AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1, and Avaya Session Border Controller for Enterprise 7.2 with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.0

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1, and Avaya Session Border Controller for Enterprise 7.2 with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. This service suite provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Communication Manager. The Communication Manager Network Call Redirection (NCR) and SIP User-to-User Information (UUI) features can be utilized together to transmit UUI within SIP signaling messages to alternate destinations via the Verizon network. These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solution & Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IPCC Services.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1, and Avaya Session Border Controller for Enterprise 7.2 with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. This service suite provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Communication Manager. The Communication Manager Network Call Redirection (NCR) and SIP User-to-User Information (UUI) features can be utilized together to transmit UUI within SIP signaling messages to alternate destinations via the Verizon network. These Application Notes update previously published Application Notes [VZ-IPCC] with a newer version of Session Manager, Communication Manager, and Avaya Session Border Controller for Enterprise.

In the sample configuration, an Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between the Avaya CPE and Verizon Business. The Avaya SBCE performs SIP header manipulation and provides topology hiding to convert the private Avaya CPE IP addressing to IP addressing or domains appropriate for the Verizon access method. Session Manager is used as the Avaya SIP trunking "hub" connecting to Communication Manager, the Avaya SBCE, and other applications.

The Verizon Business IPCC Services suite described in these Application Notes is designed for business customers. The suite provides inbound toll-free service via standards-based SIP trunks. Using SIP Network Call Redirection (NCR), trunk-to-trunk connections of certain inbound calls at Communication Manager can be avoided by requesting that the Verizon network transfer the inbound caller to an alternate destination. In addition, the Communication Manager SIP User-to-User Information (UUI) feature can be utilized with the SIP NCR feature to transmit UUI within SIP signaling messages to alternate destinations. This capability allows the service to transmit a limited amount of call-related data between call centers to enhance customer service and increase call center efficiency. Examples of UUI data might include a customer account number obtained during a database query or the best service routing data exchanged between sites using Communication Manager.

Verizon Business IPCC Services suite is a portfolio of IP Contact Center (IPCC) interaction services that includes VoIP Inbound and IP Interactive Voice Response (IP-IVR). Access to these features may use Internet Dedicated Access (IDA) or Private IP (PIP). PIP was used for the sample configuration described in these Application Notes. VoIP Inbound is the base service offering that offers core call routing and termination features. IP-IVR is an enhanced service offering that includes features such as menu-routing, custom transfer, and additional media capabilities.

For more information on the Verizon Business IP Contact Center service, visit
http://www.verizonenterprise.com/products/business-communications/customer-contact-solutions/

2. General Test Approach and Test Results

The Avaya equipment depicted in **Figure 1** was connected to the commercially available Verizon Business IPCC Services. This allowed PSTN users to dial toll-free numbers assigned by Verizon. The toll-free numbers were configured to be routed within the enterprise to Communication Manager numbers, including Vector Directory Numbers (VDNs). The VDNs were associated with vectors configured to exercise Communication Manager ACD functions as well as Verizon Business IPCC Services such as network call redirection to PSTN destinations and network call redirection with UUI.

The test approach was manual testing of inbound and referred calls using the Verizon Business IPCC Services on a production Verizon PIP access circuit, as shown in **Figure 1**.

The main objectives were to verify the following features and functionality:

- Inbound Verizon toll-free calls to Communication Manager telephones and VDNs/Vectors
- Inbound private toll-free calls (e.g., PSTN caller uses *67 followed by the toll-free number)
- Inbound Verizon toll-free calls redirected using Communication Manager SIP NCR (via SIP REFER/Refer-To) to PSTN alternate destinations
- Inbound Verizon IP toll-free calls redirected using Communication Manager SIP NCR with UUI (via SIP REFER/Refer-To with UUI) to a SIP-connected destination
- Inbound toll-free voice calls can use G.711MU or G.729A codecs
- Inbound toll-free voice calls can use DTMF transmission using RFC 2833

Testing was successful. Test observations or limitations are described in **Section 2.2**.

See **Section 3.2** for an overview of key call flows and **Section 9** for detailed verifications and traces illustrating key call flows.

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.

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 Verizon Business IPCC Services did not include use of any specific encryption features as requested by Verizon.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products wherever possible.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the execution of test cases details in the Verizon-authored interoperability test plan.

- SIP OPTIONS monitoring of the health of the SIP trunks was verified. Both the Avaya enterprise equipment and Verizon Business can monitor health using SIP OPTIONS.
- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya location. Configuration was varied such that these incoming toll-free calls were directed to Communication Manager telephone extensions, and Communication Manager VDNs containing call routing logic to exercise SIP Network Call Redirection.
- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a toll free call before the call has been answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a toll-free number directed to a busy user or resource when no redirection on busy conditions was configured (which would be unusual in a contact center).
- Proper termination of an inbound IP Toll Free call left in a ringing state for a relatively long duration, which again would be unusual in a contact center. In the sample configuration, Verizon sent a SIP CANCEL to cancel the call after three minutes of ring no answer conditions, returning busy tone to the PSTN caller.
- Privacy requests for inbound toll-free calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67 from a mobile phone), the inbound toll-free call can be successfully completed while withholding presentation of the PSTN caller ID to user displays. (When the caller requests privacy, Verizon IPCC sends the caller ID in the P-Asserted-Identity header and includes “Privacy: id” which is honored by Communication Manager).
- Inbound toll-free call long holding time call stability. The Avaya CPE sends a re-INVITE with SDP to refresh the session at the configured session refresh interval specified on the Communication Manager trunk group handling the call. In the sample configuration, the session refresh re-INVITE was sent after 900 seconds (15 minutes), the interval configured for the trunk group in **Section 6.8.1**. The call continued with proper talk path.
- Telephony features such as hold and resume. When a Communication Manager user holds a call in the sample configuration, Communication Manager will send a re-INVITE to Verizon IP Toll Free service with a media attribute “sendonly”. The Verizon 200 OK to this re-INVITE will include media attribute “recvonly”. While the call remains on hold, RTP will flow from the Avaya CPE to Verizon, but no RTP will flow from Verizon to the Avaya CPE (i.e., as intended). When the user resumes the call from hold, bi-directional media path resumes. Although it would be unexpected in a contact center, calls on hold for

longer than the session refresh interval were tested, and such calls could be resumed after the session refresh re-asserted the "sendonly" state.

- Transfer of toll-free calls between Communication Manager users.
- Incoming voice calls using the G.729A and G.711 ULAW codecs, and proper protocol procedures related to media.
- DTMF transmission using RFC2833. For inbound toll-free calls, PSTN users dialing post-answer DTMF digits are recognized properly by the Avaya CPE.
- Proper DiffServ markings for SIP signaling and RTP media flowing from the Avaya CPE to Verizon.
- Incoming fax calls using T.38.
- Remote Avaya SIP endpoints connected through Avaya SBCE were used along with local Avaya endpoints in the verification of these Application Notes.

2.2. Test Results

The interoperability compliance testing of the sample configuration was completed with successful results as described in **Section 2.1**. The following observations may be noteworthy:

- Verizon Business IPCC Services suite does not support History Info or Diversion Headers. The Avaya CPE will not send History-Info or Diversion header to Verizon IPCC in the sample configuration.

- Verizon Business IPCC Services suite does not support SIP 302 Redirect.

- Verizon Business IPCC Services suite does not support G.729 Annex B. When using G729, the Avaya CPE will always include "annexb=no" in SDP in the sample configuration.

- **Section 3.2.3** summarizes a call flow that would theoretically allow a call to remain in Communication Manager vector processing upon failure of a vector-triggered REFER attempt. However, most such call scenarios could not be verified on the production Verizon circuit used for testing. On the production circuit, Verizon would send a BYE to terminate the call upon encountering REFER transfer failures, so there was no opportunity for the call to remain in Communication Manager vector processing. See **Section 3.2.3** for additional information.

- During testing, Verizon's IP Interactive Voice Response (IP-IVR) service did not accept the SIP REFER method unless the URI in the Refer-To header included the IP address presented in the From header within the original SIP INVITE. This IP address was different from the IP address included in the Contact header. The Avaya SBCE Topology Hiding profile was used to populate the From header IP address in the Refer-To header for both the IP-IVR and IP Toll Free services. Calls were successfully diverted using REFER for both Verizon services with this Topology Hiding profile in place. See **Section 7.3.9** for additional information.

2.3. Support

2.3.1 Avaya

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com

2.3.2 Verizon

For technical support on Verizon Business IPCC Services offer, visit online support at http://www.verizonenterprise.com/support/

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Verizon Business IPCC Services node. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location is an Avaya Session Border Controller for Enterprise. The Avaya SBCE receives traffic from the Verizon Business IPCC Services on port 5060 and sends traffic to the Verizon Business IPCC Services using destination port 5072, using UDP for transport. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon Business IPCC Services node.

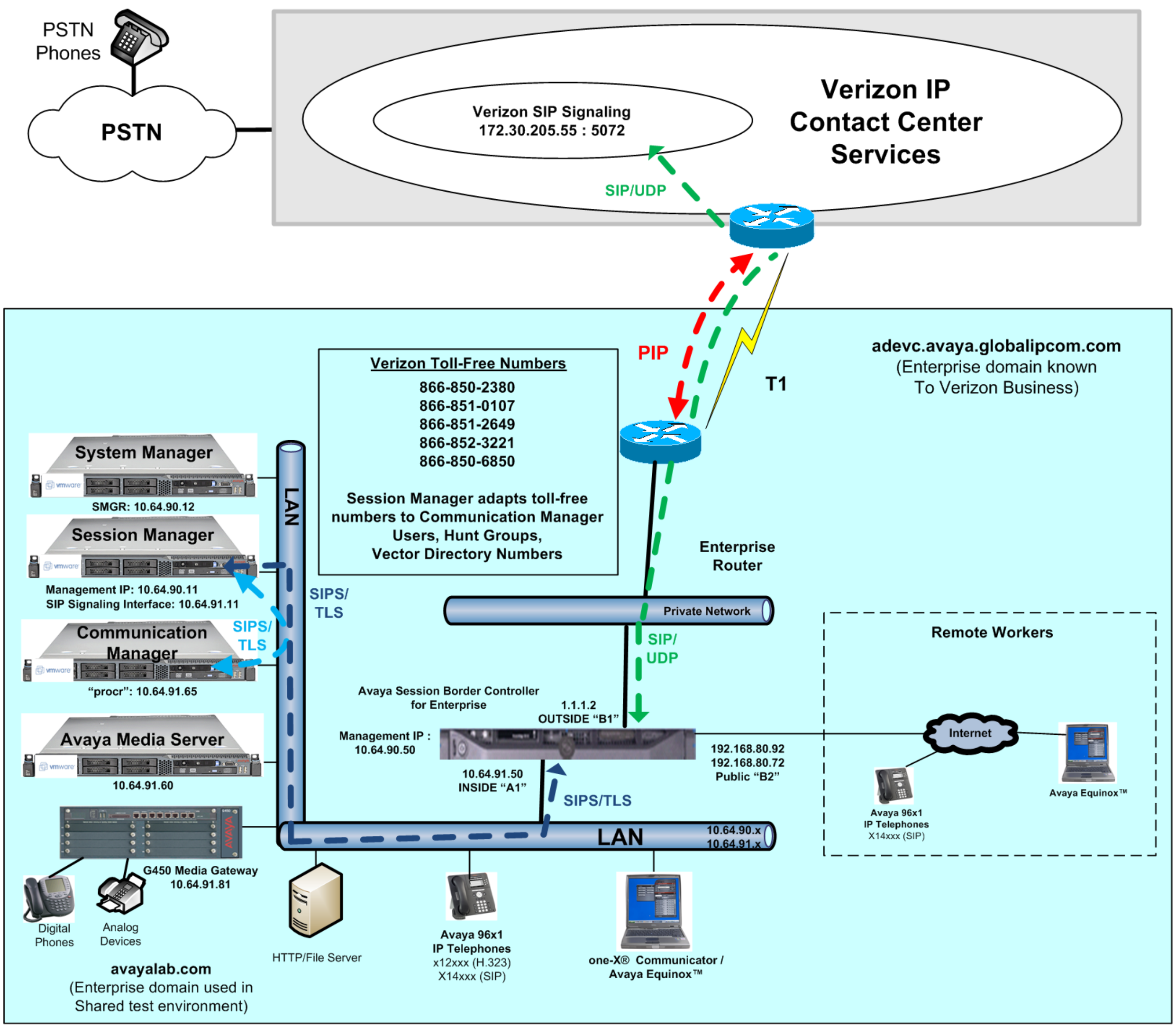


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon toll-free numbers were mapped by Session Manager to various Communication Manager extensions. The extension mappings were varied during the testing to allow inbound toll-free calls to terminate directly on user extensions or indirectly through hunt groups, vector directory numbers (VDNs) and vectors to user extensions and contact center agents.

The Avaya CPE environment was known to Verizon Business IPCC Services as FQDN "*adevc.avaya.globalipcom.com*". For efficiency, the Avaya CPE environment utilizing Session Manager Release 7.1 and Communication Manager Release 7.1 was shared among other ongoing test efforts at the Avaya Solutions and Interoperability Test lab. Access to the Verizon Business IPCC Services was added to a configuration that already used domain "*avayalab.com*" at the enterprise. As such, the Avaya SBCE is used to adapt the domains as needed. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to Verizon.

The following summarizes various header contents and manipulations for toll-free calls in the sample configuration:

- Verizon Business IPCC Services node sends the following in the initial INVITE to the CPE:
  - The CPE FQDN of ***adevc.avaya.globalipcom.com*** in the Request URI.
  - The Verizon Business IPCC Services gateway IP address in the From header.
  - The enterprise SBC outside IP address (e.g., 1.1.1.2) in the To header.
  - Sends the INVITE to Avaya CPE using destination port 5060 via UDP
- Avaya Session Border Controller for Enterprise sends Session Manager:
  - The Request URI contains ***avayalab.com.***
  - The host portion of the From header and PAI header contains ***avayalab.com***
  - The host portion of the To header contains ***avayalab.com***
  - Sends the packet to Session Manager using destination port 5060 via TCP
- Session Manager sends Communication Manager
  - The Request URI contains ***avayalab.com***, to match the shared Avaya SIL test environment.
  - Sends the packet to Communication Manager using destination port 5071 via TLS to allow Communication Manager to distinguish Verizon traffic from other traffic arriving from the same instance of Session Manager.

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use FQDNs and IP addressing appropriate for the unique customer environment.

3.1. History Info and Diversion Headers

The Verizon Business IPCC Services suite does not support SIP History Info headers or Diversion headers. Therefore, Communication Manager was provisioned not to send History Info headers or Diversion headers.

3.2. Call Flows

To understand how inbound Verizon toll-free calls are handled by Session Manager and Communication Manager, key call flows are summarized in this section.

3.2.1 Inbound IP Toll Free Call with no Network Call Redirection

The first call scenario illustrated in **Figure 3** is an inbound Verizon IP Toll Free call that is routed to Communication Manager, which in turn routes the call to a vector, agent, or phone. No redirection is performed in this simple scenario. A detailed verification of such a call with Communication Manager traces can be found in **Section 9.1.1**.

1. A PSTN phone originates a call to a Verizon IP Toll Free number.
2. The PSTN routes the call to the Verizon IP Toll Free service network.
3. The Verizon IP Toll Free service routes the call to the Avaya Session Border Controller for Enterprise.
4. The Avaya Session Border Controller for Enterprise performs any configured SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any configured SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed. In this case, Session Manager routes the call to Communication Manager using a unique port so that Communication Manager can distinguish this call as having arrived from Verizon IPCC.
6. Depending on the called number, Communication Manager routes the call to a) a hunt group or vector, which in turn routes the call to an agent or phone, or b) directly to a phone.

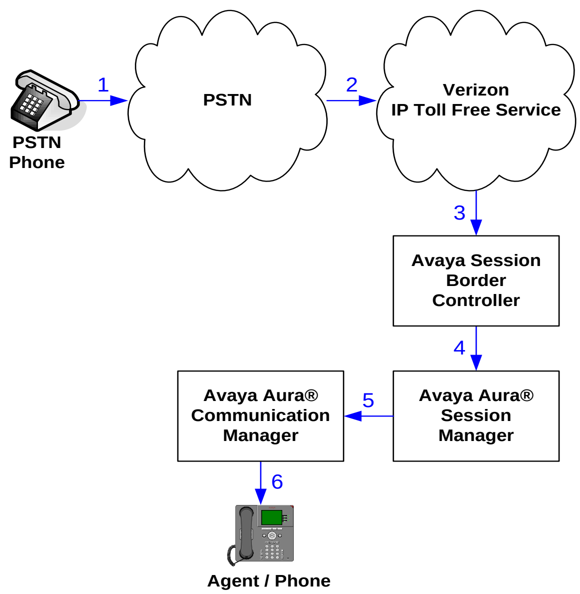


Figure 3: Inbound Verizon IP Toll Free Call – No Redirection

3.2.2 Inbound IP Toll Free Call with Post-Answer Network Call Redirection

The second call scenario illustrated in **Figure 4** is an inbound Verizon IP Toll Free call that is routed to a Communication Manager Vector Directory Number (VDN) to invoke call handling logic in a vector. The vector answers the call and then redirects the call back to the Verizon IP Toll Free service for routing to an alternate destination. Note that Verizon IP Toll Free service does not support redirecting a call before it is answered (using a SIP 302), and therefore the vector must include a step that results in answering the call, such as playing an announcement, prior to redirecting the call using REFER.

A detailed verification of such call with Communication Manager traces can be found in **Section 9.1.2** for a Verizon IP Toll Free SIP-connected alternate destination. In this example, the Verizon IP Toll Free service can be used to pass User to User Information (UUI) from the redirecting site to the alternate destination.

1. Same as the first five steps in **Figure 3**.
2. Communication Manager routes the call to a vector, which answers the call, plays an announcement, and attempts to redirect the call by sending a SIP REFER message out the SIP trunk from which the inbound call arrived. The SIP REFER message specifies the alternate destination in the Refer-To header. The SIP REFER message passes back through Session Manager and the Avaya SBCE to the Verizon IP Toll Free service network.
3. The Verizon IP Toll Free service places a call to the target party contained in the Refer-To header. Upon answer, the calling party is connected to the target party.
4. The Verizon IP Toll Free service notifies the Avaya CPE that the referred call has been answered (NOTIFY/sipfrag 200 OK). Communication Manager sends a BYE. The calling party and the target party can talk. The trunk upon which the call arrived in Step 1 is idle.

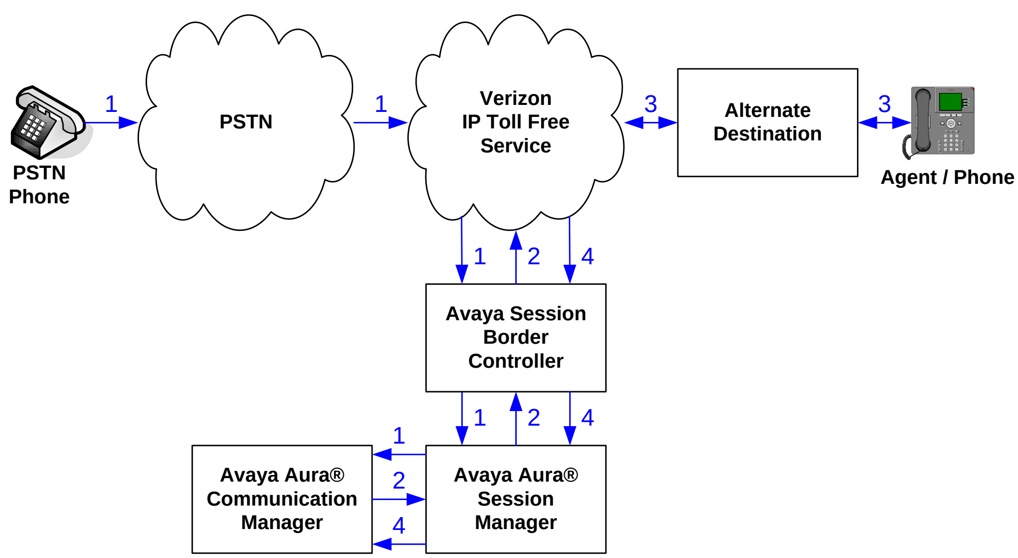


Figure 4: Inbound Verizon IP Toll Free– Post-Answer SIP REFER Redirection Successful

3.2.3 Inbound IP Toll Free Call with Unsuccessful Network Call Redirection

The next call scenario illustrated in **Figure 5** is similar to the previous call scenario, except that the redirection is unsuccessful. In theory, if redirection is successful, Communication Manager can "take the call back" and continue vector processing. For example, the call may route to an alternative agent, phone, or announcement after unsuccessful NCR.

1. Same as **Figure 4**.
2. Same as **Figure 4**.

3. The Verizon IP Toll Free service places a call to the target party (alternate destination), but the target party is busy or otherwise unavailable.
4. The Verizon IP Toll Free service notifies the redirecting/referring party (Communication Manager) of the error condition.
5. Communication Manager routes the call to a local agent, phone, or announcement.

However, as noted in **Section 2.2**, except for egregious configuration errors, this “REFER error handling” scenario could not be verified on the production Verizon circuit used for testing. On the production circuit, Verizon sends a SIP BYE which terminates Communication Manager vector processing for failure scenarios. For example, if a 486 Busy is received from the target of the REFER, Verizon will send a BYE immediately after a “NOTIFY/sipfrag 486”, which precludes any further call processing by Communication Manager. As another example, in cases where mis-configuration is introduced to cause the Refer-To header to be malformed (e.g., no “+” in Refer-To), Verizon will send a BYE immediately after a “NOTIFY/sipfrag 603 Server Internal Error”. If REFER is configured in the vector, but Network Call Redirection is not enabled for the SIP trunk group, Communication Manager will not send the REFER to Verizon, and vector processing will continue at the step following the route-to step that would normally trigger the REFER.

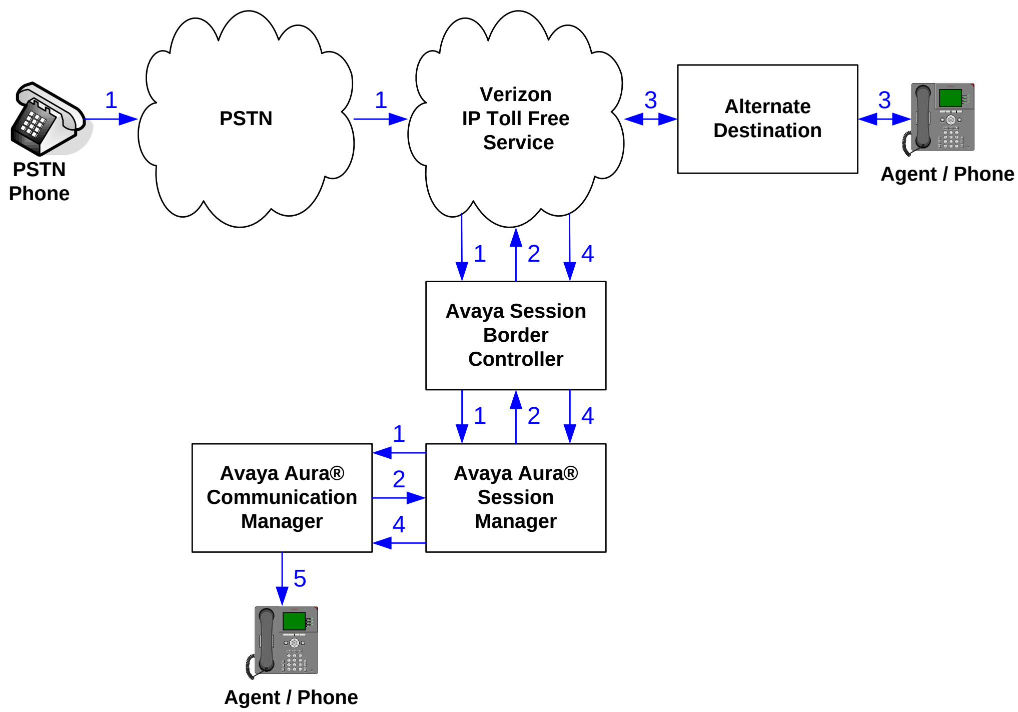


Figure 5: Inbound Verizon IP Toll Free– Post-Answer SIP REFER Redirection Unsuccessful

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	7.1.0.532.0-23985 (7.1.1.0.0-FP1)
Avaya Aura® System Manager	7.1.1.0.046931
Avaya Aura® Session Manager	7.1.1.0.711008
Avaya Session Border Controller for Enterprise	7.2.0.0-18-13712
Avaya Aura® Messaging	7.0 SP 0
Avaya Aura® Media Server	7.8.0.323
G450 Gateway	38.18.0
Avaya 96X1- Series Telephones (SIP)	R7.1.0.1.1
Avaya 96X1- Series Telephones (H323)	R6.6401
Avaya Equinox for Windows	3.2.1.11
Avaya 2400-Series Digital Telephones	N/A
Ventafax	7.9

Table 1: Equipment and Software Used in the Sample Configuration

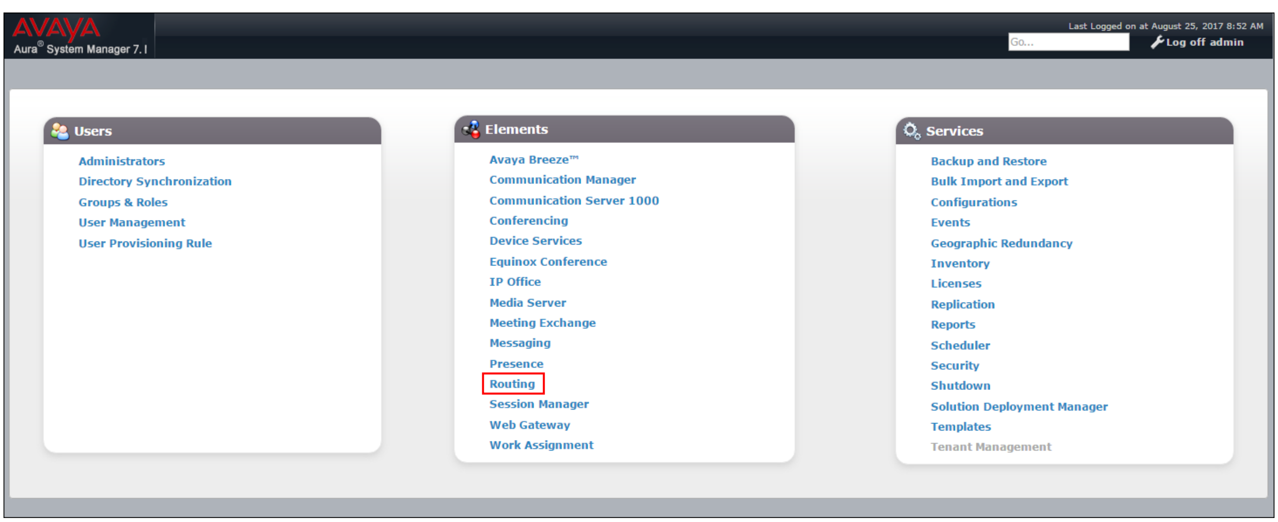
5. Configure Avaya Aura® Session Manager Release 7.1

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 https://<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**.



