



## 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 Trunking Service – Issue 1.0

## Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 7.1, Avaya Aura® Communication Manager Release 7.1, and Avaya Session Border Controller for Enterprise Release 7.2 with the Verizon Business IP Trunking service. These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

The Verizon Business IP Trunking service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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 via the DevConnect Program at the Avaya Solution and Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

# Table of Contents

1.	Introduction.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing .....	5
2.2.	Test Results.....	6
2.3.	History Info and Diversion Headers .....	7
2.4.	SIP Header Removal.....	7
2.5.	Support.....	8
3.	Reference Configuration.....	9
4.	Equipment and Software Validated .....	11
5.	Configure Avaya Aura® Session Manager .....	12
5.1.	SIP Domain.....	13
5.2.	Locations.....	13
5.2.1	Main Location.....	13
5.2.2	Common Location .....	14
5.3.	Configure Adaptations .....	15
5.3.1	Adaptation for Avaya Aura® Communication Manager Extensions .....	15
5.3.2	Adaptation for the Verizon Business IP Trunking service .....	17
5.4.	SIP Entities.....	18
5.4.1	Avaya Aura® Session Manager SIP Entity .....	19
5.4.2	Avaya Aura® Communication Manager SIP Entity – Public Trunk .....	21
5.4.3	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	22
5.4.4	Avaya Session Border Controller for Enterprise SIP Entity.....	22
5.4.5	Avaya Aura® Messaging SIP Entity .....	22
5.5.	Entity Links.....	22
5.5.1	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	22
5.5.2	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	23
5.5.3	Entity Link for the Verizon Business IP Trunking service via the Avaya SBCE.....	23
5.5.4	Entity Link to Avaya Aura® Messaging .....	23
5.6.	Time Ranges .....	24
5.7.	Routing Policies .....	24
5.7.1	Routing Policy for Verizon Routing to Avaya Aura® Communication Manager ..	24
5.7.2	Routing Policy for Inbound Routing to Avaya Aura® Messaging.....	26
5.7.3	Routing Policy for Outbound Calls to Verizon.....	26
5.8.	Dial Patterns.....	26
5.8.1	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager .....	26
5.8.2	Matching Outbound Calls to Verizon/PSTN .....	28
5.9.	Verify TLS Certificates – Session Manager .....	29
6.	Configure Avaya Aura® Communication Manager Release 7.1 .....	31
6.1.	Verify Licensed Features .....	31
6.2.	System-Parameters Features .....	33
6.3.	Dial Plan.....	34
6.4.	Node Names.....	34
6.5.	Processor Ethernet Configuration .....	35
6.6.	IP Codec Sets .....	35
6.6.1	Codecs for IP Network Region 1 (calls within the CPE) .....	35

6.6.2	Codecs for IP Network Region 2 (calls to/from Verizon) .....	37
6.7.	Network Regions .....	37
6.7.1	IP Network Region 1 – Local CPE Region .....	37
6.7.2	IP Network Region 4 – Verizon Trunk Region .....	39
6.8.	SIP Trunks .....	39
6.8.1	SIP Trunk for Inbound/Outbound Verizon calls.....	40
6.8.2	Local SIP Trunk (Avaya SIP Telephone and Messaging Access).....	43
6.9.	Public Numbering .....	43
6.10.	Private Numbering.....	44
6.11.	Route Patterns .....	45
6.11.1	Route Pattern for National Calls to Verizon .....	45
6.11.2	Route Pattern for International Calls to Verizon .....	45
6.11.3	Route Pattern for Service Calls to Verizon.....	46
6.11.4	Route Pattern for Calls within the CPE .....	46
6.12.	Automatic Route Selection (ARS) Dialing.....	47
6.13.	Automatic Alternate Routing (AAR) Dialing.....	47
6.14.	Avaya G430 Media Gateway Provisioning .....	48
6.15.	Avaya Aura® Media Server Provisioning .....	49
6.16.	Save Translations.....	50
6.17.	Verify TLS Certificates – Communication Manager.....	50
7.	Configure Avaya Session Border Controller for Enterprise Release 7.2.....	52
7.1.	System Management – Status .....	53
7.2.	TLS Management.....	54
7.2.1	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	54
7.2.2	Server Profiles.....	55
7.2.3	Client Profiles .....	56
7.3.	Global Profiles .....	57
7.3.1	Server Interworking – Avaya.....	57
7.3.2	Server Interworking – Verizon .....	60
7.3.3	Signaling Manipulation.....	61
7.3.4	Server Configuration – Session Manager .....	62
7.3.5	Server Configuration – Verizon.....	64
7.3.6	Routing – To Session Manager.....	65
7.3.7	Routing – To Verizon .....	66
7.3.8	Topology Hiding – Enterprise Side .....	67
7.3.9	Topology Hiding – Verizon Side.....	68
7.4.	Domain Policies .....	68
7.4.1	Application Rules.....	68
7.4.2	Media Rules .....	69
7.4.3	Signaling Rules .....	70
7.4.4	Endpoint Policy Groups – Enterprise Connection .....	72
7.4.5	Endpoint Policy Groups – Verizon Connection.....	72
7.5.	Device Specific Settings .....	73
7.5.1	Network Management.....	73
7.5.2	Media Interfaces.....	74
7.5.3	Signaling Interface .....	74

7.5.4	Server Flows – For Session Manager .....	75
7.5.5	Server Flows – For Verizon.....	76
8.	Verizon Business IP Trunking Services Suite Configuration.....	77
8.1.	Service Access Information .....	77
9.	Verification Steps.....	78
9.1.	Avaya Aura® Communication Manager Verifications .....	78
9.1.1	Example Incoming Call from PSTN via Verizon SIP Trunk .....	78
9.1.2	Example Outgoing Calls to PSTN via Verizon SIP Trunk.....	80
9.2.	Avaya Aura® Session Manager Verification .....	81
9.3.	Avaya Session Border Controller for Enterprise Verification.....	82
9.3.1	Welcome Screen .....	82
9.3.2	Alarms.....	82
9.3.3	Incidents.....	83
9.3.4	Diagnostics.....	83
9.3.5	Tracing .....	85
10.	Conclusion .....	86
11.	Additional References.....	87
11.1.	Avaya .....	87
11.2.	Verizon Business .....	87

# 1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 7.1, Avaya Aura® Communication Manager Release 7.1, and Avaya Session Border Controller for Enterprise Release 7.2 with the Verizon Business IP Trunking service. The Verizon Business IP Trunking service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

## 2. General Test Approach and Test Results

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

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 the Verizon Business Trunking service 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

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Communication Manager and the PSTN can be made using G.711MU or G.729A codecs.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF using RFC 2833
  - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)

- Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Communication Manager Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g., International, operator assist, 411)
- Hold / Retrieve with music on hold
- Call transfer using two approaches
  - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to “y”)
  - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to “n”)
- Conference calls
- SIP Diversion Header for call redirection
  - Call Forwarding
  - EC500
- Long hold time calls
- Remote Worker

## 2.2. Test Results

Interoperability testing of Verizon Business IP Trunking service was completed with successful results for all test cases. The following limitations are noted for the sample configuration described in these Application Notes.

1. Verizon provisioned T.38 fax on the production circuit used to verify these Application Notes. Verizon Business IP Trunking service will never send a re-Invite to T.38. If the **FAX Mode** field on the Communication Manager ip-codec-set form page 2 is set to “**t.38-standard**” (see **Section 5.6**), Communication Manager will send the proper re-Invite to T.38 for both inbound and outbound fax calls, but will not fallback to G.711 should the Verizon network reject the Communication Manager attempt to transition to T.38 by sending a 488 Not Acceptable message. If the **FAX Mode** is set to “**t.38-G711-fallback**” setting<sup>1</sup>, Communication Manager will send a re-Invite to T.38 for inbound fax calls only and relies on the far end to send a re-Invite to T.38 for outbound calls. Communication Manager assumes T.38 fax is not supported for an outbound fax call unless an Invite for T.38 is received. The result is an outbound fax sent using G.711, even though the circuit is provisioned for T.38. Inbound fax calls negotiate properly to T.38. With the limitations of T.38 on Verizon’s network, it is recommended to use an AudioCodes MP-114 or MP-124 Gateway between Session Manager and the fax device when fax is used with Verizon Business IP Trunking service.
2. When the **Initial IP-IP Direct Media** field on the Communication Manager signaling group form page 1 is set to “y”, Communication Manager sends a “183 Session Progress” without SDP during an inbound PSTN call that is forwarded to another PSTN call just before a 183 is sent with SDP information to the far end. This is undesirable to Verizon and could result in no audio. The recommendation in **Section 6.8.1.1** is to leave the **Initial IP-IP Direct Media** field to “n”.

---

<sup>1</sup> The “T.38 Fax with Fallback to G.711 Pass-Through” feature requires G430 or G450 Media Gateways with release 33.13 or higher.

3. When TLS/SRTP is used within the enterprise, the SIP headers include the SIPS URI scheme for Secure SIP. The Avaya SBCE converts these header schemes from SIPS to SIP when it sends the SIP message toward Verizon. However, for call forward and EC500 calls, the Avaya SBCE was not changing the Diversion header scheme as expected. This caused these call types that require a Diversion header to fail since Verizon does not support Secure SIP. This anomaly is currently under investigation by the Avaya SBCE development team. A workaround is to include a SigMa script for the Verizon Server Configuration profile on the Avaya SBCE to convert “sips” to “sip” in the Diversion header. See **Section 7.3.3**.
4. Verizon Business IP Trunking service does not support an E.164 formatted number for the Calling Line Identification for outbound calls. An adaptation in Session Manager is used to convert the E.164 numbers Communication Manager used in the sample configuration for Calling Line Identification (e.g., From and P-Asserted Identity headers) into 10 digit numbers. See **Section 5.3.2**.
5. Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested; therefore, it is the customer’s responsibility to ensure proper operation with its equipment/software vendor.
6. Verizon Business IP Trunking service does not support G.711A codec for domestic service (EMEA only).
7. Verizon Business IP Trunking service does not support G.729B codec.

**Note** – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

## 2.3. History Info and Diversion Headers

The Verizon Business IP Trunking service does not support SIP History Info headers. Instead, the Verizon Business IP Trunking service requires that the SIP Diversion header be sent for redirected calls. The Communication Manager SIP trunk group form provides the options for specifying whether History Info headers or Diversion headers are sent.

If Communication Manager sends the History Info header, Session Manager can convert the History Info header into the Diversion header. This is performed by specifying the “*VerizonAdapter*” adaptation in Session Manager. See **Section 5.3.2**.

The Communication Manager Call Forwarding or Extension to Cellular (EC500) features may be used for the call scenarios testing the Diversion header.

## 2.4. SIP Header Removal

To support advanced SIP telephony features in the Avaya Aura® enterprise environment, certain proprietary headers may be included in the SIP message sent toward Verizon. These extra headers

can cause the SIP message to become larger than the specified Maximum Transmission Unit (MTU), and create fragmented UDP packets. These fragmented packets may not be re-assembled properly on the far-end by Verizon's equipment, for instance, when packets arrive out of order. To prevent fragmented packets, any unnecessary or proprietary headers should be removed from the SIP message before being sent to Verizon. Session Manager can remove these headers by specifying the "*eRHdrs*" parameter within the "*VerizonAdapter*" adaptation. See **Section 5.3.2**.

In the sample configuration, the following headers were removed:

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

To help reduce the packet size further, the Avaya SBCE can remove the "*gsid*" and "*epv*" parameters that may be included within the Contact header by applying a Sigma script to the Verizon server configuration. See **Section 7.3.3** and **7.3.5**.

