party uses private-numbering
14:01:42 SIP>INVITE sips:14008@avayalab.com SIP/2.0
14:01:42     Call-ID: 197517e62b041e7947c0c2962ed4
14:01:42 SIP<SIP/2.0 100 Trying
14:01:42     Call-ID: 197517e62b041e7947c0c2962ed4
14:01:42 SIP<INVITE sips:14008@avayalab.com SIP/2.0
14:01:42     Call-ID: 197517e62b041e7947c0c2962ed4
14:01:42 SIP>INVITE sips:14008@avayalab.com SIP/2.0
14:01:42     Call-ID: 197517e62b041e7947c0c2962ed4
```

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

8.3. Avaya Aura® Session Manager

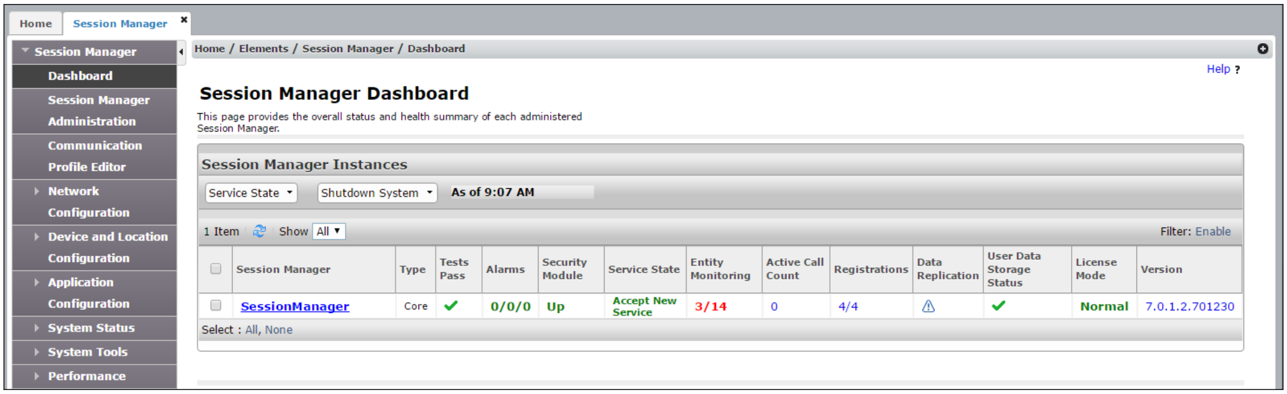
The Session Manager configuration may be verified via System Manager.

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

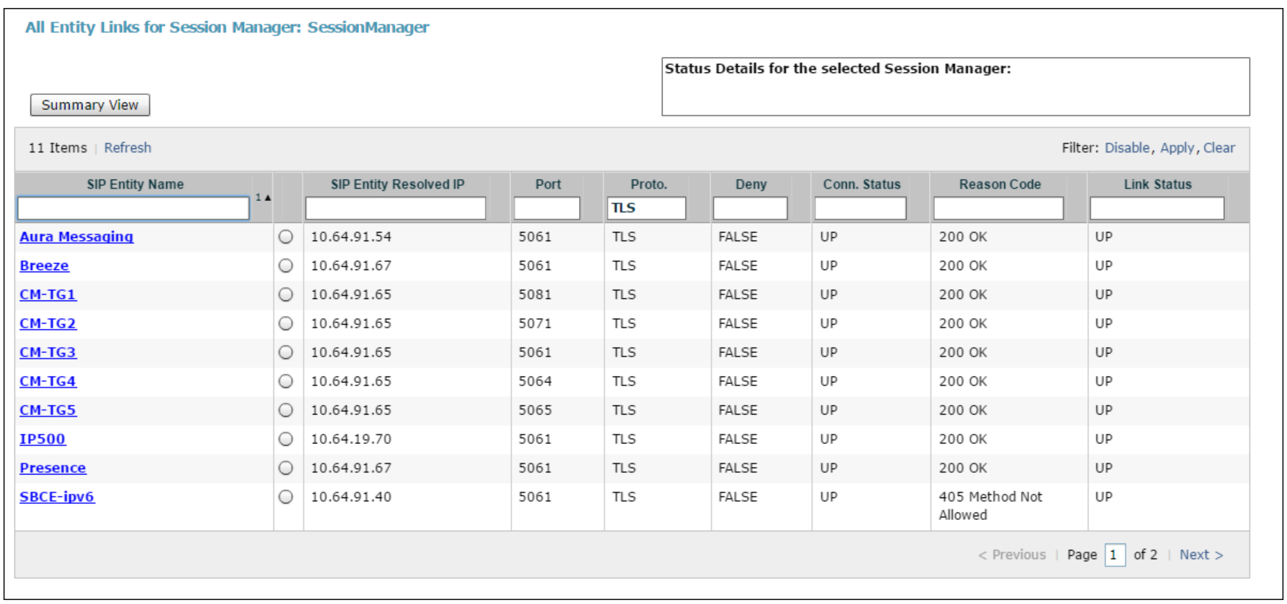


Step 2 - The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns all show good status.