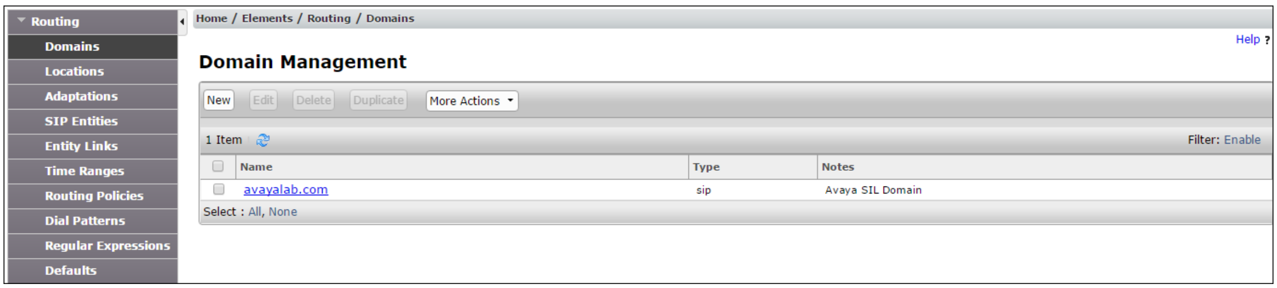
5.1. SIP Domain

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, two Locations are specified:

- **Main** – The customer site containing System Manager, Session Manager, Communication Manager and local SIP endpoints.
- **Common** – Avaya SBCE

5.2.1 Main Location

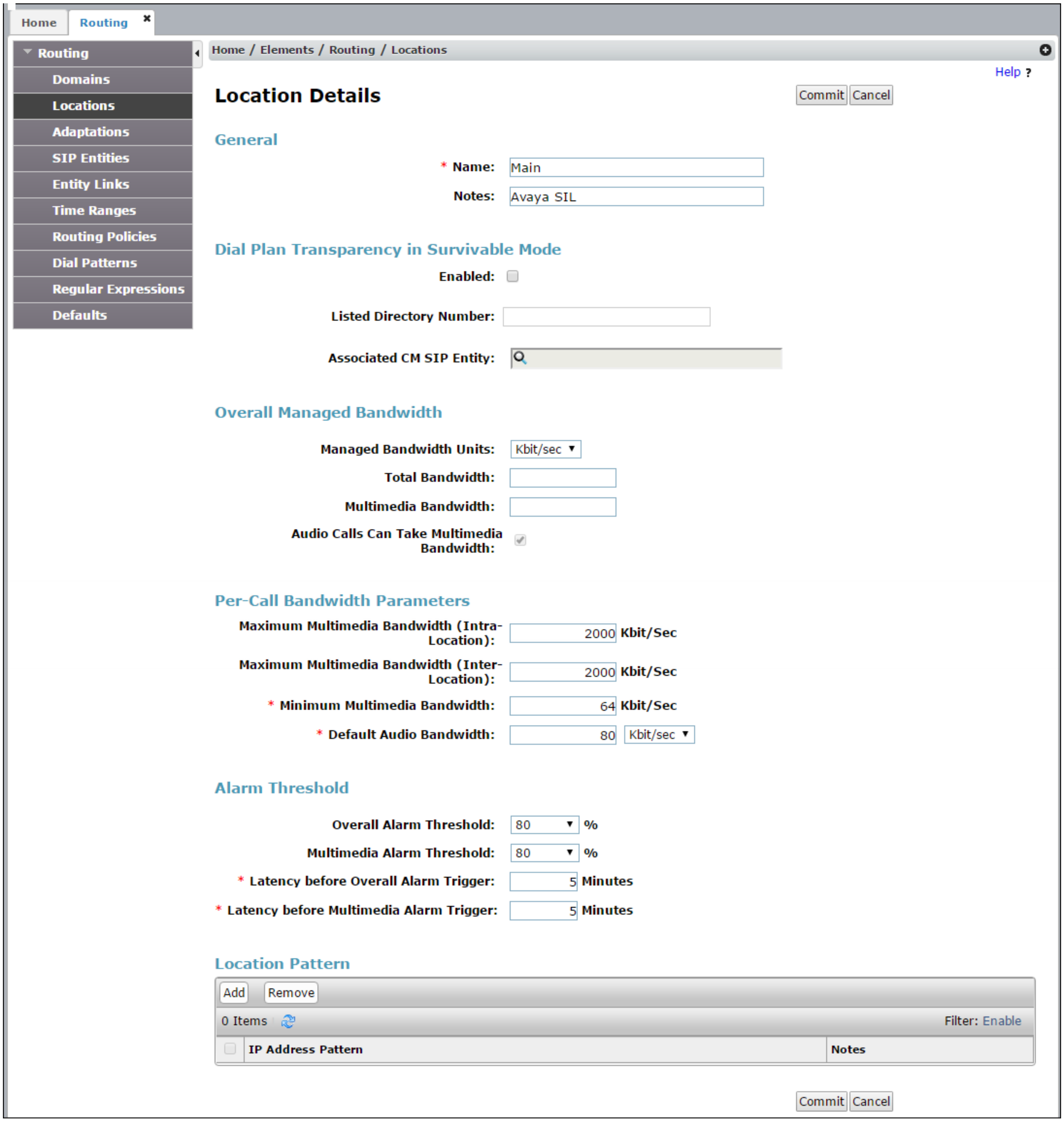
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **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 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 from Verizon to Communication Manger.

- Calls from Verizon - Modification of SIP messages sent to Communication Manager extensions/VDNs.
- The Verizon called number digit string in the Request URI is replaced with the associated Communication Manager extensions defined for Agent skill queue VDNs/telephones.

5.3.1 Adaptation for Avaya Aura® Communication Manager Extensions

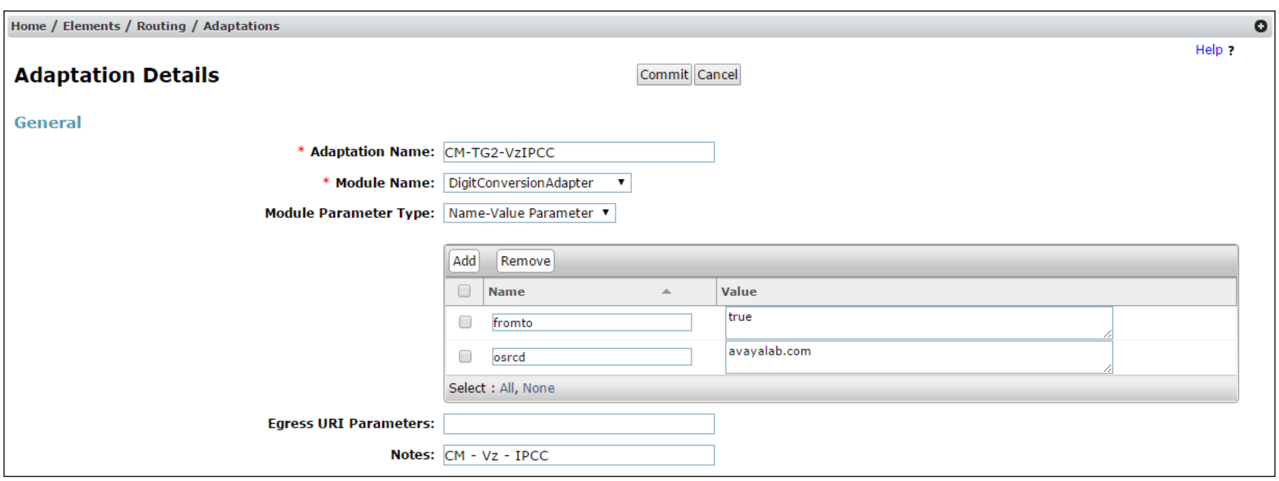
The Adaptation administered in this section is used for modification of SIP messages to Communication Manager extensions from Verizon.

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-TG2-VzIPCC**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down.
3. Select **Name-Value Parameter** from the **Module Parameter Type** drop down:
   - **Name**: **fromto** **Value**: **true**
     - This adapts the From and To headers along with the Request-Line and PAI headers.
   - **Name**: **osrcd** **Value**: **avayalab.com**
     - This enables the source domain to be overwritten with "avayalab.com". For example, for inbound PSTN calls from Verizon to Communication Manager, the PAI header will contain "avayalab.com".

Note – Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.



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

1. **Example 1 – destination extension**: 8668502380 is a DNIS string sent in the Request URI by the Verizon Business IPCC Services that is associated with Communication Manager VDN 10004.
    - Enter **8668502380** in the **Matching Pattern** column.
    - Enter **10** in the **Min/Max** columns.
    - Enter **10** in the **Delete Digits** column.
    - Enter **10004** 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 Verizon 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.

Digit Conversion for Outgoing Calls from SM

Add Remove

6 Items Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* +	* 12	* 12		* 2		origination		E.164 Calling Number Conversion
	* 8668502380	* 10	* 10		* 10	10004	destination		Call Center
	* 8668506850	* 10	* 10		* 10	14000	destination		DTMF Test
	* 8668510107	* 10	* 10		* 10	10003	destination		REFER with UUI
	* 8668512649	* 10	* 10		* 10	12003	destination		Refer-To Target of UUI Test VDN
	* 8668523221	* 10	* 10		* 10	10001	destination		Refer-To PSTN Test VDN

Select : All, None

5.3.2 Adaptation for the Verizon Business IPCC Services

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

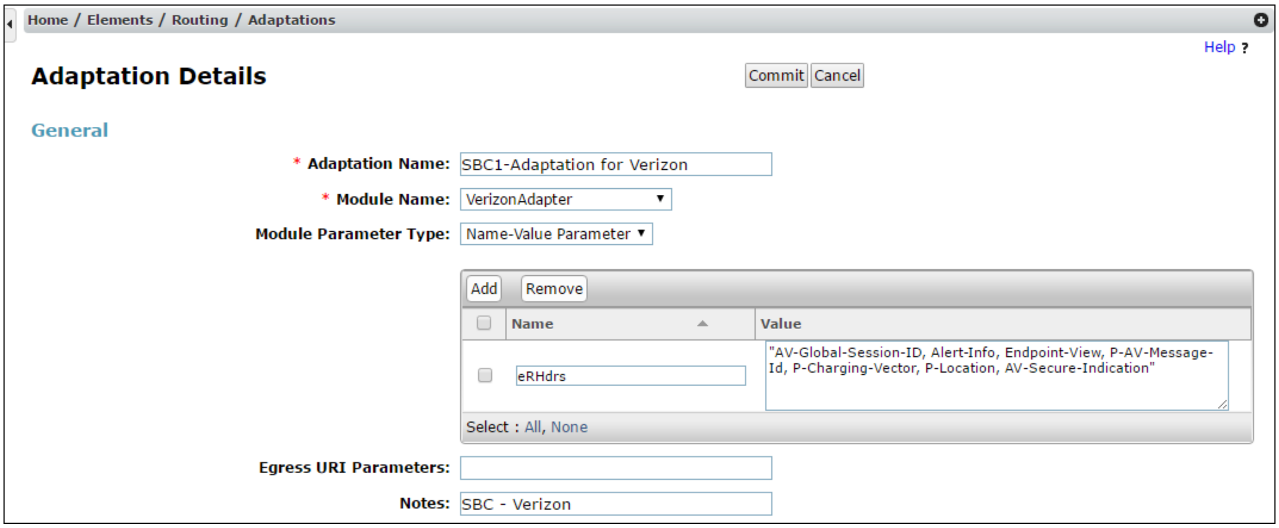
Step 1 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **SBC1-Adaptation for Verizon**).
2. Select **VerizonAdapter** from the **Module Name** drop down menu.

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**
    - **Value** – Enter the following Avaya headers to be removed by Session Manager. **"AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, AV-Correlation-ID, Av-Secure-Indication"**



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 Verizon trunk access (**Section 5.4.2**) – This entity, and its associated Entity Link (using TLS with port 5071), is for calls from Verizon 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 from the Verizon Business IPCC Services 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 5071), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the Verizon Business IPCC Services uses UDP/5072 per Verizon requirements.

5.4.1 Avaya Aura® Session Manager SIP Entity

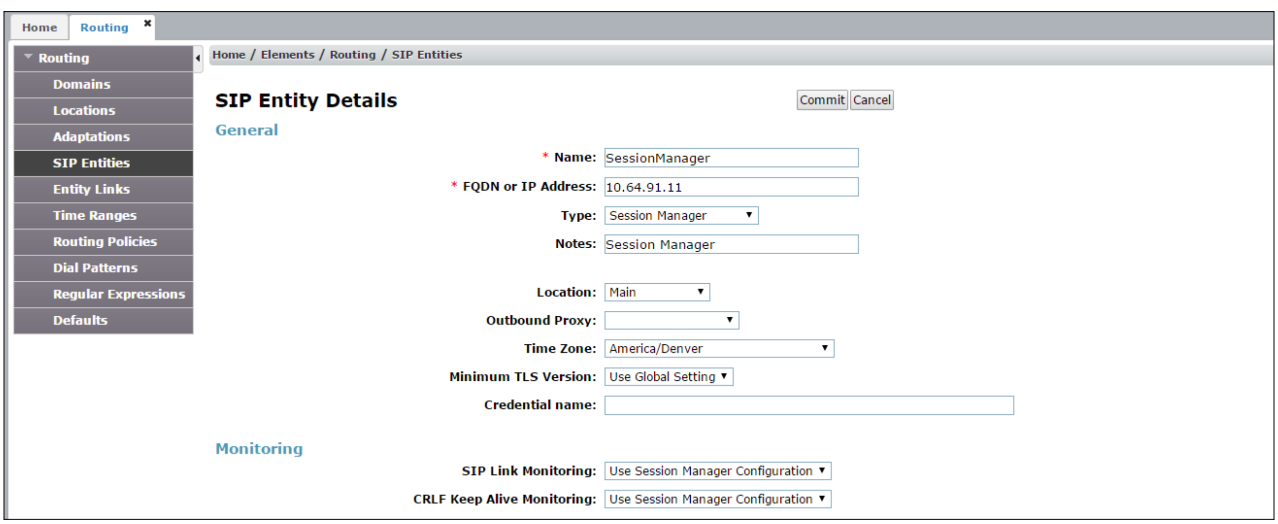
Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

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., **10.64.91.11**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 5.2.1**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.
- **Minimum TLS Version** – Select the TLS version, or select **Use Global Settings** to use the default TLS version, configurable at the global level (**Elements→Session Manager→Global Settings**).

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

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



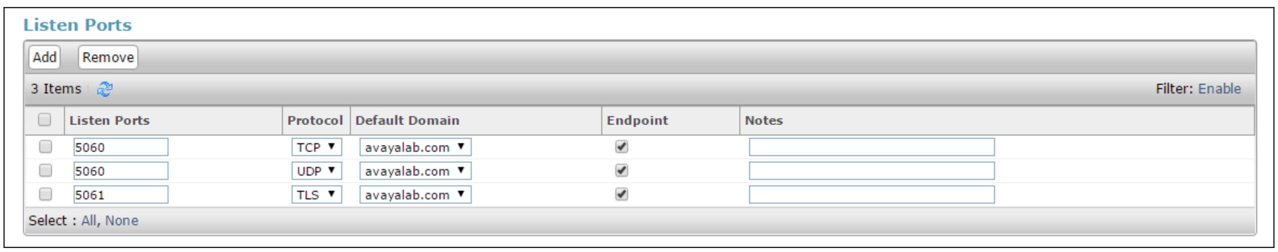
Step 4 - Scrolling down to the **Listen Port** section of the **SIP Entity Details** page. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 5.5**. Click on **Add** and provision entries as follows:

- **Port –** Enter **5061**
- **Protocol –** Select **TLS**
- **Default Domain –** Select a SIP domain administered in **Section 5.1** (e.g., **avayalab.com**)
- Check **Endpoint**.

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**
- **5060** for **Port** and **UDP** 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.

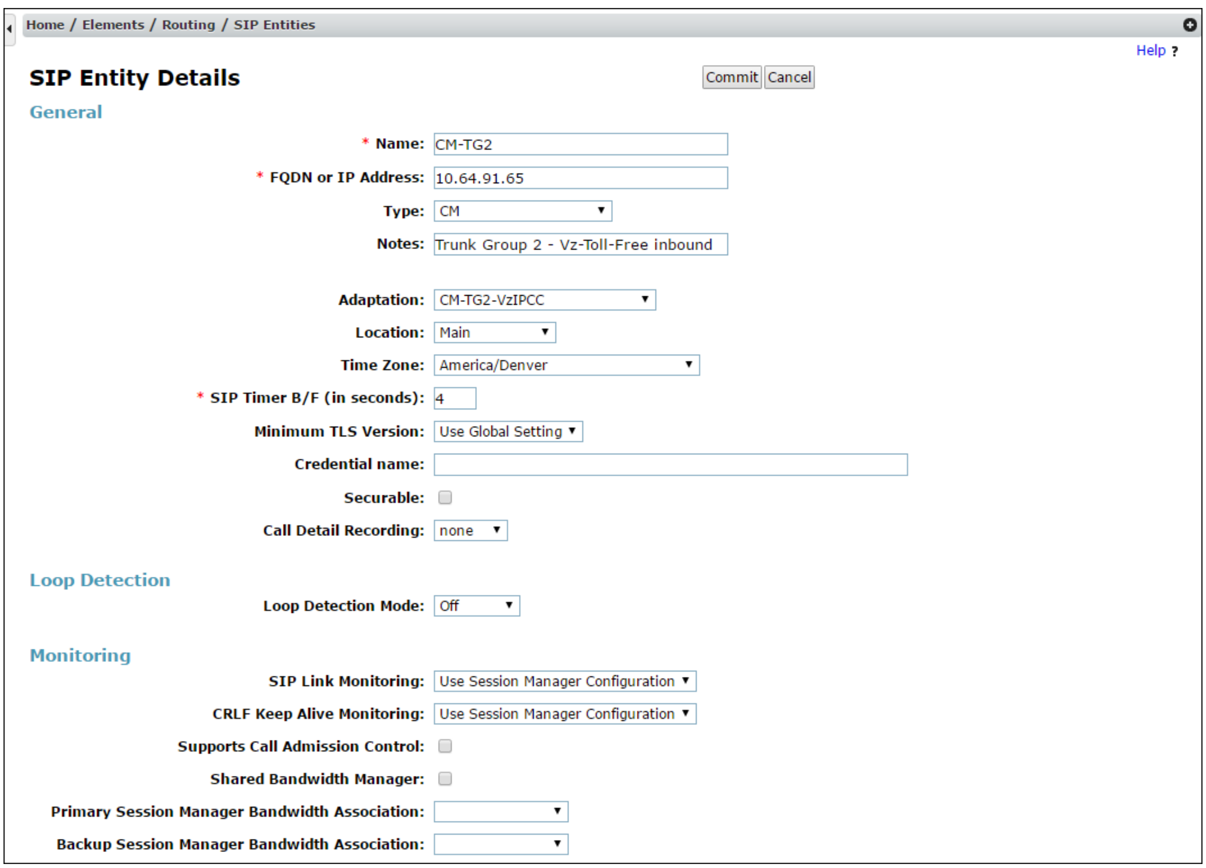
5.4.2 Avaya Aura® Communication Manager SIP Entity – Public Trunk

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-TG2**).
- **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-TG2-VzIPCC** 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** and the **CRLF Keep Alive Monitoring** fields. 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., **SBC1**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.50**, see **Section 7.5.1**).
- **Type –** Select **SIP Trunk**.
- **Adaptations –** Select Adaptation **SBC1-Adaptation for Verizon** (**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**).
- **Type –** Select **Messaging**.
- **Adaptations –** Leave this field blank.

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.

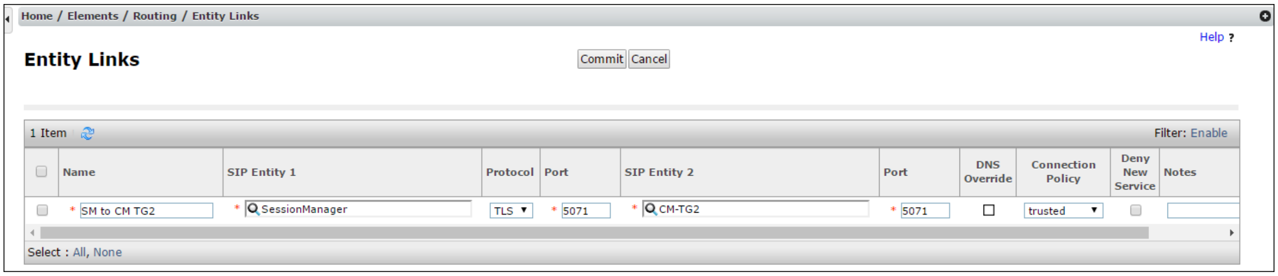
5.5.1 Entity Link to Avaya Aura® Communication Manager – Public Trunk

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 TG2**).
- **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 **5071**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **CM-TG2**).
- SIP Entity 2 **Port** – Enter **5071** (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 6.8.1**).

5.5.3 Entity Link for the Verizon Business IPCC Services 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 SBC1**).
- 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., **SBC1**).
- SIP Entity 2 **Port** – Enter **5061**.

5.5.4 Entity Link to Avaya Aura® Messaging

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

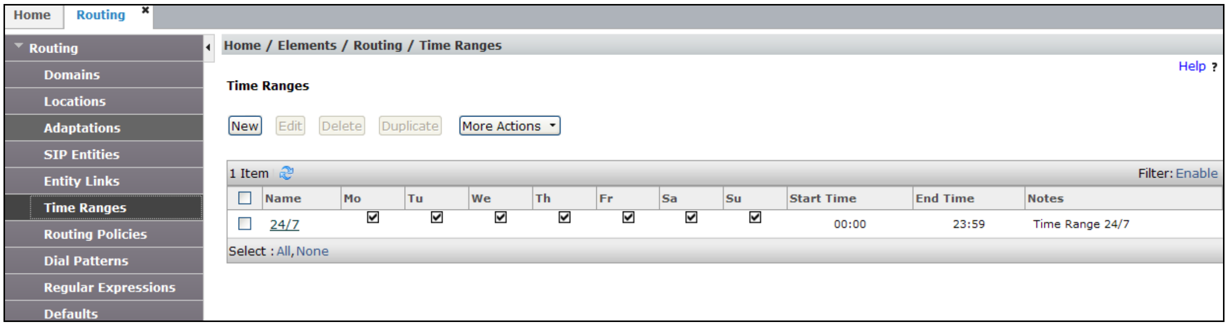
- **Name** – Enter a descriptive name for this link to Messaging (e.g., **SM to AAM**).
- SIP Entity 1 **Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.5** for the Aura® Messaging entity (e.g., **Aura Messaging**).
- SIP Entity 2 **Port** – Enter **5061**.