## 2.5. Support

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

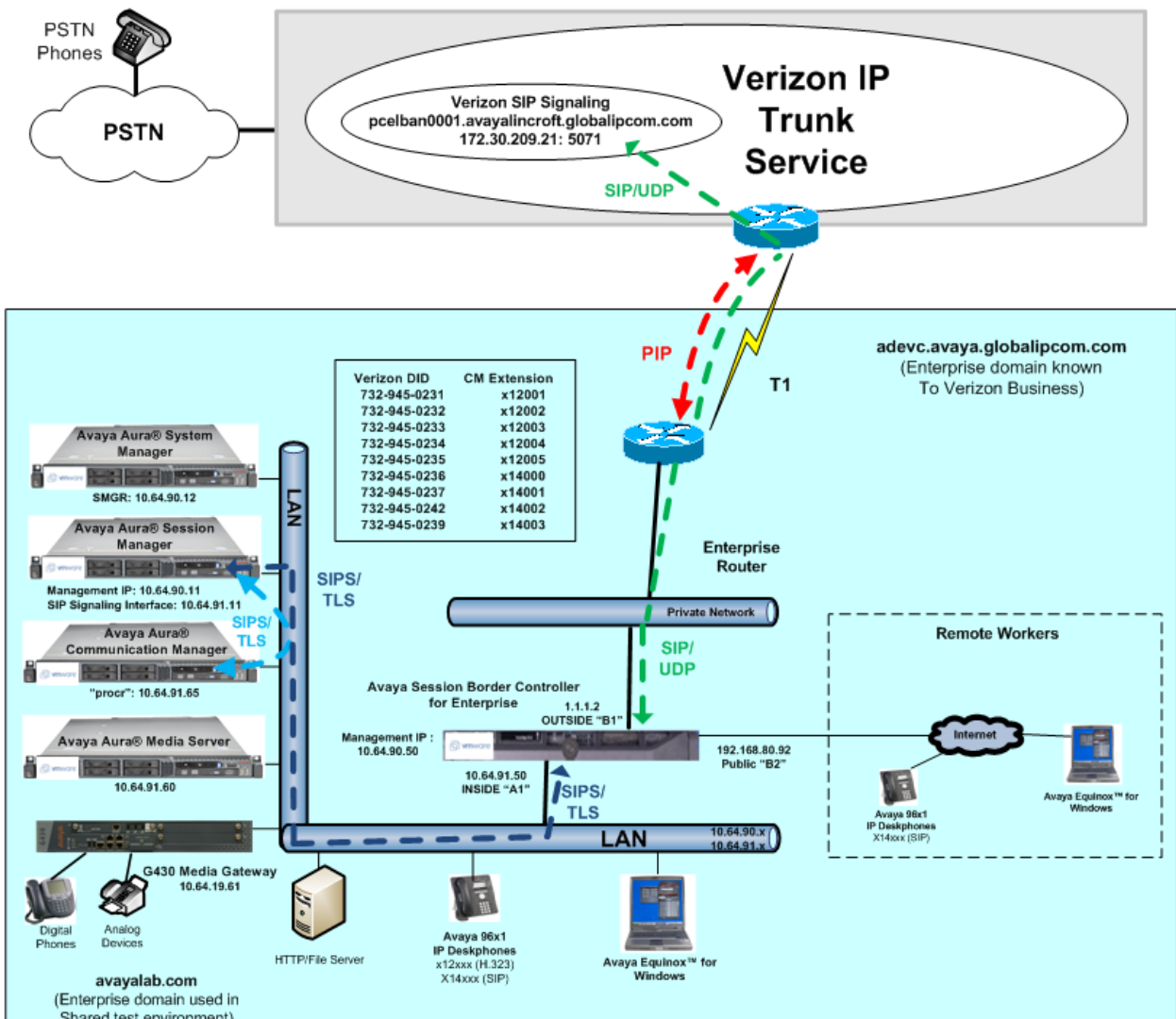
For technical support on Verizon Business IP Trunking service offer, visit online support at <http://www.verizonbusiness.com/us/customer/>



### 3. Reference Configuration

**Figure 1** illustrates the sample configuration used for the compliance testing. The Avaya CPE location simulates a customer site. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon service node.

The Avaya SBCE receives traffic from the Verizon Business IP Trunking service on port 5060 and sends traffic to the Verizon Business IP Trunking service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunking service). The Verizon Business IP Trunking service provided Direct Inward Dial (DID) 10 digit numbers. These DID numbers can be mapped by Session Manager or Communication Manager to Avaya telephone extensions.



**Figure 1: Avaya Interoperability Test Lab Configuration**

The Verizon Business IP Trunking service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunking service as FQDN *adevc.avaya.globalipcom.com*. Access to the Verizon Business IP Trunking service was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, the Avaya SBCE is used to adapt the “avayalab.com” domain to the domain known to Verizon (see **Section 7.6**). These Application Notes indicate a configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to the Verizon Business IP Trunking service.

**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 their own FQDNs and IP addressing as required.

In summary, the following components were used in the reference configuration.

- Verizon Business IP Trunking network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
  - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controllers for Enterprise
- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya G430 Media Gateway
- Avaya Media Server
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- Avaya Equinox™ for Windows
- Avaya Digital Phones
- Ventafax fax software

## 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
G430 Gateway	38.18.0
Avaya 96X1- Series Telephones (SIP)	R7.1.0.1.1
Avaya 96X1- Series Telephones (H.323)	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**

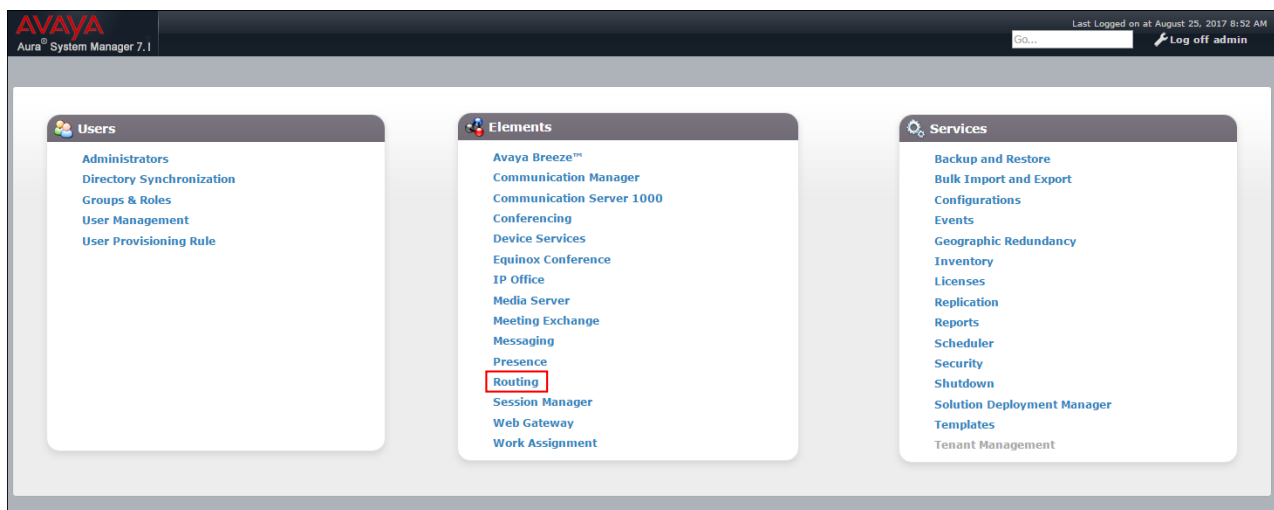
## 5. Configure Avaya Aura® Session Manager

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

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

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

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



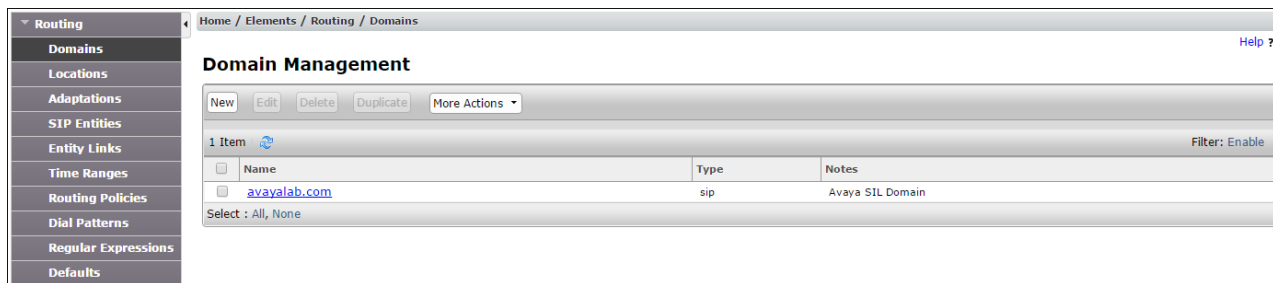
## 5.1. SIP Domain

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

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



The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table shows '1 Item' with columns 'Name', 'Type', and 'Notes'. The table contains one row with 'avayalab.com', 'sip', and 'Avaya SIL Domain'. Below the table is a 'Select : All, None' option.

Name	Type	Notes
avayalab.com	sip	Avaya SIL Domain

## 5.2. Locations

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

- **Main** – The customer site containing System Manager, Session Manager, 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 (not shown).

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

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

Home
Routing

Home / Elements / Routing / Locations

Help ?

Commit
Cancel

### Location Details

General

\* Name: Main

Notes: Avaya SIL

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

\* Minimum Multimedia Bandwidth: 64 Kbit/Sec

\* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

\* Latency before Overall Alarm Trigger: 5 Minutes

\* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add
Remove

0 Items
Filter: Enable

☐ IP Address Pattern

Notes

Commit
Cancel

## 5.2.2 Common Location

To configure the Avaya SBCE Location, repeat the steps in **Section 5.2.1** with the following changes (not shown):

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

## 5.3. Configure Adaptations

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

- Calls from Verizon (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager extensions.
  - The Verizon DNIS number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDN.
- Calls to Verizon (**Section 5.3.2**) - Modification of SIP messages sent by Communication Manager extensions.
  - The History-Info header is converted to a Diversion header automatically by the **VerizonAdapter**.
  - Avaya SIP headers not required by Verizon are removed (see **Section 2.4**).

### 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-TG1-VzIPT**).
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.

The screenshot shows the 'Adaptation Details' page in the Avaya Aura Session Manager Administration console. The left sidebar contains a navigation menu with 'Routing' selected, and 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The 'Adaptation Name' is 'CM-TG1-VzIPT', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is 'Name-Value Parameter'. Below this, there is a table with two rows of parameters:

Name	Value
fromto	true
osrcd	avayalab.com

Below the table, there is a 'Select' dropdown set to 'All, None'. At the bottom, there is a field for 'Egress URI Parameters' and a 'Notes' field containing 'CM - Vz - IPT'.

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

1. **Example 1 – destination extension:** 7329450232 is a DNIS string sent in the Request URI by the Verizon Business IP Trunking service that is associated with Communication Manager extension 12002.

- Enter **7329450232** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.
- Enter **12002** 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.

**Note – In the reference configuration, the Verizon Business IP Trunking service delivered 10-digit DNIS numbers.**

Digit Conversion for Outgoing Calls from SM

Add Remove

13 Items Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 7329450232	* 10	* 10		* 10	12002	destination ▼		
<input type="checkbox"/>	* 7329450233	* 10	* 10		* 10	12003	destination ▼		
<input type="checkbox"/>	* 7329450234	* 10	* 10		* 10	12004	destination ▼		
<input type="checkbox"/>	* 7329450235	* 10	* 10		* 10	12005	destination ▼		
<input type="checkbox"/>	* 7329450236	* 10	* 10		* 10	14000	destination ▼		
<input type="checkbox"/>	* 7329450237	* 10	* 10		* 10	14001	destination ▼		
<input type="checkbox"/>	* 7329450238	* 10	* 10		* 10	14008	destination ▼		
<input type="checkbox"/>	* 7329450239	* 10	* 10		* 10	14005	destination ▼		
<input type="checkbox"/>	* 7329450240	* 10	* 10		* 10	14006	destination ▼		
<input type="checkbox"/>	* 7329450241	* 10	* 10		* 10	12000	destination ▼		
<input type="checkbox"/>	* 7329450242	* 10	* 10		* 10	14002	destination ▼		
<input type="checkbox"/>	* 7329450243	* 10	* 10		* 10	10003	destination ▼		
<input type="checkbox"/>	* 7329450244	* 10	* 10		* 10	10005	destination ▼		

Select : All, None



### 5.3.2 Adaptation for the Verizon Business IP Trunking service

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. The VerizonAdapter will automatically remove History-Info headers, (which the Verizon Business IP Trunking service does not support), sent by Communication Manager (see **Section 6.8.1**) and replace them with Diversion headers.

**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”**

Home / Elements / Routing / Adaptations

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

**General**

\* **Adaptation Name:** SBC1-Adaptation for Verizon

\* **Module Name:** VerizonAdapter

**Module Parameter Type:** Name-Value Parameter

Name	Value
<input type="checkbox"/> eRHdrs	"AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, AV-Correlation-ID, Av-Secure-Indication"
<input type="checkbox"/> fromto	true

Select : All, None

**Egress URI Parameters:**

**Notes:** SBC - Verizon IPT

**Step 3** - Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *outbound* digits to Verizon that need to be converted to 10 digit numbers).

1. As described in **Section 2.2, Item 4**, the E.164 formatted numbers sent by Communication Manager's public-unknown numbering table (**Section 6.9**), needs to be converted to 10 digit numbers expected by Verizon.
  - Enter + in the **Matching Pattern** column.
  - Enter **12** in the **Min/Max** columns.
  - Enter **2** in the **Delete Digits** column.
  - Specify that this should be applied to the SIP **origination** headers in the **Address to modify** column.
  - Enter any desired notes

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* +	* 12	* 36		* 2		origination		E.164 to 10 digit Calling Party Number
<input type="checkbox"/>	* +13035559999	* 12	* 12		* 2		origination	7329450821	Unscreened ANI - Diversion header

Select : All, None

Commit Cancel

**Note** – The Screened Telephone Number (STN) provided by Verizon for this test is 7329450821. Typically, customers would have one or more STN; one for every location. A central Session Manager could be used to pass multiple STNs to Verizon based on a **Matching Pattern** (i.e., a user's Calling Line Identification). The STN would then be entered in the **Adaptation Data** field as shown above.

## 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 5081), is for calls to/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 to/from the Verizon Business IP Trunking service via the Avaya SBCE.
- Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Messaging.

**Note** – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5081), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the Verizon Business IP Trunking service uses UDP/5071 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.

