



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, Avaya Aura® Experience Portal 7.2 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 8.0, Avaya Aura® Communication Manager Release 8.0, Avaya Aura® Experience Portal 7.2, 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 .....	8
2.4.	SIP Header Removal.....	8
2.5.	Support.....	8
3.	Reference Configuration.....	9
3.1.	Illustrative Configuration Information.....	9
3.2.	Call Flows .....	11
3.2.1	Communication Manager.....	11
3.2.2	Experience Portal .....	14
4.	Equipment and Software Validated .....	17
5.	Configure Avaya Aura® Session Manager .....	18
5.1.	SIP Domain .....	19
5.2.	Locations .....	19
5.2.1	Main Location.....	19
5.2.2	Common Location .....	20
5.3.	Configure Adaptations .....	20
5.3.1	Adaptation for Avaya Aura® Communication Manager.....	21
5.3.2	Adaptation for the Verizon Business IP Trunking service .....	23
5.4.	SIP Entities.....	24
5.4.1	Avaya Aura® Session Manager SIP Entity .....	25
5.4.2	Avaya Aura® Communication Manager SIP Entity – Public Trunk .....	27
5.4.3	Avaya Aura® Communication Manager SIP Entity – Local Trunk.....	28
5.4.4	Avaya Session Border Controller for Enterprise SIP Entity.....	28
5.4.5	Avaya Aura® Messaging SIP Entity .....	28
5.4.6	Avaya Aura® Experience Portal SIP Entity .....	28
5.5.	Entity Links.....	28
5.5.1	Entity Link to Avaya Aura® Communication Manager – Public Trunk.....	29
5.5.2	Entity Link to Avaya Aura® Communication Manager – Local Trunk.....	29
5.5.3	Entity Link for the Verizon Business IP Trunking service via the Avaya SBCE.....	29
5.5.4	Entity Link to Avaya Aura® Messaging .....	30
5.5.5	Entity Link to Avaya Aura® Experience Portal .....	30
5.6.	Time Ranges .....	30
5.7.	Routing Policies .....	30
5.7.1	Routing Policy for Verizon Routing to Avaya Aura® Communication Manager ...	30
5.7.2	Routing Policy for Inbound Routing to Avaya Aura® Messaging.....	32
5.7.3	Routing Policy for Inbound Routing to Experience Portal .....	32
5.7.4	Routing Policy for Outbound Calls to Verizon.....	32
5.8.	Dial Patterns.....	33
5.8.1	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager .....	33
5.8.2	Matching Outbound Calls to Verizon/PSTN .....	35
5.9.	Verify TLS Certificates – Session Manager .....	36
6.	Configure Avaya Aura® Communication Manager Release 8.0 .....	38

6.1.	Verify Licensed Features .....	38
6.2.	System-Parameters Features .....	40
6.3.	Dial Plan.....	41
6.4.	Node Names.....	41
6.5.	Processor Ethernet Configuration .....	42
6.6.	IP Codec Sets .....	42
6.6.1	Codecs for IP Network Region 1 (calls within the CPE) .....	42
6.6.2	Codecs for IP Network Region 2 (calls to/from Verizon) .....	44
6.7.	Network Regions .....	44
6.7.1	IP Network Region 1 – Local CPE Region .....	44
6.7.2	IP Network Region 2 – Verizon Trunk Region .....	46
6.8.	SIP Trunks .....	46
6.8.1	SIP Trunk for Inbound/Outbound Verizon calls.....	47
6.8.2	Local SIP Trunk (Avaya SIP Telephone and Messaging Access).....	50
6.9.	Public Numbering .....	50
6.10.	Private Numbering.....	51
6.11.	Route Patterns .....	52
6.11.1	Route Pattern for National Calls to Verizon .....	52
6.11.2	Route Pattern for International Calls to Verizon .....	52
6.11.3	Route Pattern for Service Calls to Verizon.....	53
6.11.4	Route Pattern for Calls within the CPE .....	53
6.12.	Automatic Route Selection (ARS) Dialing .....	54
6.13.	Automatic Alternate Routing (AAR) Dialing.....	54
6.14.	Avaya G450 Media Gateway Provisioning .....	55
6.15.	Avaya Aura® Media Server Provisioning.....	56
6.16.	Save Translations .....	57
6.17.	Verify TLS Certificates – Communication Manager.....	57
7.	Avaya Aura® Experience Portal.....	59
7.1.	Background .....	59
7.2.	Logging In and Licensing .....	60
7.3.	VoIP Connection.....	61
7.4.	Speech Servers .....	62
7.5.	Application References .....	62
7.6.	MPP Servers and VoIP Settings .....	64
7.7.	Configuring RFC2833 Event Value Offered by Experience Portal.....	66
8.	Configure Avaya Session Border Controller for Enterprise Release 7.2.....	67
8.1.	System Management – Status .....	68
8.2.	TLS Management.....	69
8.2.1	Verify TLS Certificates – Avaya Session Border Controller for Enterprise .....	69
8.2.2	Server Profiles.....	71
8.2.3	Client Profiles .....	72
8.3.	Global Profiles .....	73
8.3.1	Server Interworking – Avaya.....	73
8.3.2	Server Interworking – Verizon .....	76
8.3.3	Signaling Manipulation.....	77
8.3.4	Server Configuration – Session Manager .....	78

8.3.5	Server Configuration – Verizon.....	80
8.3.6	Routing – To Session Manager.....	81
8.3.7	Routing – To Verizon .....	82
8.3.8	Topology Hiding – Enterprise Side .....	83
8.3.9	Topology Hiding – Verizon Side.....	84
8.4.	Domain Policies .....	84
8.4.1	Application Rules.....	84
8.4.2	Media Rules .....	85
8.4.3	Signaling Rules .....	86
8.4.4	Endpoint Policy Groups – Enterprise Connection .....	88
8.4.5	Endpoint Policy Groups – Verizon Connection.....	88
8.5.	Device Specific Settings .....	89
8.5.1	Network Management.....	89
8.5.2	Media Interfaces.....	90
8.5.3	Signaling Interface .....	91
8.5.4	Server Flows – For Session Manager .....	92
8.5.5	Server Flows – For Verizon.....	93
9.	Verizon Business IP Trunking Services Suite Configuration.....	94
9.1.	Service Access Information .....	94
10.	Verification Steps.....	95
10.1.	Avaya Aura® Communication Manager Verifications .....	95
10.2.	Avaya Aura® Session Manager Verification .....	97
10.3.	Avaya Session Border Controller for Enterprise Verification .....	99
10.3.1	Welcome Screen .....	99
10.3.2	Alarms.....	99
10.3.3	Incidents .....	100
10.3.4	Diagnostics.....	100
10.3.5	Tracing .....	102
11.	Conclusion .....	103
12.	Additional References.....	104
12.1.	Avaya .....	104
12.2.	Verizon Business .....	104
13.	Appendix A – Avaya Session Border Controller for Enterprise – Refer Handling	105

# 1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.0, Avaya Aura® Communication Manager Release 8.0, Avaya Aura® Experience Portal 7.2, 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., Aura® Messaging, Experience Portal, 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
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold), Automatic Speech Recognition, and Text to Speech
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agent extension
- Call and two-way talk path establishment between callers and Communication Manager agents following redirection from Experience Portal
- Inbound calls to a self-service Experience Portal application which forwards the call to 8YY or any other PSTN number over Verizon IPT service using SIP REFER
- 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 6.6**), 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

---

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

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”.
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 8.3.3**.
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. The Experience Portal test application used for compliance testing performs consultative call transfers using SIP INVITE with the original calling party number in the From and P-Asserted Identity headers, it does not include a Diversion header. Verizon requires a Diversion header for this scenario. This caused consultative call transfers out the Verizon Business IP Trunking service to fail. However, blind transfers out to Verizon using SIP REFER were successful. Also, consultative and blind transfers from Experience Portal to Communication Manager were successful as well.
6. 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.
7. Verizon Business IP Trunking service does not support G.711A codec for domestic service (EMEA only).
8. 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 8.3.3** and **8.3.5**.

## 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/>

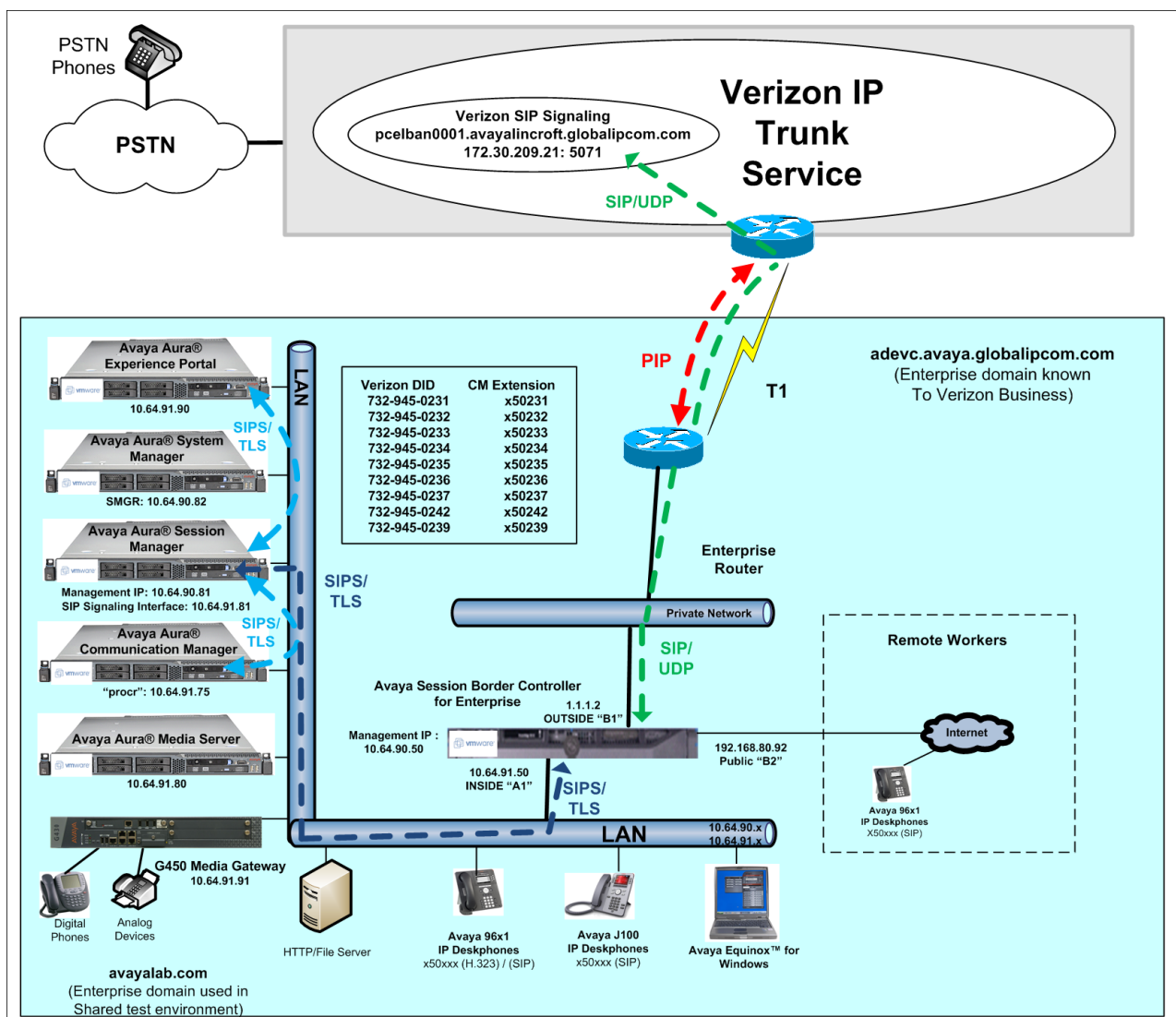


## 3. Reference Configuration

### 3.1. Illustrative Configuration Information

**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 8.3.9**). 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® Session Manager
- Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya Media Server
- Avaya Aura® Messaging
- Avaya Aura® Experience Portal
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle
- Avaya Equinox™ for Windows
- Avaya Digital Phones
- Ventafax fax software

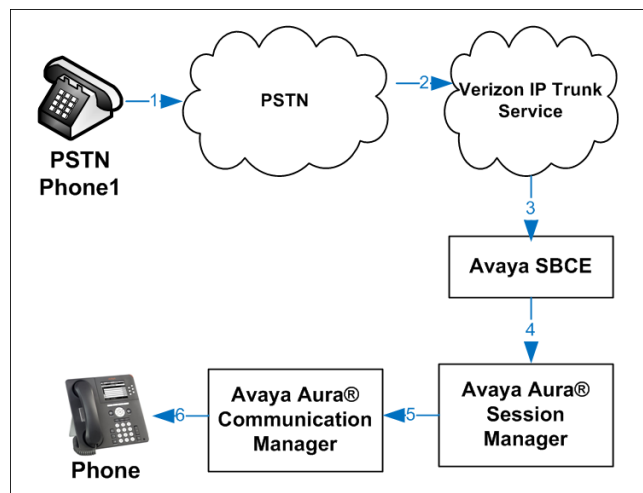
## 3.2. Call Flows

To understand how Verizon Business IP Trunking service calls are handled by the Avaya CPE environment, several call flows are described in this section.

### 3.2.1 Communication Manager

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

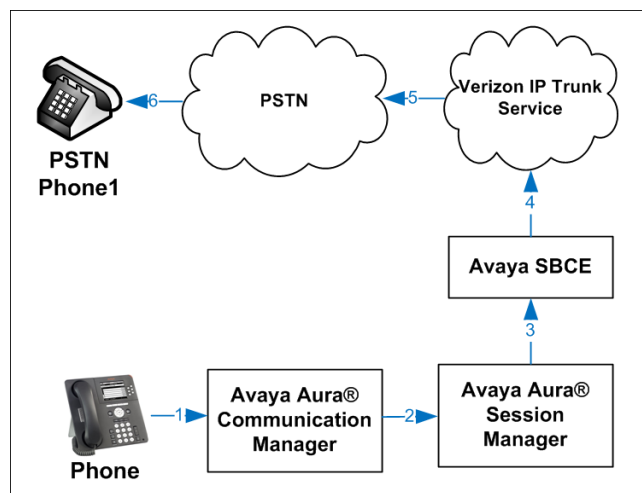
1. A PSTN phone originates a call to a Verizon Business IP Trunking service number.
2. The PSTN routes the call to the Verizon Business IP Trunking service network.
3. The Verizon Business IP Trunking service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs IP address translations and any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



**Figure 2: Inbound Verizon Call**

The second call scenario illustrated is an outbound call initiated on Communication Manager, routed to Session Manager, and is subsequently sent to the Avaya SBCE for delivery to the Verizon Business IP Trunking service.