5.6. Time Ranges

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**).

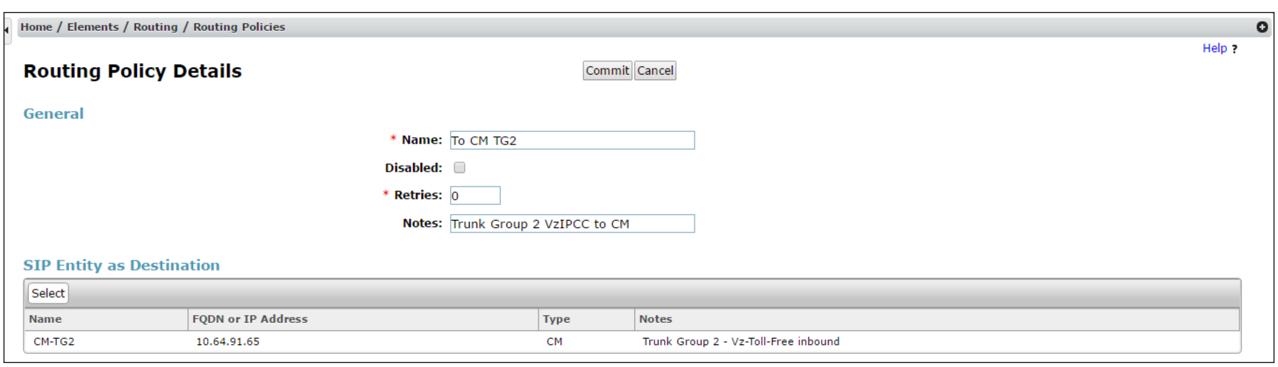
5.7.1 Routing Policy for Verizon Routing to Avaya Aura® Communication Manager

This Routing Policy is used for inbound calls from Verizon.

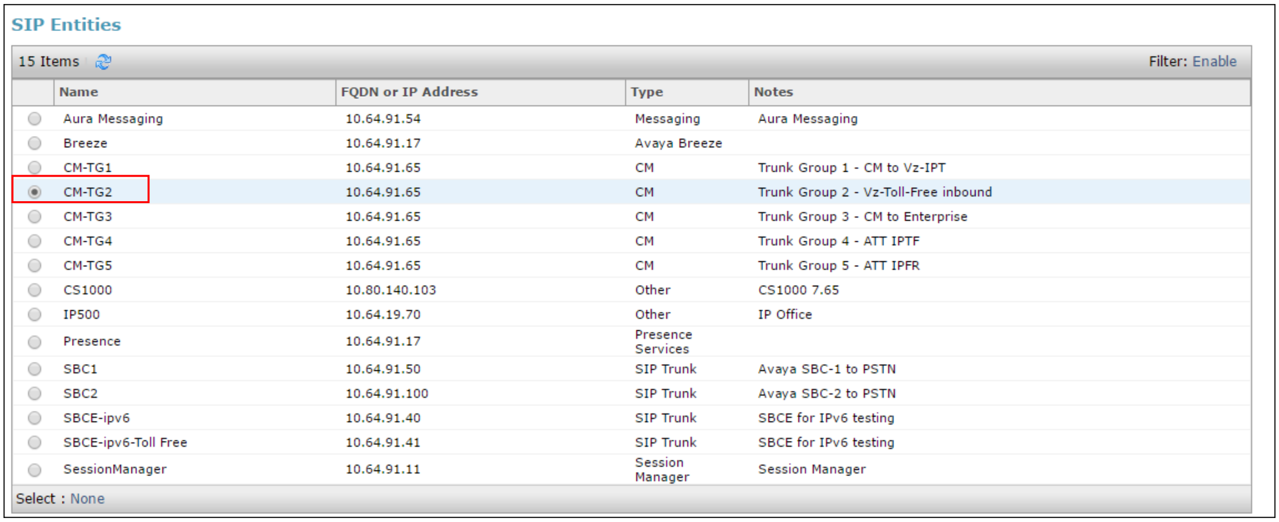
Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing Verizon calls to Communication Manager (e.g., **To CM TG1**), 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.

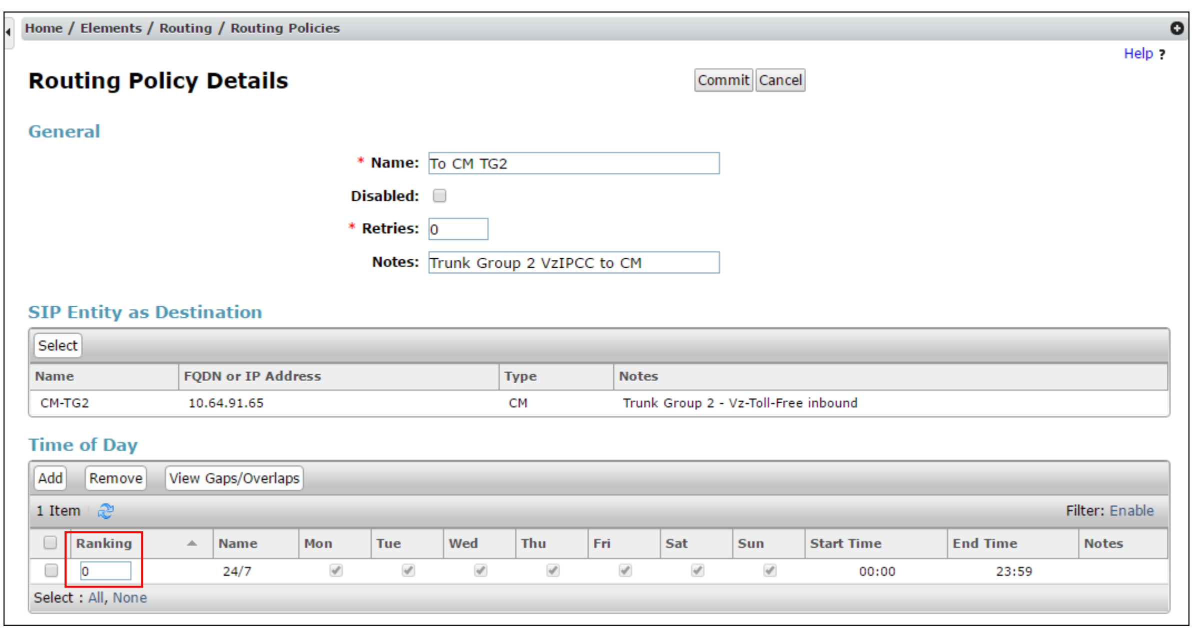


Step 4 - In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**CM-TG2**), and click on **Select**.



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 **0**.
Step 8 - No **Regular Expressions** were used in the reference configuration.
Step 9 - Click on **Commit**.

Note – Once the **Dial Patterns** are defined (**Section 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**).

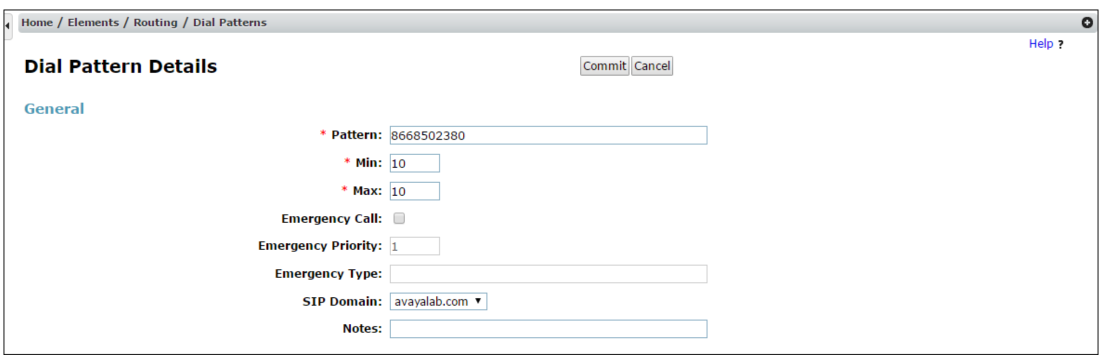
5.8. Dial Patterns

In this section, Dial Patterns are administered matching Inbound PSTN calls via the Verizon Business IPCC Services to Communication Manager. In the reference configuration inbound calls from the Verizon Business IPCC Services sent 10 DNIS digits in the SIP Request URI. The DNIS pattern must be matched for further call processing.

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:

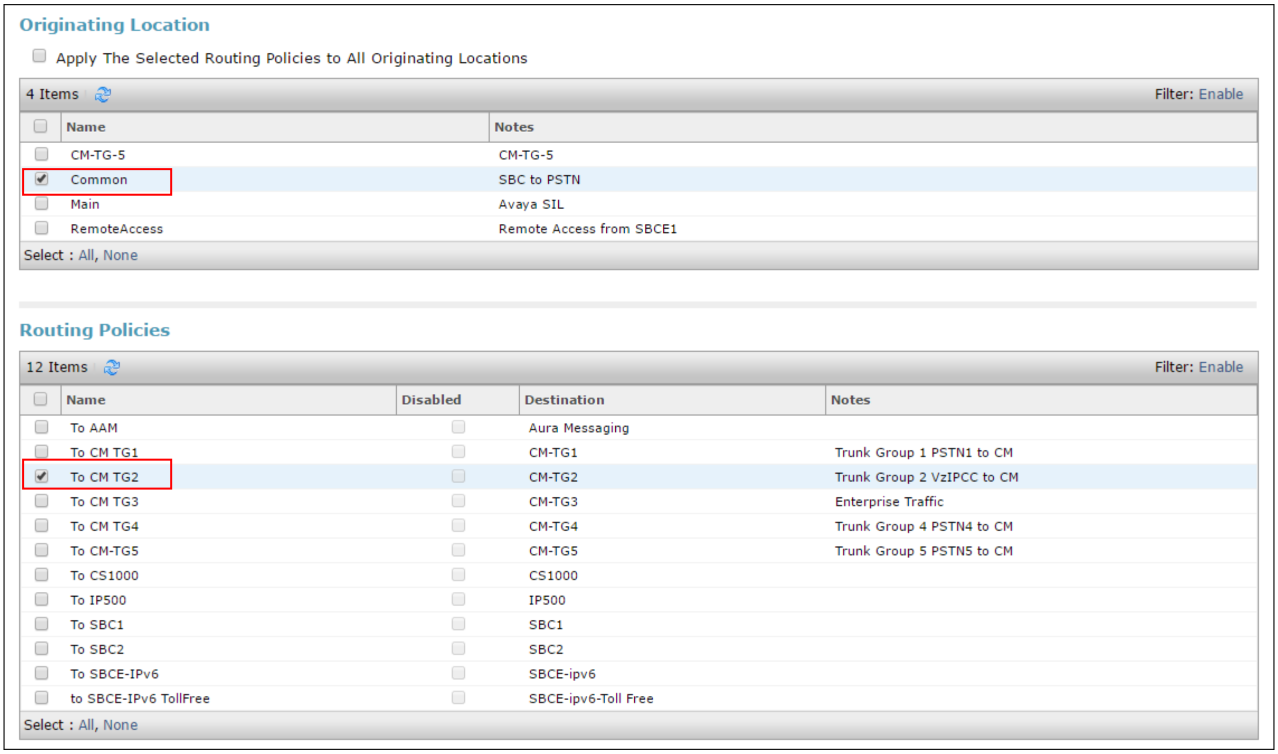
- **Pattern** – Enter **8668502380**. Note – The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 866-xxx-xxxx toll-free numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.



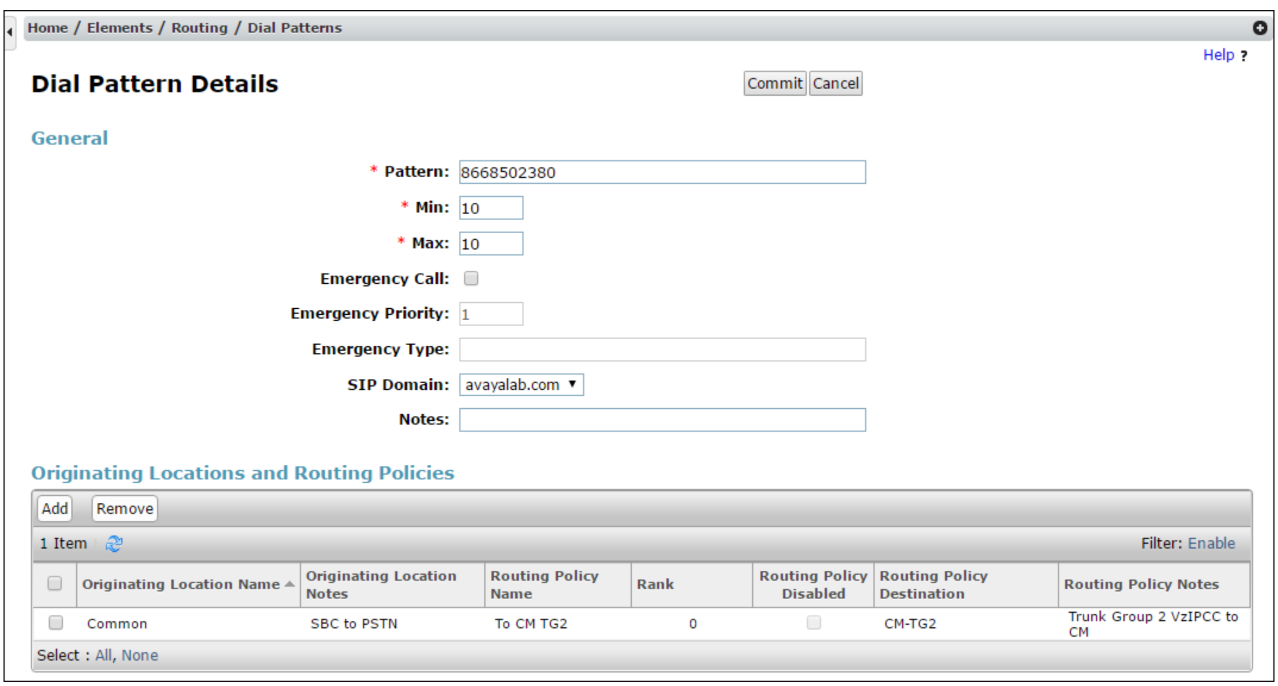
Step 3 - Scrolling down to the **Originating Location and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

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

Step 5 - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7.1** (e.g., **To CM TG2**), and click on **Select** (not shown).



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 Verizon.

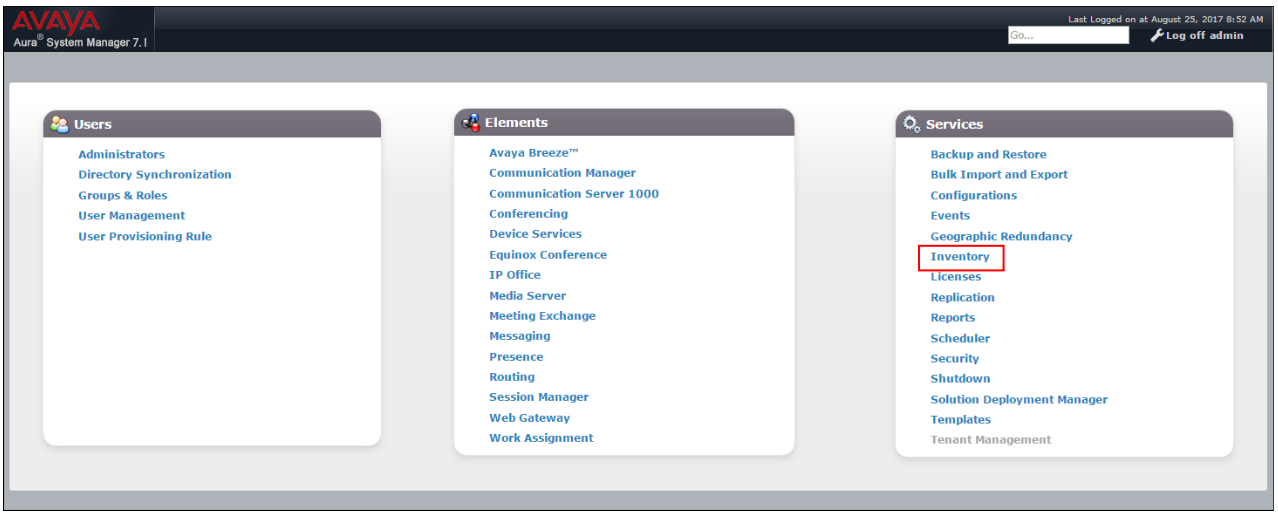


5.9. Verify TLS Certificates – Session Manager

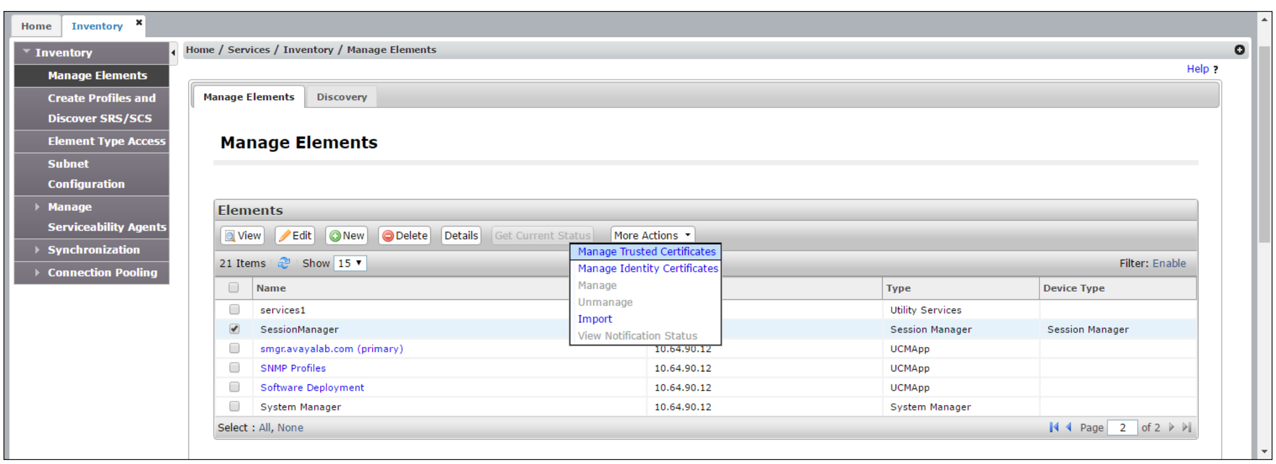
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

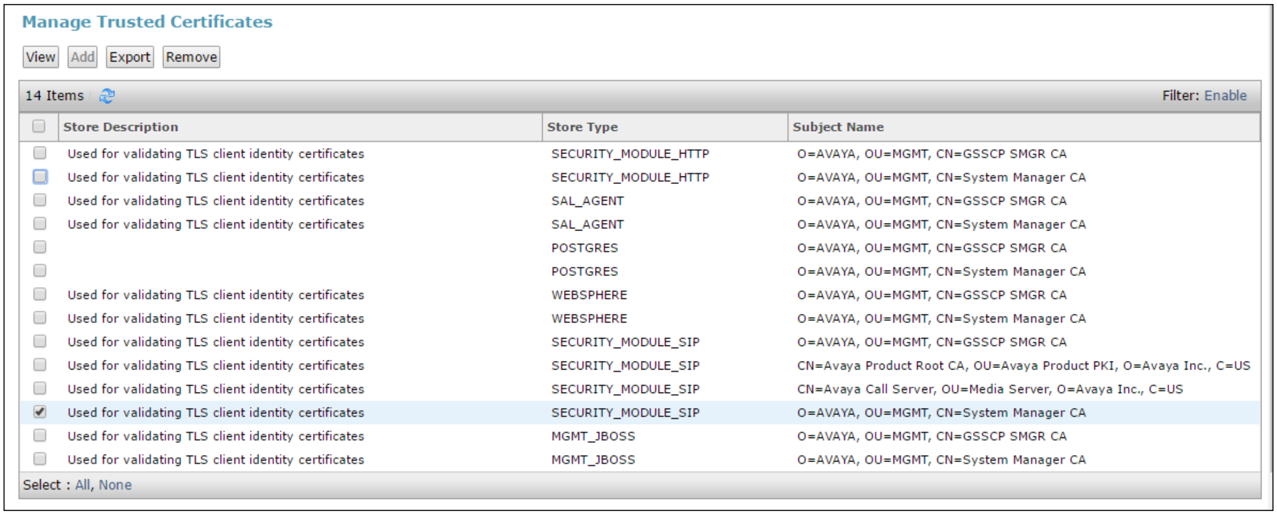
Step 1 - From the **Home screen**, under the **Services** heading in the right column, select **Inventory**.



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 → Manage Trusted Certificates**.



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

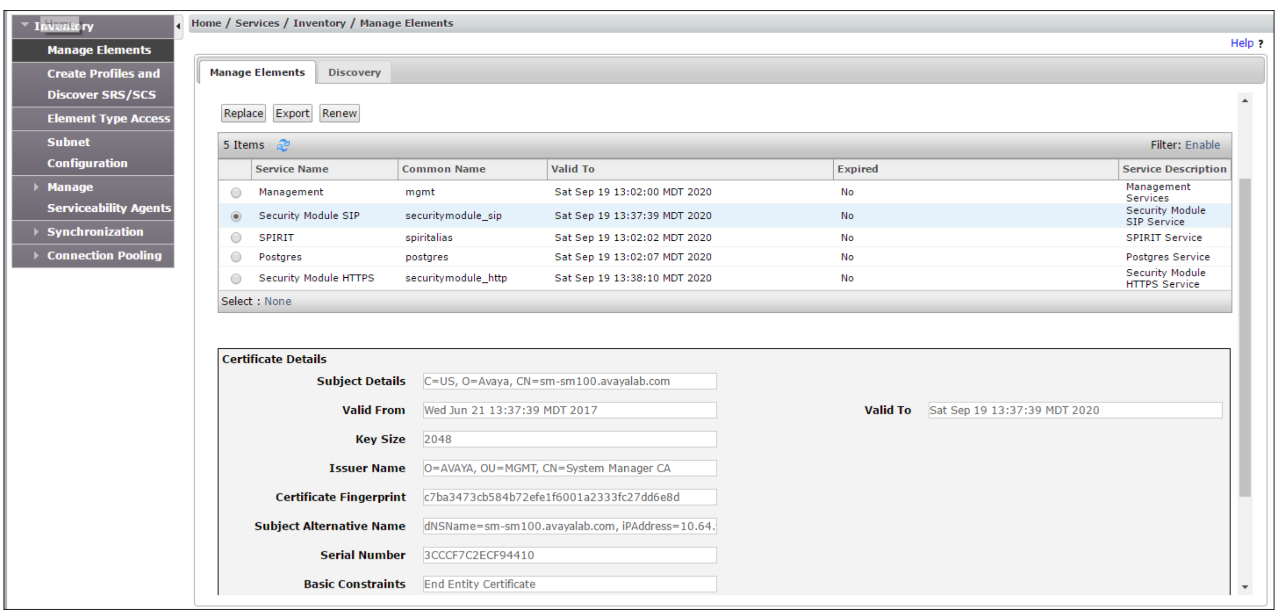


	Store Description	Store Type	Subject Name
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=System Manager CA
☐	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
☐	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=System Manager CA
☐		POSTGRES	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
☐		POSTGRES	O=AVAYA, OU=MGMT, CN=System Manager CA
☐	Used for validating TLS client identity certificates	WEBSPHERE	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
☐	Used for validating TLS client identity certificates	WEBSPHERE	O=AVAYA, OU=MGMT, CN=System Manager CA
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US
☐	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US
☑	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=System Manager CA
☐	Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
☐	Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=System Manager CA

Select : All, None

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

Step 5 - Verify the **Security Module SIP** service has a valid identity certificate signed by System Manager. If the **Subject Details** and **Subject Alternative Name** fields of the System Manager signed certificate need to be updated, click **Replace**, otherwise click **Done** (not shown).



6. Configure Avaya Aura® Communication Manager Release 7.1

This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of Communication Manager to Session Manager.

Note – The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes. Consult **[5] - [9]** for further details.

6.1. Verify Licensed Features

Note – This section describes steps to verify Communication Manager feature settings that are required for the reference configuration described in these Application Notes. Depending on access privileges and licensing, some or all of the following settings might only be viewed, and not modified. 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.

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  10
                       Maximum Administered SIP Trunks: 4000  60
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

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

```
display system-parameters customer-options                    Page   4 of  12
                                OPTIONAL FEATURES

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

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

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

           IP Attendant Consoles? y
```

Step 4 - On **Page 6** of the form, verify that the **Processor Ethernet** field is set to **y**.