The screenshot displays the 'SIP Entity Details' configuration page for a Session Manager. The left-hand navigation pane is expanded to 'Routing', which includes sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'Commit' button. It is divided into two tabs: 'General' and 'Monitoring'. The 'General' tab is active, showing fields for 'Name' (SessionManager), 'FQDN or IP Address' (10.64.91.11), 'Type' (Session Manager), 'Notes' (Session Manager), 'Location' (Main), 'Outbound Proxy' (blank), 'Time Zone' (America/Denver), 'Minimum TLS Version' (Use Global Setting), and 'Credential name' (blank). The 'Monitoring' tab is also visible, showing 'SIP Link Monitoring' and 'CRLF Keep Alive Monitoring', both set to 'Use Session Manager Configuration'.

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

**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**.

The screenshot shows the 'Listen Ports' configuration interface. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '3 Items' with a refresh icon and a 'Filter: Enable' link. The main part of the interface is a table with the following columns: 'Listen Ports', 'Protocol', 'Default Domain', 'Endpoint', and 'Notes'. There are three rows of data:

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

At the bottom left of the table, there is a 'Select : All, None' option.

**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-TG1**).
- **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-TG1-VzIPT** administered in **Section 5.3.1**.
- **Location** – Select a Location **Main** administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.

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

The screenshot shows the 'SIP Entity Details' page in the Avaya Aura Communication Manager web interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'Commit' button and a 'Cancel' button. The 'General' section is active, showing the following fields: Name (CM-TG1), FQDN or IP Address (10.64.91.65), Type (CM), Notes (Trunk Group 1 - CM to Vz-IPT), Adaptation (CM-TG1-VzIPT), Location (Main), Time Zone (America/Denver), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name (empty), Securable (checkbox), Call Detail Recording (none), Loop Detection Mode (Off), SIP Link Monitoring (Use Session Manager Configuration), CRLF Keep Alive Monitoring (Use Session Manager Configuration), Supports Call Admission Control (checkbox), Shared Bandwidth Manager (checkbox), Primary Session Manager Bandwidth Association (empty), and Backup Session Manager Bandwidth Association (empty). The 'Loop Detection' and 'Monitoring' sections are also visible.

### 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 TG1**).
- **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 **5081**.

- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **CM-TG1**).
- **SIP Entity 2 Port** – Enter **5081** (see **Section 6.8.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

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

The screenshot shows the 'Entity Links' configuration page in the Avaya Aura Configuration Manager. The left sidebar contains a navigation menu with 'Entity Links' selected. The main area displays a table with one item, 'SM to CM TG1', which links 'SessionManager' (SIP Entity 1) to 'CM-TG1' (SIP Entity 2) using the 'TLS' protocol on port '5081'. The 'Connection Policy' is set to 'trusted'. Buttons for 'Commit' and 'Cancel' are visible at the top right of the configuration area.

## 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 IP Trunking service via the Avaya SBCE

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

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **SM to 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**.

**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** (not shown). Repeat these steps to provision additional time ranges as required.

The screenshot shows the 'Time Ranges' configuration page. The left sidebar has 'Time Ranges' selected under the 'Routing' section. The main area shows a table with one item, '24/7', which is active for all days of the week (Mo, Tu, We, Th, Fr, Sa, Su) from 00:00 to 23:59. The table has columns for Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The 'Notes' column contains 'Time Range 24/7'. There are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions' at the top. A 'Filter: Enable' link is on the right.

## 5.7. Routing Policies

In this section, the following Routing Policies are administered:

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

### 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.

The screenshot shows the 'Routing Policy Details' page. The left sidebar has 'Routing Policies' selected under the 'Routing' section. The main area has two sections: 'General' and 'SIP Entity as Destination'. In the 'General' section, the 'Name' field is 'To CM TG1', the 'Disabled' checkbox is unchecked, and the 'Retries' field is '0'. The 'Notes' field contains 'Trunk Group 1 PSTN1 to CM'. In the 'SIP Entity as Destination' section, there is a 'Select' button. There are 'Commit' and 'Cancel' buttons at the top right of the 'General' section.



**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-TG1**), and click on **Select**.

**SIP Entities**

15 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
Aura Messaging	10.64.91.54	Messaging	Aura Messaging
Breeze	10.64.91.17	Avaya Breeze	
<b>CM-TG1</b>	10.64.91.65	CM	Trunk Group 1 - CM to Vz-IPT
CM-TG2	10.64.91.65	CM	Trunk Group 2 - Vz-Toll-Free inbound
CM-TG3	10.64.91.65	CM	Trunk Group 3 - CM to Enterprise
CM-TG4	10.64.91.65	CM	Trunk Group 4 - ATT IPTF
CM-TG5	10.64.91.65	CM	Trunk Group 5 - ATT IPFR
CS1000	10.80.140.103	Other	CS1000 7.65
IP500	10.64.19.70	Other	IP Office
Presence	10.64.91.17	Presence Services	
SBC1	10.64.91.50	SIP Trunk	Avaya SBC-1 to PSTN
SBC2	10.64.91.100	SIP Trunk	Avaya SBC-2 to PSTN
SBCE-ipv6	10.64.91.40	SIP Trunk	SBCE for IPv6 testing
SBCE-ipv6-Toll Free	10.64.91.41	SIP Trunk	SBCE for IPv6 testing
SessionManager	10.64.91.11	Session Manager	Session Manager

Select : None

Select Cancel

**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.

Home Routing

Home / Elements / Routing / Routing Policies

**Routing Policy Details** Commit Cancel Help ?

**General**

\* Name: To CM TG1

Disabled: ☐

\* Retries: 0

Notes: Trunk Group 1 PSTN1 to CM

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM-TG1	10.64.91.65	CM	Trunk Group 1 - CM to Vz-IPT

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

**Dial Patterns**

Add Remove

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

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

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

## 5.7.3 Routing Policy for Outbound Calls to Verizon

This Routing Policy is used for outbound calls to Verizon. Repeat the steps in **Section 5.7.1** with the following differences:

- Enter a descriptive **Name** for routing calls to the Verizon Business IP Trunking service via the Avaya SBCE (e.g., **To SBC1**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE SIP Entity (e.g., **SBC1**).

## 5.8. Dial Patterns

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

- Inbound PSTN calls via the Verizon Business IP Trunking service to Communication Manager (**Section 5.8.1**).
- Outbound calls to Verizon/PSTN (**Section 5.8.2**).

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

In the reference configuration inbound calls from the Verizon Business IP Trunking service 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 **7329450232**. Note – The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 732-945-02xx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

The screenshot shows the 'Dial Pattern Details' page in the Avaya Aura® configuration interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (selected), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and has a 'General' tab selected. It includes a 'Commit/Cancel' button and a 'Help ?' link. The form fields are as follows: 'Pattern' is set to '7329450232'; 'Min' and 'Max' are both set to '10'; 'Emergency Call' is an unchecked checkbox; 'Emergency Priority' is set to '1'; 'Emergency Type' is an empty dropdown menu; 'SIP Domain' is set to 'avayalab.com' (indicated by a dropdown arrow); and 'Notes' contains the text 'Verizon DID number'.

**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 TG1**), and click on **Select**.

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

4 Items [Filter: Enable](#)

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	CM-TG-5	CM-TG-5
<input checked="" type="checkbox"/>	Common	SBC to PSTN
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1

Select : All, None

---

**Routing Policies**

12 Items [Filter: Enable](#)

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AAM	<input type="checkbox"/>	Aura Messaging	
<input checked="" type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Trunk Group 1 PSTN1 to CM
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 PSTN2 to CM
<input type="checkbox"/>	To CM TG3	<input type="checkbox"/>	CM-TG3	Enterprise Traffic
<input type="checkbox"/>	To CM TG4	<input type="checkbox"/>	CM-TG4	Trunk Group 4 PSTN4 to CM
<input type="checkbox"/>	To CM-TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 PSTN5 to CM
<input type="checkbox"/>	To CS1000	<input type="checkbox"/>	CS1000	
<input type="checkbox"/>	To IPS00	<input type="checkbox"/>	IPS00	
<input type="checkbox"/>	To SBC1	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	To SBC2	<input type="checkbox"/>	SBC2	
<input type="checkbox"/>	To SBCE-IPv6	<input type="checkbox"/>	SBCE-ipv6	
<input type="checkbox"/>	to SBCE-IPv6 TollFree	<input type="checkbox"/>	SBCE-ipv6-Toll Free	

Select : All, None

Select Cancel

**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.

Routing | Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** [Commit](#) [Cancel](#) [Help ?](#)

**General**

\* **Pattern:** 7329450232

\* **Min:** 10

\* **Max:** 10

**Emergency Call:** ☐

**Emergency Priority:** 1

**Emergency Type:**

**SIP Domain:** avayalab.com

**Notes:** Verizon DID number

**Originating Locations and Routing Policies**

[Add](#) [Remove](#)

1 Item [Filter: Enable](#)

<input checked="" type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input checked="" type="checkbox"/>	Common	SBC to PSTN	To CM TG1	0	<input type="checkbox"/>	CM-TG1	Trunk Group 1 PSTN1 to CM

Select : All, None

## 5.8.2 Matching Outbound Calls to Verizon/PSTN

In this section, Dial Patterns are administered for all outbound calls to Verizon/PSTN. In the reference configuration E.164 numbers were used for national and international calls. Non-E.164 numbers were used for service numbers, e.g., x11, 1411, 5551212, etc.

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

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to Verizon/PSTN (e.g., +). This will match any outbound call prefixed with a plus sign (+), such as an E.164 formatted number.
- Enter a **Min** pattern of **10**.
- Enter a **Max** pattern of **36**.
- In the **Routing Policies** section of the **Originating Locations and Routing Policies** page, check the checkboxes corresponding to the Communication Manager Originating Location (e.g., **Main**) and the Routing Policy administered for routing calls to Verizon in **Section 5.7.3** (e.g., **To SBC1**).

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern: +

\* Min: 10

\* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes: E.164 Public Numbers

**Originating Locations and Routing Policies**

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main	Avaya SIL	To SBC1	0	<input type="checkbox"/>	SBC1	

**Step 2** - Repeat **Step 1** to add any additional outbound patterns as required.

**Routing** Home / Elements / Routing / Dial Patterns Help ?

**Dial Patterns**

New Edit Delete Duplicate More Actions

4 Items Found Filter: Disable, Apply, Clear

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	+	10	36	<input type="checkbox"/>			avayalab.com	outbound
<input type="checkbox"/>	1411	4	4	<input type="checkbox"/>			avayalab.com	Outbound E.164 Public Numbers
<input type="checkbox"/>	5551212	7	7	<input type="checkbox"/>			avayalab.com	Outbound PSTN Information
<input type="checkbox"/>	x11	3	3	<input type="checkbox"/>			avayalab.com	Outbound Directory Service

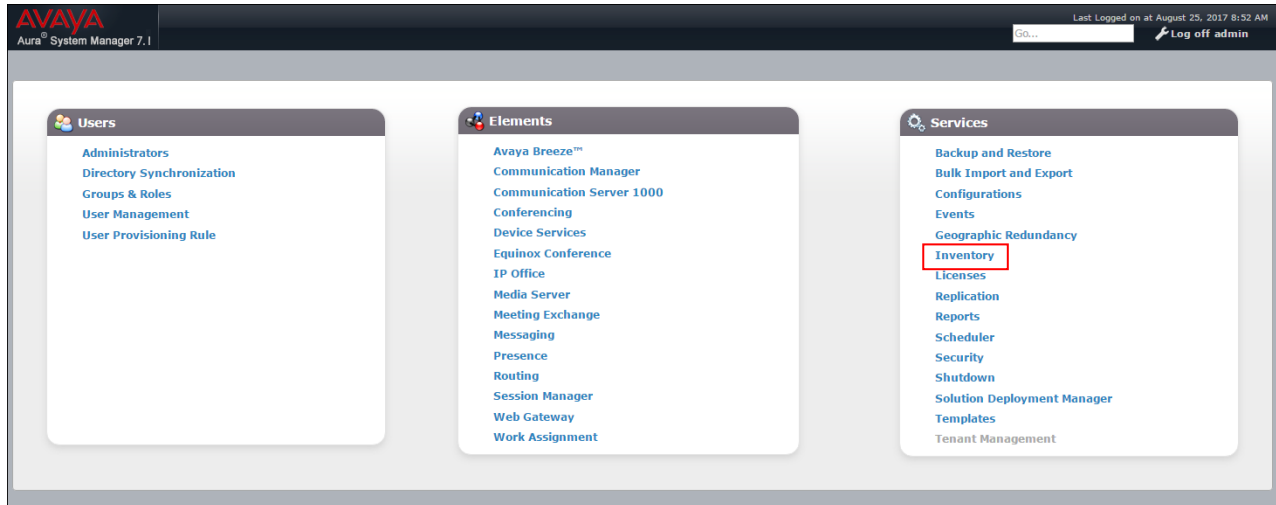
Select : All, None

## 5.9. Verify TLS Certificates – Session Manager

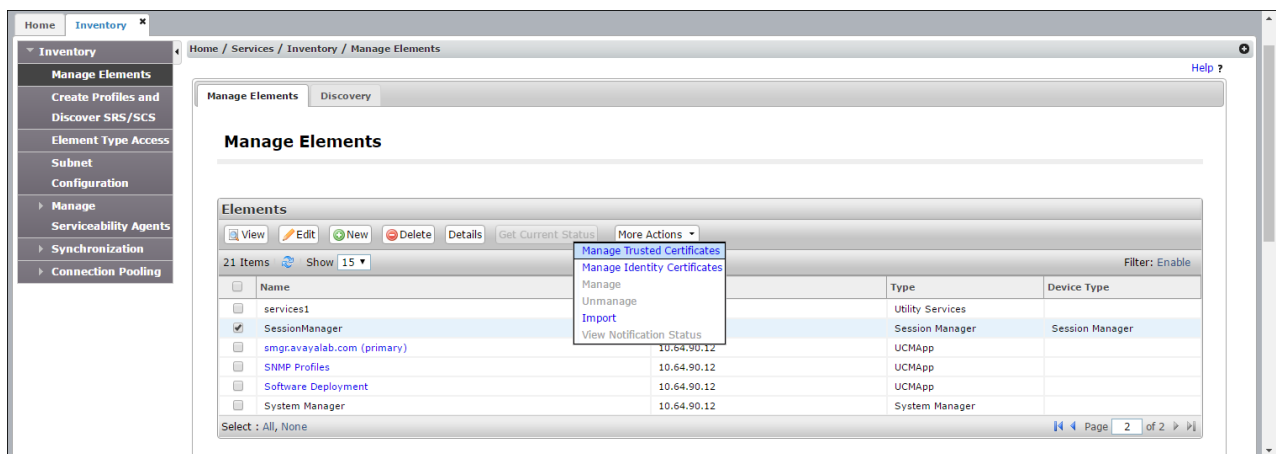
**Note** – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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.