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

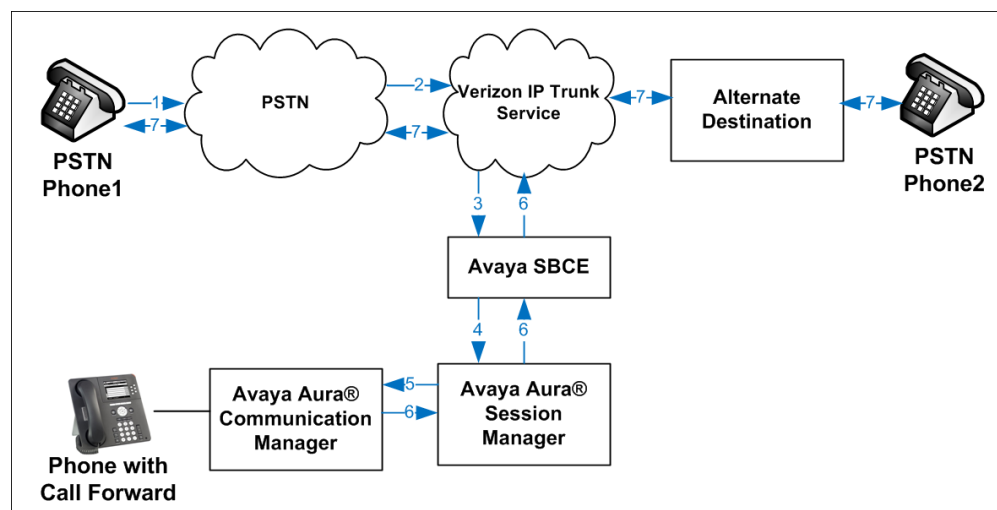


**Figure 3: Outbound Verizon Call**

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

**Note** – In cases where calls are forwarded to an alternate destination such as an 8xx numbers, the Verizon Business IP Trunking service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 6.8**).

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

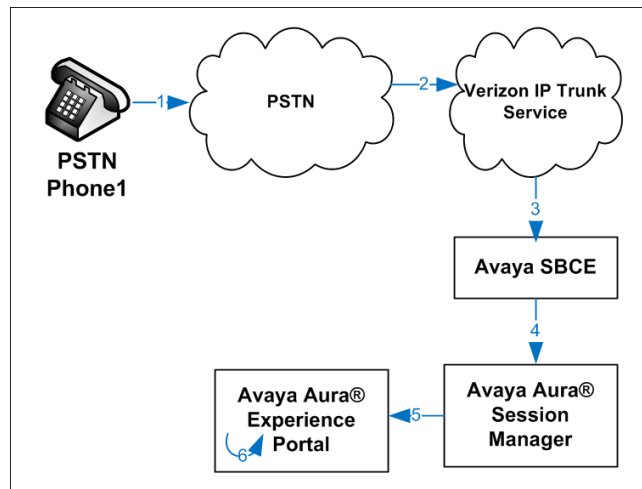


**Figure 4: Station Re-directed (e.g., Call Forward) Verizon Call**

### 3.2.2 Experience Portal

The first call scenario illustrated below is an inbound call arriving and remaining on Experience Portal.

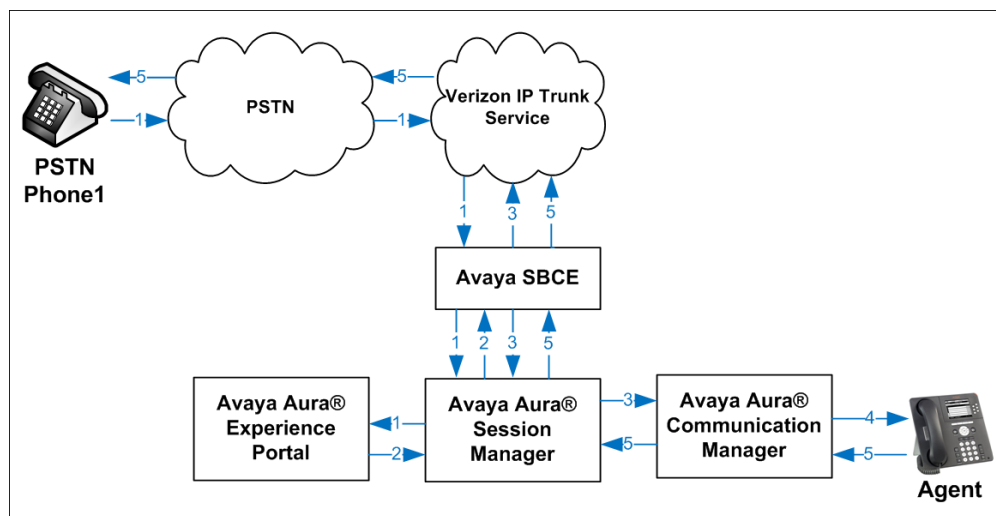
1. A PSTN phone originates a call to a Verizon Business IP Trunking service number.
2. The PSTN routes the call to the Verizon Business IP Trunking service network.
3. The Verizon Business IP Trunking service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs any necessary SIP header modifications and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Experience Portal.
6. Experience Portal matches the called party number to a VXML and/or CCXML application script, answers the call, and handles the call according to the directives specified in the application. In this scenario, the application sufficiently meets the caller's needs or requests, and thus the call does not need to be transferred to Communication Manager.



**Figure 5: Inbound Call Handling Entirely by Avaya Aura® Experience Portal**

The second call scenario illustrated below is an inbound call arriving on Experience Portal and transferred to Communication Manager without determining whether an agent is available or not.

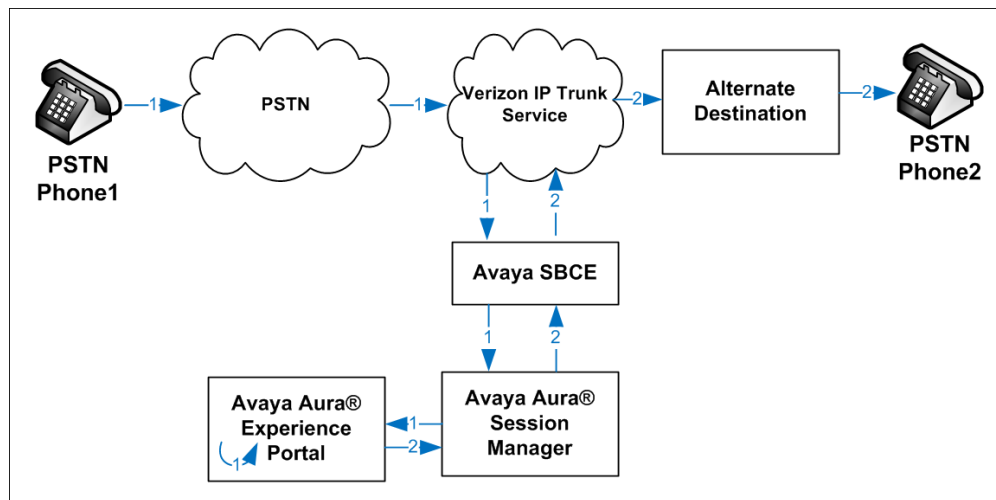
1. Same as the first five steps from the first call scenario.
2. In this scenario, when the caller selects an option requesting an agent, Experience Portal redirects the call by sending a SIP REFER to the Avaya SBCE.
3. The Avaya SBCE sends a SIP INVITE to the Communication Manager (via Session Manager) for the selected skill. In addition, the Avaya SBCE places the inbound call on hold.
4. Communication Manager routes the call to the agent.
5. When the agent answers, the Avaya SBCE takes the call off hold and the caller is connected to the agent.



**Figure 6: Avaya Aura® Experience Portal Transfers Call to Avaya Aura® Communication Manager**

The third call scenario illustrated below is an inbound call arriving on Experience Portal and forwarded to an 8YY number or any other PSTN number over the Verizon network.

1. Same as the first six steps from the first call scenario.
2. In this scenario, the application is sufficient to meet the caller's requests, and thus the call needs to be forwarded to another PSTN number. Based upon the selection, Experience Portal forwards the call to an appropriate PSTN number which can be a regular PSTN number or an 8YY number.



**Figure 7: Inbound Call forwarded by Experience Portal to another PSTN number**



## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.0.0.0-R018x.00.0.822.0
Avaya Aura® System Manager	8.0.0.0.098174
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Session Border Controller for Enterprise	7.2.2.0-11-15522
Avaya Aura® Messaging	7.0 SP 0
Avaya Aura® Experience Portal	7.2.0.0.1117
Avaya Aura® Media Server	8.0.0.117
G450 Gateway	40.10.0
Avaya 96X1– Series Telephones (SIP)	R7.1.3.0.11
Avaya 96X1– Series Telephones (H.323)	R6.66.04
Avaya J100 – Series Telephones (SIP)	3.0.0.2.2
Avaya Equinox™ for Windows	3.4.0.152.46
Avaya 2400 – Series Digital Telephones	N/A
Ventafax	7.9

**Table 1: Equipment and Software Used in the Sample Configuration**

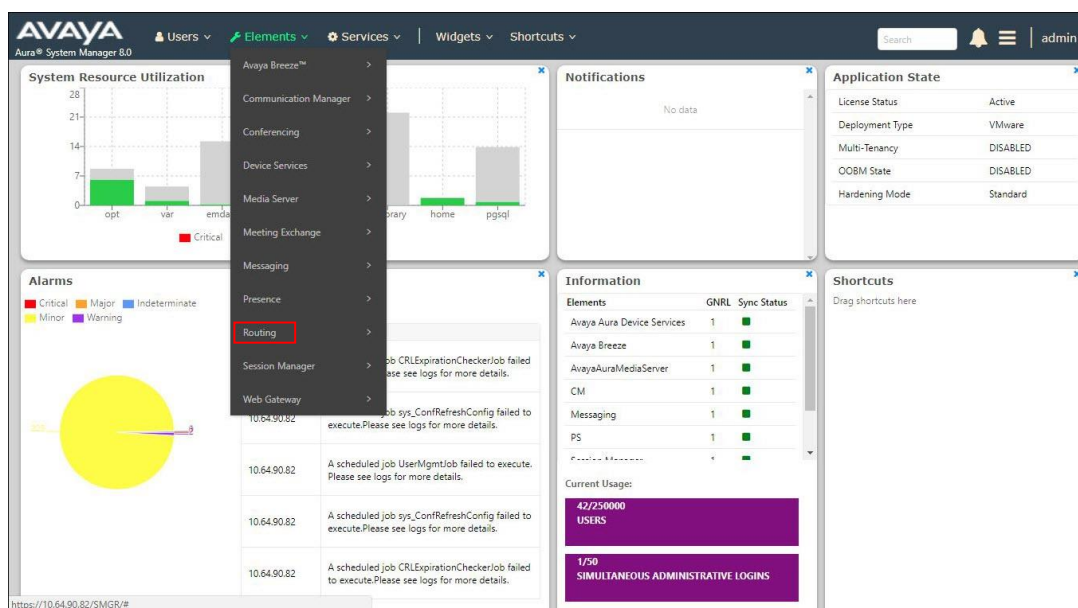
## 5. Configure Avaya Aura® Session Manager

**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, Experience Portal, the Avaya SBCE, and Messaging.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, Experience Portal, and Messaging, as well as the SIP trunks between the Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, Experience Portal, 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, 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.



## 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.

**Location Details** Commit Cancel

**General**

\* Name:

Notes:

**Dial Plan Transparency in Survivable Mode**

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

**Per-Call Bandwidth Parameters**

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

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

\* Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

**Alarm Threshold**

Overall Alarm Threshold:  %

Multimedia Alarm Threshold:  %

\* Latency before Overall Alarm Trigger:  Minutes

\* Latency before Multimedia Alarm Trigger:  Minutes

**Location Pattern**

0 Items Filter: Enable

IP Address Pattern	Notes
--------------------	-------

## 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

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 displays the 'Adaptation Details' configuration page in the Avaya Aura Administration console. The left-hand navigation pane shows the 'Routing' section expanded, with 'Adaptations' selected. The main content area is titled 'Adaptation Details' and includes a 'General' tab. Key configuration fields include:
 

- Adaptation Name:** CM-TG1-VzIPT
- Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

 Below these fields is a table for defining parameters. It has two columns: 'Name' and 'Value'. Two parameters are listed:
 

Name	Value
fromto	true
osrcd	avayalab.com

 At the bottom of the page, there is a field for 'Egress URI Parameters' which is currently empty, and a 'Notes' field containing the text '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:** 7329450231 is a DNIS string sent in the Request URI by the Verizon Business IP Trunking service that is associated with Communication Manager extension 12001.

- Enter **7329450231** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.
- Enter **12001** 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**

AddRemove

4 ItemsFilter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*7329450	*10	*10		*5		destination		Verizon DIDs
<input type="checkbox"/>	*7329450228	*10	*10		*10	12001	destination		
<input type="checkbox"/>	*7329450229	*10	*10		*10	12000	destination		analog fax
<input type="checkbox"/>	*7329450231	*10	*10		*10	12001	destination		

Select : All, None

CommitCancel

### 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 6.8.1.2**) 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 Routing

Adaptation Details

Commit Cancel

Help ?

General

\* Adaptation Name: SBC1-Adaptation for Verizon

\* Module Name: VerizonAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
eRHdrs	"AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector, P-Location, AV-Secure-Indication"
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

**Digit Conversion for Outgoing Calls from SM**

Add Remove

2 Items

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+	*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.
- Experience Portal (**Section 5.4.6**) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Experience Portal.



**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., **10.64.91.81**).
- **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. On the left, a sidebar lists navigation options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into two sections: 'General' and 'Monitoring'. The 'General' section includes fields for Name (Session Manager), IP Address (10.64.91.81), SIP FQDN, Type (Session Manager), Location (Main), Outbound Proxy, Time Zone (America/Fortaleza), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' section includes SIP Link Monitoring (Use Session Manager Configuration) and CRLF Keep Alive Monitoring (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**.