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

                Multinational Locations? n            Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                     Multiple Locations? n
                                            System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? y
                        PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? y              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
```

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** and **2** 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
   8           1   fac
   9           1   fac
   *           3   dac
   #           3   dac
```

6.4. Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used. Note that the Communication Manager procr name and IP address are entered during installation. The procr IP address was used to define the Communication Manager SIP Entities in **Section 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 **10.64.91.11**).
- 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                    10.64.91.11
default               0.0.0.0
procr                 10.64.91.65
procr6                ::
```

6.5. Processor Ethernet Configuration

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.

```
change 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 Codec Sets

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

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

```
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.722-64K                   2        20
 2: G.711MU           n         2        20
 3: G.729A            n         2        20

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
```

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

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

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits

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

Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

6.6.2 Codecs for IP Network Region 2 (calls from Verizon)

This IP codec set will be used for Verizon Business IPCC calls. Repeat the steps in **Section 6.6.1** with the following changes:

- Provision the codecs in the order shown below.
- On **Page 2**, set **FAX Mode** to **t.38-G711-fallback**, **ECM** to **y**, and **FB-Timer** to **4**.

```
change ip-codec-set 2                                           Page   1 of   2
                          IP CODEC SET
    Codec Set: 2

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

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none

change ip-codec-set 2                                           Page   2 of   2

                          IP MEDIA PARAMETERS

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits

                                           Redun-                     Packet
                          Mode             dancy                      Size(ms)
    FAX                   t.38-G711-fallback 0     ECM: y  FB-Timer: 4
    Modem                 off                0
    TDD/TTY               US                 3
    H.323 Clear-channel   n                  0
    SIP 64K Data          n                  0                          20

Media Connection IP Address Type Preferences
 1: IPv4
 2:
```

6.7. Network Regions

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway and Avaya Media Server are in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Verizon testing.

6.7.1 IP Network Region 1 – Local CPE Region

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

- Enter a descriptive name (e.g., **Enterprise**).

- Enter the enterprise domain (e.g., **avayalab.com**) in the **Authoritative Domain** field (see **Section 5.1**).
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.

```
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: 2048                       IP Audio Hairpinning? n
   UDP Port Max: 3329
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 **2** in the **dst rgn** column, enter **2** for the codec set (this means region 1 is permitted to talk to region 2 and it will use codec set 2 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
```

6.7.2 IP Network Region 4 – Verizon 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., **Verizon**).
- Enter **2** for the **Codec Set** parameter.

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

- Set codec set **2** for **dst rgn 1**.
- Note that **dst rgn 2** is pre-populated with codec set **2** (from page 1 provisioning).

```
change ip-network-region 2                                    Page   4 of  20

 Source Region: 2     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    2     y    NoLimit                                             n       t
 2    2                                                                all
 3
```

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 Verizon IPCC access – SIP Trunk 2
    - Note that this trunk will use TLS port 5071 as described in **Section 5.5.1**.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 3
    - Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

Note – Although TLS is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the Verizon Business IPCC Services. See the note in **Section 5.4** regarding the use of TLS transport protocols in the CPE.

6.8.1 SIP Trunk for Inbound Verizon calls

This section describes the steps for administering the SIP trunk to Session Manager used for Verizon IP Trunk service calls. Trunk 1 is defined. This trunk corresponds to the **CM-TG2** SIP Entity defined in **Section 5.4.2**.

6.8.1.1 Signaling Group 2

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **2**), 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 **5071**.
- **Far-end Network Region** – Set the IP network region to **2**, as set in **Section 6.6.2**.
- **Far-end Domain** – Enter **avayalab.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).

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

```
change signaling-group 2                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 2              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: 5071                  Far-end Listen Port: 5071
                                          Far-end Network Region: 2

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 2

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

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **Verizon IPCC**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***02**).
- **Direction** – Set to **incoming**.
- **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 2                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip           CDR Reports: y
  Group Name: Verizon IPCC                COR: 1        TN: 1        TAC: *02
   Direction: incoming      Outgoing Display? n
 Dial Access? n                                    Night Service:

Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     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 2                                               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 2                                                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 **Telephone Event Payload Type** to the RTP payload type recommended by Verizon (e.g., **101**).
- Set **Convert 180 to 183 for Early Media** to **y**. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP.

Note – The Verizon Business IPCC Services do not support the Diversion header or the History-Info header, and therefore both **Support Request History** and **Send Diversion Header** are set to "**n**".

```
add trunk-group 2                                                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? n
                                   Support Request History? n
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? y
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

6.8.2 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**).
- **Direction** – Set to **two-way**.
- **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 **Send 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. Contact Center Configuration

This section describes the basic commands used to configure Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke the Communication Manager SIP Network Call Redirection (NCR) functionality. These Application Notes provide rudimentary vector definitions to demonstrate and test the SIP NCR and UUI functionalities. In general, call centers will use vector functionality that is more complex and tailored to individual needs. Call centers may also use customer hosts running applications used in conjunction with Application Enablement Services (AES) to define call routing and provide associated UUI. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

6.9.1 Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command **add announcement <extension>**.

```
list announcement

                           ANNOUNCEMENTS/AUDIO SOURCES
Announcement                                                   Source      Num of
Extension              Type       Name                        Pt/Bd/Grp    Files
11001                  integrated callcenter-main              001V9       1
11002                  integ-mus  holdmusic                    001V9       1
11003                  integrated disconnect                   001V9       1
11004                  integrated no_agents                    001V9       1
11005                  integrated dtmf_test                    001V9       1
11006                  integrated please_wait                  001V9       1
11007                  integrated REFER_Test                   001V9       1
```

6.9.2 Post-Answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use post-answer redirection to a PSTN destination. A corresponding detailed verification is provided in **Section 9.1.2**. In this example, the inbound toll-free call is routed to VDN 10001 shown in the following screen. The originally dialed Verizon IP Toll Free number may be mapped to VDN 10001 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 10001                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10001
                                 Name*: Refer-to-PSTN
                           Destination: Vector Number        1
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                  COR: 1
                                  TN*: 1
                              Measured: none
```

VDN 10001 is associated with vector 1, which is shown below. Vector 1 plays an announcement (step 03) to answer the call. After the announcement, the **route-to number** (step 05) includes **~r+13035387024** where the number 303-538-7024 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes "+13035387024" as the user portion. Note that Verizon Business IPCC Services require the "+" in the Refer-To header for this type of call redirection.

```
display vector 1                                                Page   1 of   6
                                  CALL VECTOR

    Number: 1                Name: Refer-to-PSTN
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 #    Play announcement to caller in step 3. This answers the call.
03 announcement 11006
04 #    Refer the call to PSTN Destination in step 5 below.
05 route-to     number ~r+13035387024   with cov n if unconditionally
06 #    If Refer fails queue to skill 1
07 queue-to     skill 1    pri m
08
```

6.9.3 Post-Answer Redirection With UUI to a SIP Destination

This section provides an example of post-answer redirection with UUI passed to a SIP destination. In this example, the inbound call is routed to VDN 10003 shown in the following screen. The originally dialed Verizon toll-free number may be mapped to VDN 10003 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 10003                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10003
                                 Name*: REFER with UUI
                           Destination: Vector Number        3
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

To facilitate testing of NCR with UUI, the following vector variables were defined.

```
change variables                                                Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                  Type    Scope Length Start Assignment       VAC
A   uui                          asaiuui L     16     1
B   uui                          asaiuui L     16     17
C
```

VDN 10003 is associated with vector 3, which is shown below. Vector 3 sets data in the vector variables A and B (steps 03 and 04) and plays an announcement to answer the call (step 05). After the announcement, the **route-to** number step includes **~r+18668512649**. This step causes a REFER message to be sent where the Refer-To header includes **+18668512649** as the user portion. The Refer-To header will also contain the UUI set in variables A and B. Verizon will include this UUI in the INVITE ultimately sent to the SIP-connected target of the REFER, which is toll-free number “18668512649”. In the sample configuration, where only one location was used, 866-851-2649 is another toll-free number assigned to the same circuit as the original call. In practice, NCR with UUI would allow Communication Manager to send call or customer-related data along with the call to another contact center.

```
display vector 3                                                Page   1 of   6
                                  CALL VECTOR

    Number: 3               Name: Refer-with-UUI
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 set          A      = none   CATR  1234567890123456
03 set          B      = none   CATR  7890123456789012
04 #    Play announcement to answer call and route to ~r to cause Refer
05 announcement 11007
06 route-to     number ~r+18668512649   with cov n if unconditionally
07 #    If Refer fails play announcement and disconnect
08 disconnect   after announcement 11003
```

6.9.4 ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt group, and agent logins used to queue inbound Verizon IPCC calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

```
display hunt-group 1                                            Page   1 of   4
                                  HUNT GROUP

            Group Number: 1                               ACD? y
              Group Name: Agent Group                   Queue? y
         Group Extension: 19991                        Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
```

The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note Skill is set to **y**.

```
display hunt-group 1                                            Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n        Service Level Target (% in sec): 80 in 20
```

VDN 10004, shown below, is associated with vector 4.

```
display vdn 10004                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 10004
                                 Name*: Sales
                           Destination: Vector Number        4
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
```

In this simple example, vector 4 briefly plays ring back, then queues the call to skill 1. Announcement 11004 is a simple recurring announcement. If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear the announcement. Once an agent becomes available, the call will be delivered to the agent.

```
display vector 4                                                Page   1 of   6
                                  CALL VECTOR

    Number: 4                Name: Sales
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 #    Wait hearing ringback
02 wait-time    2   secs hearing ringback
03 #    Simple queue to skill with recurring announcement until available
04 queue-to     skill 1    pri m
05 announcement 11004
06 wait-time    30  secs hearing music
07 goto step    5             if unconditionally
08 stop
```

The following screen illustrates an example agent-loginID 20001. In the sample configuration, an Avaya one-X® Deskphone logged in using agent-loginID 20001 and the configured Password to staff and take calls for skill 1.

```
change agent-loginID 20001                                      Page   1 of   2
                                 AGENT LOGINID

                Login ID: 20001                                 AAS? n
                    Name: Agent 1                             AUDIX? n
                      TN: 1       Check skill TNs to match agent TN? n
                     COR: 1
           Coverage Path: 1                          LWC Reception: spe
           Security Code:                   LWC Log External Calls? n
           Attribute:                     AUDIX Name for Messaging:

                                      LoginID for ISDN/SIP Display? n
                                                          Password:
                                            Password (enter again):
                                                       Auto Answer: station
                                                 MIA Across Skills: system
                                         ACW Agent Considered Idle: system
                                         Aux Work Reason Code Type: system
                                           Logout Reason Code Type: system
```

The following abridged screen shows Page 2 for agent-loginID 20001. Note that the Skill Number (**SN**) has been set to 1.

```
change agent-loginID 20001                                      Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                              Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 1       1      16:                 31:                 46:
 2:                17:                 32:                 47:
 3:                18:                 33:                 48:
```

To enable a telephone or one-X® Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

```
change system-parameters features                               Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length: 4
```

6.10. 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 Verizon public numbers, for inclusion in any SIP headers directed to the Verizon Business IPCC Services 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 Vector Directory Numbers (VDN) and their corresponding Verizon DNIS numbers (for the public trunk to Verizon). Communication Manager will insert these Verizon 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., **10001**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **Private Prefix** – Enter the corresponding Verizon DNIS number (e.g., **18668523221**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext              Trk       CPN          CPN
Len Code             Grp(s)    Prefix       Len
                                                 Total Administered: 16
 5  10001            2         18668523221  11      Maximum Entries: 240
 5  10003            2         18668510107  11
 5  10004            2         18668502380  11   Note: If an entry applies to
```

Note – Without this configuration, calls to the VDNs would result in a 5-digit user portion of the Contact header in the 183 with SDP and 200 OK returned to Verizon. Although this did not present any user-perceivable problem in the sample configuration, the configuration in the bolded rows above illustrate how to cause Communication Manager to populate the Contact header with user portions that correspond with a Verizon Business IPCC number. In the course of the testing, multiple Verizon toll-free numbers were associated with different Communication Manager extensions and functions.

6.11. 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
```

6.12. 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 - Enter the **change route-pattern 3** command and enter the following:

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

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

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

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 G450 Media Gateway Provisioning

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

Note – Only the Media Gateway provisioning associated with the G450 registration to Communication Manager is shown below. For additional information on G450 provisioning, see **[7]**.

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

Step 2 - Enter the **show system** command and copy down the G450 serial number (e.g., **08IS38199678**).

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

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

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

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

- Set **Type** = **g450**
- Set **Name** = a descriptive name (e.g., **G450-1**)
- Set **Serial Number** = the serial number copied from **Step 2** (e.g., **08IS38199678**)
- Set the **Link Encryption Type** parameter as desired (**any-ptls/tls** was used in the reference configuration)
- Set **Network Region** = **1**

Wait a few minutes for the G450 to register to Communication Manager. When the Media Gateway registers, the G450 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., ***G450-001(super)#***).

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

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

                    Type: g450
                    Name: G450-1
               Serial No: 08IS38199678
    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: 38 .18 .0  /1
       MGP IPV4 Address: 10.64.19.61
       MGP IPV6 Address:
   Controller IP Address: 10.64.91.65
             MAC Address: 00:1b:4f:03:52:18

   Mutual Authentication? optional
```

6.15. Avaya Aura® Media Server Provisioning

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

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

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

Step 2 - On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP →Node and Routes** and add the Communication Manager Procr interface IP address (e.g., **10.64.91.65**, 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**.

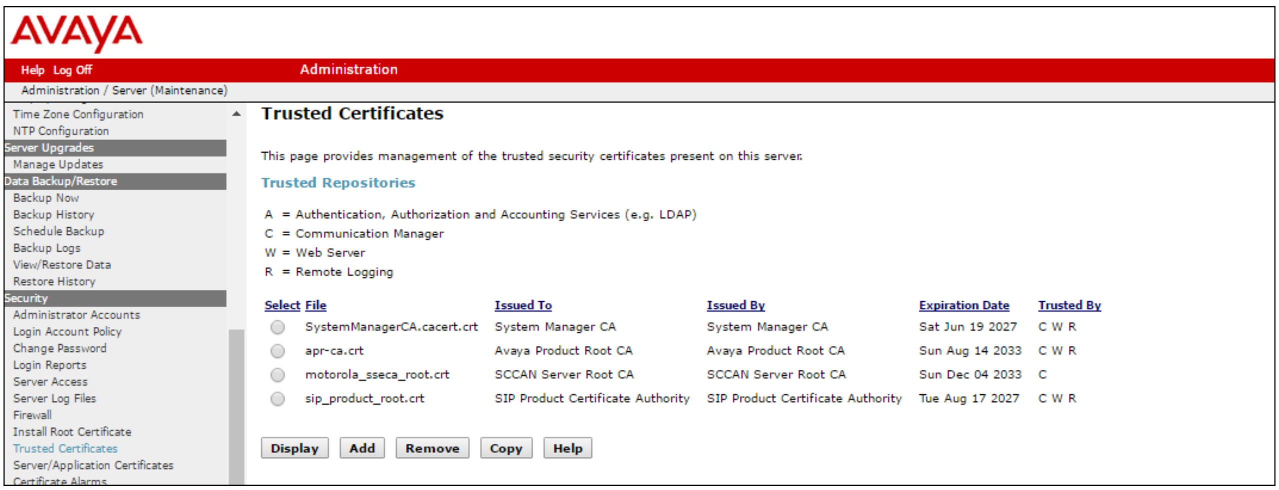
6.17. Verify TLS Certificates – Communication Manager

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.

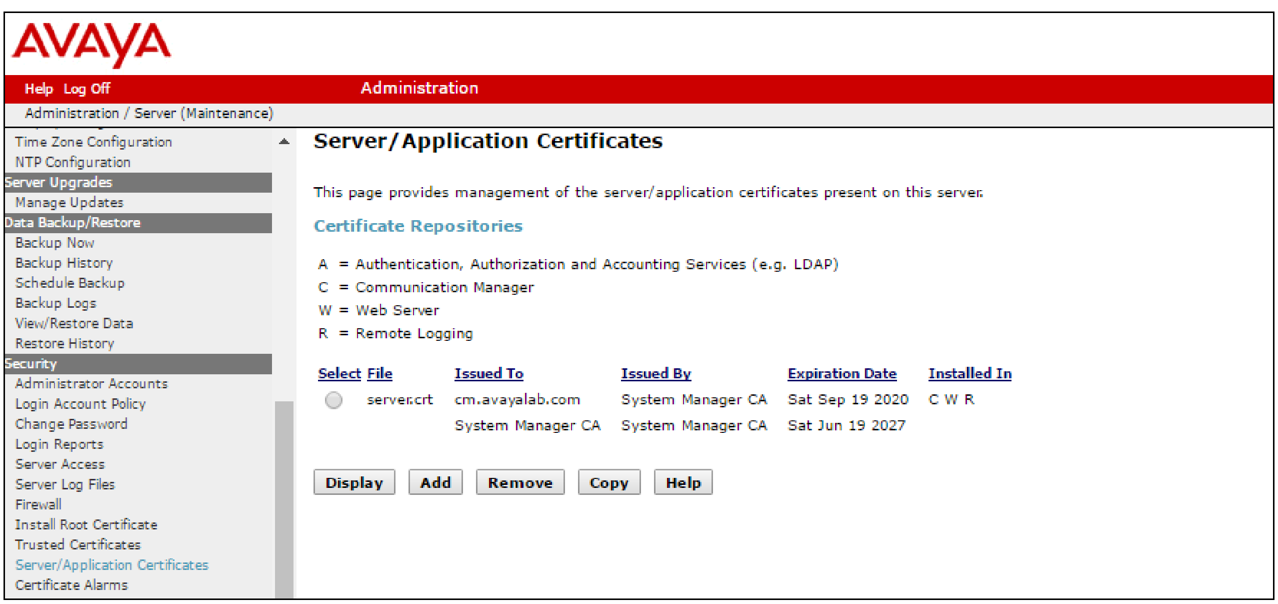
In the reference configuration, TLS transport is used for the communication between Session Manager and Communication Manager. The following procedures show how to verify the certificates used by Communication Manager.

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.



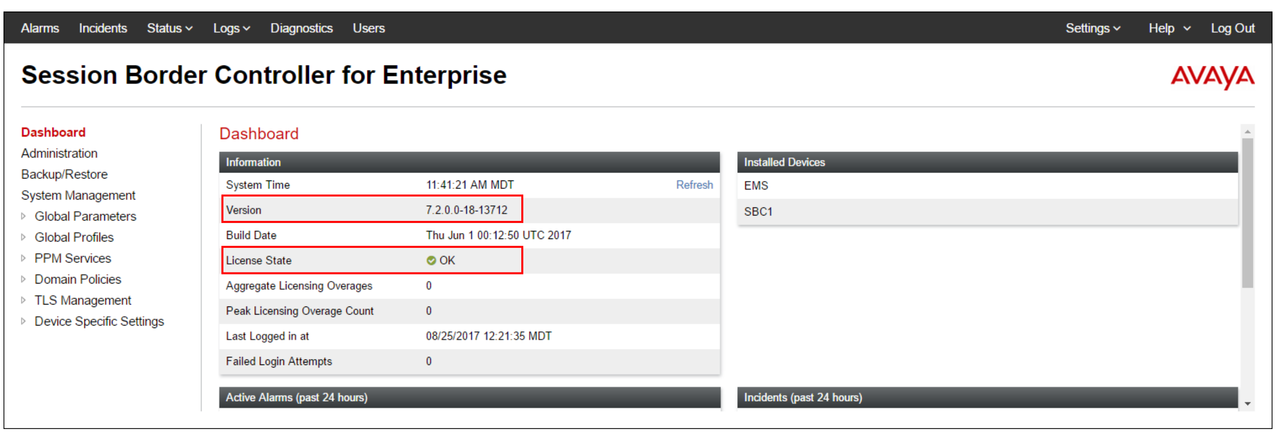
7. Configure Avaya Session Border Controller for Enterprise Release 7.2

These Application Notes assume that the installation of the Avaya SBCE and the assignment of all IP addresses have already been completed, including the management IP address. Consult **[10]** and **[11]** for additional information.

In the sample configuration, the management IP is 10.64.90.50. Access the web management interface by entering https://<ip-address> where <ip-address> is the management IP address assigned during installation. Log in with the appropriate credentials. Click **Log In**.

The main page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is **"OK"**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

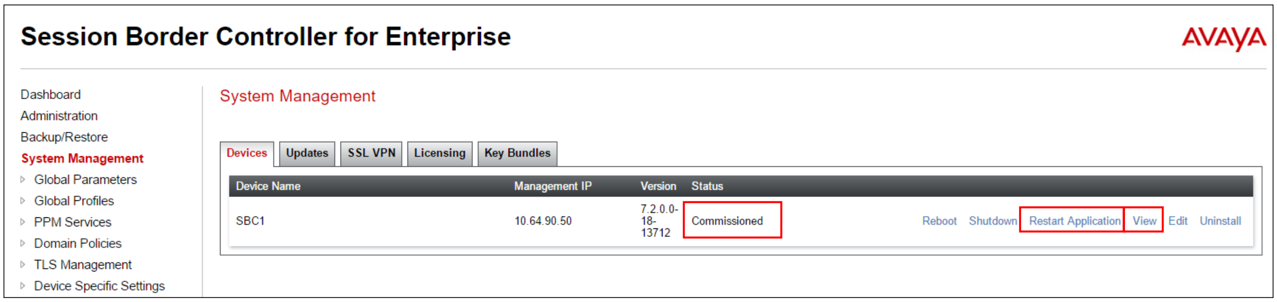
Note – The provisioning described in the following sections use the menu options listed in the left-hand column shown below.



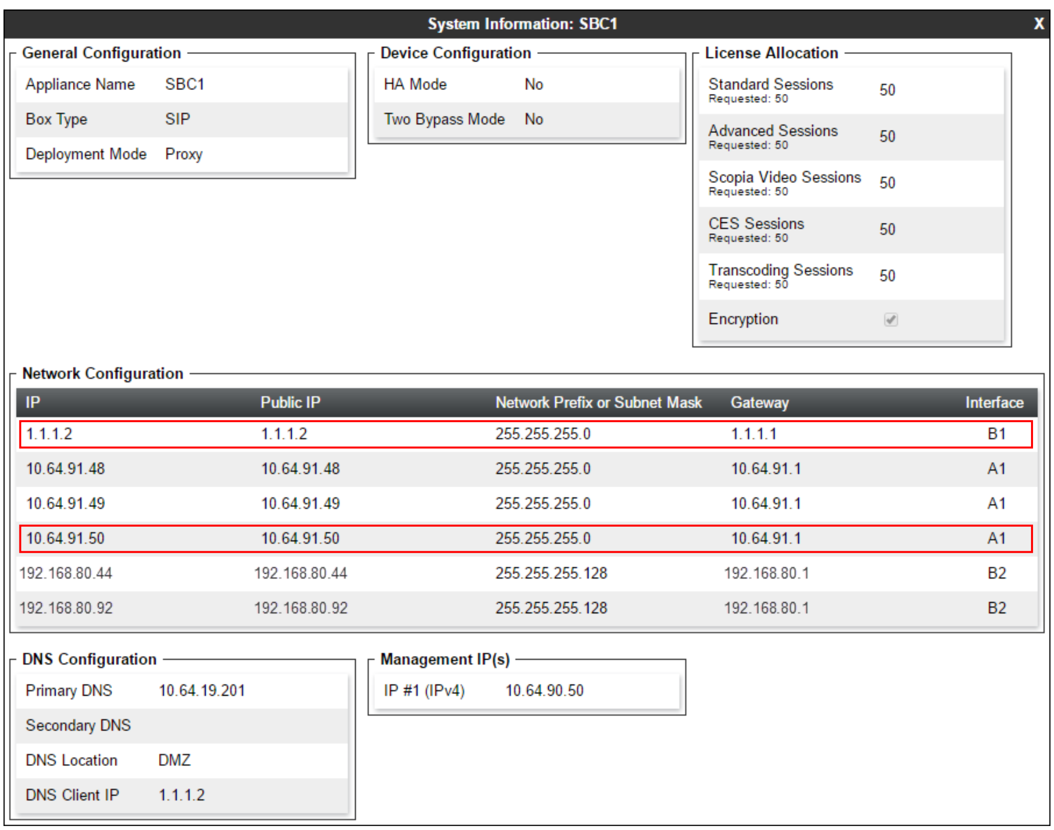
7.1. System Management – Status

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. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Verizon. Other IP addresses assigned to these interfaces and interface **B2** on the screen below are used to support remote workers and are not the focus of these Application Notes. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.