**Manage Trusted Certificates**

View Add Export Remove

14 Items Filter: Enable

	Store Description	Store Type	Subject Name
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
<input checked="" type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>		POSTGRES	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
<input type="checkbox"/>		POSTGRES	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	WEBSPPHERE	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	WEBSPPHERE	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US
<input checked="" type="checkbox"/>	Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/>	Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=GSSCP SMGR CA
<input type="checkbox"/>	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).

**Inventory** Home / Services / Inventory / Manage Elements

Manage Elements Discovery

Replace Export Renew

5 Items Filter: Enable

	Service Name	Common Name	Valid To	Expired	Service Description
<input type="radio"/>	Management	mgmt	Sat Sep 19 13:02:00 MDT 2020	No	Management Services
<input checked="" type="radio"/>	Security Module SIP	securitymodule_sip	Sat Sep 19 13:37:39 MDT 2020	No	Security Module SIP Service
<input type="radio"/>	SPIRIT	spiritalias	Sat Sep 19 13:02:02 MDT 2020	No	SPIRIT Service
<input type="radio"/>	Postgres	postgres	Sat Sep 19 13:02:07 MDT 2020	No	Postgres Service
<input type="radio"/>	Security Module HTTPS	securitymodule_https	Sat Sep 19 13:38:10 MDT 2020	No	Security Module HTTPS Service

Select : None

**Certificate Details**

**Subject Details** C=US, O=Avaya, CN=sm-sm100.avayalab.com

**Valid From** Wed Jun 21 13:37:39 MDT 2017 **Valid To** Sat Sep 19 13:37:39 MDT 2020

**Key Size** 2048

**Issuer Name** O=AVAYA, OU=MGMT, CN=System Manager CA

**Certificate Fingerprint** c7ba3473cb584b72efe1f6001a2333fc27dd6e8d

**Subject Alternative Name** dNSName=sm-sm100.avayalab.com, iPAddress=10.64.

**Serial Number** 3CCC7C2ECF94410

**Basic Constraints** End Entity Certificate

## 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.

### 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	
<b>Maximum Administered SIP Trunks: 4000</b>		<b>60</b>	
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	
<b>ARS? y</b>	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? y		

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

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



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

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

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

### 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 String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call 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
                                                           Gatekeeper Priority: 5

Network Region: 1

                                                           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          20
3: G.729A             n          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			
	Mode	Redun- dancy	Packet Size(ms)
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>	<b>ECM: y</b>
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20
Media Connection IP Address Type Preferences			
1: IPv4			
2:			

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

This IP codec set will be used for Verizon Business IP Trunking calls. Repeat the steps in **Section 5.5.1** 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**. See **Section 2.2** for limitations regarding fax.

change ip-codec-set 2

Page 1 of 2

IP CODEC SET

Codec Set: 2

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

Media Encryption

Encrypted SRTP: enforce-unenc-srtpc

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

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

Media Connection IP Address Type Preferences

1: IPv4

## 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 G430 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		
<b>Region: 1</b>		
Location: 1	<b>Authoritative Domain: avayalab.com</b>	
Name: <b>Enterprise</b>	Stub Network Region: n	
<b>MEDIA PARAMETERS</b>		
Codec Set: 1	<b>Intra-region IP-IP Direct Audio: yes</b>	
UDP Port Min: 2048	<b>Inter-region IP-IP Direct Audio: yes</b>	
UDP Port Max: 3329	IP Audio Hairpinning? n	
<b>DIFFSERV/TOS PARAMETERS</b>		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
<b>802.1P/Q PARAMETERS</b>		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	<b>AUDIO RESOURCE RESERVATION PARAMETERS</b>	
RSVP Enabled? n		
<b>H.323 IP ENDPOINTS</b>		
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		
<b>RTCP Reporting to Monitor Server Enabled? y</b>		
<b>RTCP MONITOR SERVER PARAMETERS</b>		
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 rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions			Dyn CAC	A R	G L	c e	
1	1									all		
2	2	y	NoLimit						n		t	

## 6.7.2 IP Network Region 2 – 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 rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr Regions			Dyn CAC	A R	G L	c 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/outbound Verizon access – SIP Trunk 1
  - Note that this trunk will use TLS port 5081 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 IP Trunk service. See the note in **Section 5.4** regarding the use of TLS transport protocols in the CPE.

## 6.8.1 SIP Trunk for Inbound/Outbound 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-TG1** SIP Entity defined in **Section 5.4.2**.

### 6.8.1.1 Signaling Group 1

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., 1), 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 **5081**.
- **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).
- **Initial IP-IP Direct Media** is set to **n**. See **Section 2.2** for details.
- **H.323 Station Outgoing Direct Media** is set to **n**.

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

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	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: 5081	Far-end Listen Port: 5081	
	Far-end Network Region: 2	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	



### 6.8.1.2 Trunk Group 1

**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 IPT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **\*01**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 6.8.1.1** (e.g., **1**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

<b>add trunk-group 1</b>		<b>Page 1 of 21</b>	
TRUNK GROUP			
Group Number: 1	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: Verizon IPT</b>	COR: 1	TN: 1	<b>TAC: *01</b>
<b>Direction: two-way</b>	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
<b>Service Type: public-ntwrk</b>	Auth Code? n		
	Member Assignment Method: auto		
	<b>Signaling Group: 1</b>		
	<b>Number of Members: 10</b>		

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

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

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

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

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

<b>add trunk-group 1</b>	<b>Page 3 of 21</b>
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: public</b>
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

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

- Verify **Network Call Redirection** is set to **y**.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by Verizon (e.g., **101**).

**Note** – The Verizon Business IP Trunking service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, the History Info header is automatically removed from SIP signaling by Session Manager, as part of the *VerizonAdapter* (see **Section 5.3.2**). Alternatively, History Info may be disabled here with the Diversion Header enabled.

<b>add trunk-group 1</b>	<b>Page 4 of 21</b>
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	Send Transferring Party Information? n
	<b>Network Call Redirection? y</b>
Build Refer-To URI of REFER From Contact For NCR? n	
	Send Diversion Header? n
	Support Request History? y
	<b>Telephone Event Payload Type: 101</b>
	Shuffling with SDP? n
	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**).
- **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. 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 IP Trunking service via the public trunk.

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

**Step 2** - Add each Communication Manager station extension and their corresponding 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., **12002**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **1**).
- **Private Prefix** – Enter the corresponding Verizon DNIS number (e.g., **17329450232**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **11**).

change public-unknown-numbering 5 ext-digits 12002					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	12002	1	17329450232	11	Total Administered: 32
5	14006	1	17329450236	11	Maximum Entries: 240
5	14007	1	17329450237	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	14008	1	17329450238	11	
					Communication Manager automatically inserts a '+' digit in this case.

## 6.10. Private Numbering

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

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

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

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

## 6.11. Route Patterns

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

### 6.11.1 Route Pattern for National Calls to Verizon

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

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

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

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

### 6.11.2 Route Pattern for International Calls to Verizon

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

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

- In the **Grp No** column, enter **1** for public trunk 1, and the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, leave blank (default).
- In the **No. Del Digits** column, enter **3** to have Communication Manager remove the international 011 prefix from the number.
- In the **Inserted Digits** column, enter **p** to have Communication Manager insert a plus sign (+) in front of the number dialed to convert it to an E.164 formatted number.

change route-pattern 2															Page 1 of 3			
Pattern Number: 2															Pattern Name: 011 to E.164			
SCCAN? n															Secure SIP? n		Used for SIP stations? n	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted				DCS/		IXC					
No			Mrk	Lmt	List	Del	Digits				QSIG							
							Dgts				Intw							
1:	1	0					3		p			n	user					
2:												n	user					
3:												n	user					
BCC		VALUE	TSC	CA-TSC	ITC		BCIE	Service/Feature		PARM	Sub	Numbering		LAR				
0		1	2	M	4	W	Request				Dgts	Format						
1:	y	y	y	y	y	n	n	rest						none				

### 6.11.3 Route Pattern for Service Calls to Verizon

Repeat the steps in **Section 6.11.1** to add a route pattern for x11 and other service numbers that do not require a leading plus sign:

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

- In the **Grp No** column, enter **1** for public trunk 1, and the **FRL** column enter **0** (zero).
- In the **Pfx mrk** column, leave blank (default).
- In the **Inserted Digits** column, leave blank (default).

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

### 6.11.4 Route Pattern for Calls within the CPE

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

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

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

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

## 6.12. Automatic Route Selection (ARS) Dialing

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

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

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

**Step 2** - Repeat **Step 1** for all other outbound call strings.

change ars analysis 1720										Page 1 of 2
ARS DIGIT ANALYSIS TABLE										
Location: all										Percent Full: 1
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd			
	1720	11	11	1	fnpa		n			
	18	11	11	1	fnpa		n			
	19	11	11	1	fnpa		n			
	1900	11	11	deny	fnpa		n			
	1900555	11	11	deny	fnpa		n			
	1xxx976	11	11	deny	fnpa		n			
	311	3	3	4	svcl		n			
	011	10	18	2	intl		n			
	411	3	3	4	svcl		n			
	5	10	10	1	fnpa		n			
	511	3	3	4	svcl		n			
	555	7	7	deny	hnpa		n			
	5551212	7	7	1	svcl		n			

## 6.13. Automatic Alternate Routing (AAR) Dialing

AAR is used for outbound calls within the CPE.

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

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

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

change aar analysis 0							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 1		
	Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Reqd
14		5	5	3	lev0		n

## 6.14. Avaya G430 Media Gateway Provisioning

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

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

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

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

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

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

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

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

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

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



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

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

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

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

Mutual Authentication? optional
```

## 6.15. Avaya Aura® Media Server Provisioning

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

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

**Step 1** - Access the Media Server Element Manager web interface by typing

“**https://x.x.x.x:8443**” (where x.x.x.x is the IP address of the Media Server) (not shown).

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

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**
- Verify that **Peer Detection Enabled?** – Set to **n**.
- **Peer Server** to **AMS**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.4**.
- **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 6.4** (e.g., **AMS**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**.
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 6.6.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

```

add signaling-group 60                                     Page 1 of 2
                                     SIGNALING GROUP

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

Peer Detection Enabled? n Peer Server: AMS

Near-end Node Name: procr           Far-end Node Name: AMS
Near-end Listen Port: 5060         Far-end Listen Port: 5060
                                   Far-end Network Region: 1

Far-end Domain: 10.64.91.60

```

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

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

```

add media-server 1                                     Page 1 of 1
                                     MEDIA SERVER