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

**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., **10.64.91.75**).
- **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**.

**SIP Entity Details** Commit Cancel Help ?

**General**

\* **Name:** CM-TG1

\* **FQDN or IP Address:** 10.64.91.75

**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:**

**Securable:** ☐

**Call Detail Recording:** none

**Loop Detection**

**Loop Detection Mode:** Off

**Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

**CRLF Keep Alive Monitoring:** Use Session Manager Configuration

**Supports Call Admission Control:** ☐

**Shared Bandwidth Manager:** ☐

**Primary Session Manager Bandwidth Association:**

**Backup Session Manager Bandwidth Association:**

### 5.4.3 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 8.5.1**).
- **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.

### 5.4.6 Avaya Aura® Experience Portal SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **ExperiencePortal**).
- **FQDN or IP Address** – Enter the IP address of Experience Portal (e.g., **10.64.91.90**).
- **Type** – Select **Voice Portal**.
- **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**).
- Session Manager to Experience Portal (**Section 5.5.5**).

**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**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
SM to CM TG1	SessionManager	TLS	5081	CM-TG1	5081	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

### 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**.

### 5.5.5 Entity Link to Avaya Aura® Experience Portal

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 ExperiencePortal**).
- **SIP Entity 1 Port** – Enter **5061**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.6** for the Experience Portal entity (e.g., **ExperiencePortal**).
- **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. On the left is a navigation menu with 'Time Ranges' selected. The main area has a breadcrumb 'Home / Elements / Routing / Time Ranges' and a 'Help ?' link. Below the breadcrumb are buttons: 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. A table lists one item with the following details:

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Below the table, it says 'Select : All, None' and 'Filter: Enable'.

## 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 Messaging (**Section 5.7.2**).
- Inbound calls to Experience Portal (**Section 5.7.3**).
- Outbound calls to Verizon/PSTN (**Section 5.7.4**).

### 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.

**Routing Policy Details** [Commit] [Cancel] [Help ?]

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM-TG1	10.64.91.75	CM	Trunk Group 1 - CM to Vz-IPT

- 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** [Select] [Cancel]

**SIP Entities**

14 Items [Filter: Enable]

Name	FQDN or IP Address	Type	Notes
Aura Messaging	10.64.91.84	Messaging	Aura Messaging
Breeze	10.64.91.18	Avaya Breeze	
CM-TG1	10.64.91.75	CM	Trunk Group 1 - CM to Vz-IPT
CM-TG2	10.64.91.75	CM	Trunk Group 2 - Vz-Toll-Free inbound
CM-TG3	10.64.91.75	CM	Trunk Group 3 - CM to Enterprise
CM-TG4	10.64.91.75	CM	Trunk Group 4 - ATT IPTF
CM-TG5	10.64.91.75	CM	Trunk Group 5 - ATT IPFR
ExperiencePortal	10.64.91.90	Voice Portal	
IPS00	10.64.19.70	Other	IP Office
Presence	10.64.91.18	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-ATT	10.64.91.40	SIP Trunk	SBCE for AT&T testing
SBCE-Toll Free	10.64.91.41	SIP Trunk	SBCE for IPTF testing

Select : None

- Step 5** - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**.
- Step 6** - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 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.

**Routing Policy Details** Commit Cancel Help ?

**General**

\* **Name:**

**Disabled:** ☐

\* **Retries:**

**Notes:**

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM-TG1	10.64.91.75	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

### 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 Inbound Routing to Experience Portal

This routing policy is for inbound calls to Experience Portal. Repeat the steps in **Section 5.7.1** with the following differences:

- Enter a descriptive **Name** (e.g., **To Experience Portal**), 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 5.4.6** for Experience Portal (e.g., **ExperiencePortal**).

### 5.7.4 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 **7329450231**. Note – The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 732-945-0xxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* **Pattern:**

\* **Min:**

\* **Max:**

**Emergency Call:** ☐

**SIP Domain:**

**Notes:**

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

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

Select : All, None

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

**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 VzIPCC 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 Experience Portal	<input type="checkbox"/>	ExperiencePortal	
<input type="checkbox"/>	To IP500	<input type="checkbox"/>	IP500	
<input type="checkbox"/>	To SBC1	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	To SBC2	<input type="checkbox"/>	SBC2	
<input type="checkbox"/>	To SBCE-ATT	<input type="checkbox"/>	SBCE-ATT	
<input type="checkbox"/>	to SBCE TollFree	<input type="checkbox"/>	SBCE-Toll Free	

Select : All, None

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

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

## 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 5.7.4** (e.g., **To SBC1**).

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern: +

\* Min: 10

\* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: Outbound E.164 Public Numbers

**Originating Locations and Routing Policies**

Add Remove

5 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"/>	RemoteAccess	Remote Access from SBCE1	To SBC2	1	<input type="checkbox"/>	SBC2	
<input type="checkbox"/>	RemoteAccess	Remote Access from SBCE1	To SBC1	0	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	Main	Avaya SIL	To SBC2	1	<input type="checkbox"/>	SBC2	
<input type="checkbox"/>	Main	Avaya SIL	To SBC1	0	<input type="checkbox"/>	SBC1	
<input type="checkbox"/>	CM-TG-5	CM-TG-5	To SBCE-ATT	0	<input type="checkbox"/>	SBCE-ATT	

Select : All, None

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

**Routing** 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

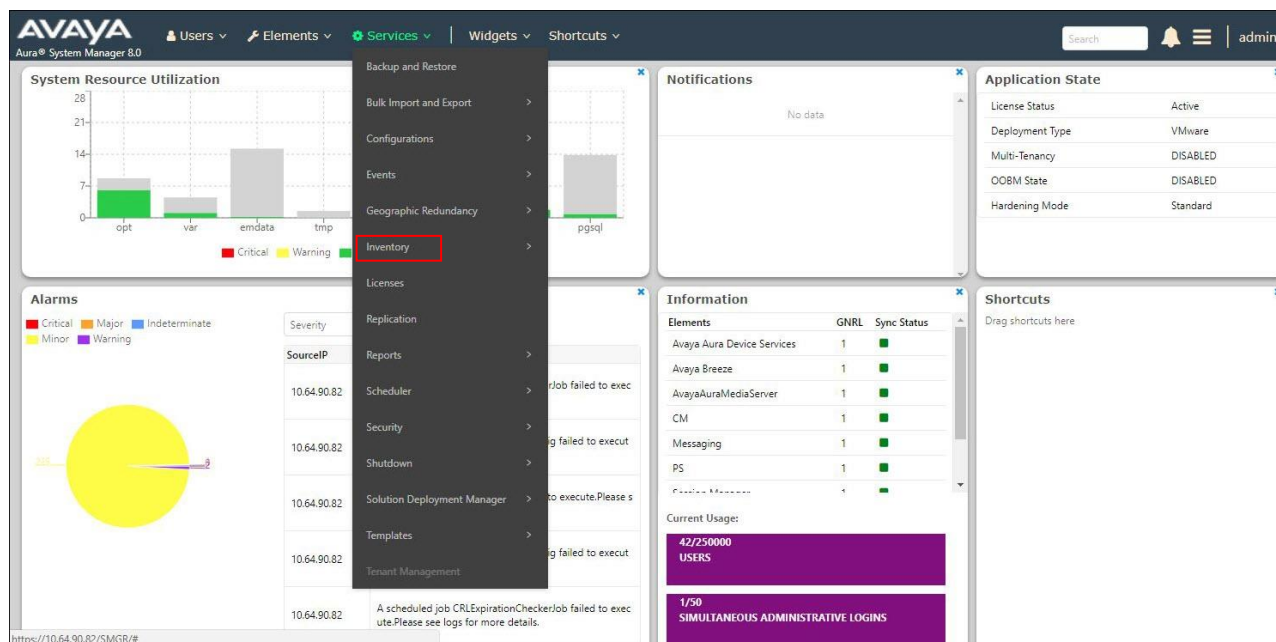
Select : All, None

## 5.9. Verify TLS Certificates – Session Manager

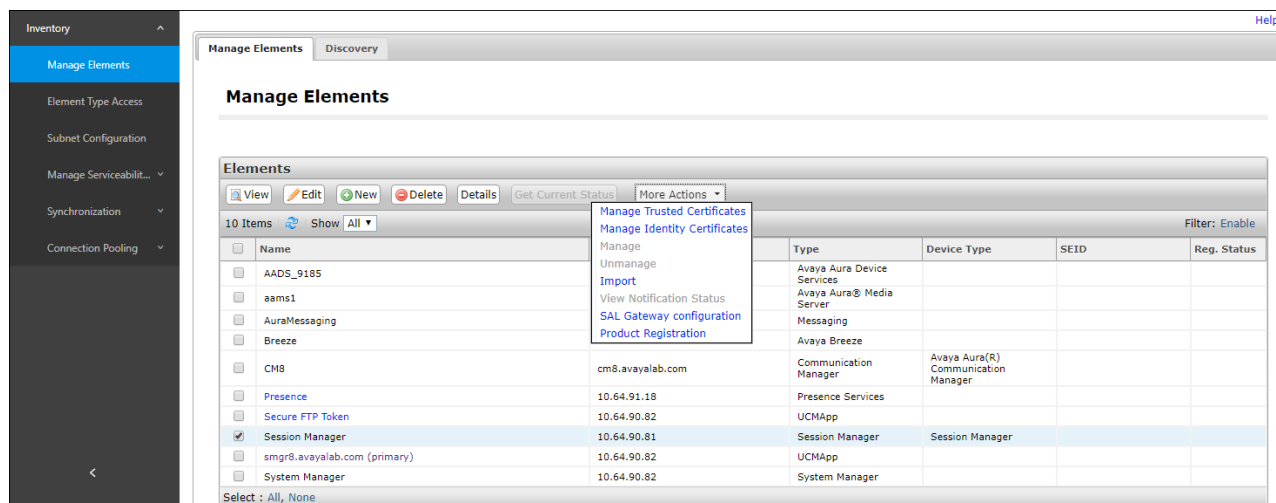
**Note** – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

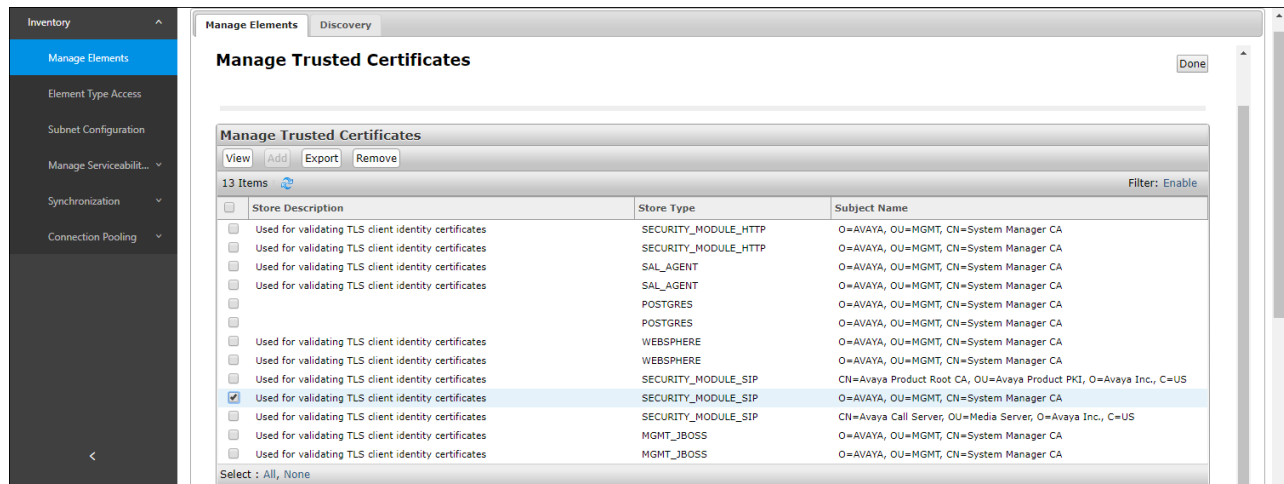
**Step 1** - From the **Home** screen, under the **Services** heading, select **Inventory**.



**Step 2** - In the left pane under **Inventory**, click on **Manage Elements** and select the Session Manager element, e.g., **SessionManager**. Click on **More Actions** → **Manage Trusted Certificates**.

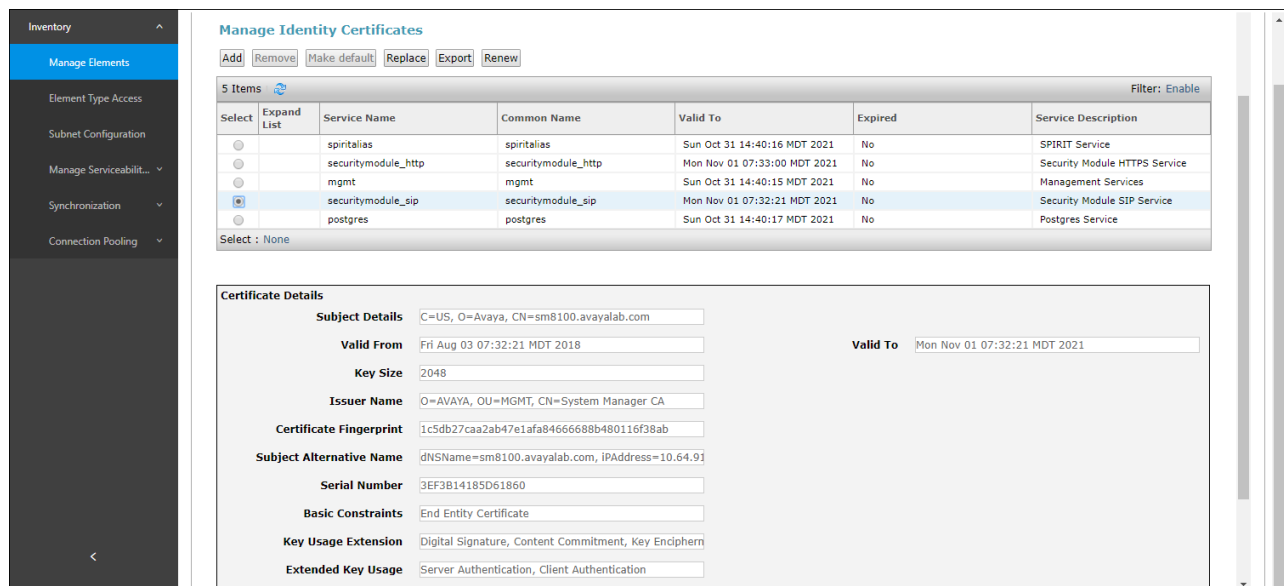


**Step 3** - Verify the **System Manager Certificate Authority** certificate is listed in the trusted store, **SECURITY\_MODULE\_SIP**. Click **Done** to return to the previous screen.