7.2. TLS Management

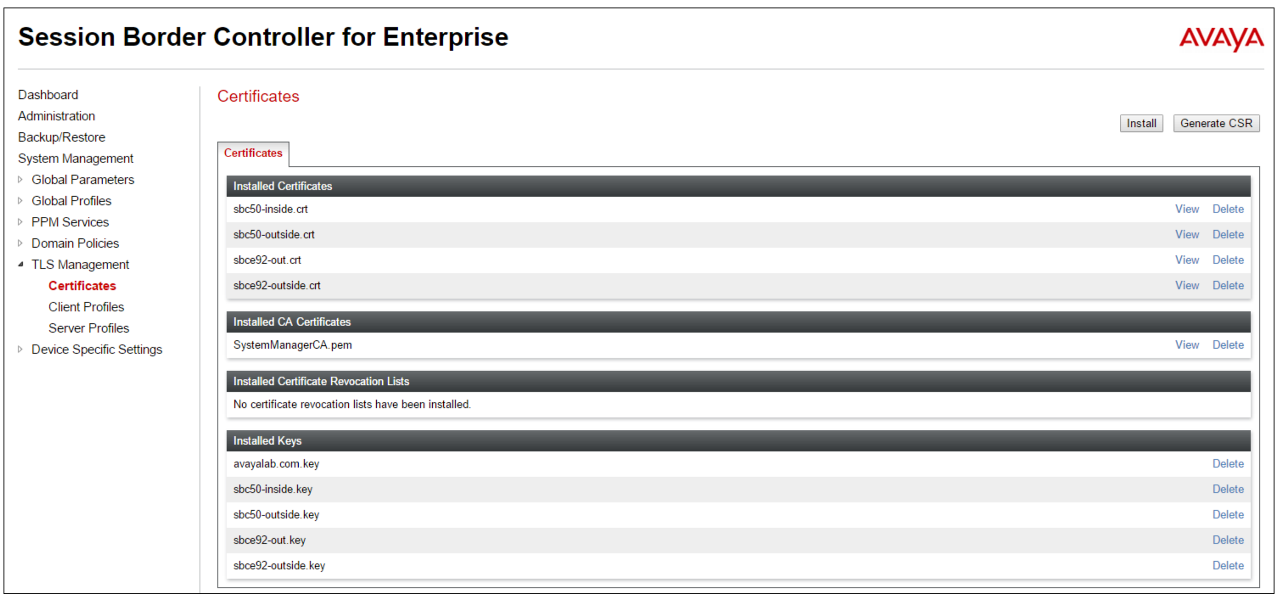
Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

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.

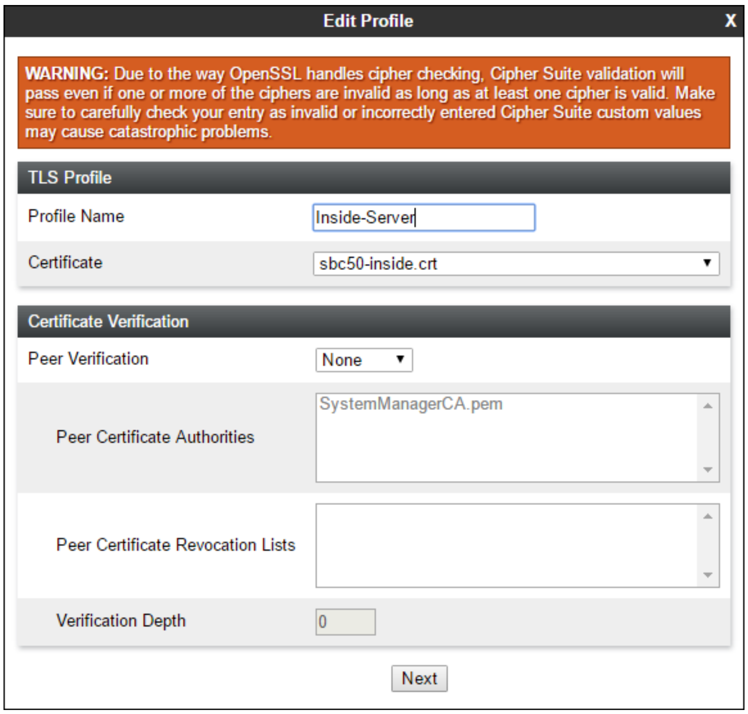


7.2.2 Server Profiles

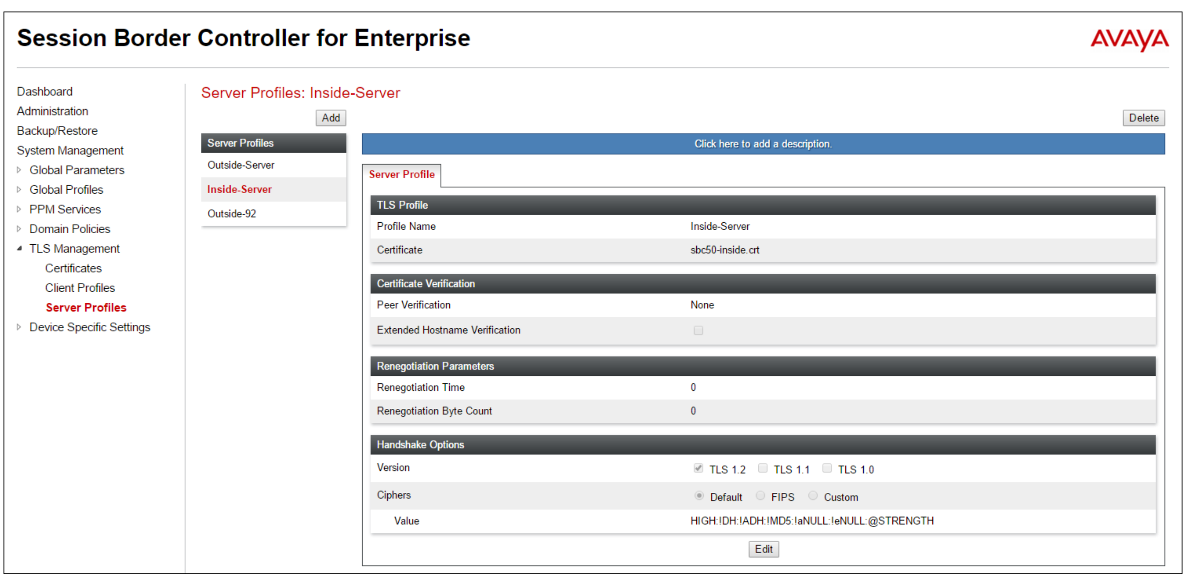
Step 1 - Select **TLS Management → Server Profiles**, and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **Inside-Server**, 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:

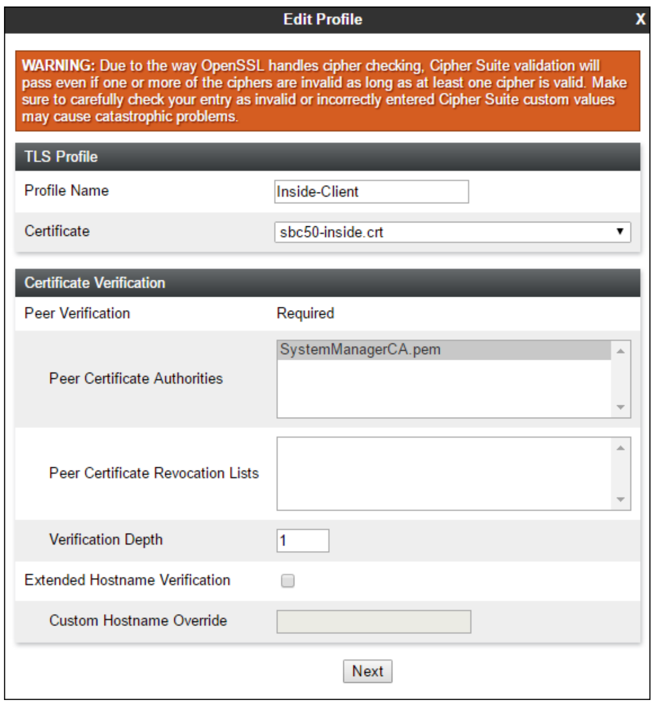


7.2.3 Client Profiles

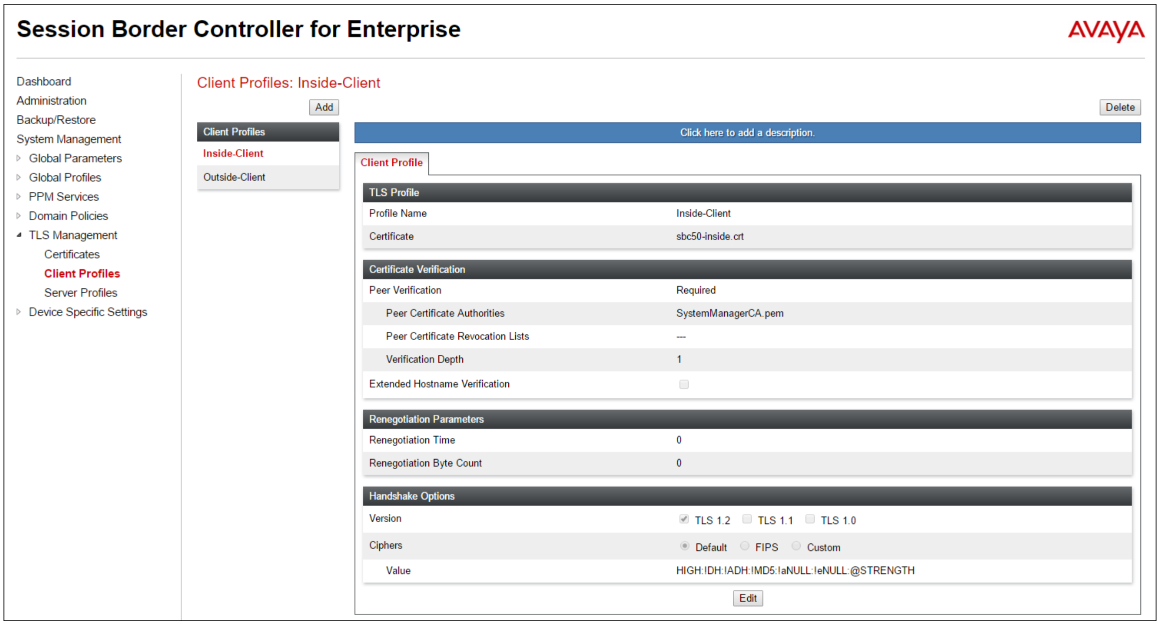
Step 1 - Select **TLS Management → Server Profiles**, and click on **Add**. Enter the following:

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

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



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



7.3. Global Profiles

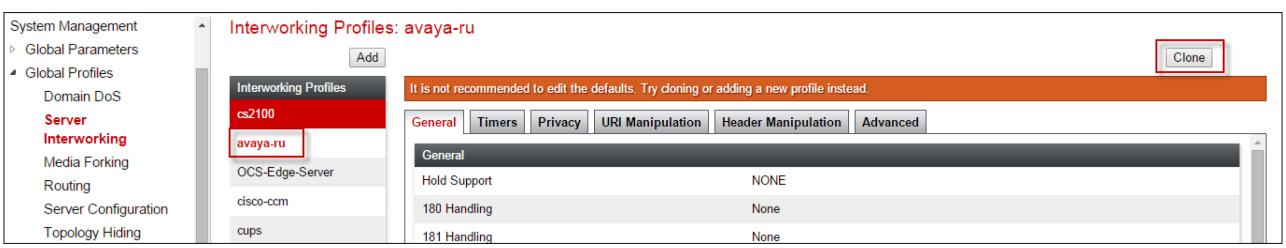
Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

7.3.1 Server Interworking – Avaya

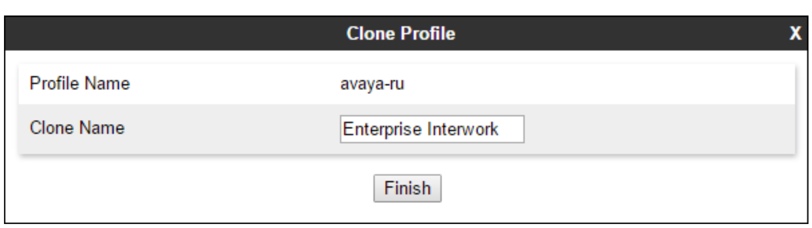
Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Session Manager.

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

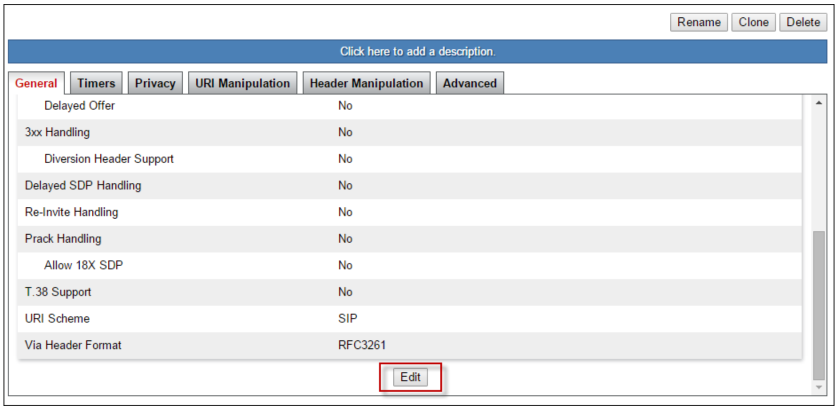
Step 2 - Select the pre-defined **avaya-ru** profile and click the **Clone** button.



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

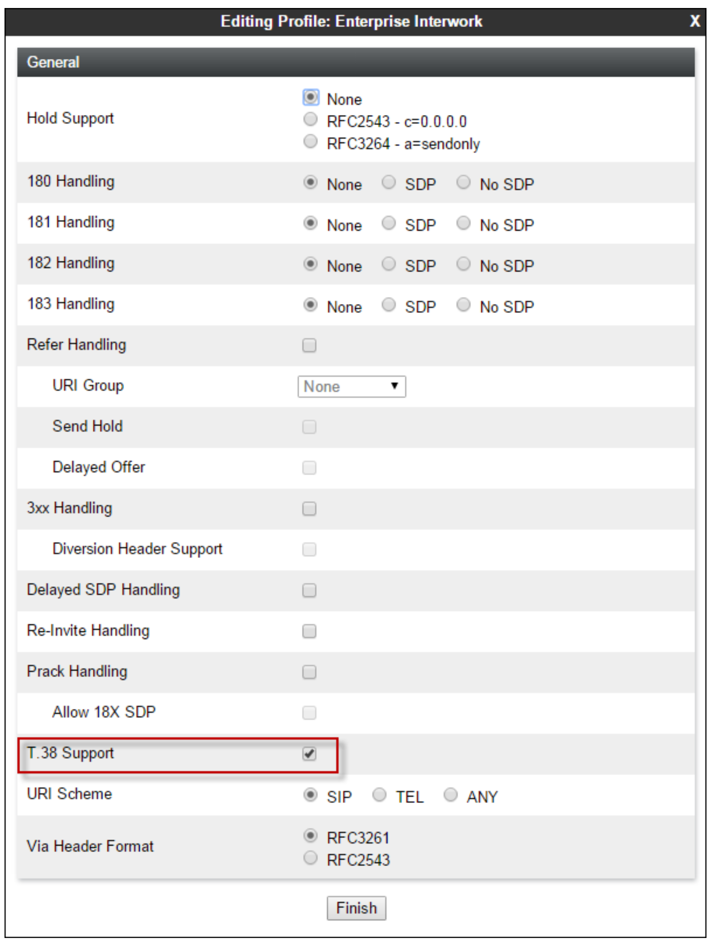


Step 4 - The new Enterprise Interwork profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.

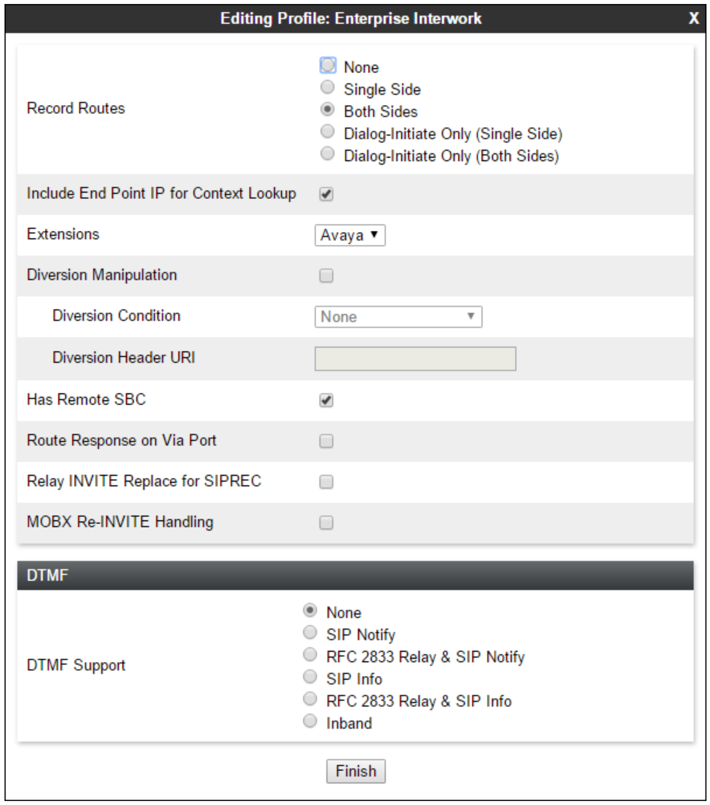


Step 5 - The **General** screen will open.

- 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 – Verizon

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

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

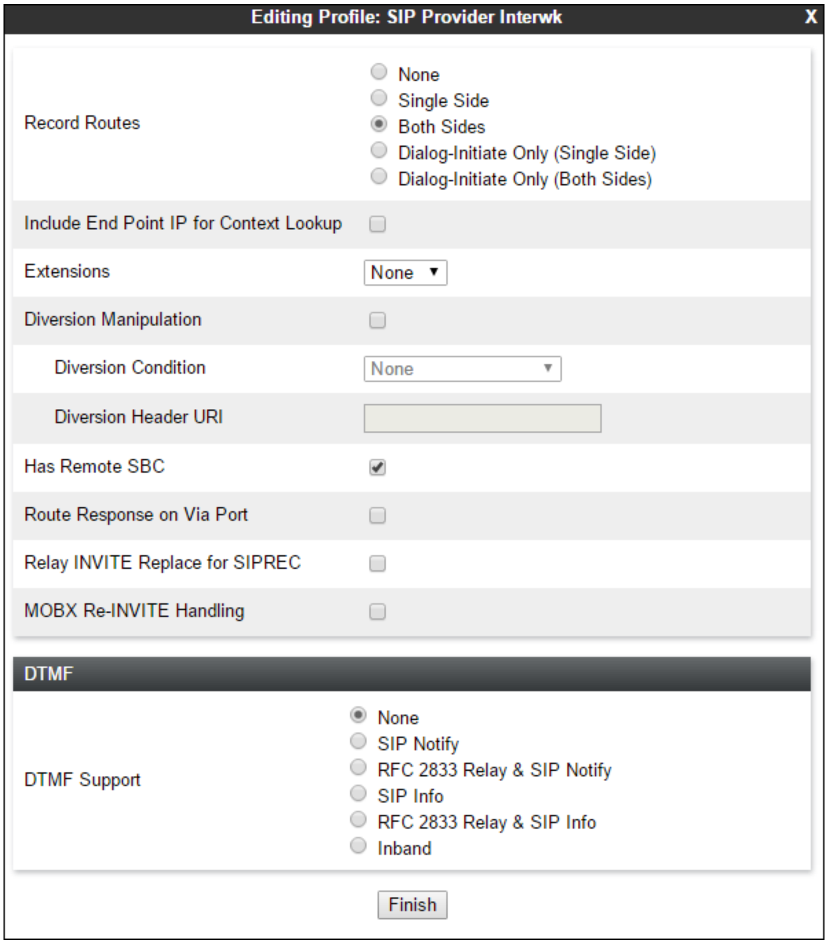
Step 2 - The **General** screen will open (not shown):

- 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

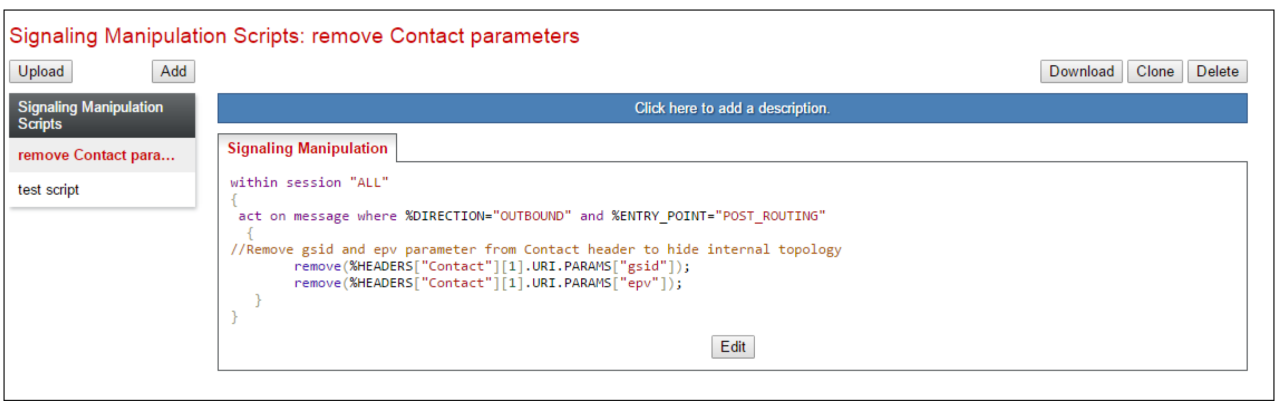
Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, one signaling manipulation script is used.

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 or Interworking Profiles does not meet the desired result. Refer to **[10]** for information on the Avaya SBCE scripting language.

Step 1 - Select **Global Profiles → Signaling Manipulation** from the left-hand menu (not shown).
Step 2 - Select **Add**.
Step 3 - Enter a name for the script in the **Title** box (e.g., **remove Contact parameter**). The following script is defined:

```
within session "ALL"
{
 act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
//Remove gsid and epv parameter from Contact header to hide internal topology
        remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
        remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
   }
}
```

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

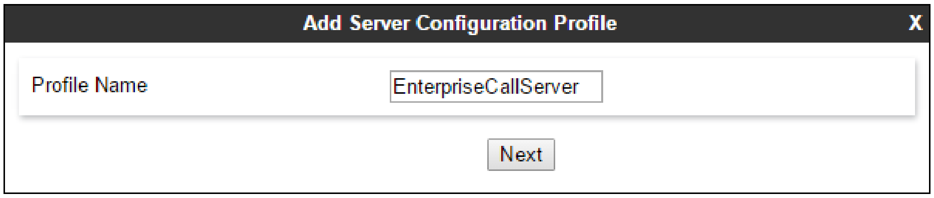


Note – These parameters contain unnecessary information for Verizon, including the internal domain. Removing these parameters helps to mask the internal topology of the enterprise and reduces the size of the SIP packet sent to Verizon. The Endpoint-View header and other proprietary headers are removed using an adaptation as illustrated in **Section 5.3**.

7.3.4 Server Configuration – Session Manager

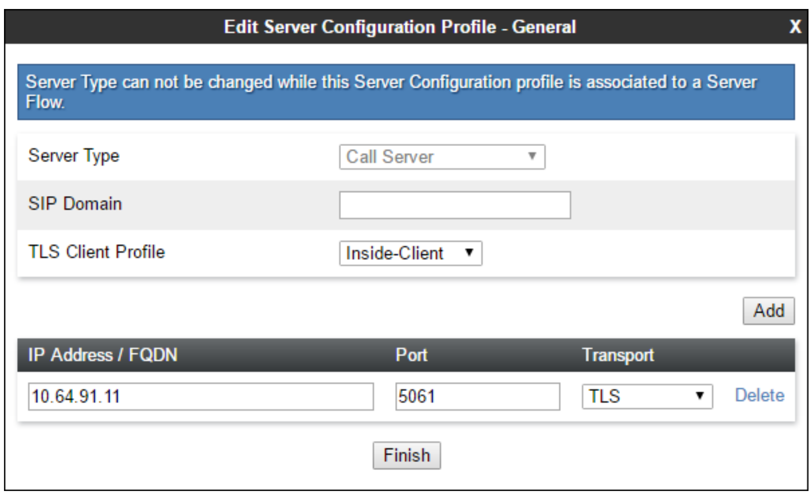
This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

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 7.2.3** (e.g., **Inside-Client**)
- **IP Address**: **10.64.91.11** (Session Manager network IP address)
- **Transport**: Select **TLS**
- **Port**: **5061**
- Select **Next**



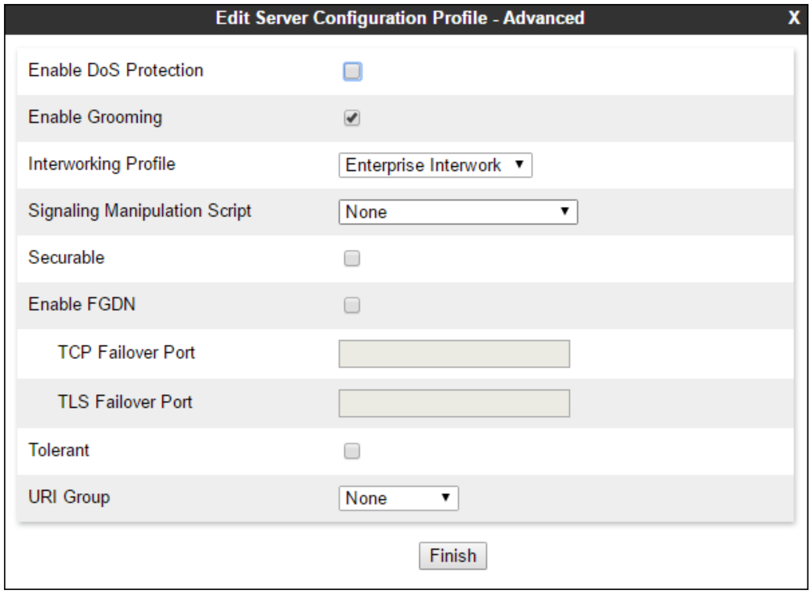
Step 4 - The **Authentication** and **Heartbeat** windows will open (not shown).