Media Server ID: 1

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

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

```

## 6.16. Save Translations

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

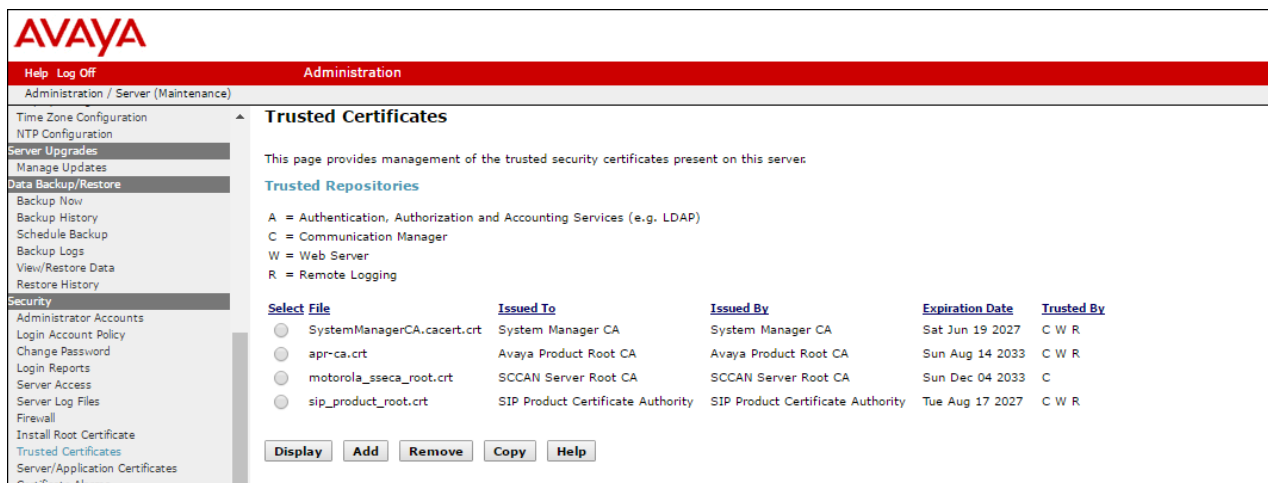
## 6.17. Verify TLS Certificates – Communication Manager

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

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

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

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



**AVAYA**

Help Log Off Administration

Administration / Server (Maintenance)

**Trusted Certificates**

This page provides management of the trusted security certificates present on this server:

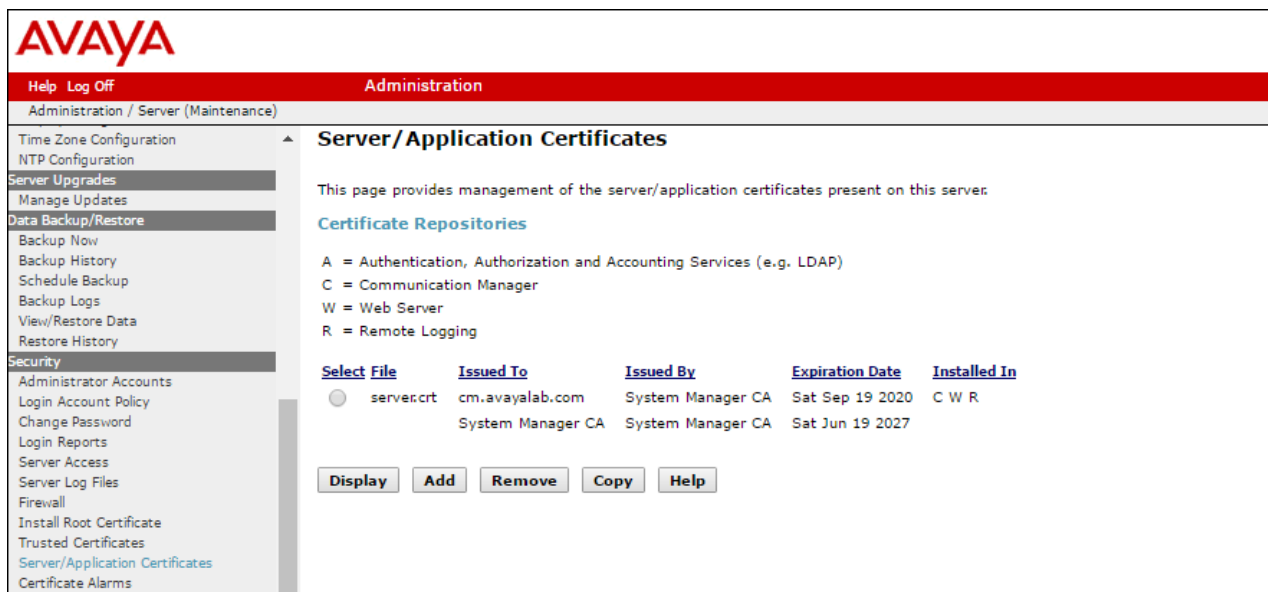
**Trusted Repositories**

A = Authentication, Authorization and Accounting Services (e.g. LDAP)  
C = Communication Manager  
W = Web Server  
R = Remote Logging

Select File	Issued To	Issued By	Expiration Date	Trusted By
<input type="radio"/> SystemManagerCA.cacert.crt	System Manager CA	System Manager CA	Sat Jun 19 2027	C W R
<input type="radio"/> apr-ca.crt	Avaya Product Root CA	Avaya Product Root CA	Sun Aug 14 2033	C W R
<input type="radio"/> motorola_sseca_root.crt	SCCAN Server Root CA	SCCAN Server Root CA	Sun Dec 04 2033	C
<input type="radio"/> sip_product_root.crt	SIP Product Certificate Authority	SIP Product Certificate Authority	Tue Aug 17 2027	C W R

Display Add Remove Copy Help

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



**AVAYA**

Help Log Off Administration

Administration / Server (Maintenance)

**Server/Application Certificates**

This page provides management of the server/application certificates present on this server:

**Certificate Repositories**

A = Authentication, Authorization and Accounting Services (e.g. LDAP)  
C = Communication Manager  
W = Web Server  
R = Remote Logging

Select File	Issued To	Issued By	Expiration Date	Installed In
<input type="radio"/> server.crt	cm.avayalab.com	System Manager CA	Sat Sep 19 2020	C W R
	System Manager CA	System Manager CA	Sat Jun 19 2027	

Display Add Remove Copy Help

## 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.

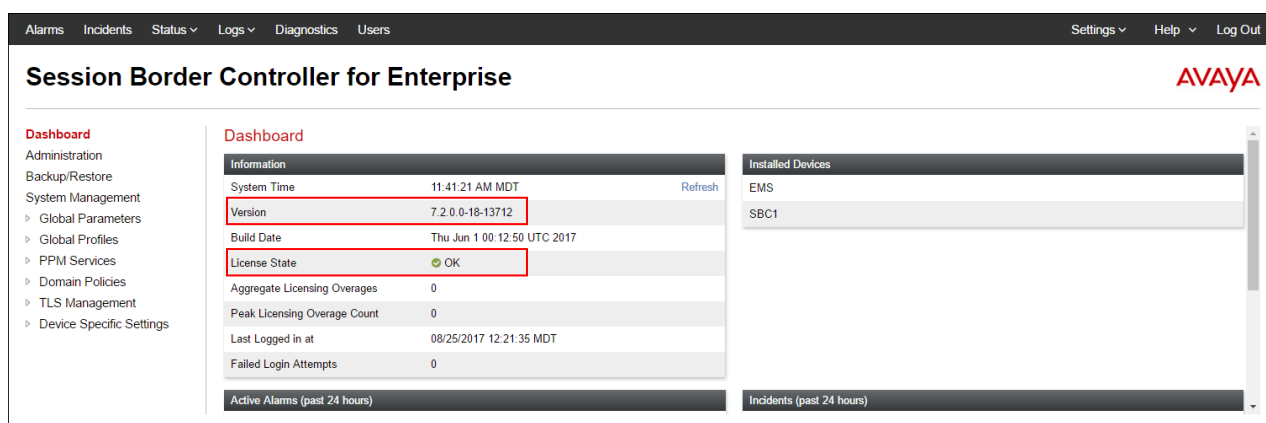
In the sample configuration, the management IP is 10.64.90.50. Access the web management interface by entering `https://<ip-address>` where `<ip-address>` is the management IP address assigned during installation. Log in with the appropriate credentials. Click **Log In**.



The login page features the Avaya logo and the text "Session Border Controller for Enterprise". It includes a "Log In" section with fields for "Username:" (containing "ucsec") and "Password:", followed by a "Log In" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, a disclaimer about unauthorized access, a statement about system monitoring, and a copyright notice for 2011-2017 Avaya Inc.

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.



The dashboard displays system information, installed devices, and active alarms/incidents. The "Information" section includes a table with the following data:

Information	
System Time	11:41:21 AM MDT
Version	7.2.0.0-18-13712
Build Date	Thu Jun 1 00:12:50 UTC 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/25/2017 12:21:35 MDT
Failed Login Attempts	0

The "Installed Devices" section lists the following devices:

Installed Devices
EMS
SBC1

The dashboard also includes sections for "Active Alarms (past 24 hours)" and "Incidents (past 24 hours)".

## 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.

**Session Border Controller for Enterprise**

System Management

Devices Updates SSL VPN Licensing Key Bundles

Device Name	Management IP	Version	Status	
SBC1	10.64.90.50	7.2.0.0-18-13712	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

**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

**System Information: SBC1**

**General Configuration**

Appliance Name: SBC1  
Box Type: SIP  
Deployment Mode: Proxy

**Device Configuration**

HA Mode: No  
Two Bypass Mode: No

**License Allocation**

Standard Sessions Requested: 50  
Advanced Sessions Requested: 50  
Scopia Video Sessions Requested: 50  
CES Sessions Requested: 50  
Transcoding Sessions Requested: 50  
Encryption: ☒

**Network Configuration**

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
1.1.1.2	1.1.1.2	255.255.255.0	1.1.1.1	B1
10.64.91.48	10.64.91.48	255.255.255.0	10.64.91.1	A1
10.64.91.49	10.64.91.49	255.255.255.0	10.64.91.1	A1
10.64.91.50	10.64.91.50	255.255.255.0	10.64.91.1	A1
192.168.80.44	192.168.80.44	255.255.255.128	192.168.80.1	B2
192.168.80.92	192.168.80.92	255.255.255.128	192.168.80.1	B2

**DNS Configuration**

Primary DNS: 10.64.19.201  
Secondary DNS:  
DNS Location: DMZ  
DNS Client IP: 1.1.1.2

**Management IP(s)**

IP #1 (IPv4): 10.64.90.50

## 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.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management (selected), Certificates (selected), Client Profiles, Server Profiles, and Device Specific Settings. The main content area is titled 'Certificates' and features an 'Install' button and a 'Generate CSR' button. The interface is divided into three sections: 'Installed Certificates' showing four certificates (sbc50-inside.crt, sbc50-outside.crt, sbce92-out.crt, sbce92-outside.crt) with 'View' and 'Delete' links; 'Installed CA Certificates' showing one certificate (SystemManagerCA.pem) with 'View' and 'Delete' links; and 'Installed Certificate Revocation Lists' showing a message that no lists have been installed. Below these is the 'Installed Keys' section, which lists five keys (avayalab.com.key, sbc50-inside.key, sbc50-outside.key, sbce92-out.key, sbce92-outside.key) with 'Delete' links.

Installed Certificates	
sbc50-inside.crt	<a href="#">View</a> <a href="#">Delete</a>
sbc50-outside.crt	<a href="#">View</a> <a href="#">Delete</a>
sbce92-out.crt	<a href="#">View</a> <a href="#">Delete</a>
sbce92-outside.crt	<a href="#">View</a> <a href="#">Delete</a>

Installed CA Certificates	
SystemManagerCA.pem	<a href="#">View</a> <a href="#">Delete</a>

No certificate revocation lists have been installed.

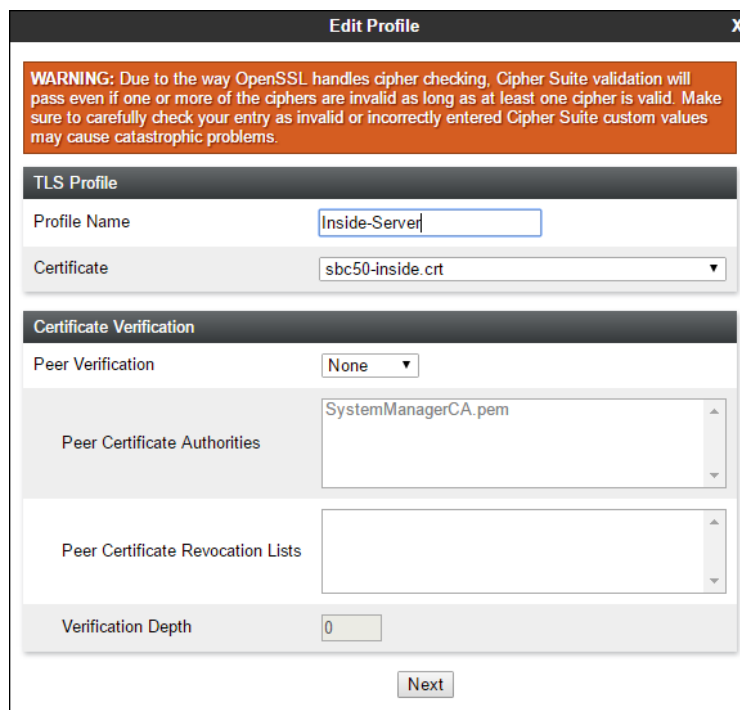
Installed Keys	
avayalab.com.key	<a href="#">Delete</a>
sbc50-inside.key	<a href="#">Delete</a>
sbc50-outside.key	<a href="#">Delete</a>
sbce92-out.key	<a href="#">Delete</a>
sbce92-outside.key	<a href="#">Delete</a>

## 7.2.2 Server Profiles

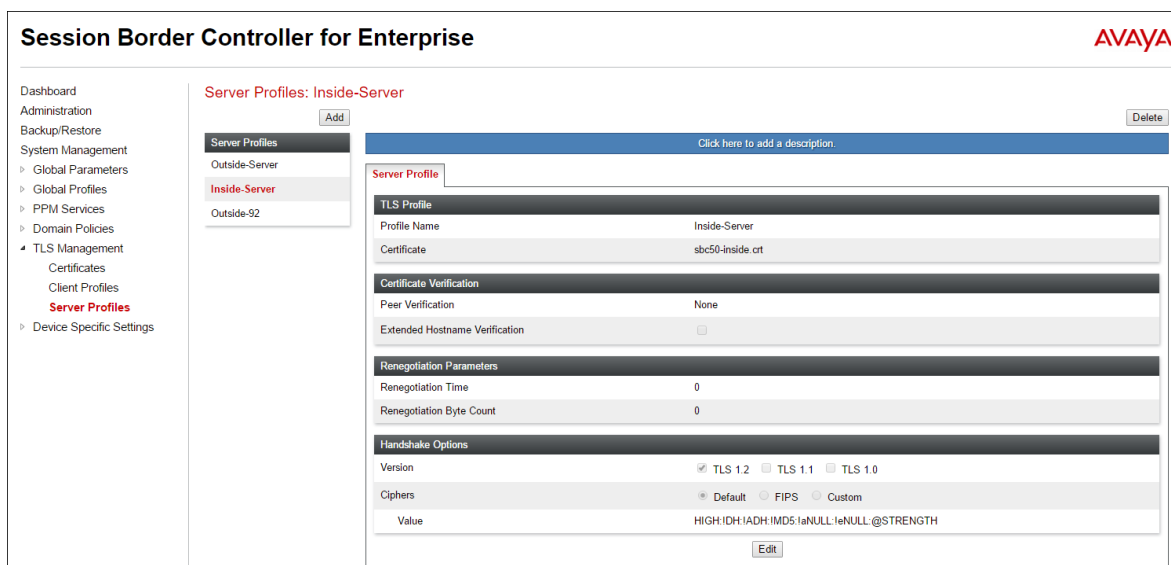
**Step 1** - Select **TLS Management** → **Server Profiles**, and click on **Add**. Enter the following:

- **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 screenshot shows a window titled "Edit Profile" with a close button (X) in the top right corner. At the top, there is a warning message in an orange box: "WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems." Below the warning, the "TLS Profile" section contains a "Profile Name" text field with "Inside-Client" entered and a "Certificate" dropdown menu showing "sbc50-inside.crt". The "Certificate Verification" section includes a "Peer Verification" label with the value "Required", a "Peer Certificate Authorities" dropdown menu showing "SystemManagerCA.pem", and a "Peer Certificate Revocation Lists" dropdown menu. Below these, there is a "Verification Depth" text field with the value "1", an "Extended Hostname Verification" checkbox which is unchecked, and a "Custom Hostname Override" text field. At the bottom center of the dialog is a "Next" button.



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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu includes options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Certificates, Client Profiles (highlighted), Server Profiles, and Device Specific Settings. The main content area is titled 'Client Profiles: Inside-Client' and features an 'Add' button. Below this, there's a 'Client Profile' section with a 'Click here to add a description' link. The profile configuration is divided into several sections: 'TLS Profile' (Profile Name: Inside-Client, Certificate: sbc50-inside.crt), 'Certificate Verification' (Peer Verification: Required, Peer Certificate Authorities: SystemManagerCA.pem, Peer Certificate Revocation Lists: ---, Verification Depth: 1, Extended Hostname Verification: unchecked), 'Renegotiation Parameters' (Renegotiation Time: 0, Renegotiation Byte Count: 0), and 'Handshake Options' (Version: TLS 1.2 selected, Ciphers: Default selected, Value: HIGH IDH:1ADH:1MD5:1aNULL:1eNULL:@STRENGTH). An 'Edit' button is located at the bottom right of the configuration area.

## 7.3. Global Profiles

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

### 7.3.1 Server Interworking – Avaya

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

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

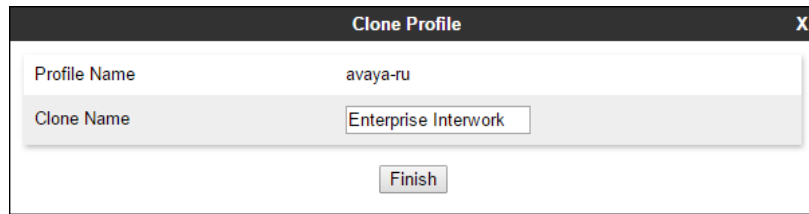
**Step 2** - Select the pre-defined **avaya-ru** profile and click the **Clone** button.

The screenshot shows the 'Server Interworking Profiles: avaya-ru' configuration page. The left-hand navigation menu is expanded to 'Global Profiles' > 'Server' > 'Interworking'. The 'Interworking Profiles' list on the left includes 'cs2100', 'avaya-ru' (highlighted), 'OCS-Edge-Server', 'disco-ccm', and 'cups'. The main content area has a warning banner: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, there are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table with the following data:

Parameter	Value
Hold Support	NONE
180 Handling	None
181 Handling	None

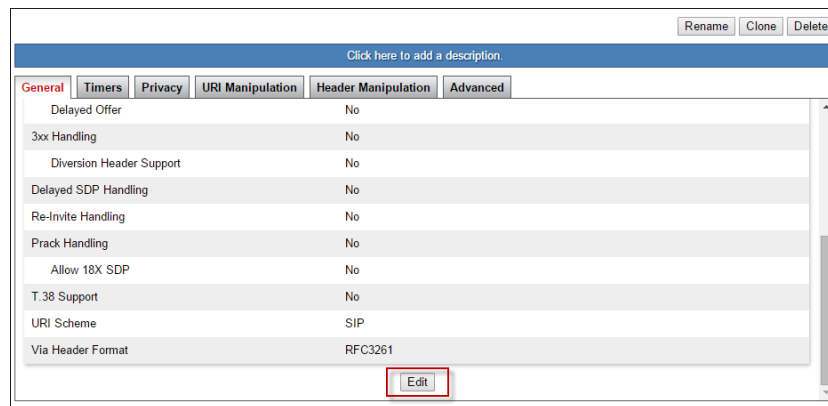
A 'Clone' button is located in the top right corner of the configuration area.

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



The image shows a 'Clone Profile' dialog box with a dark header bar containing the title 'Clone Profile' and a close button 'X'. The main area has two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Enterprise Interwork'. Below these fields is a 'Finish' button.

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



The image shows a profile configuration screen with a blue header bar containing the text 'Click here to add a description.' and three buttons: 'Rename', 'Clone', and 'Delete'. Below the header is a tabbed interface with tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is selected, showing a list of settings with their values: Delayed Offer (No), 3xx Handling (No), Diversion Header Support (No), Delayed SDP Handling (No), Re-Invite Handling (No), Prack Handling (No), Allow 18X SDP (No), T.38 Support (No), URI Scheme (SIP), and Via Header Format (RFC3261). At the bottom of the list is an 'Edit' button, which is highlighted with a red rectangle.

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

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

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

- Hold Support**: ☒ None, ☐ RFC2543 - c=0.0.0.0, ☐ RFC3264 - a=sendonly
- 180 Handling**: ☒ None, ☐ SDP, ☐ No SDP
- 181 Handling**: ☒ None, ☐ SDP, ☐ No SDP
- 182 Handling**: ☒ None, ☐ SDP, ☐ No SDP
- 183 Handling**: ☒ None, ☐ SDP, ☐ No SDP
- Refer Handling**: ☐
- URI Group**:
- Send Hold**: ☐
- Delayed Offer**: ☐
- 3xx Handling**: ☐
- Diversion Header Support**: ☐
- Delayed SDP Handling**: ☐
- Re-Invite Handling**: ☐
- Prack Handling**: ☐
- Allow 18X SDP**: ☐
- T.38 Support**: ☒ (highlighted with a red box)
- URI Scheme**: ☒ SIP, ☐ TEL, ☐ ANY
- Via Header Format**: ☒ RFC3261, ☐ RFC2543

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

**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**.

**Editing Profile: SIP Provider Interwk**

**Record Routes**

- ☐ None
- ☐ Single Side
- ☒ Both Sides
- ☐ Dialog-Initiate Only (Single Side)
- ☐ Dialog-Initiate Only (Both Sides)

**Include End Point IP for Context Lookup** ☐

**Extensions**

**Diversion Manipulation** ☐

**Diversion Condition**

**Diversion Header URI**

**Has Remote SBC** ☒

**Route Response on Via Port** ☐

**Relay INVITE Replace for SIPREC** ☐

**MOBX Re-INVITE Handling** ☐

**DTMF**

**DTMF Support**

- ☒ None
- ☐ SIP Notify
- ☐ RFC 2833 Relay & SIP Notify
- ☐ SIP Info
- ☐ RFC 2833 Relay & SIP Info
- ☐ Inband

**Finish**

### 7.3.3 Signaling Manipulation

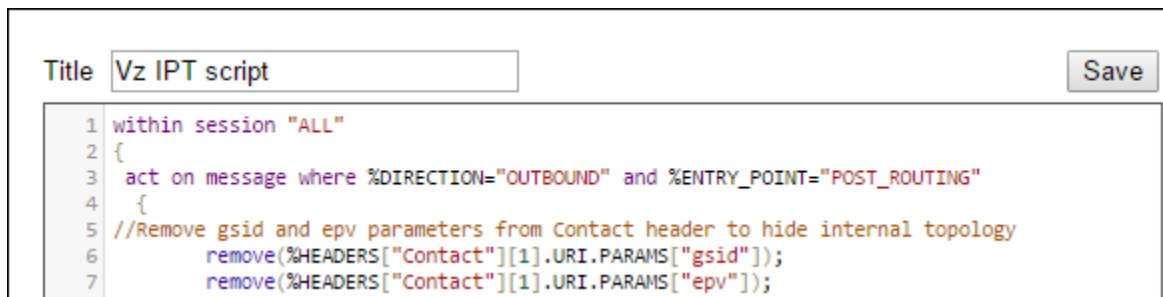
Signaling Manipulations are SigMa scripts the Avaya SBCE can use to manipulate SIP headers/messages. In the reference configuration, one signaling manipulation script is used.

**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** - As described in **Section 2.4**, Avaya SIP endpoints may send requests with Endpoint-View headers containing private network information. These are removed by Session Manager, as shown in **Section 5.3.2**. However an “epv” parameter is also inserted into the Contact header of these requests. This parameter also contains private network information. The following signaling manipulation is used to remove this “epv” parameter from the Contact

header, along with the “gsid” parameter. The “gsid” parameter was removed to further reduce packet size.

- Select **Global Profiles** from the menu on the left-hand side.
- Select **Signaling Manipulation**.
- Click **Add Script** (not shown) and the script editor window will open.
- Enter a name for the script in the **Title** box (e.g., **Vz IPT script**). The following script is defined:



The screenshot shows a script editor window with a title bar containing 'Title' and 'Vz IPT script', and a 'Save' button. The script content is as follows:

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

**Step 2** - As described in **Section 2.2, Item 3**, the Diversion header includes the SIPS URI scheme toward Verizon. The following signaling manipulation script is added to the script defined in **Step 1** above, to convert “sips” to “sip”.

- The following script is added:



The screenshot shows the same script editor window, but with additional lines of code added to the script:

```
8 // fix call-fwd
9   %HEADERS["Diversion"][1].regex_replace("sips","sip");
10 }
11 }
```

**Step 3** - 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**.

### 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**.

**Add Server Configuration Profile** X

Profile Name: EnterpriseCallServer

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**

**Edit Server Configuration Profile - General** X

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

Server Type: Call Server

SIP Domain:

TLS Client Profile: Inside-Client

Add

IP Address / FQDN	Port	Transport
10.64.91.11	5061	TLS

Delete

Finish

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

- Select **Next** to accept default values

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

- 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 IPT**) and select **Next** (not shown).

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

- **Server Type:** Select **Trunk Server**
- **IP Address:** **172.30.209.21** (Verizon-provided IP address)
- **Transport:** Select **UDP**
- **Port:** **5071**
- 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 **Vz IPT script** (created in **Section 7.3.3**) for **Signaling Manipulation Script**.
- Select **Finish** (not shown)

The screenshot shows the 'Server Configuration: Verizon IPT' window with the 'Advanced' tab selected. The left-hand menu is visible, showing 'Global Parameters' expanded. The main area displays configuration options for the 'Verizon IPT' server profile. The 'Advanced' tab includes checkboxes for 'Enable DoS Protection', 'Enable Grooming', 'Securable', 'Enable FGDN', and 'Tolerant'. It also shows the 'Interworking Profile' set to 'SIP Provider Interwk' and the 'Signaling Manipulation Script' set to 'Vz IPT script'. The 'URI Group' is set to 'None'. Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

## 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**.

The screenshot shows the 'Routing Profile' window with the 'Profile Name' field containing 'route to SM'. A 'Next' button is visible at the bottom right.

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

The screenshot shows the 'Routing Profile' window with various configuration options. The 'URI Group' is set to '\*' and 'Time of Day' is set to 'default'. 'Load Balancing' is set to 'Priority' and 'NAPTR' is unchecked. 'Transport' is set to 'None' and 'Next Hop Priority' is checked. 'Next Hop In-Dialog' is unchecked and 'Ignore Route Header' is unchecked. 'ENUM' is unchecked and 'ENUM Suffix' is empty. An 'Add' button is visible at the bottom right. A blue banner at the bottom says 'Click the Add button to add a Next-Hop Address.' Below the banner are 'Back' and 'Finish' buttons.

**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**.

**Routing Profile**

URI Group: \* Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

**Add**

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

**Delete**

**Back 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 IPT**).

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

- **Priority/Weight** = **1**
- **Server Configuration** = **Verizon IPT** (from **Section 7.3.5**).
- **Next Hop Address:** select **172.30.209.21:5071 (UDP)**.

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

**Profile : route to Vz IPT - Edit Rule**

URI Group: \* Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

**Add**

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Verizon IPT	172.30.209.21:5071 (UDP)	None

**Delete**

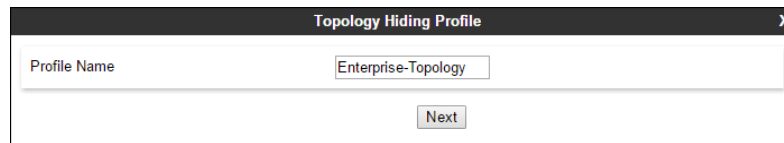
**Finish**

### 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**.

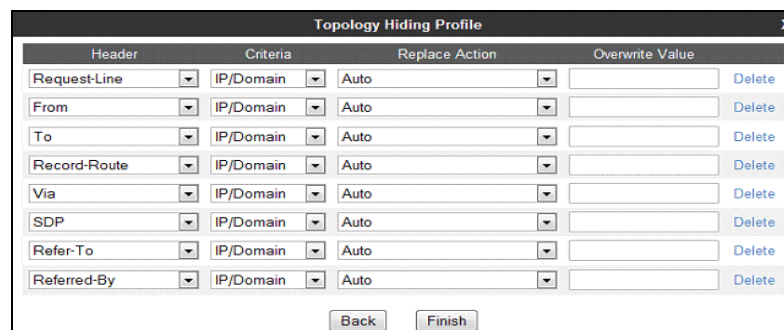


Topology Hiding Profile	
Profile Name	Enterprise-Topology
<div>Next</div>	

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

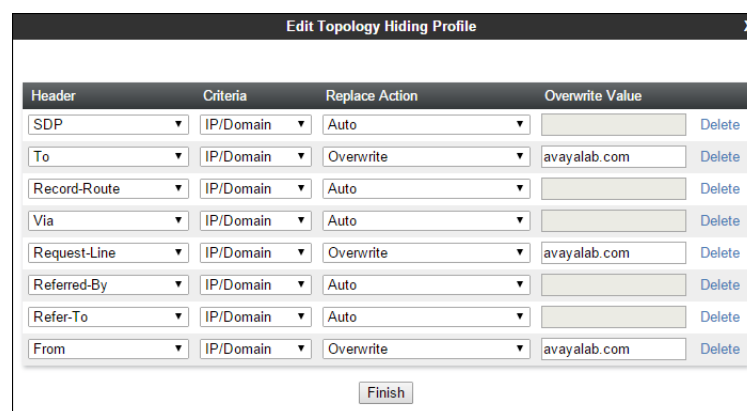


Topology Hiding Profile				
<div>Add Header</div>				
Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Auto		Delete
<div>Back Finish</div>				



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

**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**).



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

### 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 th profile**).
- Overwrite the headers as shown below with the FQDNs known by Verizon.

Topology Hiding Profiles: Vz th profile

Add Rename Clone Delete

Topology Hiding Profiles

- default
- cisco\_th\_profile
- Vz th profile**
- Enterprise-Topology
- Vz IPCC th profile
- IP500v2-Topology
- IPOSE-Topology

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
Referred-By	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com

Edit

## 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.

Dashboard

Administration

Backup/Restore

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies

**Application Rules**

- Border Rules
- Media Rules
- Security Rules
- Signaling Rules
- End Point Policy Groups
- Session Policies

Application Rules: sip-trunk

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

## 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**.

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	RTP ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^N <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	RTP ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^N <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

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

Finish

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

### 7.4.2.2 Verizon – Media Rule

Repeat the steps in **Section 7.3.2.1**, 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**.

Signaling QoS

Enabled ☒

☐ ToS

Precedence Routine 000

ToS Minimize Delay 1000

☒ DSCP

Value EF 101110

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**(not shown)

**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**.

Signaling QoS

Enabled ☒

☐ ToS

Precedence Routine 000

ToS Minimize Delay 1000

☒ DSCP

Value AF32 011100

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.

The screenshot shows the 'Policy Groups: enterprise-sip-trunk' configuration page. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area has a list of policy groups on the left, with 'enterprise-sip-trunk' selected. The right side shows the configuration details for this group, including a table with columns: Order, Application, Border, Media, Security, and Signaling. The table contains one row with the following values: Order 1, Application sip-trunk, Border default, Media enterprise med rule, Security default-low, and Signaling enterprise sig rule. There are also buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'.

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

## 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).

The screenshot shows the 'Policy Groups: Vz-policy-group' configuration page. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area has a list of policy groups on the left, with 'Vz-policy-group' selected. The right side shows the configuration details for this group, including a table with columns: Order, Application, Border, Media, Security, and Signaling. The table contains one row with the following values: Order 1, Application default-server-high, Border default, Media Vz SIPTrk Med Rule, Security default-low, and Signaling Vz SIPTrk Sig Rule. There are also buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'.

Order	Application	Border	Media	Security	Signaling
1	default-server-high	default	Vz SIPTrk Med Rule	default-low	Vz SIPTrk Sig Rule



## 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.

The screenshot shows the 'Network Management: SBC1' page. On the left is a sidebar menu with 'Device Specific Settings' expanded and 'Network Management' selected. The main area has two tabs: 'Interfaces' (active) and 'Networks'. Below the tabs is a table with columns 'Interface Name', 'VLAN Tag', and 'Status'. The table lists four interfaces: A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Enabled). An 'Add VLAN' button is in the top right corner.

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

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

The screenshot shows the 'Network Management: SBC1' page with the 'Networks' tab selected. The table displays IP provisioning details for three networks: Verizon B1, Inside A1, and Public B2. Each row includes columns for Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address, along with 'Edit' and 'Delete' links.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Verizon B1	1.1.1.1	255.255.255.0	B1	1.1.1.2	<a href="#">Edit</a> <a href="#">Delete</a>
Inside A1	10.64.91.1	255.255.255.0	A1	10.64.91.48, 10.64.91.49, 10.64.91.50	<a href="#">Edit</a> <a href="#">Delete</a>
Public B2	192.168.0.1	255.255.255.128	B2	192.168.0.44 192.168.0.92	<a href="#">Edit</a> <a href="#">Delete</a>

## 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.

Name	Media IP Network	Port Range	TLS Profile	
Inside-Med-50	10.64.91.50 Inside A1 (A1, VLAN 0)	35000 - 40000	None	Edit Delete
Vz-Med-B1	1.1.1.2 Verizon B1 (B1, VLAN 0)	35000 - 40000	None	Edit Delete

## 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**).

The screenshot shows the 'Signaling Interface: SBC1' configuration page. On the left is a navigation menu with options like System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The 'Signaling Interface' option is highlighted. The main content area has a tab labeled 'Signaling Interface'. Below the tab is a warning message: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below the warning is a table with the following data:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Vz-sig	1.1.1.2 Verizon B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete
Inside-sig-50	10.64.91.50 Inside A1 (A1, VLAN 0)	---	---	5061	Inside-Server	Edit Delete

## 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 7.5.4).
- **Signaling Interface:** **Inside-sig-50** (Section 7.5.4).
- **Media Interface:** **Inside-Med-50** (Section 7.5.3).
- **End Point Policy Group:** **enterprise-sip-trunk** (Section 7.4.4).
- **Routing Profile:** **route to Vz IPT** (Section 7.3.7).
- **Topology Hiding Profile:** **Enterprise-Topology** (Section 7.3.8).
- Let other values default.

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

The screenshot shows a dialog box titled 'View Flow: Vz enterprise side'. It contains two panels: 'Criteria' and 'Profile'. The 'Criteria' panel lists the following values:

Criteria	Value
Flow Name	Vz enterprise side
Server Configuration	EnterpriseCallServer
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Vz-sig

The 'Profile' panel lists the following values:

Profile	Value
Signaling Interface	Inside-sig-50
Media Interface	Inside-Med-50
Secondary Media Interface	None
End Point Policy Group	enterprise-sip-trunk
Routing Profile	route to Vz IPT
Topology Hiding Profile	Enterprise-Topology
Signaling Manipulation Script	None
Remote Branch Office	Any

## 7.5.5 Server Flows – For Verizon

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

- **Flow Name:** Verizon IPT Flow.
- **Server Configuration:** Verizon IPT (Section 7.3.5).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** Inside-sig-50 (Section 7.5.4).
- **Signaling Interface:** Vz-sig (Section 7.5.4).
- **Media Interface:** Vz-Med-B1 (Section 7.5.3).
- **End Point Policy Group:** Vz-policy-group (Section 7.4.5).
- **Routing Profile:** route to SM (Section 7.3.6).
- **Topology Hiding Profile:** Vz th profile (Section 7.3.9).

View Flow: Verizon IPT Flow

Criteria	
Flow Name	Verizon IPT Flow
Server Configuration	Verizon IPT
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside-sig-50

Profile	
Signaling Interface	Vz-sig
Media Interface	Vz-Med-B1
Secondary Media Interface	None
End Point Policy Group	Vz-policy-group
Routing Profile	route to SM
Topology Hiding Profile	Vz th profile
Signaling Manipulation Script	None
Remote Branch Office	Any

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

Server Configuration: EnterpriseCall Server							
Update							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Vz enterprise side	*	Vz-sig	Inside-sig-50	enterprise-sip-trunk	route to Vz IPT	View Clone Edit Delete

Server Configuration: Verizon IPT							
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Verizon IPT Flow	*	Inside-sig-50	Vz-sig	Vz-policy-group	route to SM	View Clone Edit Delete

## 8. Verizon Business IP Trunking Services Suite Configuration

Information regarding the Verizon Business IP Trunking Services suite offer can be found at <http://www.verizonbusiness.com/Products/communications/ip-telephony/> or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes is located in the Avaya Solutions and Interoperability Test Lab. Access to the Verizon Business IP Trunking 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, ports, DID numbers) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i> <i>UDP port 5060</i>	<i>pcelban0001.avayalincroft.globalipcom.com</i> <i>UDP Port 5071</i>

IP DID Numbers
732-945-0231
732-945-0232
732-945-0233
732-945-0234
732-945-0235
732-945-0236
732-945-0237
732-945-0238
732-945-0239

## 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 SIP Trunk

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 1 and trunk group 1.

The following edited Communication Manager *list trace tac* trace output shows a call incoming on trunk group 1. The PSTN telephone dialed 732-945-0233. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x12003). Extension 12002 is an IP Deskphone with IP address 10.64.91.156 in Region 1. The RTP media path is “ip-direct” from the IP Deskphone (**10.64.91.156**) to the “inside” of the Avaya SBCE (**10.64.91.50**) in Region 2.