In the **Entity Monitoring** column, Session Manager shows that there are **3** alarms out of the **14** Entities defined.



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



Note – The **SBCE-ipv6** Entity from the list of monitored entities above. The **Reason Code** column indicates that Session Manager has received a SIP **405 Method Not Allowed** response to the SIP OPTIONS it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Also note that the Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T IPFR-EF Border Element, and it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends it back to Session Manager.

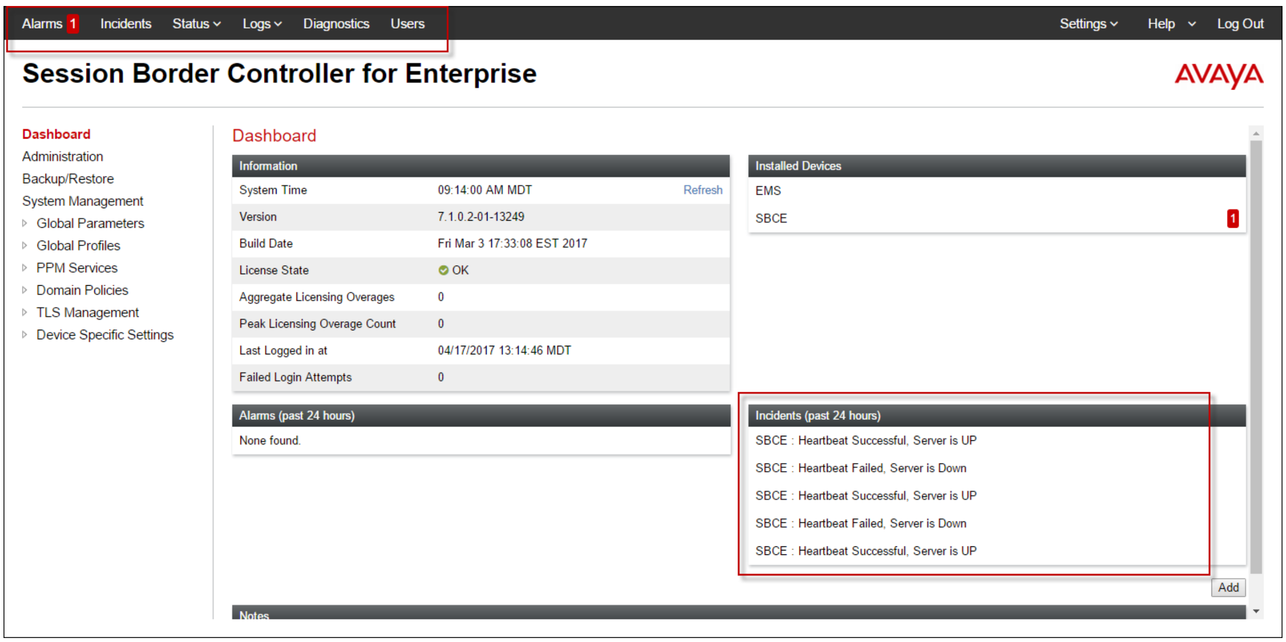
Another useful tool is to select **System Tools → Call Routing Test** (not shown) from the left hand menu. This tool allows specific call criteria to be entered, and the simulated routing of this call through Session Manager is then verified.