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

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



## 6. Configure Avaya Aura® Communication Manager Release 8.0

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		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		

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

display system-parameters customer-options		Page 5 of 12
OPTIONAL FEATURES		
Emergency Access to Attendant? y	<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, 5, 7** and **8** for Communication Manager extensions.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code **\*xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 6.8**.

change dialplan analysis										Page 1 of 12	
DIAL PLAN ANALYSIS TABLE											
Location: all											
Percent Full: 1											
	Dialed	Total	Call		Dialed	Total	Call		Dialed	Total	Call
	String	Length	Type		String	Length	Type		String	Length	Type
1		5	ext								
2		5	ext								
3		5	ext								
4		5	ext								
5		5	ext								
60		3	ext								
66		2	fac								
7		5	ext								
8		5	ext								
9		1	fac								
*		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 **10.64.91.81**).
- Media Server (e.g., **AMS** and **10.64.91.80**). 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	10.64.91.80			
SM	10.64.91.81			
default	0.0.0.0			
procr	10.64.91.75			
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
Network Region: 1                                           Allow H.248 Gateways? y
                                                           Gatekeeper Priority: 5

                                                           IPV4 PARAMETERS
Node Name: procr                                           IP Address: 10.64.91.75

Subnet Mask: /24
```

## 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-aescml28-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 : 15360:Kbits			
Maximum Call Rate for Priority Direct-IP Multimedia : 15360: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 6.6.1** with the following changes:

- Provision the codecs in the order shown below.
- On **Page 2**, set **FAX Mode** to **t.38-G711-fallback**, **ECM** to **y**, and **FB-Timer** to **4**. See **Section 2.2** for limitations regarding fax.

<b>change ip-codec-set 2</b>		Page 1 of 2	
IP CODEC SET			
Codec Set: 2			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: <b>G.729A</b>	<b>n</b>	<b>2</b>	<b>20</b>
2: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>
3:			
Media Encryption		Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80			
2: none			
<b>change ip-codec-set 2</b>		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 G450 Media Gateway and Avaya Media Server are in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Verizon testing.

### 6.7.1 IP Network Region 1 – Local CPE Region

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

- Enter a descriptive name (e.g., **Enterprise**).
- Enter the enterprise domain (e.g., **avayalab.com**) in the **Authoritative Domain** field (see **Section 5.1**).

- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
<b>Region: 1</b>		
Location: 1	Authoritative Domain: avayalab.com	
Name: Enterprise	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	Inter-region IP-IP Direct Audio: yes	
UDP Port Max: 3329	IP Audio Hairpinning? n	
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS		RSVP Enabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

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

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

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

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

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **2** in the **dst rgn** column, enter **2** for the codec set (this means region 1 is permitted to talk to region 2 and it will use codec set 2 to do so). The **direct WAN** and **Units** columns will self-populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

change ip-network-region 1										Page	4	of	20
Source Region: 1		Inter Network Region Connection Management								I			M
										G	A		t
dst 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 6.7.1** 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	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 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**).

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

Group Number: 1                      Group Type: sip          CDR Reports: y
  Group Name: Verizon IPT             COR: 1                 TN: 1          TAC: *01
  Direction: two-way                 Outgoing Display? n
Dial Access? n                      Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 10
```

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

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

```
add trunk-group 1                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

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

Disconnect Supervision - In? y Out? y

XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n

Caller ID for Service Link Call to H.323 1xC: station-extension
```



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

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

<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**).
- Set **Convert 180 to 183 for Early Media** to **y**. Verizon prefers to have Communication Manager send 183 with SDP rather than a 180 with SDP.

**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
	<b>Convert 180 to 183 for Early Media? y</b>
	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 12001					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	12001	1	17329450231	11	Total Administered: 46
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	
5	50	1	173294	11	

## 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., **5**, **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	1	11		5	Total Administered: 11
5	5	3		5	Maximum Entries: 540
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		
									Intw		
1: 3		0							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	
										Numbering LAR	
										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 50xxx, therefore enter **50**.
- **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	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
50	5	5	3	lev0		n	

## 6.14. Avaya G450 Media Gateway Provisioning

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

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

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

**Step 2** - Enter the **show system** command and copy down the G450 serial number (e.g., **11N507727041**).

**Step 3** - Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.64.91.75**, see **Section 6.5**).

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

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

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

- Set **Type** = **g450**
- Set **Name** = a descriptive name (e.g., **G450-1**)
- Set **Serial Number** = the serial number copied from **Step 2** (e.g., **11N507727041**)
- Set the **Link Encryption Type** parameter as desired (**any-ptls/tls** was used in the reference configuration)

Set **Network Region** = 1

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

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

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

                                MEDIA GATEWAY 1

                                Type: g450
                                Name: G450-1
                                Serial No: 11N507727041
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: 40 .10 .0 /1
MGP IPV4 Address: 10.64.91.91
MGP IPV6 Address:
Controller IP Address: 10.64.91.75
MAC Address: b4:b0:17:90:61:d8

Mutual Authentication? optional
```

## 6.15. Avaya Aura® Media Server Provisioning

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

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

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

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

**Step 2** - On the Media Server Element Manager, navigate to **Home → System Configuration → Signaling Protocols → SIP → Node and Routes** and add the Communication Manager Procr interface IP address (e.g., **10.64.91.75**, 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 **5061**.
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 6.6.1**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.



```

add signaling-group 60
                                SIGNALING GROUP
                                Page 1 of 2

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: 5061      Far-end Listen Port: 5061
                                Far-end Network Region: 1

Far-end Domain: 10.64.91.80

```

**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
                                MEDIA SERVER
                                Page 1 of 1

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.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) with the 'Administration' tab selected. The left sidebar shows the 'Security' menu, and the main content area displays the 'Trusted Certificates' page. This page provides management of trusted security certificates and lists the following 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"/> SystemManager8CA.crt	System Manager CA	System Manager CA	Sun Jul 30 2028	A 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_sscca_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

Buttons: Display, Add, Remove, Copy, Help

© 2001-2018 Avaya Inc. All Rights Reserved.

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

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) with the 'Administration' tab selected. The left sidebar shows the 'Security' menu, and the main content area displays the 'Server/Application Certificates' page. This page provides management of server/application certificates and lists the following 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	cm8.avayalab.com	System Manager CA	Mon Nov 01 2021	C R
<input type="radio"/> server.crt	192.11.13.6	System Manager CA	Sun Jul 30 2028	
<input type="radio"/> server.crt	192.11.13.6	SIP Product Certificate Authority	Tue Jan 28 2025	W

Buttons: Display, Add, Remove, Copy, Help

© 2001-2018 Avaya Inc. All Rights Reserved.

## 7. Avaya Aura® Experience Portal

These Application Notes assume that the necessary Experience Portal licenses have been installed and basic Experience Portal administration has already been performed. Consult [13] and [14] for further details if necessary.

### 7.1. Background

Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. A single “server configuration” was used in the reference configuration. This consisted of a single MPP and EPM, running on a VMware environment, including an Apache Tomcat Application Server (hosting the Voice XML (VXML) and/or Call Control XML (CCXML) application scripts), that provide the directives to Experience Portal for handling the inbound calls.

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DNIS number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled, and disconnects the call<sup>2</sup>.

For the sample configuration described in these Application Notes, a simple VXML test application was used to exercise various SIP call flow scenarios with the Verizon Business IP Trunk service. In production, enterprises can develop their own VXML and/or CCXML applications to meet specific customer self-service needs, or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes.

---

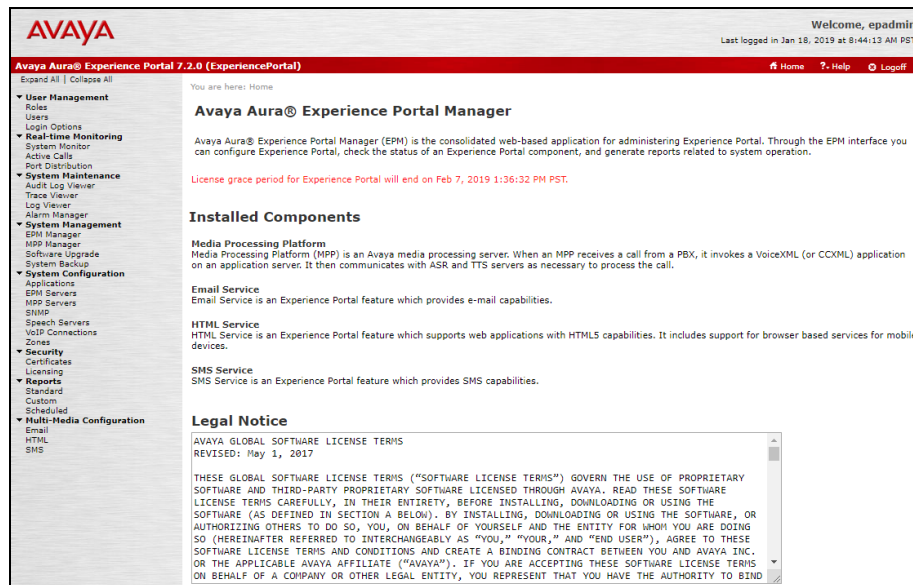
<sup>2</sup> An application may be configured with “inbound default” as the called number, to process all inbound calls that do not match any other application references.

## 7.2. Logging In and Licensing

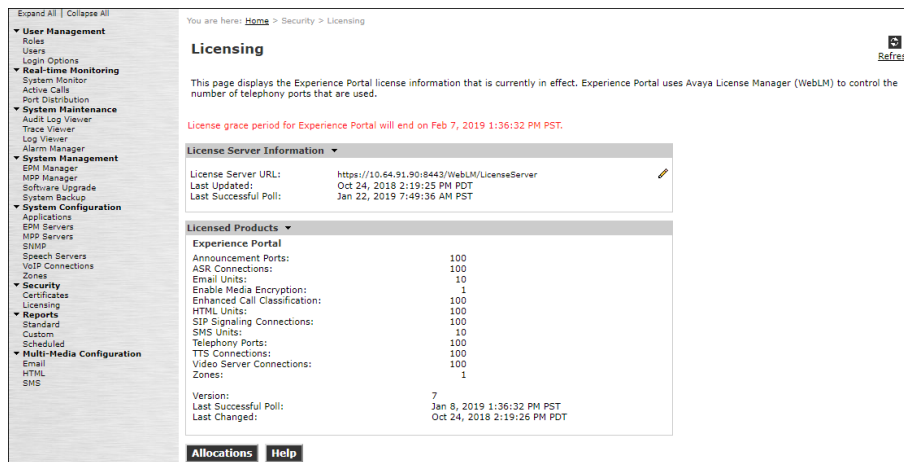
This section describes the steps on Experience Portal for administering a SIP connection to the Session Manager.

**Step 1** - Launch a web browser, enter `http://<IP address of the Avaya EPM server>/` in the URL, log in with the appropriate credentials and the following screen is displayed.

**Note** – All page navigation described in the following sections will utilize the menu shown on the left pane of the screenshot below.



**Step 2** - In the left pane, navigate to **Security**→**Licensing**. On the **Licensing** page, verify that Experience Portal is properly licensed. If required licenses are not enabled, contact an authorized Avaya account representative to obtain the licenses.



## 7.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager (**Section 5.5.5**).

**Step 1** - In the left pane, navigate to **System Configuration**→**VoIP Connections**. On the **VoIP Connections** page, select the **SIP** tab and click **Add** to add a SIP trunk.

**Note** – Only *one* SIP trunk can be active at any given time on Experience Portal.

Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls
SM8	Yes	TLS	10.64.91.81	5061	5061	avayalab.com	10

**Step 2** - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **SM8**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TLS**.
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = **10.64.91.81** (the IP address of the Session Manager signaling interface defined in **Section 5.4.1**).
  - **Port** = **5061**
  - **Priority** = **0** (default)
  - **Weight** = **0** (default)
- **Listener Port** – Set to **5061**.
- **SIP Domain** – Set to **avayalab.com** (see **Section 5.1**).
- **Consultative Transfer** – Select **INVITE with REPLACES**.
- **SIP Reject Response Code** – Select **ASM (503)**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = **Yes**
- **Encryption Algorithm** = **AES\_CM\_128**
- **Authentication Algorithm** = **HMAC\_SHA1\_80**
- **RTCP Encryption Enabled** = **No**
- **RTP Authentication Enabled** = **Yes**
- Use default values for all other fields.
- Click **Save**.

Expand All | Collapse All

- User Management
- Real-time Monitoring
- System Maintenance
- System Management
- ▼ System Configuration
  - Applications
  - EPM Servers
  - MPP Servers
  - SNMP
  - Speech Servers
  - VoIP Connections
  - Zones
- Security
- Reports
- Multi-Media Configuration

You are here: [Home](#) > [System Configuration](#) > [VoIP Connections](#) > [Change SIP Connection](#)

## Change SIP Connection

Use this page to change the configuration of a SIP connection.

Name: SM8

Enable: ☒ Yes ☐ No

Proxy Transport: **TLS**

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.64.91.81	5061	0	0	Remove

[Additional Proxy Server](#)

Listener Port: 5061

SIP Domain: avayalab.com

P-Asserted-Identity:

Maximum Redirection Attempts: 2

Consultative Transfer: ☒ INVITE with REPLACES ☐ REFER

SIP Reject Response Code: ☒ ASM (503) ☐ SES (480) ☐ Custom 503

### SIP Timers

T1: 250 milliseconds

T2: 2000 milliseconds

B and F: 4000 milliseconds

### Call Capacity

Maximum Simultaneous Calls: 10

☒ All Calls can be either inbound or outbound

☐ Configure number of inbound and outbound calls allowed

### SRTP

Enable: ☒ Yes ☐ No

Encryption Algorithm: ☒ AES\_CM\_128 ☐ NONE

Authentication Algorithm: ☒ HMAC\_SHA1\_80 ☐ HMAC\_SHA1\_32

RTCP Encryption Enabled: ☐ Yes ☒ No

RTP Authentication Enabled: ☒ Yes ☐ No

**Add**

### Configured SRTP List

<No SRTP List>

## 7.4. Speech Servers

The installation and administration of the ASR and TSR Speech Servers are beyond the scope of this document. Some of the values shown below were defined during the Speech Server installations. Note that in the reference configuration the ASR and TTS servers used the same IP address.

Expand All | Collapse All

- User Management
- Real-time Monitoring
- System Maintenance
- System Management
- ▼ System Configuration
  - Applications
  - EPM Servers
  - MPP Servers
  - SNMP
  - Speech Servers
  - VoIP Connections
  - Zones
- Security
- Reports
- Multi-Media Configuration

You are here: [Home](#) > [System Configuration](#) > [Speech Servers](#)

## Speech Servers

This page displays the list of Automated Speech Recognition (ASR) and Text-to-Speech (TTS) servers that Experience Portal communicates with.

**ASR** **TTS**

	Name	Enable	Network Address	Engine Type	MRCP	Base Port	Total Number of Licensed ASR Resources	Languages
<input type="checkbox"/>	LVASR	Yes	10.64.101.83	LumenVox	MRCP V2 TCP	5060	10	en-US

**Add** **Delete** **Customize** **Help**

## 7.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. In the sample configuration, the applications were co-resident on one Experience Portal server, with IP Address 10.64.90.91.

**Step 1** - In the left pane, navigate to **System Configuration**→**Applications**. On the **Applications** page (not shown), click **Add** to add an application and configure as follows:

- **Name** – Set to a descriptive name (e.g., **Test-ccxml**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Select **VoiceXML**, **CCXML**, or **CCXML/VoiceXML** according to the application type.
- **VoiceXML** and/or **CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Experience Portal test application on a single server is referenced.
- **Speech Servers ASR** and **TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Set to **Inbound**.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message, and click **Add**. In the sample configuration illustrated in these Application Notes, the dialed Verizon IP Trunk DID number 732-945-0232 was used. Repeat to define additional called party numbers as needed. Inbound Verizon Business calls with these called party numbers will be handled by the application defined in this section.

**Change Application**

Use this page to change the configuration of an application.

Name: Test-ccxml

Enable: ☒ Yes ☐ No

Type: CCXML

Reserved SIP Calls: ☒ None ☐ Minimum ☐ Maximum

Requested:

URI

☒ Single ☐ Fail Over ☐ Load Balance

CCXML URL:  **Verify**

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

**Speech Servers**

ASR: LumenVox

Languages: <None>

Selected Languages: en-US

TTS: LumenVox

Voices: <None>

Selected Voices: en-US Chris M

**Application Launch**

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:  **Add**

55556  
7329450232  
8668512649 **Remove**

## 7.6. MPP Servers and VoIP Settings

This section illustrates the procedure for viewing or changing the MPP Settings. In the sample configuration, the MPP Server is co-resident on a single server with the Experience Portal Management server (EPM).

**Step 1** - In the left pane, navigate to **System Configuration**→**MPP Servers** and the following screen is displayed. Click **Add**.

Expand All | Collapse All

You are here: [Home](#) > System Configuration > MPP Servers

### MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Experience Portal system. When an MPP receives a call from a PBX, it invokes a VoiceXML application on an application server and communicates with ASR and TTS servers as necessary to process the call.

Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/> mpp1	10.64.91.90	<Default>	<Default>	<Default>	11	Use MPP Settings

**Add** **Delete**

**MPP Settings** **Browser Settings** **Video Settings** **VoIP Settings** **Help**

**Step 2** - Enter any descriptive name in the **Name** field (e.g., **mpp1**) and the IP address of the MPP server in the **Host Address** field and click **Continue** (not shown).

**Step 3** - The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.

Expand All | Collapse All

You are here: [Home](#) > System Configuration > [MPP Servers](#) > Change MPP Server

### Change MPP Server

Use this page to change the configuration of an MPP. Take care when changing the MPP Trace Logging Thresholds. Do not set Trace Levels to Finest if your Experience Portal system has heavy call traffic. The system might experience performance issues if Trace Levels are set to Finest. Set Trace Levels to Finest only when you are troubleshooting the system.

Name: mpp1

Host Address: 10.64.91.90

Network Address (VoIP): <Default>

Network Address (MRCP): <Default>

Network Address (AppSvr): <Default>

Maximum Simultaneous Calls: 11

Restart Automatically: ☒ Yes ☐ No

#### MPP Certificate