```
list trace tac *01                                     Page 1
LIST TRACE
time          data
09:23:31 TRACE STARTED 09/07/2017 CM Release String cold-01.0.532.0-23985
09:23:35 SIP<INVITE sips:12002@avayalab.com SIP/2.0
09:23:35      Call-ID: f14f2d0a16982f678095537cec633269
09:23:35      active trunk-group 1 member 1      cid 0x52d
09:23:35 SIP>SIP/2.0 183 Session Progress
09:23:35      Call-ID: f14f2d0a16982f678095537cec633269
09:23:35      dial 12002
09:23:35      ring station      12002 cid 0x52d
09:23:35      Alerting party uses public-unknown-numbering
09:23:35      G729 ss:off ps:20
09:23:35      rgn:2 [10.64.91.50]:35052
09:23:35      rgn:1 [10.64.91.60]:6016
09:23:35      G72264K ss:off ps:20
09:23:35      rgn:1 [10.64.91.156]:21892
09:23:35      rgn:1 [10.64.91.60]:6018
09:23:38 SIP>SIP/2.0 200 OK
09:23:38      Call-ID: f14f2d0a16982f678095537cec633269
09:23:38      active station      12002 cid 0x52d
09:23:38      Connected party uses public-unknown-numbering
09:23:38 SIP<ACK sips:+17329450232@10.64.91.65:5081;transport=tls SI
09:23:38 SIP<P/2.0
09:23:38      Call-ID: f14f2d0a16982f678095537cec633269
<continued on next page>
```

```

<continued from previous page>

09:23:38 SIP>INVITE sips:3035382177@10.64.91.50:5061;transport=tls;g
09:23:38 SIP>sid=83e3ef00-93e0-11e7-9cb3-000c29e8354a SIP/2.0
09:23:38 Call-ID: f14f2d0a16982f678095537cec633269
09:23:39 SIP<SIP/2.0 100 Trying
09:23:39 Call-ID: f14f2d0a16982f678095537cec633269
09:23:39 SIP<SIP/2.0 200 OK
09:23:39 Call-ID: f14f2d0a16982f678095537cec633269
09:23:39 SIP>ACK sips:3035382177@10.64.91.50:5061;transport=tls;gsid
09:23:39 SIP>=83e3ef00-93e0-11e7-9cb3-000c29e8354a SIP/2.0
09:23:39 Call-ID: f14f2d0a16982f678095537cec633269
09:23:39 G729A ss:off ps:20
09:23:39 rgn:2 [10.64.91.50]:35052
09:23:39 rgn:1 [10.64.91.156]:21892
09:23:39 G729 ss:off ps:20
09:23:39 rgn:1 [10.64.91.156]:21892
09:23:39 rgn:2 [10.64.91.50]:35052
09:23:44 SIP<BYE sips:+17329450232@10.64.91.65:5081;transport=tls SI
09:23:44 SIP<P/2.0
09:23:44 Call-ID: f14f2d0a16982f678095537cec633269
09:23:44 SIP>SIP/2.0 200 OK
09:23:44 Call-ID: f14f2d0a16982f678095537cec633269
09:23:44 idle trunk-group 1 member 1 cid 0x52d

```

The following screen shows **Page 2** of the output of the *status trunk* command pertaining to this same call. Note the signaling using port 5081 between Communication Manager and Session Manager. Note the media is “ip-direct” from the IP Telephone (**10.64.91.32**) to the inside IP address of Avaya SBCE (**10.64.91.50**) using codec G.729a.