8.4. Avaya Session Border Controller for Enterprise

8.4.1. System Status

Various system conditions monitored by the Avaya SBCE may be displayed as follows.

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



8.4.2. Protocol Traces

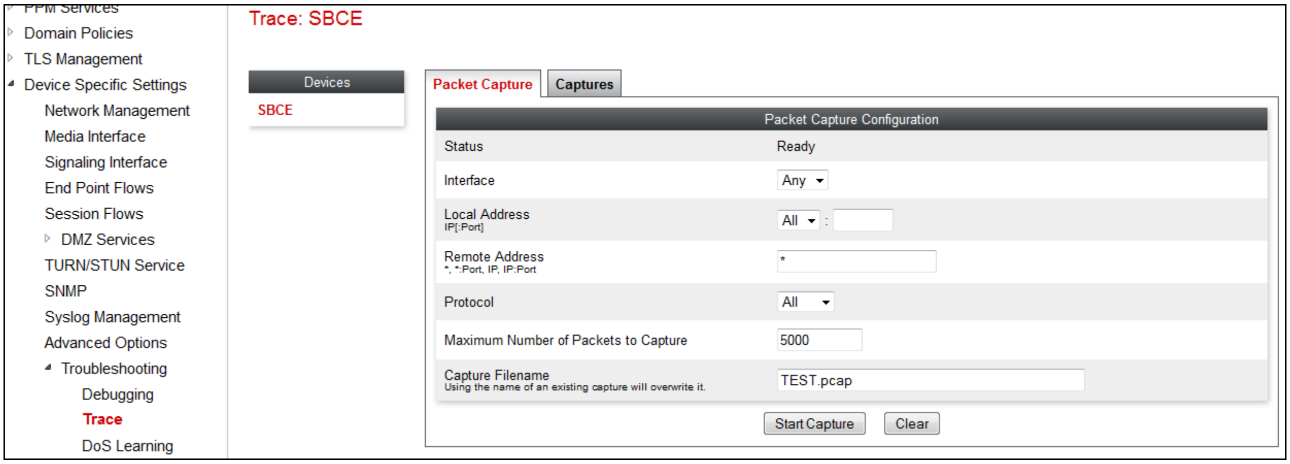
The Avaya SBCE can take internal traces of specified interfaces.

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

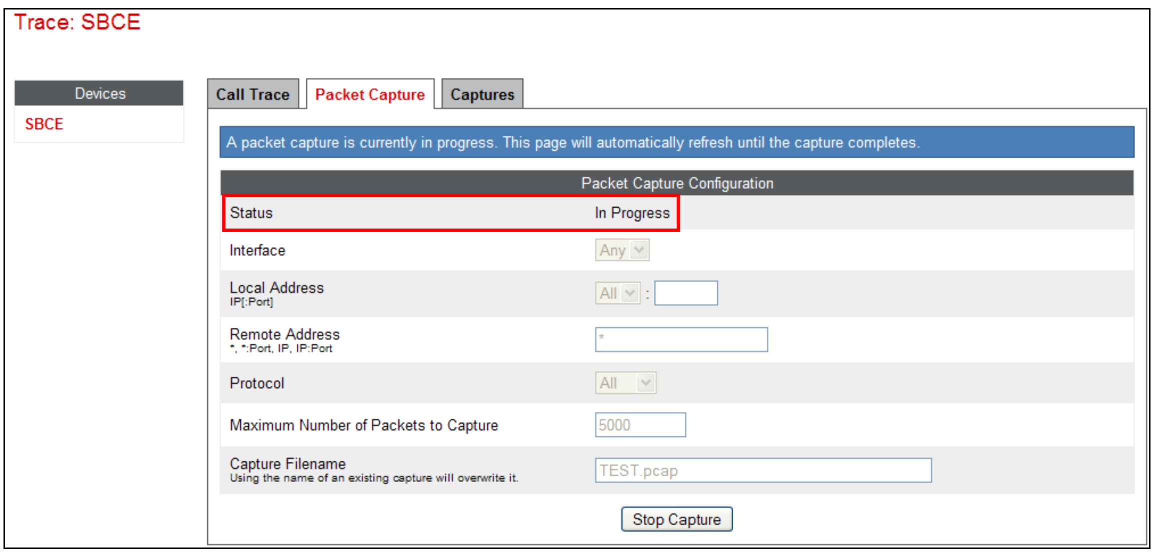
Step 2 - Select the **Packet Capture** tab and select the following:

- Select the desired **Interface** from the drop down menu (e.g., **All**).