```
Owner: CN=ep.avayalab.com,O=Avaya,OU=EPM
Issuer: CN=ep.avayalab.com,O=Avaya,OU=EPM
Serial Number: 89f44cd176674542
Signature Algorithm: SHA256withRSA
Valid from: October 17, 2018 11:03:28 AM PDT until October 14, 2028 11:03:28 AM PDT
Certificate Fingerprints
MD5: dd:26:1a:d3:d1:62:d3:04:55:40:1b:98:0b:38:44:46
SHA: 4d:26:ba:2f:55:8d:3b:5f:8e:d8:6f:ee:7f:48:49:22:38:79:ae:bf
SHA-256: 17:6d:d2:9a:9b:ee:e3:35:da:67:c2:99:38:e6:14:03:c7:84:1d:94:a9:a0:f9:ac:66:57:da:28:43:59:ae:c7
Subject Alternative Names
DNS Name: ep
DNS Name: ep.avayalab.com
IP Address: 10.64.91.90
```

Categories and Trace Levels ▾

**Save** **Apply** **Cancel** **Help**



**Step 4** - Click **VoIP Settings** tab on the screen displayed in **Step 1**, and the following screen is displayed.

- In the Port Ranges section, default ports were used.

Expand All | Collapse All

▶ User Management  
▶ Real-time Monitoring  
▶ System Maintenance  
▶ System Management  
▼ System Configuration  
  Applications  
  EPM Servers  
  MPP Servers  
  SNMP  
  Speech Servers  
  VoIP Connections  
  Zones  
▶ Security  
▶ Reports  
▶ Multi-Media Configuration

You are here: [Home](#) > [System Configuration](#) > [MPP Servers](#) > VoIP Settings

### VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.

Port Ranges	
	Low High
UDP:	11000 30999
TCP:	31000 33499
MRCP:	34000 36499
H.323 Station:	37000 39499

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format:

- In the Codecs section set:
  - Set **Packet Time** to **20**.
  - Verify the **G729 Codec** is enabled.
  - Set **G729 Discontinuous Transmission** to **No** (G.729A).
  - Set the **Offer Order** to the preferred codec. In the sample configuration, **G729** is the first codec, followed by **G711uLaw**, then **G711aLaw**.
- Use default values for all other fields.

**Step 5** - Click on **Save**.

Expand All | Collapse All

▶ User Management  
▶ Real-time Monitoring  
▶ System Maintenance  
▶ System Management  
▼ System Configuration  
  Applications  
  EPM Servers  
  MPP Servers  
  SNMP  
  Speech Servers  
  VoIP Connections  
  Zones  
▶ Security  
▶ Reports  
▶ Multi-Media Configuration

Station:

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format:

Codecs

Offer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G729	1
<input checked="" type="checkbox"/>	G711uLaw	2
<input checked="" type="checkbox"/>	G711aLaw	3

Packet Time:  milliseconds

G729 Discontinuous Transmission: ☐ Yes ☒ No

Answer

Enable	Codec	Order
<input checked="" type="checkbox"/>	G711uLaw	1
<input checked="" type="checkbox"/>	G711aLaw	1
<input checked="" type="checkbox"/>	G729	1

G729 Discontinuous Transmission: ☐ Yes ☐ No ☒ Either

G729 Reduced Complexity Encoder: ☒ Yes ☐ No

QoS Parameters

	VLAN	Diffserv
H.323:	6	46
SIP:	6	46
RTSP:	6	46

## 7.7. Configuring RFC2833 Event Value Offered by Experience Portal

The configuration change example noted in this section is not required for any of the call flows illustrated in these Application Notes. For incoming calls from Verizon services to Experience Portal, Verizon specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Experience Portal answers, the SDP from Experience Portal matches this Verizon offered value.

When Experience Portal sends an INVITE with SDP as part of an INVITE-based transfer (e.g., bridged transfer), Experience Portal offers the SDP. By default, Experience specifies the value 127 for the RFC2833 telephone-events. Optionally, the value that is offered by Experience Portal can be changed, and this section outlines the procedure that can be performed by an Avaya authorized representative.

- Access Experience Portal via the command line interface.
- Navigate to the following directory: /opt/Avaya/ ExperiencePortal /MPP/config
- Edit the file mppconfig.xml.
- Search for the parameter “mpp.sip.rfc2833.payload”. If there is no such parameter specified, add a line such as the following to the file, where the value 101 is the value to be used for the RFC2833 events. If the parameter is already specified in the file, simply edit the value assigned to the parameter.  
`<parameter name="mpp.sip.rfc2833.payload">101</parameter>`
- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

After saving the file with the change, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the **Restart** button available via the Experience Portal GUI at **System Management → MPP Manager**.

Note that the **State** column shows when the MPP is running after the restart.

The screenshot shows the MPP Manager GUI. The left sidebar contains a navigation menu with options like User Management, Real-time Monitoring, System Maintenance, System Management, EPM Manager, MPP Manager, Software Upgrade, System Backup, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled 'MPP Manager (Jan 22, 2019 9:07:05 AM PST)' and includes a 'Refresh' button. Below the title, there is a table with columns: Server Name, Mode, State, Config, Auto Restart, Restart Schedule (Today, Recurring), and Active Calls (In, Out). The 'State' column is highlighted with a red box. The table shows one entry for 'mpp1' with 'Online' mode and 'Running' state. Below the table, there are sections for 'State Commands' (Start, Stop, Restart, Reboot, Halt, Cancel) and 'Mode Commands' (Offline, Test, Online). A 'Restart/Reboot Options' section is also present with radio buttons for 'One server at a time' and 'All servers'.

Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
					Today	Recurring	In	Out
<input checked="" type="checkbox"/> mpp1	Online	Running	OK	Yes	No	None	0	0

## 8. Configure Avaya Session Border Controller for Enterprise Release 7.2

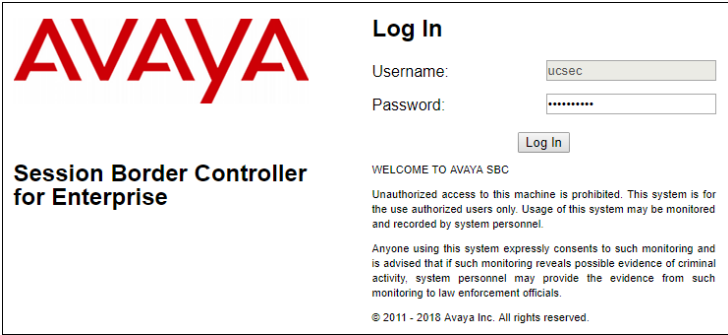
These Application Notes assume that the installation of the Avaya SBCE and the assignment of all IP addresses have already been completed, including the management IP address.

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. Enter the **Username** and click on **Continue**.



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left, the Avaya logo is in red, and below it, the text "Session Border Controller for Enterprise" is in black. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, there is a "WELCOME TO AVAYA SBC" message, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Below this is a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, it says "© 2011 - 2018 Avaya Inc. All rights reserved."

Enter the password and click on **Log In**.



This screenshot is similar to the previous one, but the "Username:" input field now contains the text "ucsec". Below it, the "Password:" label is followed by a password input field filled with asterisks. A "Log In" button is now visible below the password field. The rest of the page content, including the Avaya logo, disclaimer, and copyright notice, remains the same.

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.

**Session Border Controller for Enterprise**

**Dashboard**

**Information**

System Time	09:40:19 AM MST	Refresh
Version	7.2.2.0-11-15522	
Build Date	Tue May 29 11:31:10 UTC 2018	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	12/21/2018 08:23:42 MST	
Failed Login Attempts	0	

**Installed Devices**

EMS
SBC1

**Active Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

SBC1 : Heartbeat Successful, Server is UP

## 8.1. 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	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
SBC1	10.64.90.50	7.2.2.0-11-15522	Commissioned						

**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																																							
<b>General Configuration</b> Appliance Name    SBC1 Box Type            SIP Deployment Mode   Proxy		<b>Device Configuration</b> HA Mode            No Two Bypass Mode   No		<b>Dynamic License Allocation</b> <table border="1"> <thead> <tr> <th></th> <th>Min License Allocation</th> <th>Max License Allocation</th> </tr> </thead> <tbody> <tr> <td>Standard Sessions</td> <td>10</td> <td>500</td> </tr> <tr> <td>Advanced Sessions</td> <td>10</td> <td>500</td> </tr> <tr> <td>Scopia Video Sessions</td> <td>10</td> <td>500</td> </tr> <tr> <td>CES Sessions</td> <td>10</td> <td>500</td> </tr> <tr> <td>Transcoding Sessions</td> <td>10</td> <td>500</td> </tr> <tr> <td>CLID</td> <td colspan="2">---</td> </tr> <tr> <td>Encryption Available: Yes</td> <td colspan="2"><input checked="" type="checkbox"/></td> </tr> </tbody> </table>		Min License Allocation	Max License Allocation	Standard Sessions	10	500	Advanced Sessions	10	500	Scopia Video Sessions	10	500	CES Sessions	10	500	Transcoding Sessions	10	500	CLID	---		Encryption Available: Yes	<input checked="" type="checkbox"/>												
	Min License Allocation	Max License Allocation																																					
Standard Sessions	10	500																																					
Advanced Sessions	10	500																																					
Scopia Video Sessions	10	500																																					
CES Sessions	10	500																																					
Transcoding Sessions	10	500																																					
CLID	---																																						
Encryption Available: Yes	<input checked="" type="checkbox"/>																																						
<b>Network Configuration</b> <table border="1"> <thead> <tr> <th>IP</th> <th>Public IP</th> <th>Network Prefix or Subnet Mask</th> <th>Gateway</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>1.1.1.2</td> <td>1.1.1.2</td> <td>255.255.255.0</td> <td>1.1.1.1</td> <td>B1</td> </tr> <tr> <td>10.64.91.48</td> <td>10.64.91.48</td> <td>255.255.255.0</td> <td>10.64.91.1</td> <td>A1</td> </tr> <tr> <td>10.64.91.49</td> <td>10.64.91.49</td> <td>255.255.255.0</td> <td>10.64.91.1</td> <td>A1</td> </tr> <tr> <td>10.64.91.50</td> <td>10.64.91.50</td> <td>255.255.255.0</td> <td>10.64.91.1</td> <td>A1</td> </tr> <tr> <td>192.168.80.44</td> <td>192.168.80.44</td> <td>255.255.255.128</td> <td>192.168.80.1</td> <td>B2</td> </tr> <tr> <td>192.168.80.92</td> <td>192.168.80.92</td> <td>255.255.255.128</td> <td>192.168.80.1</td> <td>B2</td> </tr> </tbody> </table>					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
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																																			
<b>DNS Configuration</b> Primary DNS        172.30.209.4 Secondary DNS DNS Location       DMZ DNS Client IP      1.1.1.2		<b>Management IP(s)</b> IP #1 (IPv4)        10.64.90.50																																					

## 8.2. 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.

### 8.2.1 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.

- Dashboard
- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
  - PPM Services
  - Domain Policies
  - TLS Management
    - Certificates**
    - Client Profiles
    - Server Profiles
  - Device Specific Settings

## Certificates

[Install](#) [Generate CSR](#)

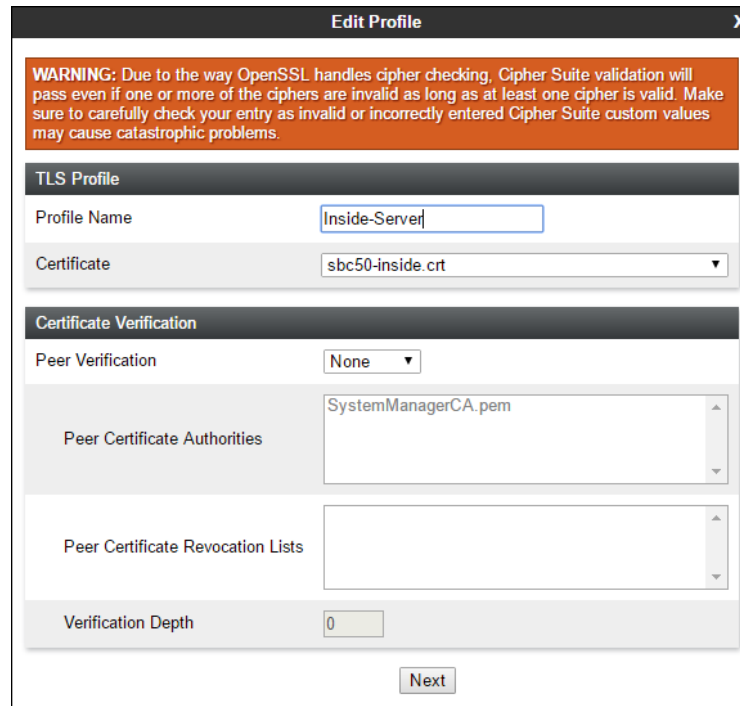
Certificates	
Installed Certificates	
sbcb50-inside.crt	<a href="#">View</a> <a href="#">Delete</a>
sbcb50-outside.crt	<a href="#">View</a> <a href="#">Delete</a>
sbcb92-out.crt	<a href="#">View</a> <a href="#">Delete</a>
sbcb92-outside.crt	<a href="#">View</a> <a href="#">Delete</a>
Installed CA Certificates	
SystemManagerCA.pem	<a href="#">View</a> <a href="#">Delete</a>
Installed Certificate Revocation Lists	
No certificate revocation lists have been installed.	
Installed Keys	
avaya.com.key	<a href="#">Delete</a>
sbcb50-inside.key	<a href="#">Delete</a>
sbcb50-outside.key	<a href="#">Delete</a>
sbcb92-out.key	<a href="#">Delete</a>
sbcb92-outside.key	<a href="#">Delete</a>

## 8.2.2 Server Profiles

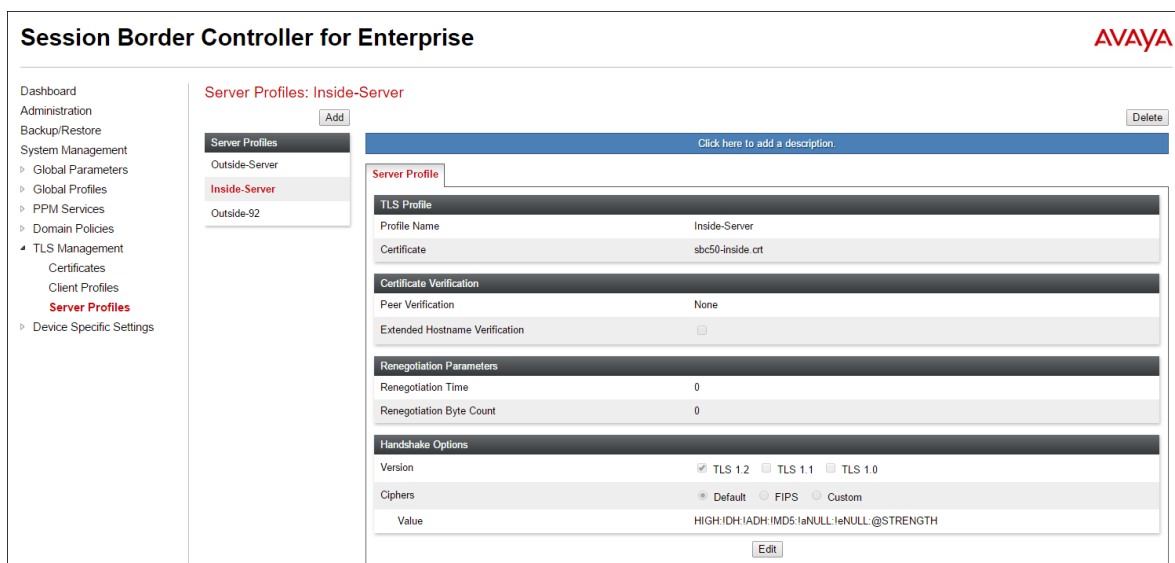
**Step 1** - Select **TLS Management** → **Server Profiles** and click on **Add**. Enter the following:

- **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:



### 8.2.3 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 "1" entered, an "Extended Hostname Verification" checkbox which is unchecked, and a "Custom Hostname Override" text field. At the bottom center, there is a "Next" button.



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

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left-hand menu is expanded to 'TLS Management' > 'Client Profiles'. The main area is titled 'Client Profiles: Inside-Client'. It features a list of profiles with 'Inside-Client' selected. The 'Add' button is visible. The 'Client Profile' form is displayed, showing the following configuration:

TLS Profile	
Profile Name	Inside-Client
Certificate	sbcs50-inside.crt
Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	SystemManagerCA.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>
Renegotiation Parameters	
Renegotiation Time	0
Renegotiation Byte Count	0
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:DH:1ADH:1MD5:1aNULL:1eNULL:@STRENGTH

The 'Edit' button is located at the bottom right of the form.

## 8.3. Global Profiles

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

### 8.3.1 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.

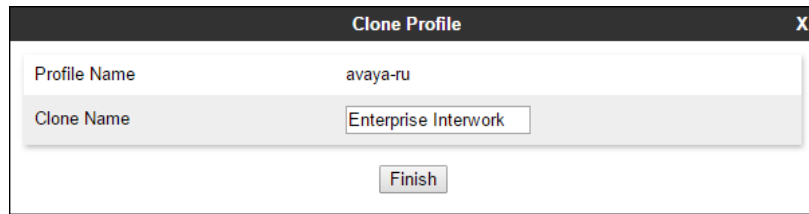
**Step 2** - Select the pre-defined **avaya-ru** profile and click the **Clone** button.

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left-hand menu is expanded to 'Global Profiles' > 'Server Interworking'. The main area is titled 'Interworking Profiles: avaya-ru'. It features a list of profiles with 'avaya-ru' selected. The 'Add' button is visible. The 'Clone' button is highlighted with a red box. The 'General' tab is selected, showing the following configuration:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None