- 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.



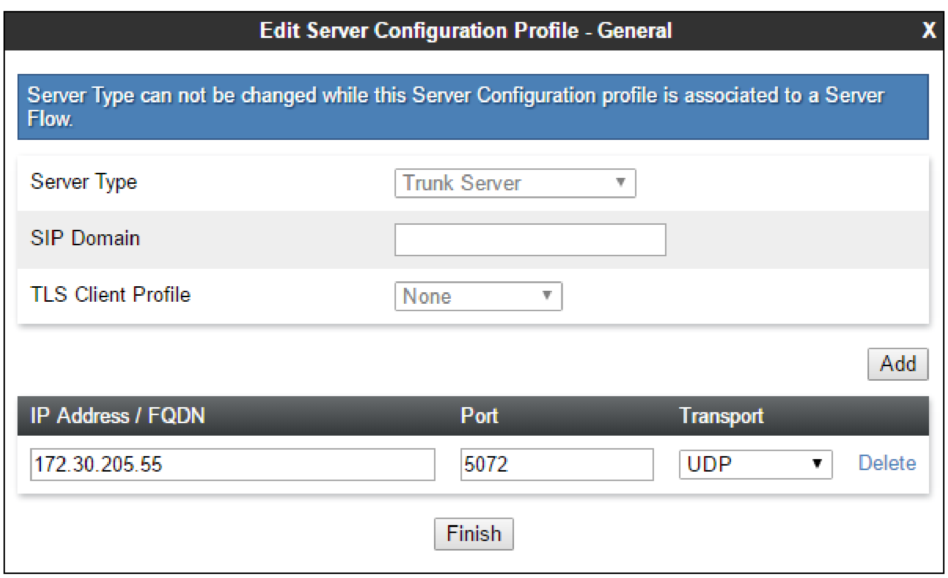
7.3.5 Server Configuration – Verizon

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

Step 1 - Select **Add** and enter a Profile Name (e.g., **Verizon IPCC**) and select **Next** (not shown).

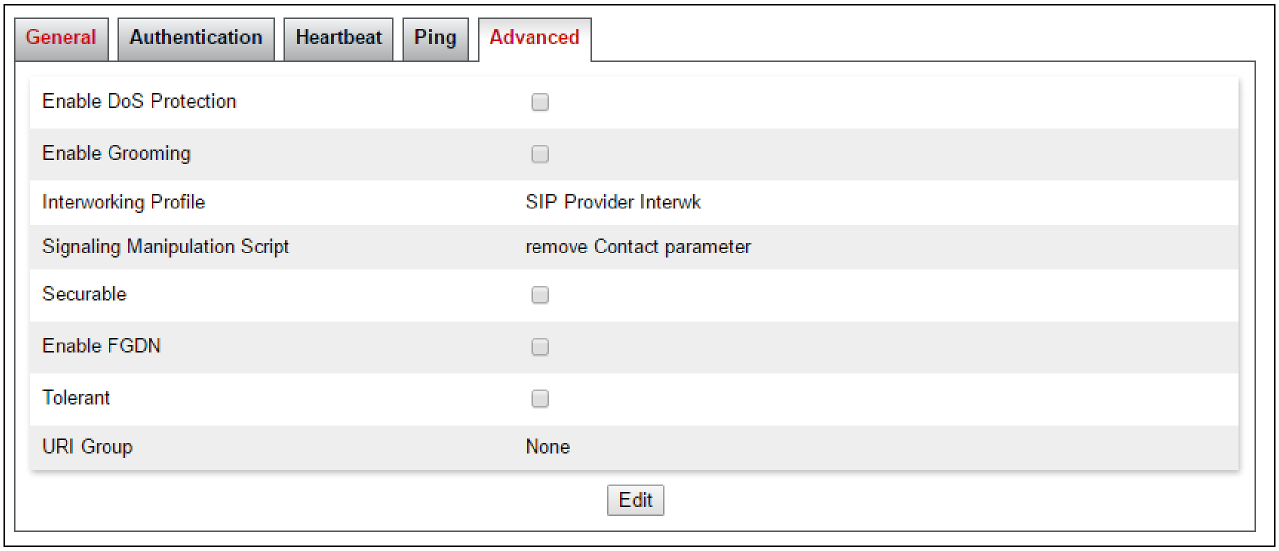
Step 2 - On the **General** window, enter the following:

- **Server Type:** Select **Trunk Server**
- **IP Address: 172.30.205.55** (Verizon-provided IP address)
- **Transport**: Select **UDP**
- **Port: 5072**
- Select **Next** until the Advanced tab is reached



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

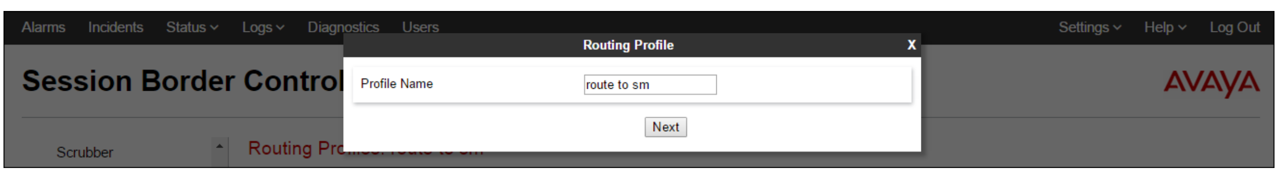
- Select **SIP Provider Interwk** (created in **Section 7.3.2**), for **Interworking Profile**.
- Select **remove Contact parameter** (created in **Section 7.3.3**) for **Signaling Manipulation Script**.
- Select **Finish** (not shown).



7.3.6 Routing – To Session Manager

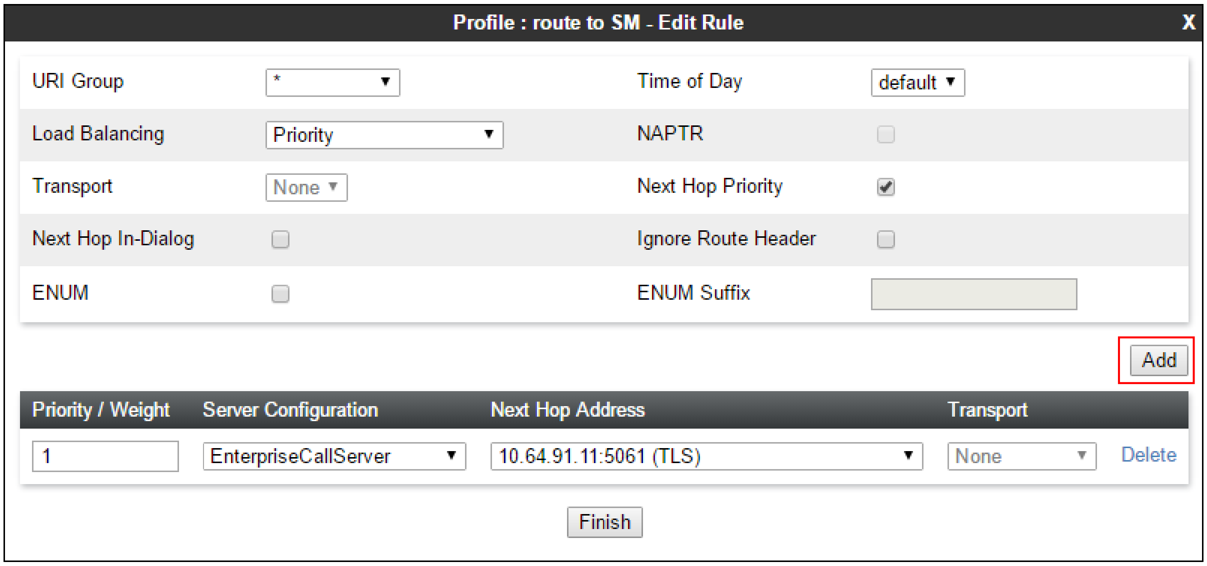
This provisioning defines the Routing Profile for the connection to Session Manager.

Step 1 - Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown)
Step 2 - Enter a **Profile Name**: (e.g., **route 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 **Section 7.3.4**).
- **Next Hop Address:** Verify that the **10.64.91.11:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
- Click on **Finish**.



7.3.7 Routing – To Verizon

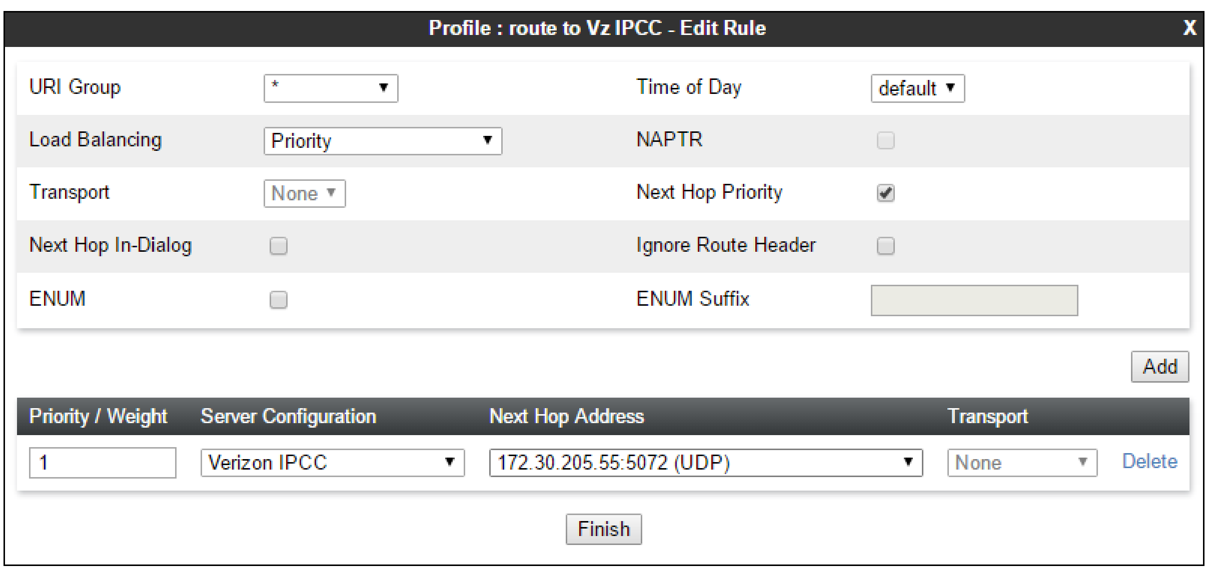
Repeat the steps in **Section 7.3.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Verizon.

Step 1 - On the **Global Profiles → Routing Profile** window, enter a Profile Name: (e.g., **route to Vz IPCC**).

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

- **Priority/Weight** = **1**
- **Server Configuration** = **Verizon IPCC** (**from Section 7.3.5**).
- **Next Hop Address:** select **172.30.205.55:5072 (UDP)**.

Step 3 - Click **Finish**.



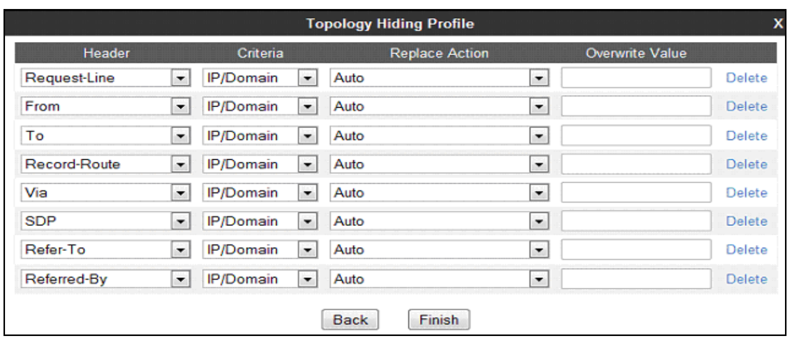
7.3.8 Topology Hiding – Enterprise Side

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.

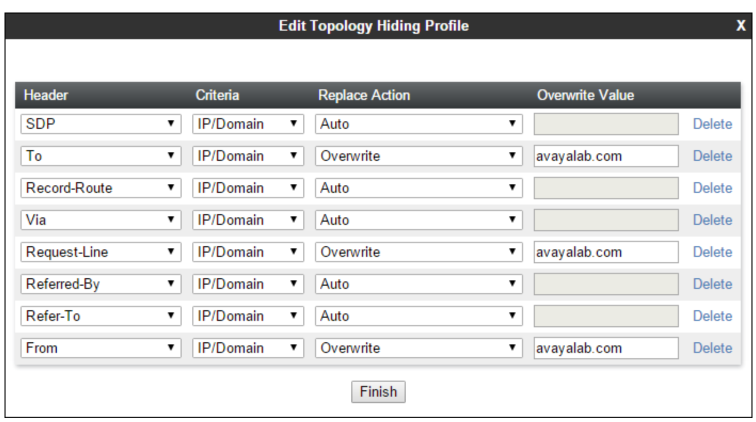
Step 1 - Select **Global Profiles → Topology Hiding** from the left-hand side menu.

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**, **6.7**, and **6.8**).

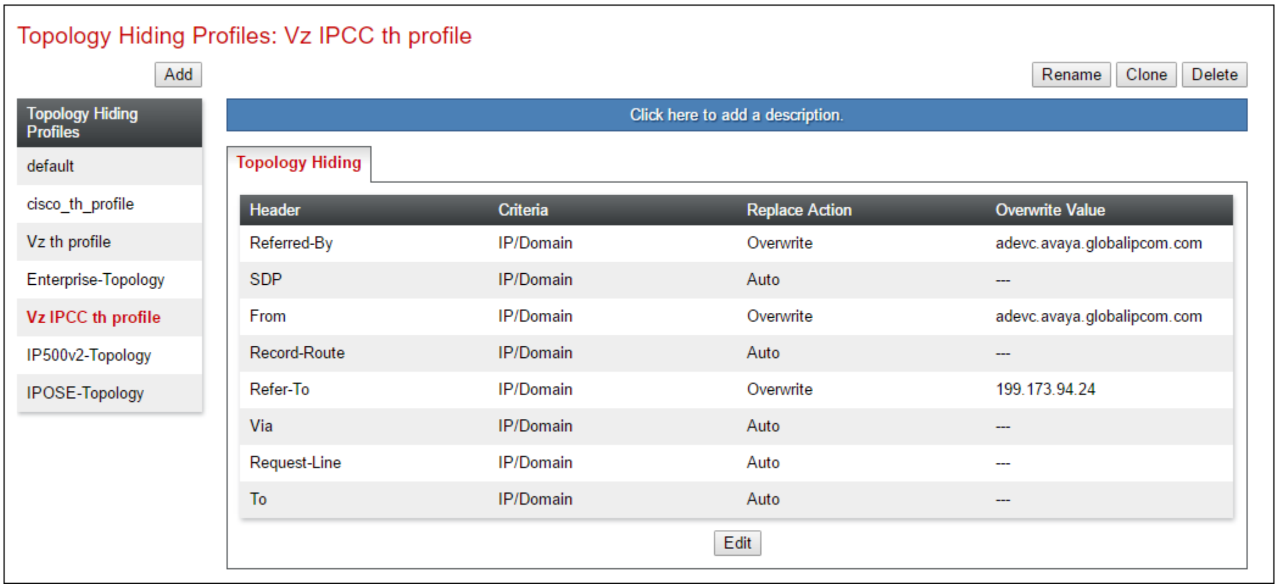


7.3.9 Topology Hiding – Verizon Side

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

- Enter a Profile Name (e.g., **Vz IPCC th profile**).
- Overwrite the headers as shown below with the FQDNs known by Verizon.

Note – The Refer-To header's domain is overwritten with the IP address presented in the original INVITE from Verizon's IP-IVR service. If the IP-IVR service is not used, the Refer-To header can retain the default **Replace Action** of "**Auto**".



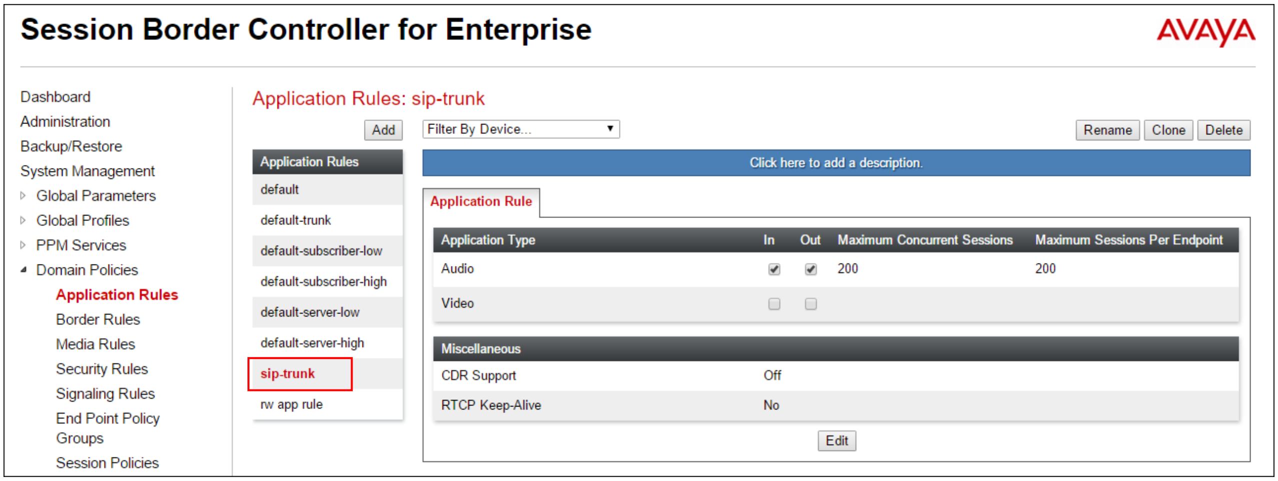
7.4. Domain Policies

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

7.4.1 Application Rules

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

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



7.4.2 Media Rules

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

7.4.2.1 Enterprise – Media Rule

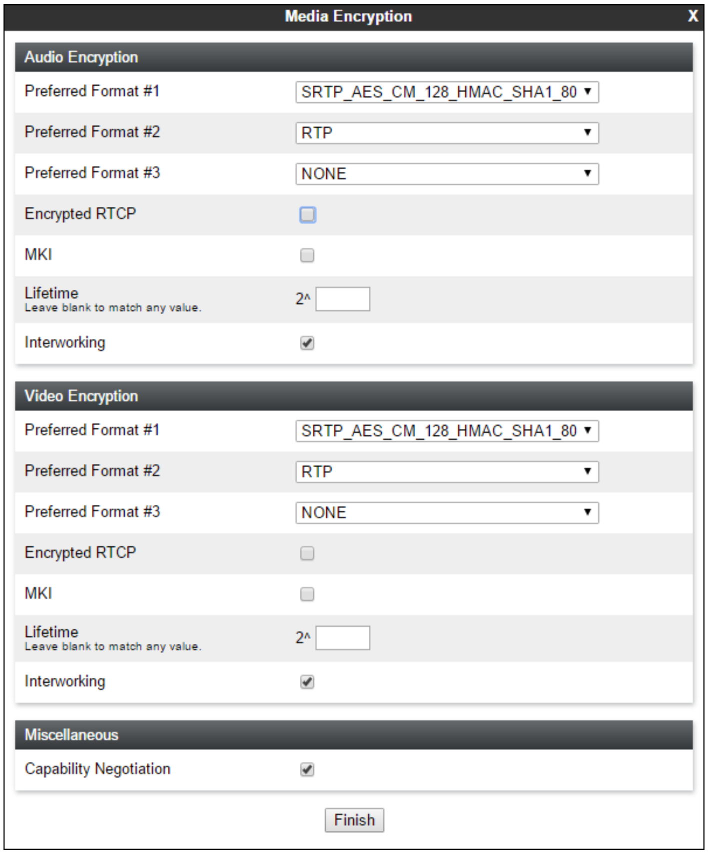
Step 1 - Select **Domain Policies → Media Rules** from the left-hand side menu (not shown).
Step 2 - From the Media Rules menu, select the **avaya-low-med-enc** rule.
Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

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

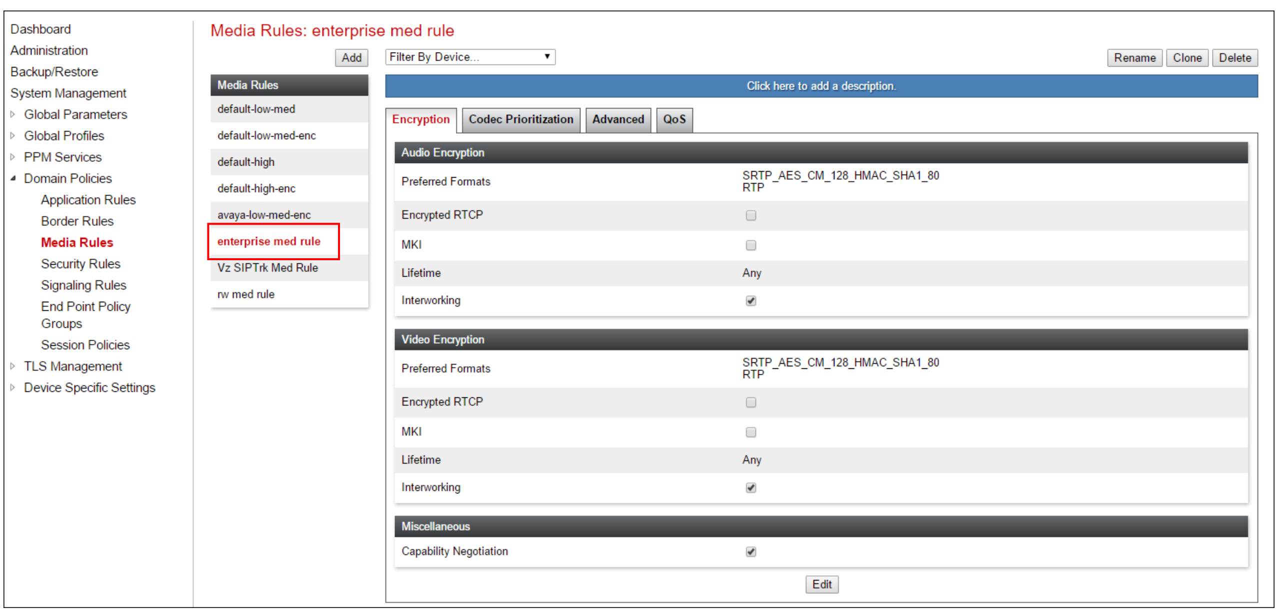
Step 4 - Highlight the **enterprise med rule** just created (not shown):

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

Step 5 - Click **Finish**.