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**)
- Specify a **Capture Filename** (e.g., **TEST.pcap**).
- Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
- Click **Start Capture** to begin the trace.

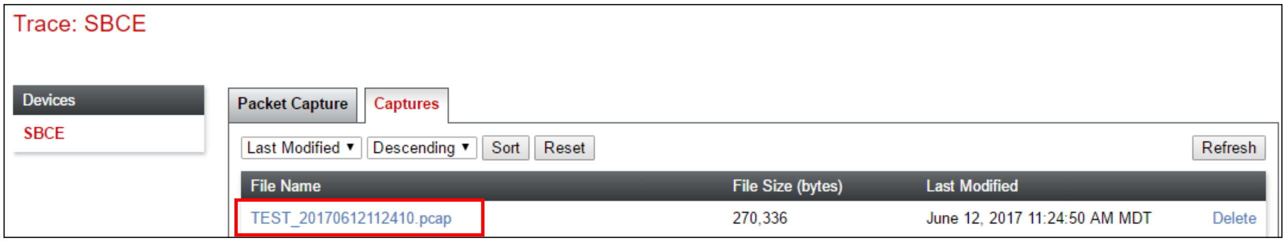
Note – Specifying **All** in the **Interface** field will result in the Avaya SBCE capturing traffic from both the A1 and B1 interfaces defined in the reference configuration. Also, when specifying the **Maximum Number of Packets to Capture**, be sure to estimate a number large enough to include all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



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



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.



9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.0.1, Avaya Aura® Session Manager 7.0.1, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.1, can be configured to interoperate successfully with the AT&T IP Flexible Reach – Enhanced Features service using IPv6, within the constraints described in **Section 2.2**.

Testing was performed on a production AT&T IP Flexible Reach – Enhanced Features service circuit. The reference configuration shown in these Application Notes is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

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 7.0.1, Issue 3, November 2016

[2] Administering Avaya Aura® Session Manager, Release 7.0.1, Issue 2, May 2016

[3] Deploying Avaya Aura® System Manager, Release 7.0.1, Issue 2, August 2016

[4] Administering Avaya Aura® System Manager for Release 7.0.2, Issue 3, January 2017

Avaya Aura® Communication Manager

[5] Deploying Avaya Aura® Communication Manager, Release 7.0.1, Issue 2.1, October 2016

[6] Administering Avaya Aura® Communication Manager, Release 7.0.1, 03-300509, Issue 2.1, August 2016

[7] Administering Avaya G430 Branch Gateway, Release 7.0.1, 03-603228, Issue 2, May 2016

[8] Deploying and Updating Avaya Aura® Media Server Appliance, Release 7.7, Issue 2, October 2015

[9] Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager, August 2015

Avaya Session Border Controller for Enterprise

[10] Administering Avaya Session Border Controller for Enterprise, Release 7.0, Issue 1, August 2015

[11] Deploying Avaya Session Border Controller for Enterprise, Release 7.0, Issue 1, August 2015

Avaya Aura® Messaging

[12] Administering Avaya Aura® Messaging, Release 6.3.3, Issue 1, August 2015

AT&T IP Flexible Reach - Enhanced Features Service:

[13] AT&T IP Flexible Reach - Enhanced Features Service description http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/

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.