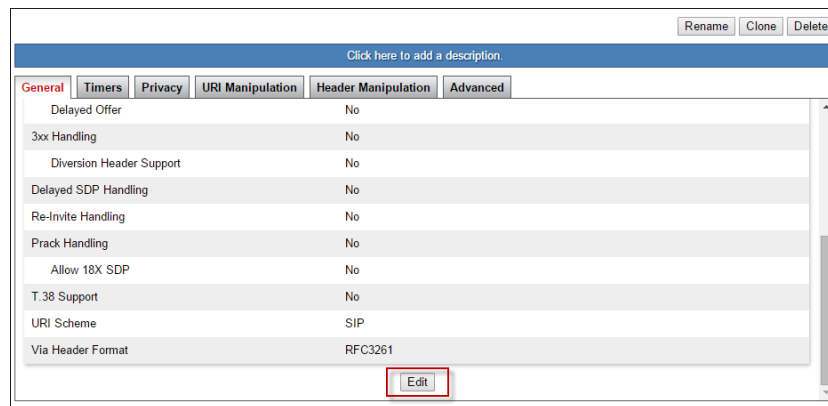
The 'Clone' button is located at the top right of the main area.

**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 buttons for '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: '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:** Radio buttons for ☒ None, ☐ RFC2543 - c=0.0.0.0, and ☐ RFC3264 - a=sendonly.
- 180 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 181 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 182 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- 183 Handling:** Radio buttons for ☒ None, ☐ SDP, and ☐ No SDP.
- Refer Handling:** ☐
- URI Group:** A dropdown menu showing "None".
- Send Hold:** ☐
- Delayed Offer:** ☐
- 3xx Handling:** ☐
- Diversion Header Support:** ☐
- Delayed SDP Handling:** ☐
- Re-Invite Handling:** ☐
- Prack Handling:** ☐
- Allow 18X SDP:** ☐
- T.38 Support:** ☒ (This row is highlighted with a red border in the image).
- URI Scheme:** Radio buttons for ☒ SIP, ☐ TEL, and ☐ ANY.
- Via Header Format:** Radio buttons for ☒ RFC3261 and ☐ RFC2543.

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

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

**Editing Profile: Enterprise Interwork**

**Record Routes**

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

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

**Extensions** Avaya ▼

**Diversion Manipulation** ☐

**Diversion Condition** None ▼

**Diversion Header URI**

**Has Remote SBC** ☒

**Route Response on Via Port** ☐

**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**

### 8.3.2 Server Interworking – Verizon

Repeat the steps shown in **Section 8.3.1** to add an Interworking Profile for the connection to Verizon via the public network, with the following changes:

**Note** – See **Section 13** for additional steps necessary for Experience Portal to redirect calls to Communication Manager using SIP REFER.

**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**

### 8.3.3 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:

**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:

**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 8.3.5, Step 3**.

### 8.3.4 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., **SM8**) and click **Next**.

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

- Select **Server Type: Call Server**
- **SIP Domain:** Leave blank (default)
- **DNS Query Type:** Select **NONE/A** (default)

- **TLS Client Profile:** Select the profile create in **Section 8.2.3** (e.g., **Inside-Client**)
- **IP Address:** **10.64.91.81** (Session Manager network IP address)
- **Transport:** Select **TLS**
- **Port:** **5061**
- Select **Next** (not shown)

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

Server Type: Call Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: Inside-Client

Add

IP Address / FQDN	Port	Transport
10.64.91.81	5061	TLS

Delete

Finish

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

- Select **Next** to accept default values

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

- Select **Enterprise Interwork** (created in **Section 8.3.1**), 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.

### 8.3.5 Server Configuration – Verizon

Repeat the steps in **Section 8.3.4**, 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** (not shown) until the Advanced tab is reached

IP Address / FQDN	Port	Transport
172.30.209.21	5071	UDP



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

- Select **SIP Provider Interwk** (created in **Section 8.3.2**), for **Interworking Profile**.
- Select **Vz IPT script** (created in **Section 8.3.3**) for **Signaling Manipulation Script**.
- Select **Finish** (not shown)

### 8.3.6 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 SM8**) and click **Next**.

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

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

- **Priority/Weight = 1**
- **Server Configuration = SM8** (from **Section 8.3.4**).

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

URI Group	Time of Day	Load Balancing	NAPTR	Transport	Next Hop Priority	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Priority	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	SM8	10.64.91.81:5061 (TLS)	None

### 8.3.7 Routing – To Verizon

Repeat the steps in **Section 8.3.6**, 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 8.3.5**).
- **Next Hop Address:** select **172.30.209.21:5071 (UDP)**.

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

URI Group	Time of Day	Load Balancing	NAPTR	Transport	Next Hop Priority	Next Hop In-Dialog	Ignore Route Header	ENUM	ENUM Suffix
*	default	Priority	<input type="checkbox"/>	None	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

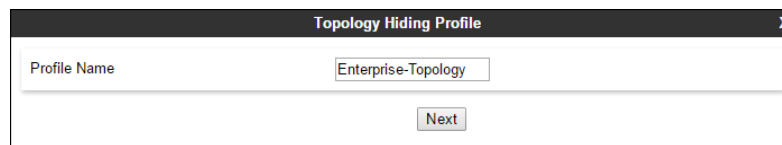
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Verizon IPT	172.30.209.21:5071 (UDP)	None

### 8.3.8 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**.

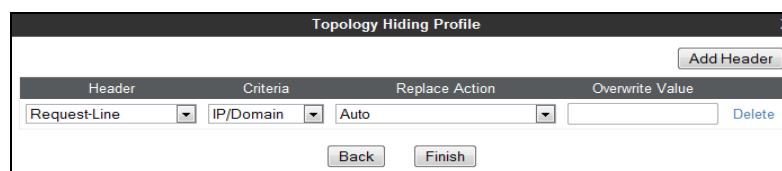


Topology Hiding Profile

Profile Name: Enterprise-Topology

Next

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

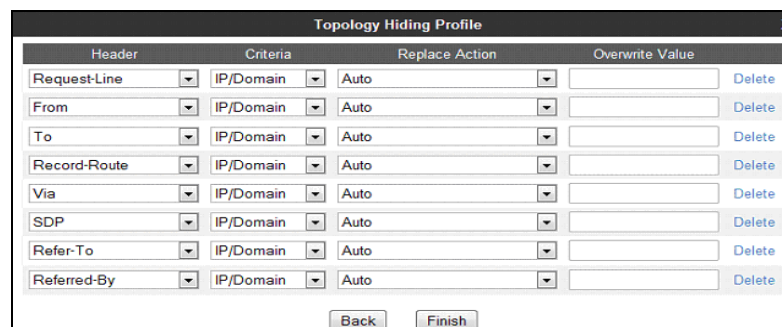


Topology Hiding Profile

Add Header

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

Back Finish

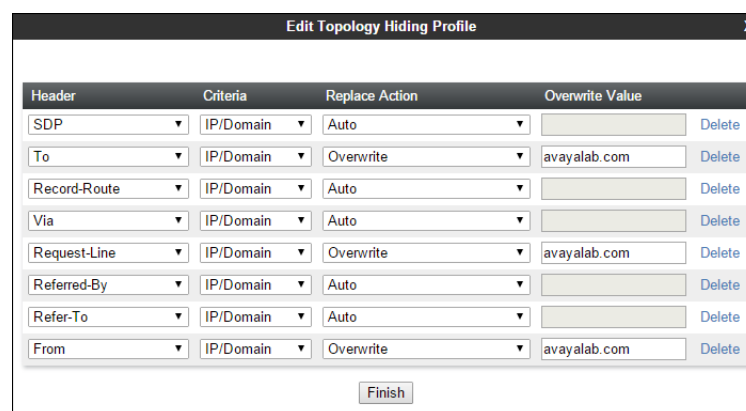


Topology Hiding Profile

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

Back Finish

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

Finish

### 8.3.9 Topology Hiding – Verizon Side

Repeat the steps in **Section 8.3.8**, 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

## 8.4. 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.

### 8.4.1 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

Application Rules

- default
- default-trunk
- default-subscriber-low
- default-subscriber-high
- default-server-low
- default-server-high
- sip-trunk**
- RW app rule

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

## 8.4.2 Media Rules

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

### 8.4.2.1 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.

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  
TLS Management  
Device Specific Settings

Media Rules: enterprise med rule

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

**Audio Encryption**

Preferred Formats SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Encrypted RTCP ☐

MKI ☐

Lifetime Any

Intervorking ☒

**Video Encryption**

Preferred Formats SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80

Encrypted RTCP ☐

MKI ☐

Lifetime Any

Intervorking ☒

**Miscellaneous**

Capability Negotiation ☒

Edit

### 8.4.2.2 Verizon – Media Rule

Repeat the steps in Section 8.4.2.1, with the following changes, to create a Media Rule for Verizon.

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

The completed **Vz SIPTrk Med Rule** screen is shown below.

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  
TLS Management  
Device Specific Settings

Media Rules: Vz SIPTrk Med Rule

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

**Audio Encryption**

Preferred Formats RTP

Intervorking ☒

**Video Encryption**

Preferred Formats RTP

Intervorking ☒

**Miscellaneous**

Capability Negotiation ☐

Edit

## 8.4.3 Signaling Rules

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

### 8.4.3.1 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.

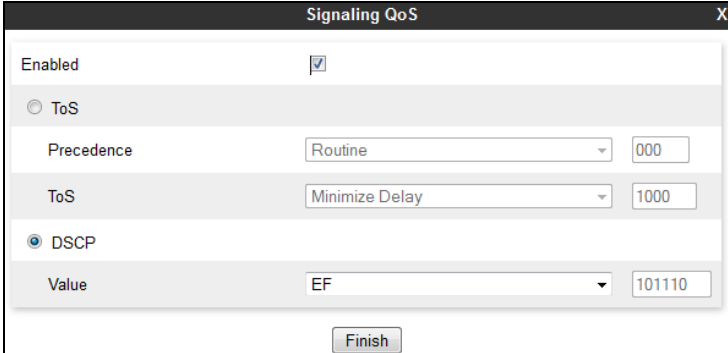
**Step 3** - Select the **Clone** button and the **Clone Rule** window will open (not shown).

- 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

#### 8.4.3.2 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

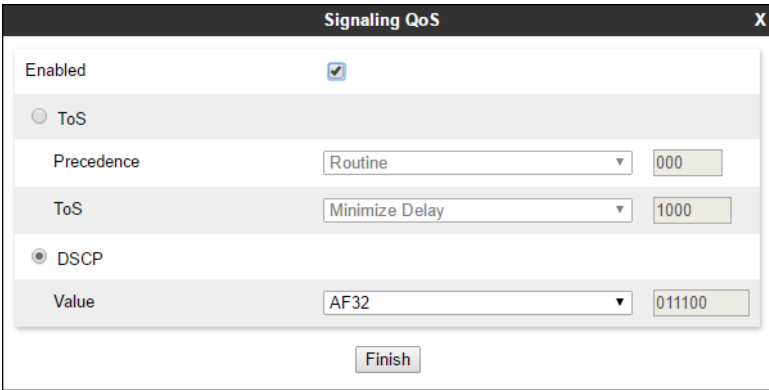
- Enter a name: **Vz SIPTrk Sig Rule**

**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

## 8.4.4 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 8.4.1)
- **Border Rule:** default
- **Media Rule:** enterprise med rule (created in Section 8.4.2.1)
- **Security Rule:** default-low
- **Signaling Rule:** enterprise sig rule (created in Section 8.4.3.1)

**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, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'avaya-def-low-enc', 'avaya-def-high-subscriber', 'avaya-def-high-server', 'Vz-policy-group', and 'enterprise-sip-trunk'. The 'enterprise-sip-trunk' group is selected. To the right, there is a 'Filter By Device...' dropdown, 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.' A 'Policy Group' section contains a table with the following data:

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

## 8.4.5 Endpoint Policy Groups – Verizon Connection

**Step 1** - Repeat steps 1 through 4 from Section 8.4.4 with the following changes:

- **Group Name:** Vz-policy-group
- **Media Rule:** Vz SIPTrk Med Rule (created in Section 8.4.2.2)
- **Signaling Rule:** Vz SIPTrk Sig Rule (created in Section 8.4.3.2)

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

The screenshot shows the 'Policy Groups: Vz-policy-group' configuration page. The navigation menu on the left is the same, with 'End Point Policy Groups' highlighted. The main area shows a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'avaya-def-low-enc', 'avaya-def-high-subscriber', 'avaya-def-high-server', 'Vz-policy-group', and 'enterprise-sip-trunk'. The 'Vz-policy-group' group is selected. To the right, there is a 'Filter By Device...' dropdown, 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.' A 'Policy Group' section contains a table with the following data:

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



## 8.5. 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.

### 8.5.1 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 content 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 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. The 'Add' button is in the top right corner.

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

## 8.5.2 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 8.1**).

The completed **Media Interface** screen in the shared test environment is shown below.

Media Interface: SBC1

Devices: SBC1

Media Interface

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

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

Add

### 8.5.3 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 8.2.2** (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 8.1**).

System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings
  - Network Management
  - Media Interface
  - Signaling Interface**
  - End Point Flows

Signaling Interface: SBC1

Devices

SBC1

Signaling Interface

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

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	<a href="#">Edit</a> <a href="#">Delete</a>
Inside-sig-50	10.64.91.50 Inside A1 (A1, VLAN 0)	---	---	5061	Inside-Server	<a href="#">Edit</a> <a href="#">Delete</a>

Add

## 8.5.4 Server Flows – For Session Manager

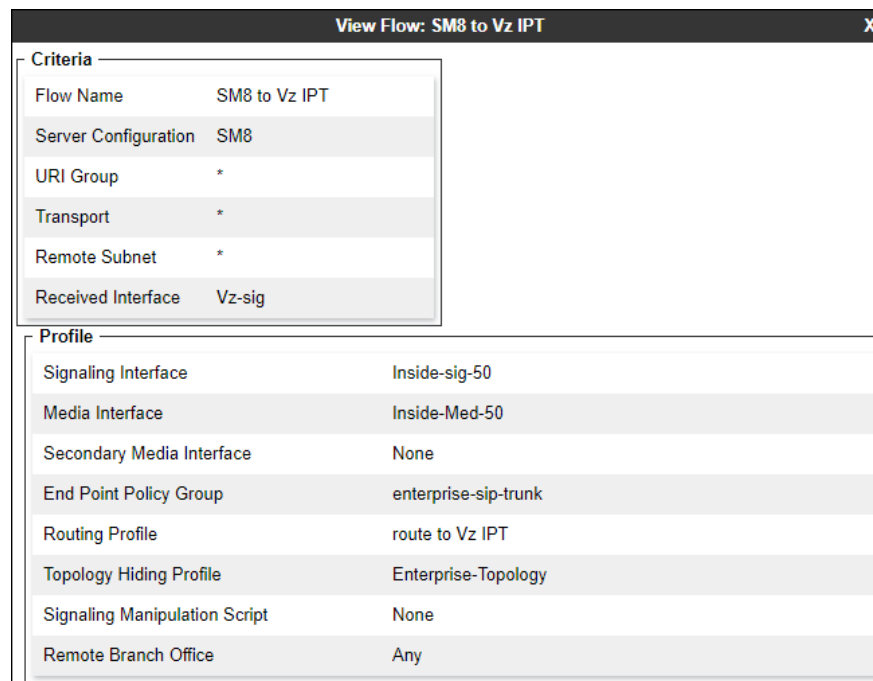
**Step 1** - Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side (not shown).

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

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

- **Flow Name:** SM8 to Vz IPT.
- **Server Configuration:** SM8 (Section 8.3.4).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** Vz-sig (Section 8.5.3).
- **Signaling Interface:** Inside-sig-50 (Section 8.5.3).
- **Media Interface:** Inside-Med-50 (Section 8.5.2).
- **End Point Policy Group:** enterprise-sip-trunk (Section 8.4.4).
- **Routing Profile:** route to Vz IPT (Section 8.3.7).
- **Topology Hiding Profile:** Enterprise-Topology (Section 8.3.8).
- Let other values default.

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



Criteria	
Flow Name	SM8 to Vz IPT
Server Configuration	SM8
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Vz-sig

Profile	
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

## 8.5.5 Server Flows – For Verizon

**Step 1** - Repeat steps 1 through 4 from **Section 8.5.4**, with the following changes:

- **Flow Name:** Verizon IPT Flow.
- **Server Configuration:** Verizon IPT (Section 8.3.5).
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** Inside-sig-50 (Section 8.5.3).
- **Signaling Interface:** Vz-sig (Section 8.5.3).
- **Media Interface:** Vz-Med-B1 (Section 8.5.2).
- **End Point Policy Group:** Vz-policy-group (Section 8.4.5).
- **Routing Profile:** route to SM8 (Section 8.3.6).
- **Topology Hiding Profile:** Vz th profile (Section 8.3.9).

View Flow: Verizon IPT Flow
X

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 SM8
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: SM8									
Update									
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile			
1	SM8 to Vz IPT	*	Vz-sig	Inside-sig-50	enterprise-sip-trunk	route to Vz IPT	View	Clone	Edit Delete

Server Configuration: Verizon IPT									
Update									
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 SM8	View	Clone	Edit Delete

## 9. 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.

### 9.1. 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

## 10. Verification Steps

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

### 10.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

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 (x50233).