```

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

Near-end Signaling Loc: PROCR
  Signaling IP Address Port
  Near-end: 10.64.91.65 : 5081
  Far-end: 10.64.91.11 : 5081
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: 10.64.91.156 : 21892
Far-end: 10.64.91.50 : 35052

```

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 1/1                                     Page 3 of 3
SRC PORT TO DEST PORT TALKPATH

src port: T00001
T00001:TX:10.64.91.50:35052/g729/20ms/1-srtp-aescm128-hmac80
S00000:RX:10.64.91.156:21892/g729a/20ms/1-srtp-aescm128-hmac80

```

## 9.1.2 Example Outgoing Calls to PSTN via Verizon SIP Trunk

The following edited trace shows an outbound ARS call from IP Telephone x12002 to the PSTN number 9-1-303-538-2177. The call is routed to route pattern 1 and trunk group 1. The call initially uses the Avaya Media Server (**10.64.91.60**), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (**10.64.91.156**) and the “inside” of the Avaya SBCE (**10.64.91.50**).

list trace tac *01		Page 1
LIST TRACE		
time	data	
09:11:55	TRACE STARTED 09/07/2017 CM Release String cold-01.0.532.0-23985	
09:12:01	dial 913035382177 route:PREFIX FNPA ARS	
09:12:01	route-pattern 1 preference 1 location 1/ALL cid 0x520	
09:12:01	seize trunk-group 1 member 6 cid 0x520	
09:12:01	Calling Number & Name 12002 theodore roos	
09:12:01	SIP>INVITE sips:+13035382177@avayalab.com SIP/2.0	
09:12:01	Call-ID: e6671c893de41e787690c292817b9	
09:12:01	Setup digits +13035382177	
09:12:01	Calling Number & Name +17329450232 theodore roos	
09:12:01	Calling party uses public-unknown-numbering	
09:12:01	SIP<SIP/2.0 100 Trying	
09:12:01	Call-ID: e6671c893de41e787690c292817b9	
09:12:01	Proceed trunk-group 1 member 6 cid 0x520	
09:12:04	SIP<SIP/2.0 183 Session Progress	
09:12:04	Call-ID: e6671c893de41e787690c292817b9	
09:12:04	G729 ss:off ps:20	
	rgn:2 [10.64.91.50]:35046	
	rgn:1 [10.64.91.60]:6008	
09:12:05	SIP<SIP/2.0 200 OK	
09:12:05	Call-ID: e6671c893de41e787690c292817b9	
09:12:05	SIP>ACK sips:+13035382177@10.64.91.50:5061;transport=tls;gs	
09:12:05	SIP>id=e66717c6-93de-41e7-8766-000c292817b9 SIP/2.0	
09:12:05	Call-ID: e6671c893de41e787690c292817b9	
09:12:05	active trunk-group 1 member 6 cid 0x520	
09:12:05	SIP>INVITE sips:+13035382177@10.64.91.50:5061;transport=tls	
09:12:05	SIP>;gsid=e66717c6-93de-41e7-8766-000c292817b9 SIP/2.0	
09:12:05	Call-ID: e6671c893de41e787690c292817b9	
09:12:05	SIP<SIP/2.0 100 Trying	
09:12:05	Call-ID: e6671c893de41e787690c292817b9	
09:12:05	SIP<SIP/2.0 200 OK	
09:12:05	Call-ID: e6671c893de41e787690c292817b9	
09:12:05	G729 ss:off ps:20	
	rgn:1 [10.64.91.156]:21892	
	rgn:2 [10.64.91.50]:35046	
09:12:05	SIP>ACK sips:+13035382177@10.64.91.50:5061;transport=tls;gs	
09:12:05	SIP>id=e66717c6-93de-41e7-8766-000c292817b9 SIP/2.0	
09:12:05	Call-ID: e6671c893de41e787690c292817b9	
09:12:05	G729A ss:off ps:20	
	rgn:2 [10.64.91.50]:35046	
	rgn:1 [10.64.91.156]:21892	
09:12:10	SIP<BYE sips:+17329450232@10.64.91.65:5081;transport=tls SI	
09:12:10	SIP<P/2.0	
09:12:10	Call-ID: e6671c893de41e787690c292817b9	
09:12:10	SIP>SIP/2.0 200 OK	
09:12:10	Call-ID: e6671c893de41e787690c292817b9	
09:12:10	idle trunk-group 1 member 6 cid 0x520	



## 9.2. Avaya Aura® Session Manager Verification

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.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring [Help ?](#)

### SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

[SIP Entities Status for All Monitoring Session Manager Instances](#)

[Run Monitor](#)

1 Items | [Refresh](#) Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Monitored Entities					Total
			Down	Partially Up	Up	Not Monitored	Deny	
<input type="checkbox"/>	<a href="#">SessionManager</a>	Core	3	0	11	0	0	14

Select: All, None

[All Monitored SIP Entities](#)

[Run Monitor](#)

14 Items | [Refresh](#) Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	<a href="#">CM-TG3</a>
<input type="checkbox"/>	<a href="#">CM-TG2</a>
<input type="checkbox"/>	<a href="#">SBC1</a>
<input type="checkbox"/>	<a href="#">CM-TG1</a>

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.

[All Entity Links to SIP Entity: SBC1](#)

[Summary View](#)

Status Details for the selected Session Manager:

1 Items | [Refresh](#) Filter: Enable

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> <a href="#">SessionManager</a>	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP

## 9.3. Avaya Session Border Controller for Enterprise Verification

### 9.3.1 Welcome Screen

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

The screenshot shows the 'Session Border Controller for Enterprise' welcome screen. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main content area is divided into three sections: 'Information', 'Installed Devices', and 'Active Alarms (past 24 hours)'. The 'Information' section displays system details such as System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, and Failed Login Attempts. The 'Installed Devices' section lists 'EMS' and 'SBC1'. The 'Active Alarms' section is currently empty.

Information	
System Time	11:41:21 AM MDT
Version	7.2.0.0-18-13712
Build Date	Thu Jun 1 00:12:50 UTC 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	08/25/2017 12:21:35 MDT
Failed Login Attempts	0

Installed Devices	
EMS	
SBC1	

Active Alarms (past 24 hours)	
-------------------------------	--

### 9.3.2 Alarms

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

The screenshot shows the 'Alarms' tab selected in the top navigation bar. The main content area displays the title 'Session Border Controller for Enterprise'.

Alarm Viewer:

The screenshot shows the 'Alarm Viewer' interface. The left sidebar lists 'Devices' with 'EMS' and 'SBC1'. The main content area displays the 'Alarms' tab, which shows a table with columns: ID, Details, State, Time, and Device. The table is currently empty, displaying the message 'No alarms found for this device.' Below the table are buttons for 'Clear Selected' and 'Clear All'.

ID	Details	State	Time	Device
No alarms found for this device.				

### 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:

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	751976454033216	8/28/17	2:41 PM	Policy	SBC1	No Subscriber Flow Matched	
Message Dropped	751976451992077	8/28/17	2:41 PM	Policy	SBC1	No Subscriber Flow Matched	
Message Dropped	751976304032669	8/28/17	2:36 PM	Policy	SBC1	No Subscriber Flow Matched	
Message Dropped	751976301994346	8/28/17	2:36 PM	Policy	SBC1	No Subscriber Flow Matched	

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	August 28, 2017 2:41:48 PM MDT	Device	SBC1	
Cause	No Subscriber Flow Matched			
Message Data				
Method Name	OPTIONS			
Call ID	6e87a16c3c5021861c9affb4ef9ea3b0	From	10.64.19.170	
To	10.64.91.50	Source IP	10.64.19.170	
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**”.

Full Diagnostic

Ping Test

Start Diagnostic

Task Description	Status
⊖ EMS Link Check	
⊖ SBC Link Check: A1	
⊖ SBC Link Check: B1	
⊖ SBC Link Check: B2	
⊖ Ping: SBC (10.64.91.49 [A1]) to Gateway (10.64.91.1)	
⊖ Ping: SBC (10.64.91.49 [A1]) to Primary DNS (10.64.19.201)	
⊖ Ping: SBC (10.64.91.50 [A1]) to Gateway (10.64.91.1)	
⊖ Ping: SBC (10.64.91.50 [A1]) to Primary DNS (10.64.19.201)	
⊖ Ping: SBC (1.1.1.2 [B1]) to Gateway (1.1.1.1)	
⊖ Ping: SBC (1.1.1.2 [B1]) to Primary DNS (10.64.19.201)	

A green check mark or a red x will indicate success or failure.

Full Diagnostic

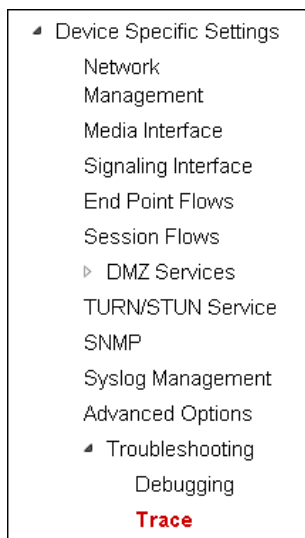
Ping Test

Stop Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B2	B2 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (10.64.91.49 [A1]) to Gateway (10.64.91.1)	Average ping from 10.64.91.49 [A1] to 10.64.91.1 is 0.571ms.
✓ Ping: SBC (10.64.91.49 [A1]) to Primary DNS (10.64.19.201)	Average ping from 10.64.91.49 [A1] to 10.64.19.201 is 0.219ms.
✓ Ping: SBC (10.64.91.50 [A1]) to Gateway (10.64.91.1)	Average ping from 10.64.91.50 [A1] to 10.64.91.1 is 0.236ms.
✓ Ping: SBC (10.64.91.50 [A1]) to Primary DNS (10.64.19.201)	Average ping from 10.64.91.50 [A1] to 10.64.19.201 is 0.208ms.

### 9.3.5 Tracing

To take a call trace, Select **Device Specific Settings** → **Troubleshooting** → **Tracing** from the left-side menu as shown below.



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

A screenshot of the 'Packet Capture' configuration interface. The interface has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section contains the following fields:

- Status: Ready
- Interface: B1 (dropdown)
- Local Address IP[:Port]: All (dropdown) and an empty text box
- Remote Address \*: \*:Port, IP, IP:Port: \* (text box)
- Protocol: All (dropdown)
- Maximum Number of Packets to Capture: 1000 (text box)
- Capture Filename: Test-Trace.pcap (text box). Below the text box is a note: 'Using the name of an existing capture will overwrite it.'

At the bottom of the form are two buttons: 'Start Capture' and 'Clear'.

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

**Packet Capture** **Captures**

Please wait while your settings are saved and the capture is started...

**Packet Capture Configuration**

Status: Ready

Interface: B1

Local Address IP[:Port]: All

Remote Address \*, \*:Port, IP, IP:Port: \*

Protocol: All

Maximum Number of Packets to Capture: 1000

Capture Filename: Test-Trace.pcap  
Using the name of an existing capture will overwrite it.

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.

**Packet Capture** **Captures**

Refresh

File Name	File Size (bytes)	Last Modified	
Test-Trace_20150807161226.pcap	0	August 7, 2015 4:12:27 PM MDT	Delete

## 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 Trunking service. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users access to the PSTN using a Verizon Business IP Trunking public SIP trunk service connection.

## 11. Additional 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 G430 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

### 11.2. Verizon Business

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

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

---

**©2017 Avaya Inc. All Rights Reserved.**

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

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