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

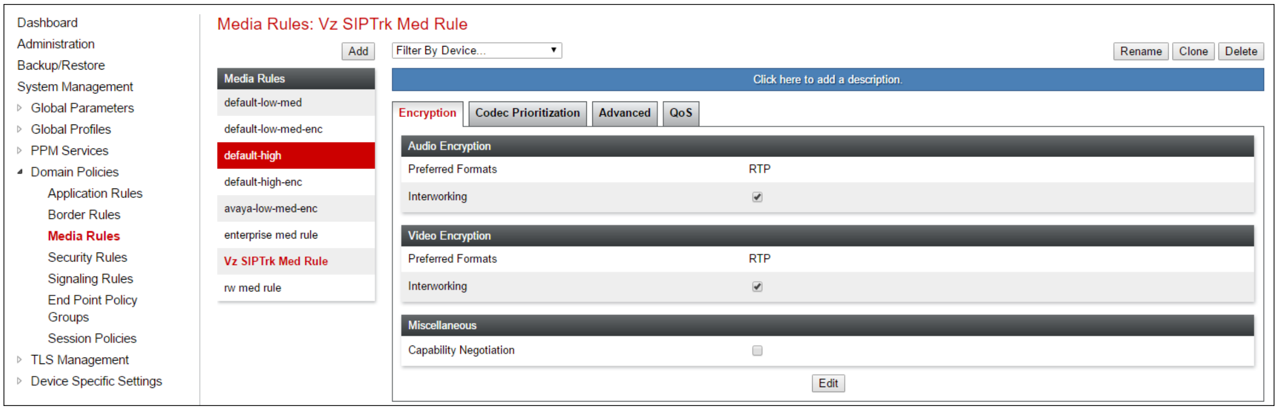


7.4.2.2 Verizon – Media Rule

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

1. Clone the **default-low-med** profile
2. In the **Clone Name** field enter **Vz SIPTrk Med Rule**

The completed **Vz SIPTrk 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 Verizon – Signaling Rule

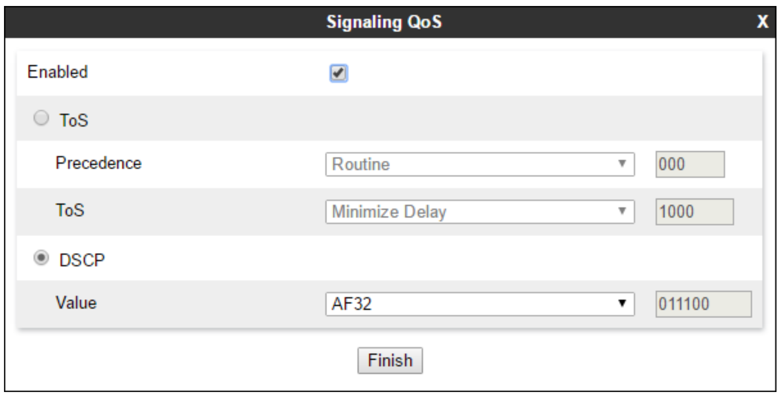
Step 1 - Select **Domain Policies** from the menu on the left-hand side menu (not shown).
Step 2 - Select **Signaling Rules** (not shown).
Step 3 - From the Signaling Rules menu, select the **default** rule.
Step 4 - Select **Clone Rule** button

- Enter a name**: Vz SIPTrk Sig Rule**

Step 5 - Click **Finish**
Step 6 - Highlight the **Vz SIPTrk 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** = **AF32**

Step 5 - Click **Finish**.

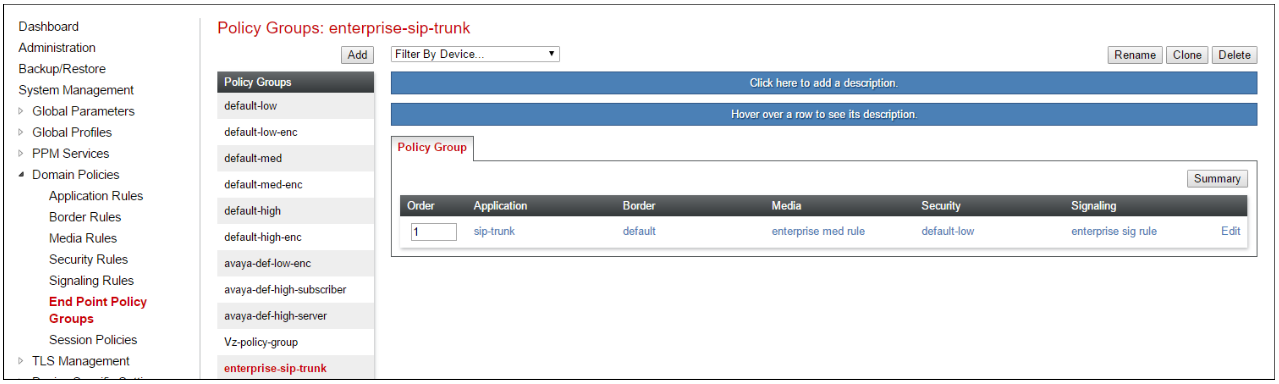


7.4.4 Endpoint Policy Groups – Enterprise Connection

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-sip-trunk**
- **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.

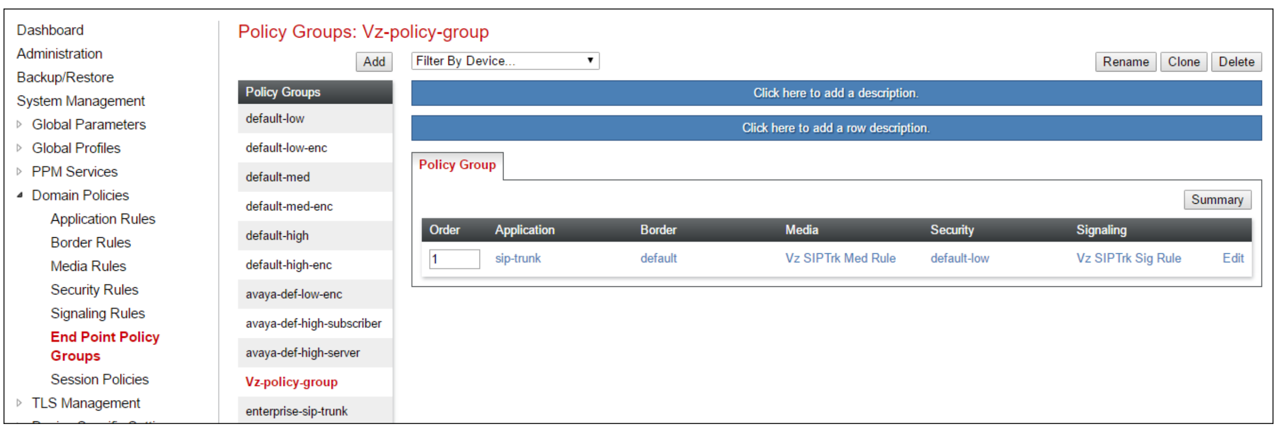


7.4.5 Endpoint Policy Groups – Verizon Connection

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

- **Group Name**: **Vz-policy-group**
- **Media Rule**: **Vz SIPTrk Med Rule** (created in **Section 7.4.2.2**)
- **Signaling Rule**: **Vz SIPTrk Sig Rule** (created in **Section 7.4.3.2**)

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



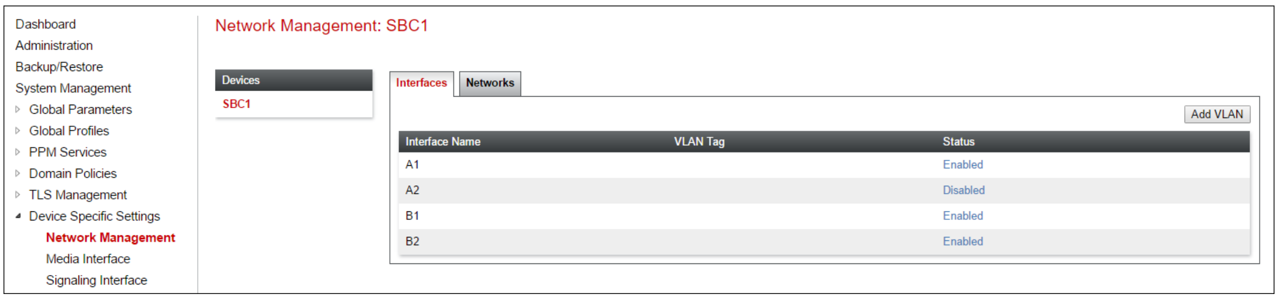
7.5. Device Specific Settings

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

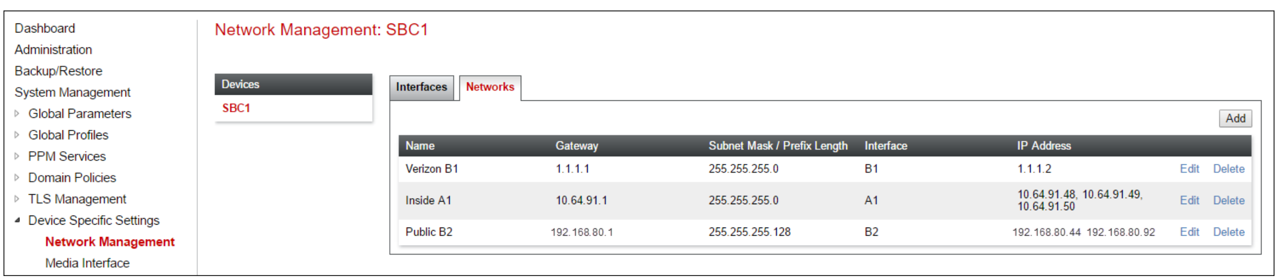
7.5.1 Network Management

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

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

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces.

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

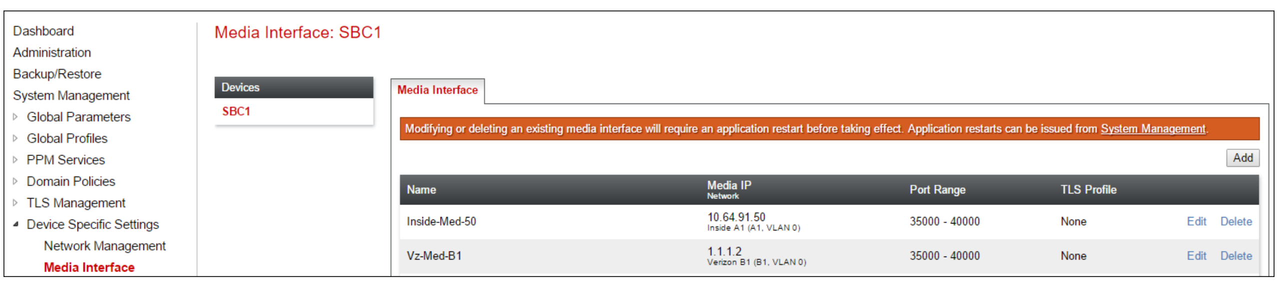
- **Name**: **Inside-Med-50**
- **IP Address**: Select **Inside-A1 (A1,VLAN0)** and **10.64.91.50**
- **Port Range**: **35000 – 40000**

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

- **Name**: **Vz-Med-B1**
- **IP Address**: Select **Verizon-B1 (B1,VLAN0)** and **1.1.1.2**
- **Port Range**: **35000 – 40000**

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.



7.5.3 Signaling Interface

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

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

Step 2 - Select **Signaling Interface**.

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

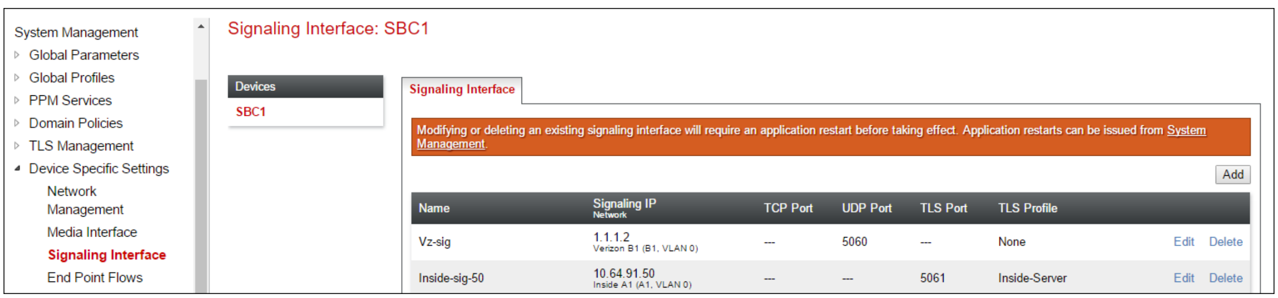
- **Name**: **Inside-Sig-50**
- **IP Address**: Select **Inside A1 (A1,VLAN0)** and **10.64.91.50**
- **TLS Port**: **5061**
- **TLS Profile**: Select the TLS server profile created in **Section 7.2.2** (e.g., **Inside-Server**)

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

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

- **Name**: **Vz-sig**
- **IP Address**: Select **Verizon B1 (B1,VLAN0)** and **1.1.1.2**
- **UDP Port**: **5060**

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



7.5.4 Server Flows – For Session Manager

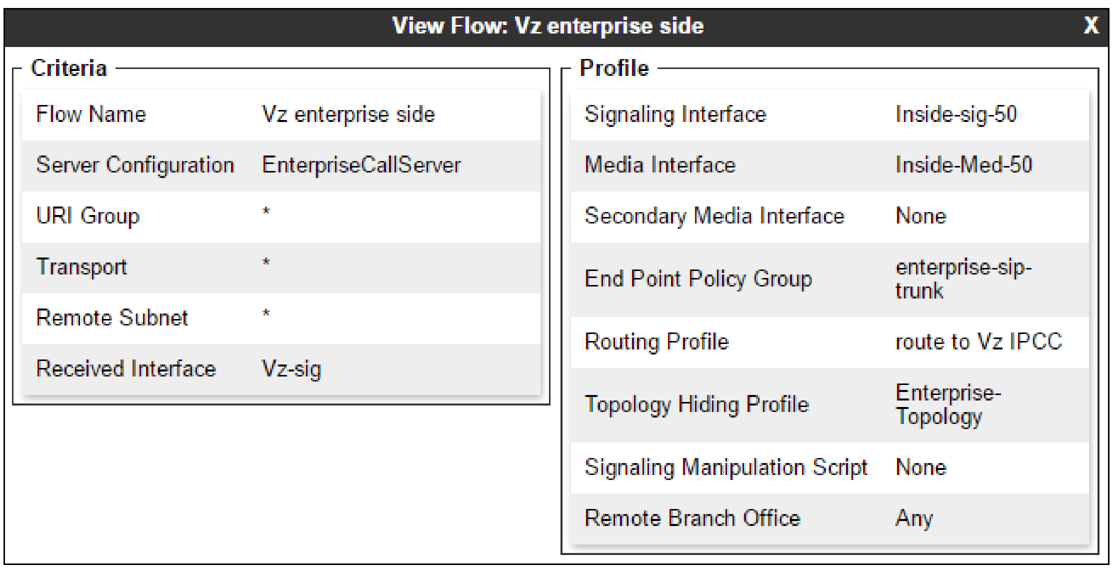
Step 1 - Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).

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

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

- **Flow Name**: **Vz enterprise side**.
- **Server Configuration**: **EnterpriseCallServer** (**Section 7.3.4**).
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Vz-sig** (**Section 7.5.3**).
- **Signaling Interface**: **Inside-sig-50** (**Section 7.5.3**).
- **Media Interface**: **Inside-Med-50** (**Section 7.5.2**).
- **End Point Policy Group**: **enterprise-sip-trunk** (**Section 7.4.4**).
- **Routing Profile**: **route to Vz IPCC** (**Section 7.3.7**).
- **Topology Hiding Profile**: **Enterprise-Topology** (**Section 7.3.8**).
- Let other values default.

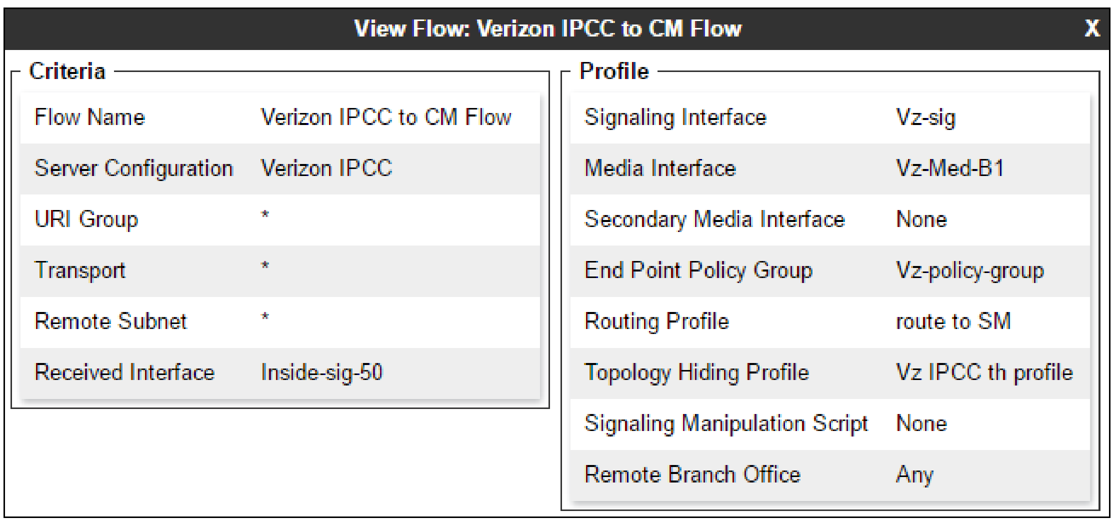
Step 4 - Click **Finish** (not shown).



7.5.5 Server Flows – For Verizon

Step 1 - Repeat steps **1** through **4** from **Section 7.5.4**, with the following changes:

- **Flow Name**: **Verizon IPCC to CM Flow**.
- **Server Configuration**: **Verizon IPCC** (**Section 7.3.5**).
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Inside-sig-50** (**Section 7.5.3**).
- **Signaling Interface**: **Vz-sig (Section 7.5.3**).
- **Media Interface**: **Vz-Med-B1** (**Section 7.5.2**).
- **End Point Policy Group**: **Vz-policy-group** (**Section 7.4.5**).
- **Routing Profile**: **route to SM** (**Section 7.3.6**).
- **Topology Hiding Profile**: **Vz IPCC th profile** (**Section 7.3.9**).



8. Verizon Business IPCC Services Suite Configuration

Information regarding Verizon Business IPCC Services suite offer can be found at http://www.verizonbusiness.com/products/contactcenter/ip/ or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IPCC Services suite was via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

8.1. Service Access Information

The following service access information (FQDN, IP addressing, ports, toll free numbers) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
adevc.avaya.globalipcom.com ***UDP port 5060***	***172.30.205.55*** ***UDP Port 5072***

Toll Free Numbers
866-850-2380
866-851-0107
866-851-2649
866-852-3221
866-850-6850

9. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) Trunk service.

9.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

9.1.1 Example Incoming Call from PSTN via Verizon IPCC to Telephone

Incoming PSTN calls arrive from Verizon at Avaya SBCE, which sends the call to Session Manager. Session Manager sends the call to Communication Manager. On Communication Manager, the incoming call arrives via signaling group 2 and trunk group 2.

The following edited Communication Manager **list trace tac** trace output shows a call incoming on trunk group 2. The PSTN telephone dialed 866-850-6850. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x12003). Extension 12003 is an IP Telephone with IP address 10.64.91.157 in Region 1. Initially, the G450 Media Gateway (10.64.91.81) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is “ip-direct” from the IP Telephone (10.64.91.157) to the “inside” of the Avaya SBCE (10.64.91.50) in Region 2.

```
                                  LIST TRACE
time            data
/* Incoming call arrives to Communication Manager for x12003 */
11:58:07 TRACE STARTED 09/14/2017 CM Release String cold-01.0.532.0-23985
11:58:11 SIP<INVITE sips:12003@avayalab.com SIP/2.0
11:58:11     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:11     active trunk-group 2 member 1    cid 0x5ea
/* Communication Manager sends 183 with SDP as a result of TG 2 configuration */
11:58:11 SIP>SIP/2.0 183 Session Progress
11:58:11     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:11     dial 12003
11:58:11     ring station      12003 cid 0x5ea
/* Media Server at 10.64.91.60, ringback tone heard by caller */
11:58:11     G729 ss:off ps:20
             rgn:2 [10.64.91.50]:35056
             rgn:1 [10.64.91.60]:6090
11:58:11     G72264K ss:off ps:20
             rgn:1 [10.64.91.157]:25426
             rgn:1 [10.64.91.60]:6092
/* User Answers call, Communication Manager sends 200 OK */
11:58:11 SIP>SIP/2.0 200 OK
11:58:11     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:11     active station      12003 cid 0x5ea
11:58:12 SIP<ACK sips:10.64.91.65:5071;transport=tls SIP/2.0
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:12 SIP>INVITE sips:+13035382177@10.64.91.50:5061;transport=tls
11:58:12 SIP>;gsid=45b06bf0-9976-11e7-9cb3-000c29e8354a;sipappsessio
11:58:12 SIP>nid=app-ybxwefkfgh8k SIP/2.0
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:12 SIP<SIP/2.0 100 Trying
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:12 SIP<SIP/2.0 200 OK

<continued on next page>
```

```
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
/* Communication Manager sends re-INVITE to begin shuffle to ip-direct */
11:58:12 SIP>INVITE sips:+13035382177@10.64.91.50:5061;transport=tls
11:58:12 SIP>;gsid=45b06bf0-9976-11e7-9cb3-000c29e8354a;wlsscid=-270
11:58:12 SIP>f46a416660660;sipappsessionid=app-ybxwefkfgh8k SIP/2.0
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
/* Final media path is ip-direct from answering IP (10.64.91.157) to inside of
SBC (10.64.91.50) */
11:58:12     G729A ss:off ps:20
             rgn:2 [10.64.91.50]:35056
             rgn:1 [10.64.91.157]:25426
11:58:12     G729 ss:off ps:20
             rgn:1 [10.64.91.157]:25426
             rgn:2 [10.64.91.50]:35056
11:58:12 SIP<SIP/2.0 100 Trying
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
/* Communication Manager receives 200 OK with SDP, sends ACK with SDP */
11:58:12 SIP<SIP/2.0 200 OK
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
11:58:12 SIP>ACK sips:+13035382177@10.64.91.50:5061;transport=tls;gs
11:58:12 SIP>id=45b06bf0-9976-11e7-9cb3-000c29e8354a;wlsscid=-270f46
11:58:12 SIP>a416660660;sipappsessionid=app-ybxwefkfgh8k SIP/2.0
11:58:12     Call-ID: a4b93e1fefa7ee2746dfc32772f2cf69
```

The following screen shows **Page 2** of the output of the **status trunk** command pertaining to this same call. Note the signaling using port 5071 between Communication Manager and Session Manager. Note the media is “**ip-direct**” from the IP Telephone (10.64.91.157) to the inside IP address of Avaya SBCE (10.64.91.50) using codec G.729.