```
list trace tac *01                                     Page 1

LIST TRACE

time          data
11:38:55 TRACE STARTED 01/02/2019 CM Release String R018x.00.0.822.0
11:39:09 SIP<INVITE sips:50233@avayalab.com SIP/2.0
11:39:09      Call-ID: 98150601e5575f4ef875381771400a3f
11:39:09      active trunk-group 1 member 1      cid 0x7b6
11:39:09      dial 50233
11:39:09      term station      50233 cid 0x7b6
11:39:09      Called party uses private-numbering
11:39:09 SIP>INVITE sips:50233@avayalab.com SIP/2.0
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP<SIP/2.0 100 Trying
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP<INVITE sips:50233@avayalab.com SIP/2.0
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP>INVITE sips:50233@avayalab.com SIP/2.0
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP<SIP/2.0 100 Trying
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP>SIP/2.0 100 Trying
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP<SIP/2.0 180 Ringing
11:39:09      Call-ID: b0f526d6ebd41e9b82c0c29742c4c
11:39:09 SIP>SIP/2.0 180 Ringing
```

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 (**10.64.91.154**) 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:     10.64.91.75      : 5081
  Far-end:      10.64.91.81      : 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:  10.64.91.154      : 5004
Far-end:   10.64.91.50      : 35938

```

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:10.64.91.50:35938/g729/20ms/1-srtp-aescm128-hmac80
T00028:RX:10.64.91.154:5004/g729/20ms/1-srtp-aescm128-hmac80

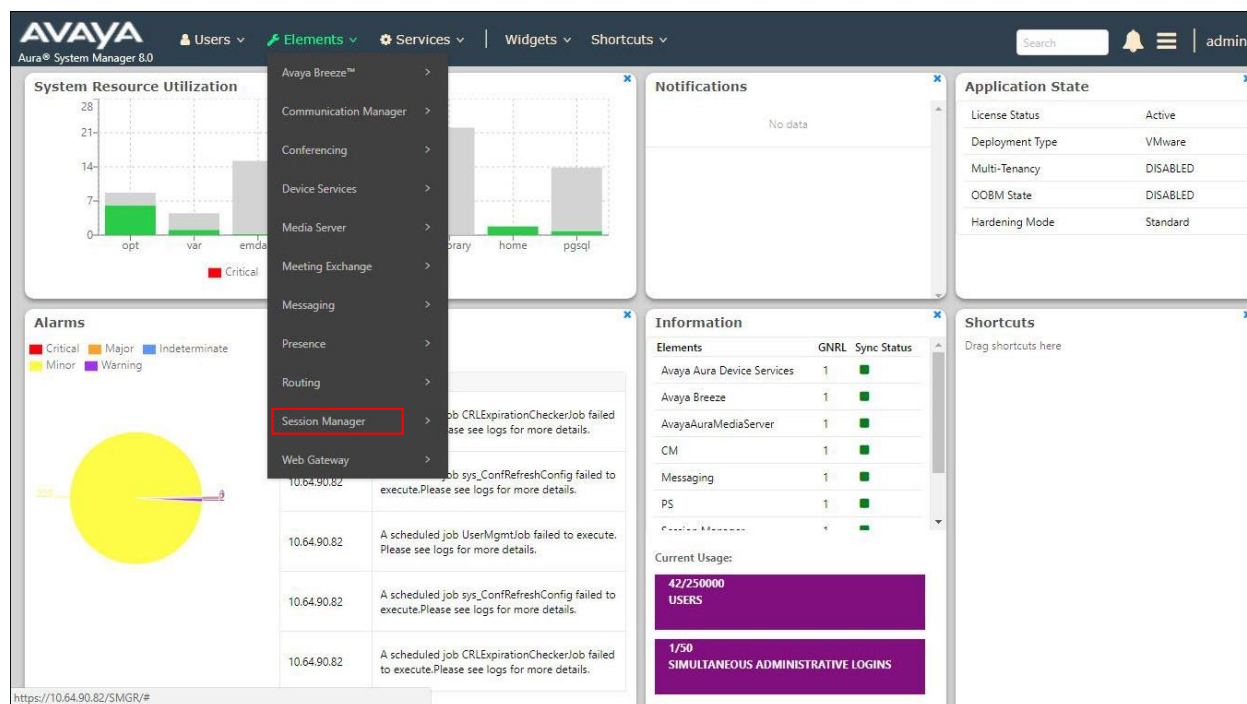
```



## 10.2. Avaya Aura® Session Manager Verification

The Session Manager configuration may be verified via System Manager.

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



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

In the **Entity Monitoring** column, Session Manager shows that there is **1** alarm out of the **14** Entities defined.

Session Manager

Dashboard

Session Manager Admin...

Global Settings

Communication Profile ...

Network Configuration

Device and Location ...

Application Configur...

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State

Shutdown System

EASG

As of 10:43 AM

1 Item

Show

All

Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
<input type="checkbox"/>	<a href="#">Session Manager</a>	Core	✓	0/0/0	Up	Accept New Service	1/14	0	7/7		✓	Normal	Enabled	8.0.0.0.800035

Select : All, None

**Step 3** - Clicking on the **1/14** entry (shown above) in the **Entity Monitoring** column, results in the following display:

Session Manager	<b>Session Manager Entity Link Connection Status</b> This page displays detailed connection status for all entity links from a Session Manager.								
Dashboard	Status Details for the selected Session Manager:								
Session Manager Admin...	<b>All Entity Links for Session Manager: Session Manager</b>								
Global Settings	Summary View								
Communication Profile ...	14 Items								
Network Configuration	Filter: Enable								
Device and Location ...	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
Application Configur...	Aura Messaging	IPv4	10.64.91.84	5061	TLS	FALSE	UP	200 OK	UP
System Status	ExperiencePortal	IPv4	10.64.91.90	5061	TLS	FALSE	UP	200 OK	UP
System Tools	Breeze	IPv4	10.64.91.18	5061	TLS	FALSE	UP	200 OK	UP
Performance	CM-TG4	IPv4	10.64.91.75	5064	TLS	FALSE	UP	200 OK	UP
	Presence	IPv4	10.64.91.18	5061	TLS	FALSE	UP	200 OK	UP
	CM-TG3	IPv4	10.64.91.75	5061	TLS	FALSE	UP	200 OK	UP
	CM-TG2	IPv4	10.64.91.75	5071	TLS	FALSE	UP	200 OK	UP
	CM-TG1	IPv4	10.64.91.75	5081	TLS	FALSE	UP	200 OK	UP
	SBCE-ATT	IPv4	10.64.91.40	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
	SBCE-Toll Free	IPv4	10.64.91.41	5061	TLS	FALSE	UP	405 Method Not Allowed	UP
	CM-TGS	IPv4	10.64.91.75	5065	TLS	FALSE	UP	200 OK	UP
	SBC2	IPv4	10.64.91.100	5061	TLS	FALSE	UP	403 Forbidden	UP
	SBC1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
	IP500	IPv4	10.64.19.70	5061	TLS	FALSE	DOWN	408 Request Timeout	DOWN
	Select : None								

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.

Session Manager	<b>SIP Entity, Entity Link Connection Status</b> This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.								
Dashboard	Status Details for the selected Session Manager:								
Session Manager Admin...	<b>All Entity Links to SIP Entity: SBC1</b>								
Global Settings	Summary View								
Communication Profile ...	1 Item								
Network Configuration	Filter: Enable								
Device and Location ...	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
Application Configur...	Session Manager	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
	Select : None								

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

## 10.3. Avaya Session Border Controller for Enterprise Verification

### 10.3.1 Welcome Screen

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

The screenshot shows the Avaya 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 header displays the title "Session Border Controller for Enterprise" and the Avaya logo. The left sidebar lists the Dashboard and various management options. The main content area is divided into three sections: Information, Installed Devices, and Active Alarms/Incidents.

Information	
System Time	09:40:19 AM MST <a href="#">Refresh</a>
Version	7.2.2.0-11-15522
Build Date	Tue May 29 11:31:10 UTC 2018
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	12/21/2018 08:23:42 MST
Failed Login Attempts	0

Installed Devices
EMS
SBC1

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBC1 : Heartbeat Successful, Server is UP

### 10.3.2 Alarms

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

The screenshot shows the Avaya Session Border Controller for Enterprise interface with the Alarms tab selected. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, and Settings. The main header displays the title "Session Border Controller for Enterprise".

Alarm Viewer:

The screenshot shows the Avaya Session Border Controller for Enterprise Alarm Viewer. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, and Settings. The main header displays the title "Alarm Viewer". The left sidebar lists the Devices and Alarms. The main content area shows a table of alarms for the selected device, SBC1.

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

Clear Selected Clear All

### 10.3.3 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			

### 10.3.4 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

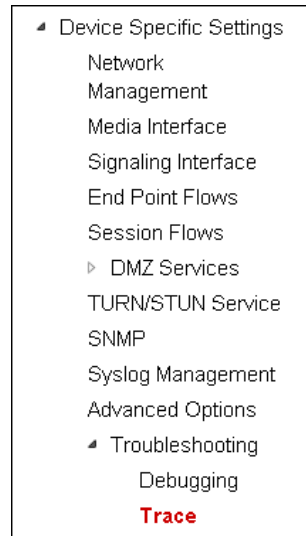
Ping Test

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.

### 10.3.5 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 form. The form has two tabs: 'Packet Capture' (selected) and 'Captures'. The 'Packet Capture' tab contains a 'Packet Capture Configuration' section with the following fields:

- Status: Ready
- Interface: B1 (dropdown)
- Local Address IP[:Port]: All (dropdown) : [ ]
- Remote Address \*, \*:Port, IP, IP:Port: \*
- Protocol: All (dropdown)
- Maximum Number of Packets to Capture: 1000
- Capture Filename: Test-Trace.pcap (text input)

Below the configuration fields 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

## 11. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0, Avaya Aura® Experience Portal 7.2, 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.

## 12. Additional References

### 12.1. 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 and Branch Session Manager in Virtualized Environment*, Release 8.0, Issue 2, August 2018
- [2] *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2, August 2018
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.0, Issue 2, September 2018
- [4] *Administering Avaya Aura® System Manager for Release 8.0*, Issue 4, September 2018

#### **Avaya Aura® Communication Manager**

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.0, Issue 4, September 2018
- [6] *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 1, July 2018
- [7] *Administering Avaya G450 Branch Gateway*, Release 8.0, Issue 1, July 2018
- [8] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, Issue 2, July 2018
- [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 7.2.2, Issue 9, April 2018
- [11] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2.2, Issue 7, April 2018

#### **Avaya Aura® Messaging**

- [12] *Administering Avaya Aura® Messaging*, Release 7.0.0, Issue 4, April 2018

#### **Avaya Aura® Experience Portal**

- [13] *Administering Avaya Aura® Experience Portal*, Release 7.2.1, Issue 1, March 2018
- [14] *Implementing Avaya Aura® Experience Portal on a single server*, Release 7.2, Issue 1, July 2017

### 12.2. Verizon Business

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

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



## 13. Appendix A – Avaya Session Border Controller for Enterprise – Refer Handling

One of the capabilities important to the Experience Portal environment is the Avaya SBCE Refer Handling option. As described in **Section 3.2.2**, Experience Portal inbound call processing may include call redirection to Communication Manager agents, or other CPE destinations. This redirection is accomplished by having Experience Portal send SIP REFER messaging to the Avaya SBCE. Enabling the Refer Handling option causes the Avaya SBCE to intercept and process the REFER and generate a new SIP INVITE messages back to the CPE (e.g., Communication Manager).

As an additional option, the Refer Handling feature can also specify *URI Group* criteria as a discriminator, whereby SIP REFER messages matching the URI Group criteria are processed by the Avaya SBCE, while SIP REFER messages that do not match the URI Group criteria, are passed through to Verizon.

Create a URI Group for numbers intended for Communication Manager.

**Step 1** - Select **Global Profiles → URI Groups** from the left-hand menu.

**Step 2** - Select **Add** and enter a descriptive **Group Name**, e.g., **internal-extension**, and select **Next** (not shown).

**Step 3** - Enter the following:

- **Scheme:** sip:/sips:
- **Type:** Regular Expression
- **URI:** 12[0-9]{3}@.\* This will match 5-digit local extensions starting with 12, e.g., 12001.
- Select **Finish**.

**Edit URI** X

Each entry should match a valid SIP URI.

**WARNING:** Invalid or incorrectly entered regular expressions may cause unexpected results.

Note: This regular expression is case-insensitive.

Ex: [0-9]{3,5}\.user@domain\.com, (simple|advanced)\.user[A-Z]{3}@.\*

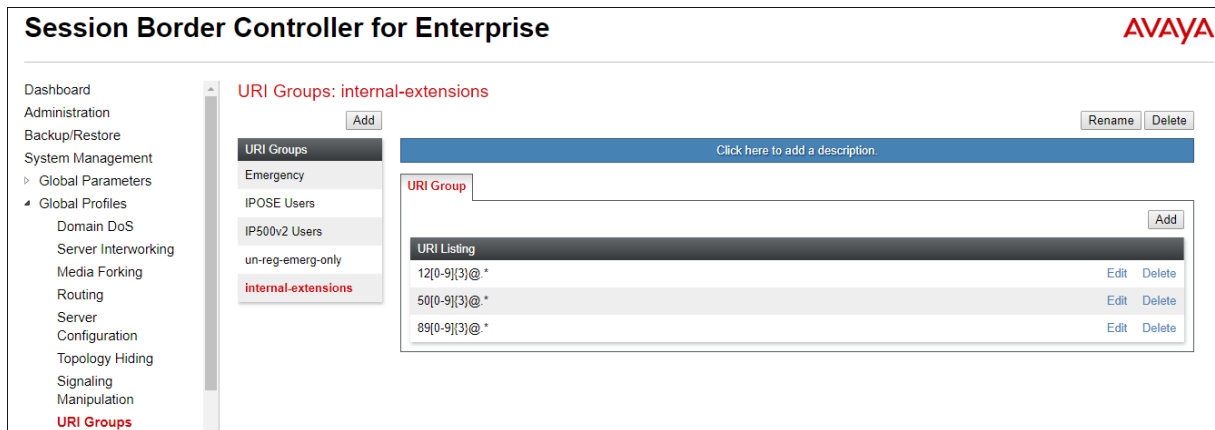
Scheme: ☒ sip:/sips: ☐ tel:

Type: ☐ Plain ☐ Dial Plan ☒ Regular Expression

URI:

Finish

**Step 4** - For additional entries, select **Add** on the right-hand side of the URI Group tab and repeat **Step 3**.

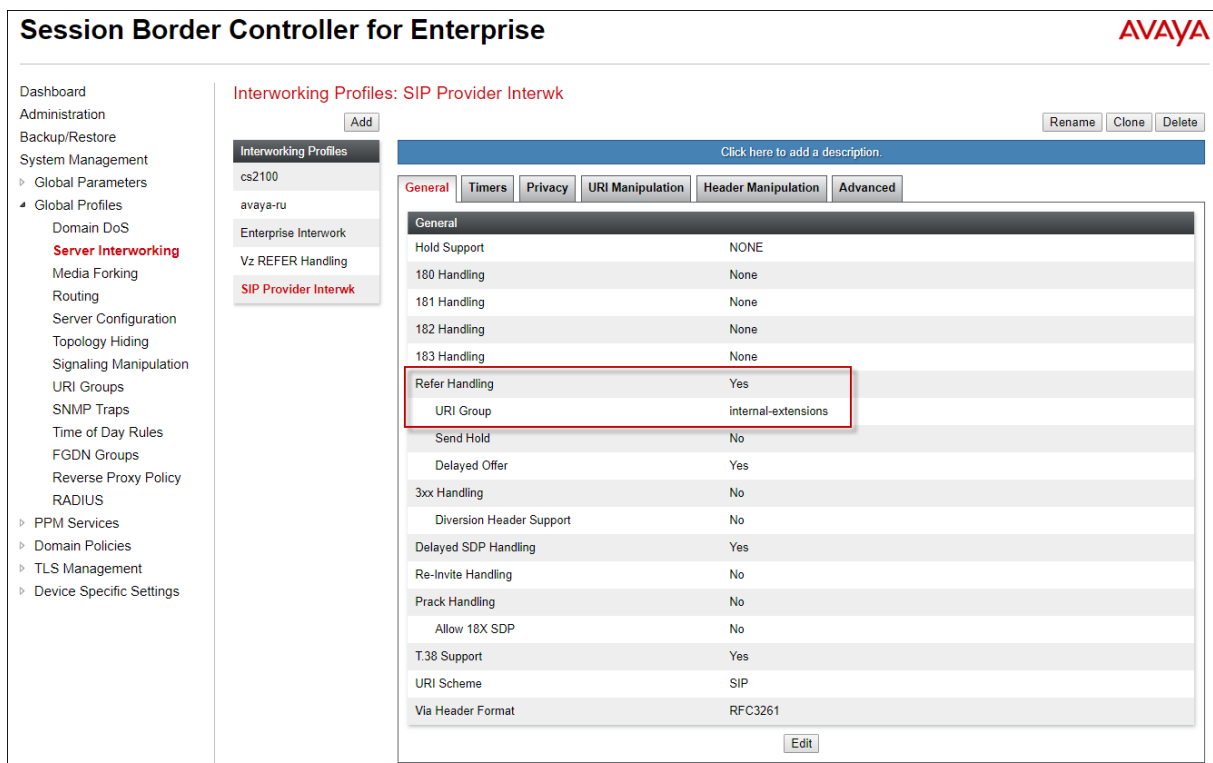


Edit the existing Verizon Server Interworking Profile to enable Refer Handling and assign the newly created URI Group.

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

**Step 2** - Select the Verizon Server Interworking Profile created in **Section 8.3.2** and click **Edit**

- Check **Refer Handling**.
- **URI Group: internal-extensions**
- Select **Finish**.



---

**©2019 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).