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

Near-end Signaling Loc: PROCR
  Signaling   IP Address                              Port
   Near-end:  10.64.91.65                           : 5071
    Far-end:  10.64.91.11                           : 5071
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                              Port
   Near-end:  10.64.91.157                          : 25426
    Far-end:  10.64.91.50                           : 35056

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

The following screen shows **Page 3** of the output of the **status trunk** command pertaining to this same call. Here it can be observed that G.729 codec is used.

```
status trunk 2/1                                              Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00011
T00011:TX:10.64.91.50:35056/g729/20ms/1-srtp-aescm128-hmac80
S00003:RX:10.64.91.157:25426/g729a/20ms/1-srtp-aescm128-hmac80
```

9.1.2 Example Incoming Call Referred via Call Vector to PSTN Destination

The following edited and annotated Communication Manager **list trace tac** trace output shows a call incoming on trunk group 2. The call was routed to a Communication Manager vector directory number (VDN 10001) associated with a call vector (call vector 1). The vector answers the call, plays an announcement to the caller, and then uses a "route-to" step to cause a REFER message to be sent with a Refer-To header containing the number configured in the vector "route-to" step. The PSTN telephone dialed 866-852-3221. Session Manager can map the number received from Verizon to the VDN extension (x10001), or the incoming call handling table for trunk group 1 can do the same. In the trace below, Session Manager had already mapped the Verizon number to the Communication Manager VDN extension. The annotations in the edited trace highlight key behaviors. At the conclusion, the PSTN caller that dialed the Verizon toll-free number is talking to the Referred-to PSTN destination, and no trunks (i.e., from trunk 1 handling the call) are in use.

```
list trace tac *02                                                     Page   1
/* Session Manager has adapted the dialed number 8668523221 to VDN 10001 */
12:28:09 TRACE STARTED 09/14/2017 CM Release String cold-01.0.532.0-23985
12:28:15 SIP<INVITE sips:10001@avayalab.com SIP/2.0
12:28:15     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:15     active trunk-group 2 member 1    cid 0x62d
12:28:15    0  0 ENTERING TRACE cid 1581
12:28:15    2  1 vdn e10001 bsr appl   0 strategy 1st-found override n
12:28:15    2  1 AVDN: 10001 AVRD:
12:28:15    2  1 wait 2 secs hearing ringback
/* Vector step plays ringback. 183 with SDP is sent*/
12:28:15 SIP>SIP/2.0 183 Session Progress
12:28:15     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:15     dial 10001
12:28:15     ring vector 2      cid 0x62d
12:28:15     G729 ss:off ps:20
             rgn:2 [10.64.91.50]:35082
             rgn:1 [10.64.91.60]:6134
12:28:17    2  2 # Play announcement to caller i...
12:28:17    2  3 announcement 11006
12:28:17 SIP>SIP/2.0 183 Session Progress
12:28:17     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:17    2  3      announcement: board 001V9 ann ext: 11006
/* Vector step answers call with announcement. 200 OK is sent */
12:28:17 SIP>SIP/2.0 200 OK
12:28:17     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:17     active announcement      11006 cid 0x62d
12:28:17     hear annc source 001V9 ext 11006 cid 0x62d
12:28:17     Connected party uses public-unknown-numbering
12:28:17 SIP<ACK sips:+18668523221@10.64.91.65:5071;transport=tls SI
12:28:17 SIP<P/2.0

<continued on next page>
```

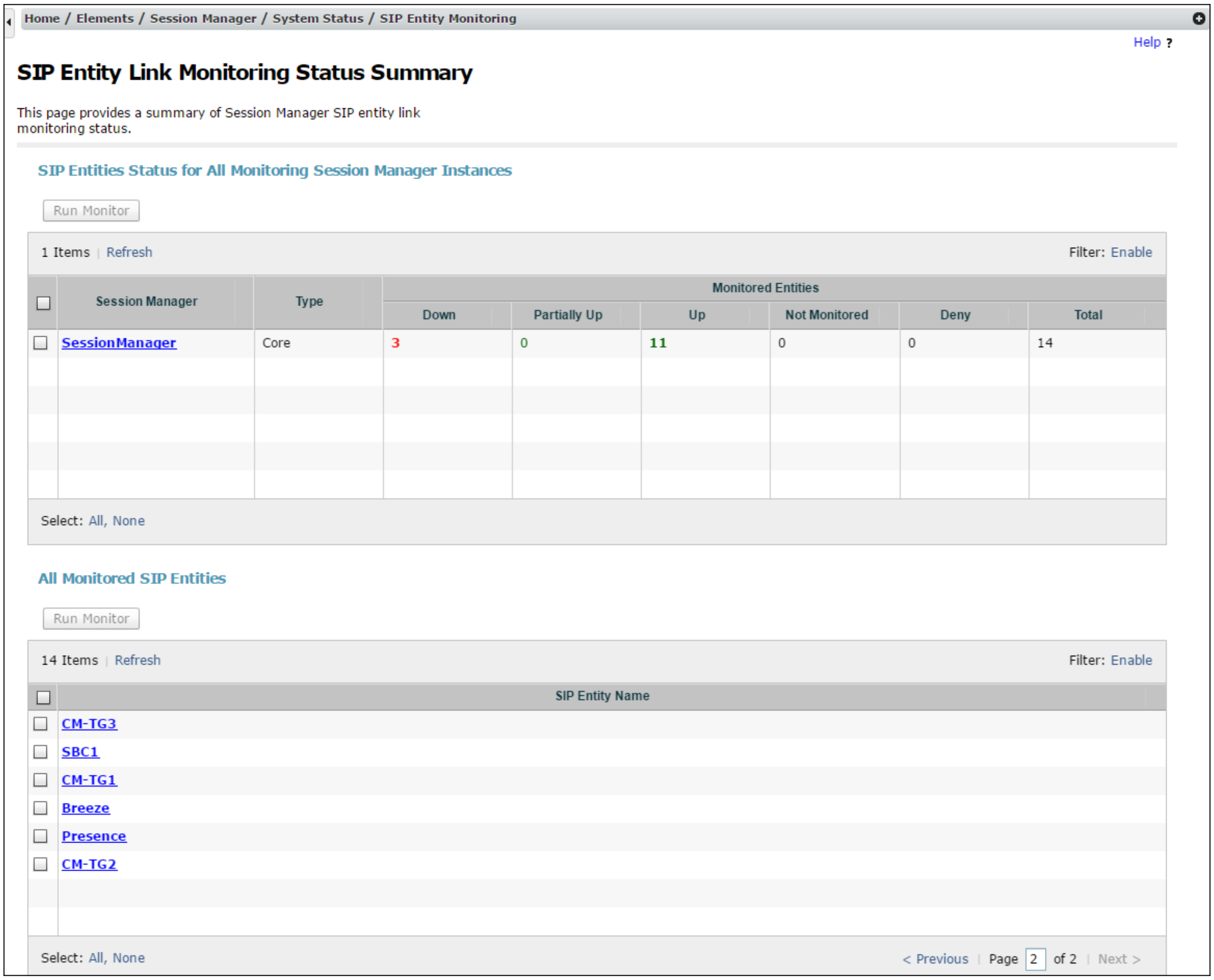
```
12:28:17     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:18     idle announcement       cid 0x62d
12:28:18    2  4 # Refer the call to PSTN Destin...
12:28:18    2  5 route-to number ~r+13035387024 cov n if unconditionally
/* Caller hears pre-REFER announcement, announcement completes, REFER sent */
12:28:18 SIP>REFER sips:+13035382177@10.64.91.50:5061;transport=tls;
12:28:18 SIP>gsid=78db7e80-997a-11e7-9cb3-000c29e8354a;sipappsession
12:28:18 SIP>id=app-qr3kvtjmaso5 SIP/2.0
12:28:18     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
/* Communication Manager receives 202 Accepted sent by Verizon IPCC */
12:28:19 SIP<SIP/2.0 202 Accepted
12:28:19     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
/* Verizon IPCC sends NOTIFY with sipfrag 100 Trying and CM sends 200 OK */
12:28:19 SIP<NOTIFY sips:+18668523221@10.64.91.65:5071;transport=tls
12:28:19 SIP< SIP/2.0
12:28:19     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:19 SIP>SIP/2.0 200 OK
12:28:19     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
* Note that caller does not hear ringback or any audible feedback until answer
*/
/* Verizon IPCC sends NOTIFY with sipfrag 200 OK and CM sends 200 OK and BYE */
12:28:28 SIP<NOTIFY sips:+18668523221@10.64.91.65:5071;transport=tls
12:28:28 SIP< SIP/2.0
12:28:28     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:28 SIP>SIP/2.0 200 OK
12:28:28     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:28    2  5 LEAVING VECTOR PROCESSING cid 1581
12:28:28 SIP>BYE sips:+13035382177@10.64.91.50:5061;transport=tls;gs
12:28:28 SIP>id=78db7e80-997a-11e7-9cb3-000c29e8354a;sipappsessionid
12:28:28 SIP>=app-qr3kvtjmaso5 SIP/2.0
12:28:28     Call-ID: 9990ed3160377b0d0c7d822a3d541b55
12:28:28     idle vector 0      cid 0x62d
/* Trunks are now idle. Caller and refer-to target are connected by Verizon */
```

When the initial call arrived from Verizon, it used trunk member 1 from trunk group 2. In the final state when the PSTN caller is speaking with the answering agent at the Refer-To target, trunk member 1 is idle, reflecting the successful REFER.

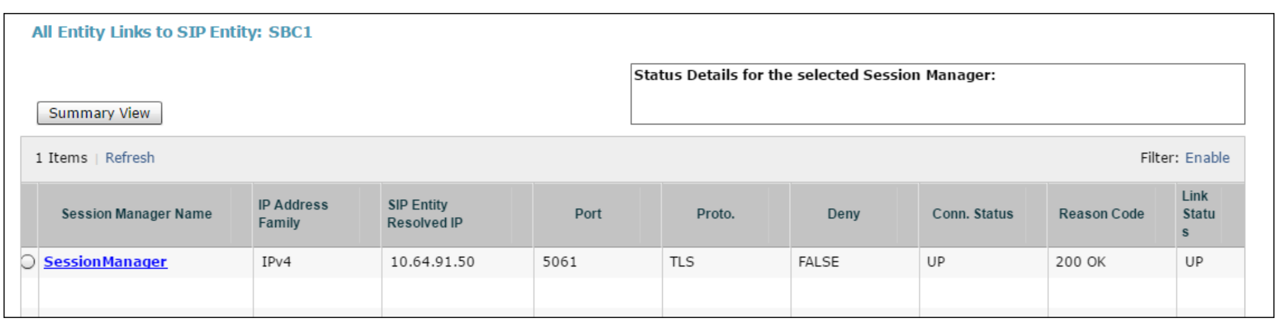
```
status trunk 2
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00011   in-service/idle    no
0002/002 T00012   in-service/idle    no
0002/003 T00013   in-service/idle    no
0002/004 T00014   in-service/idle    no
0002/005 T00015   in-service/idle    no
0002/006 T00016   in-service/idle    no
0002/007 T00017   in-service/idle    no
0002/008 T00018   in-service/idle    no
0002/009 T00019   in-service/idle    no
0002/010 T00020   in-service/idle    no
```

9.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager. Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. A screen such as the following is displayed.



From the list of monitored entities, select an entity of interest, such as **SBC1**. Under normal operating conditions, the **Link Status** should be "**UP**" as shown in the example screen below.

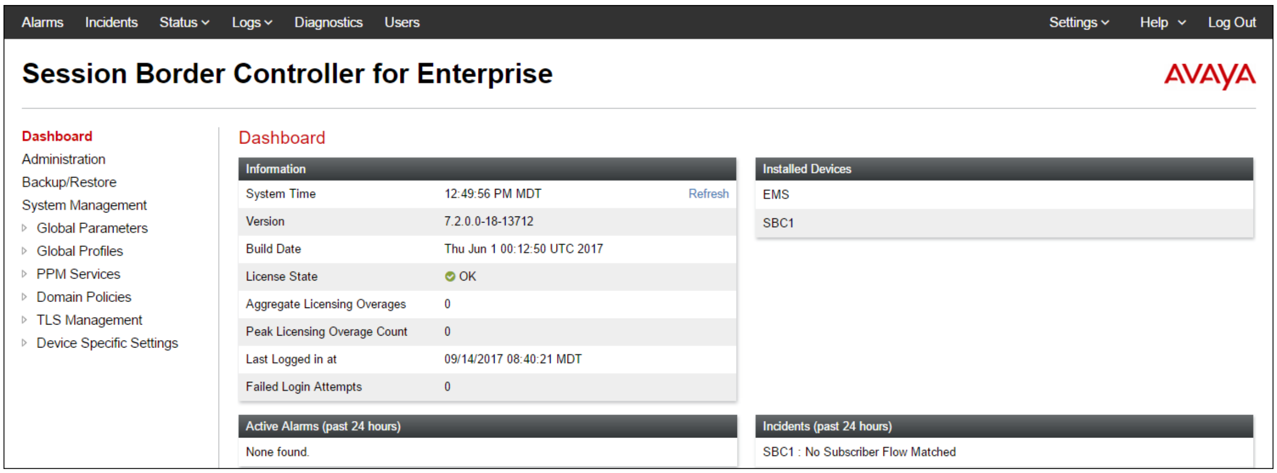


9.3. Avaya Session Border Controller for Enterprise Verification

This section illustrates verifications from Avaya Session Border Controller for Enterprise.

9.3.1 Welcome Screen

The welcome screen shows alarms, incidents, and the status of all managed Avaya SBCEs at a glance.



9.3.2 Alarms

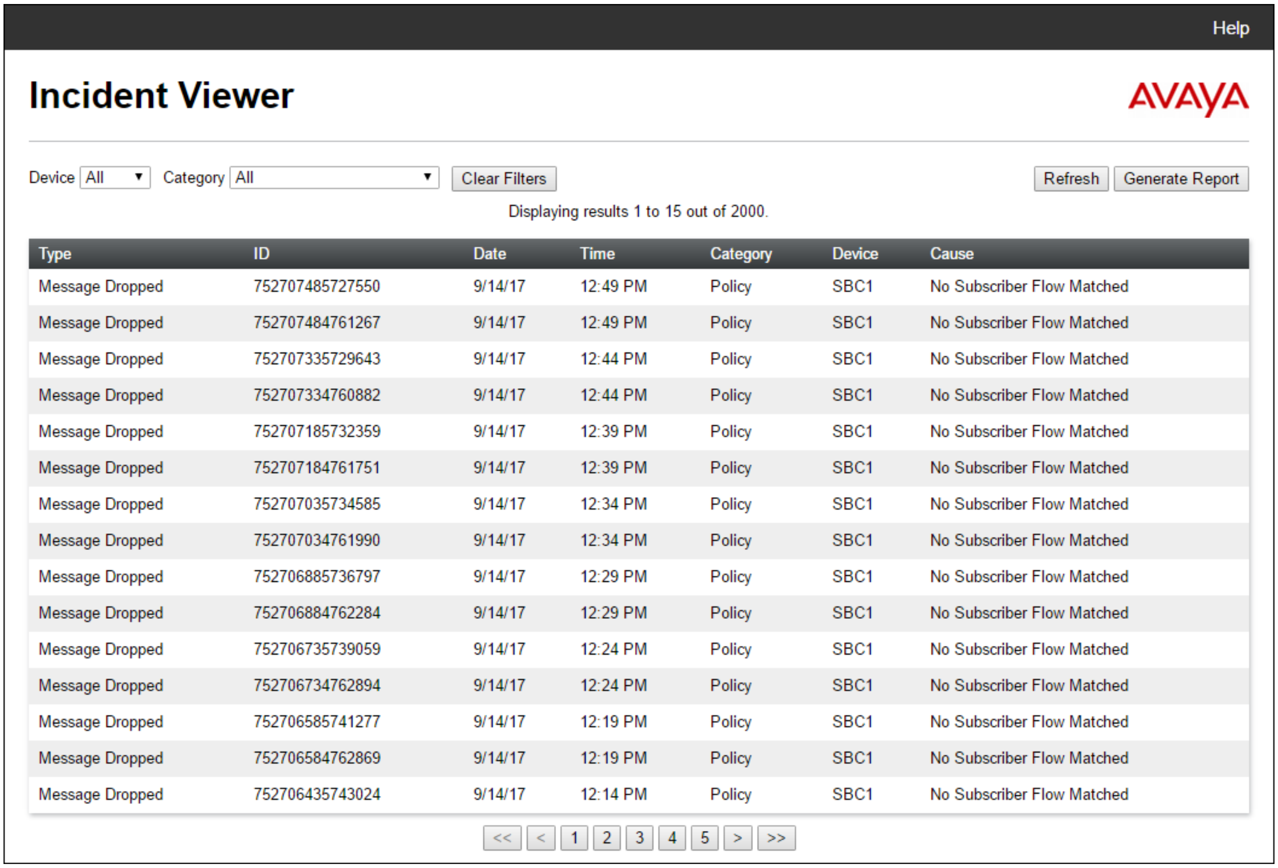
A list of the most recent alarms can be found under the Alarm tab on the top left bar.

Alarm Viewer:

9.3.3 Incidents

A list of all recent incidents can be found under the incidents tab at the top left next to the Alarms.

Incident Viewer:



Help

Incident Viewer

AVAYA

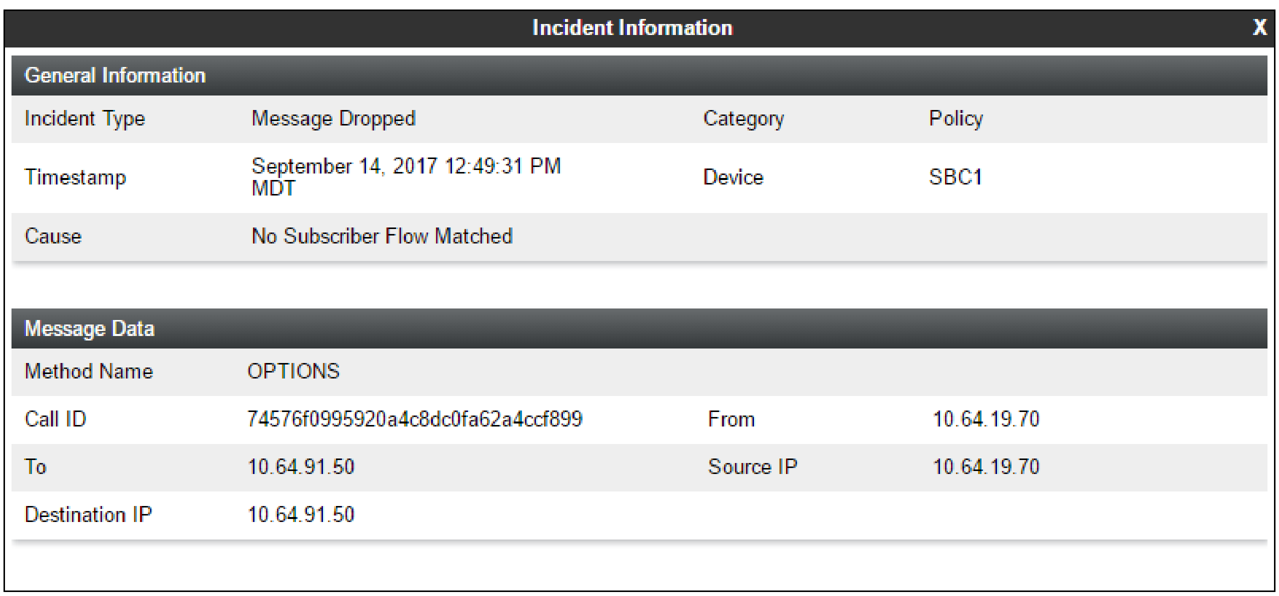
Device All Category All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2000.

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	752707485727550	9/14/17	12:49 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707484761267	9/14/17	12:49 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707335729643	9/14/17	12:44 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707334760882	9/14/17	12:44 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707185732359	9/14/17	12:39 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707184761751	9/14/17	12:39 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707035734585	9/14/17	12:34 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752707034761990	9/14/17	12:34 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706885736797	9/14/17	12:29 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706884762284	9/14/17	12:29 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706735739059	9/14/17	12:24 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706734762894	9/14/17	12:24 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706585741277	9/14/17	12:19 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706584762869	9/14/17	12:19 PM	Policy	SBC1	No Subscriber Flow Matched
Message Dropped	752706435743024	9/14/17	12:14 PM	Policy	SBC1	No Subscriber Flow Matched

<< < 1 2 3 4 5 > >>

Further Information can be obtained by clicking on an incident in the incident viewer.



Incident Information X

General Information

Incident Type	Message Dropped	Category	Policy
Timestamp	September 14, 2017 12:49:31 PM MDT	Device	SBC1
Cause	No Subscriber Flow Matched		

Message Data

Method Name	OPTIONS		
Call ID	74576f0995920a4c8dc0fa62a4ccf899	From	10.64.19.70
To	10.64.91.50	Source IP	10.64.19.70
Destination IP	10.64.91.50		

9.3.4 Diagnostics

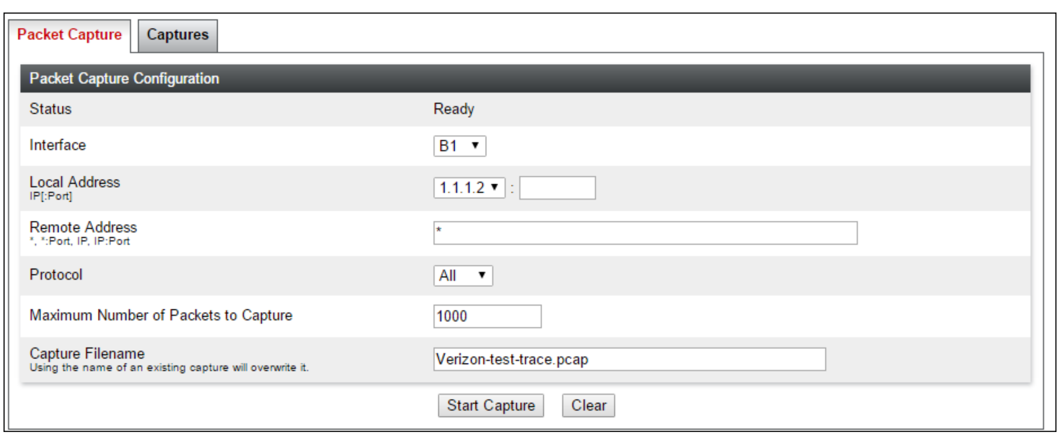
The full diagnostics check will verify the link of each interface, and ping the configured next-hop gateways and DNS servers.

Click on Diagnostics on the top bar, select the Avaya SBCE from the list of devices and then click "Start Diagnostics".

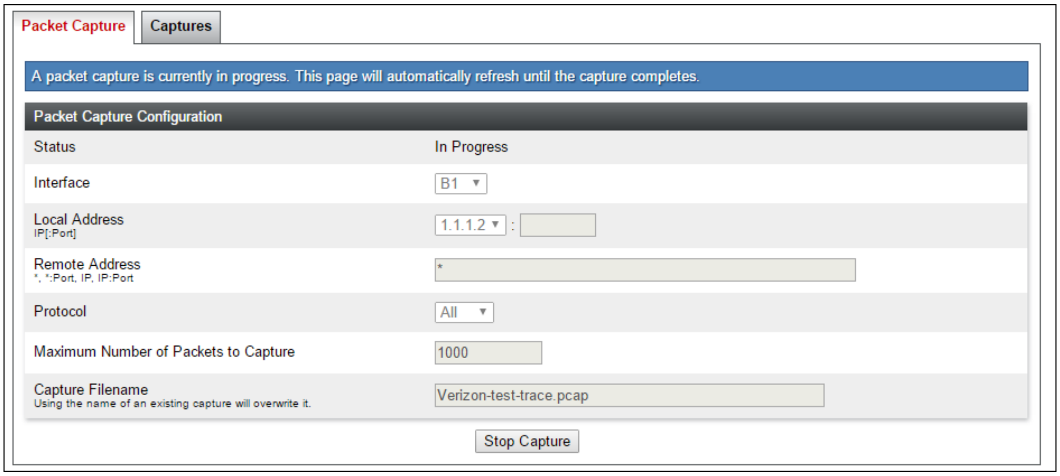
9.3.5 Tracing

To take a call trace, select **Device Specific Settings → Troubleshooting → Tracie** from the left-side menu (not shown).

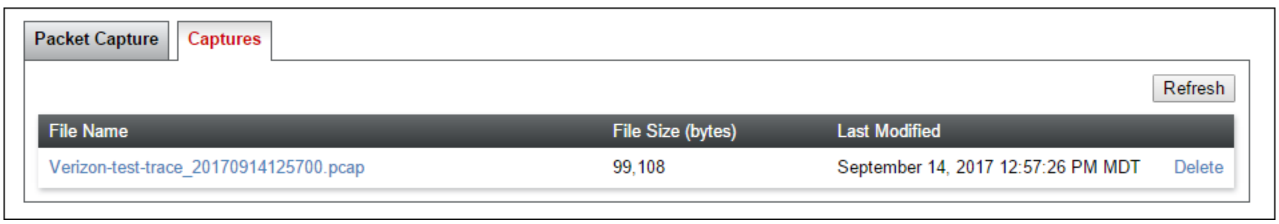
Select the Packet Capture tab and set the desired configuration for a call trace and click **Start Capture**.



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



Select the **Captures** tab at the top and the capture will be listed; select the File Name and choose to open it with an application like Wireshark.



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1, and Avaya Session Border Controller for Enterprise 7.2 can be configured to interoperate successfully with Verizon Business IP Contact Center Services suite. This solution enables inbound toll free calls over a Verizon Business VoIP Inbound SIP trunk service connection. In addition, these Application Notes further demonstrate that the Avaya Aura® Communication Manager implementation of SIP Network Call Redirection (SIP-NCR) can work in conjunction with Verizon's Business IP Contact Center services implementation of SIP-NCR to support call redirection over SIP trunks inclusive of passing User-User Information (UUI).

Please note that the sample configurations shown in these Application Notes are intended to provide configuration guidance to supplement other Avaya product documentation.

11. References

11.1. Avaya

Avaya product documentation, including the following, is available at http://support.avaya.com

Avaya Aura® Session Manager/System Manager

[1] Deploying Avaya Aura® Session Manager, Release 7.1, Issue 1, May 2017

[2] Administering Avaya Aura® Session Manager, Release 7.1.1, Issue 2, August 2017

[3] Deploying Avaya Aura® System Manager, Release 7.1.1, Issue 3, August 2017

[4] Administering Avaya Aura® System Manager for Release 7.1.1, Issue 6, August 2017

Avaya Aura® Communication Manager

[5] Deploying Avaya Aura® Communication Manager, Release 7.1.1, Issue 2, August 2017

[6] Administering Avaya Aura® Communication Manager, Release 7.1.1, Issue 2, August 2017

[7] Administering Avaya G450 Branch Gateway, Release 7.1, Issue 1, May 2017

[8] Deploying and Updating Avaya Aura® Media Server Appliance, Release 7.8, Issue 3, August 2017

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

Avaya Session Border Controller for Enterprise

[10] Administering Avaya Session Border Controller for Enterprise, Release 7.2, Issue 2, August 2017

[11] Deploying Avaya Session Border Controller for Enterprise, Release 7.2, Issue 2, August 2017

Avaya Aura® Messaging

[12] Administering Avaya Aura® Messaging, Release 7.0.0, Issue 1, January 2017

Avaya Application Notes, including the following, are also available at http://support.avaya.com

The following Application Notes cover Session Manager 7.0 with Verizon Business IP Contact Center Services.

[VZ-IPCC] – Application Notes for Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Controller for Enterprise 7.0 with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.0

11.2. Verizon Business

The following documents may be obtained by contacting a Verizon Business Account Representative.

- *Retail VoIP Interoperability Test Plan*
- *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)*