



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1 with Verizon Business IP Trunking Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.1, Avaya Aura® Communication Manager Release 8.1 and Avaya Session Border Controller for Enterprise Release 8.1 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 | 6 |
| 2.2. | Test Results | 7 |
| 2.3. | History Info and Diversion Headers | 8 |
| 2.4. | SIP Header Optimization | 8 |
| 2.5. | Support..... | 8 |
| 3. | Reference Configuration..... | 9 |
| 3.1. | Illustrative Configuration Information..... | 9 |
| 3.2. | Call Flows | 12 |
| 3.2.1 | Inbound Call..... | 12 |
| 3.2.2 | Outbound Call | 13 |
| 3.2.3 | Call Forward Redirection..... | 14 |
| 3.2.4 | Attended/Unattended Transfer Call Flow initiated by Communication Manager Station | 15 |
| 4. | Equipment and Software Validated | 16 |
| 5. | Configure Avaya Aura® Communication Manager | 17 |
| 5.1. | Verify Licensed Features | 17 |
| 5.2. | System-Parameters Features | 19 |
| 5.3. | Dial Plan..... | 20 |
| 5.4. | Node Names..... | 20 |
| 5.5. | Processor Ethernet Configuration | 21 |
| 5.6. | IP Codec Sets | 22 |
| 5.6.1 | Codecs for IP Network Region 1 (calls within the CPE)..... | 22 |
| 5.6.2 | Codecs for IP Network Region 2 (calls to/from Verizon) | 23 |
| 5.7. | Network Regions | 24 |
| 5.7.1 | IP Network Region 1 – Local CPE Region | 24 |
| 5.7.2 | IP Network Region 2 – Verizon Trunk Region | 25 |
| 5.8. | SIP Trunks | 26 |
| 5.8.1 | SIP Trunk for Inbound/Outbound Verizon calls..... | 26 |
| 5.8.2 | Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.) | 30 |
| 5.9. | Public Numbering | 31 |
| 5.10. | Private Numbering | 32 |
| 5.11. | Route Patterns | 32 |
| 5.11.1 | Route Pattern for National Calls to Verizon | 32 |
| 5.11.2 | Route Pattern for International Calls to Verizon | 33 |
| 5.11.3 | Route Pattern for Service Calls to Verizon..... | 34 |
| 5.11.4 | Route Pattern for Calls within the CPE | 34 |
| 5.12. | Automatic Route Selection (ARS) Dialing..... | 35 |
| 5.13. | Automatic Alternate Routing (AAR) Dialing..... | 35 |
| 5.14. | Avaya G430 Media Gateway Provisioning | 36 |
| 5.15. | Avaya Aura® Media Server Provisioning..... | 37 |
| 5.16. | Save Translations | 38 |
| 5.17. | Verify TLS Certificates – Communication Manager..... | 39 |
| 6. | Configure Avaya Aura® Session Manager | 40 |

| | | |
|-------|--|----|
| 6.1. | System Manager Login and Navigation | 41 |
| 6.2. | SIP Domain | 42 |
| 6.3. | Locations | 42 |
| 6.3.1 | Main Location | 42 |
| 6.3.2 | Common-SBCs Location | 43 |
| 6.4. | Configure Adaptations | 44 |
| 6.4.1 | Adaptation for Avaya Aura® Communication Manager..... | 44 |
| 6.4.2 | Adaptation for the Verizon Business IP Trunking service | 46 |
| 6.5. | SIP Entities..... | 47 |
| 6.5.1 | Avaya Aura® Session Manager SIP Entity | 48 |
| 6.5.2 | Avaya Aura® Communication Manager SIP Entity – Public Trunk | 50 |
| 6.5.3 | Avaya Aura® Communication Manager SIP Entity – Local Trunk..... | 51 |
| 6.5.4 | Avaya Session Border Controller for Enterprise SIP Entity | 51 |
| 6.6. | Entity Links..... | 52 |
| 6.6.1 | Entity Link to Avaya Aura® Communication Manager – Public Trunk..... | 52 |
| 6.6.2 | Entity Link to Avaya Aura® Communication Manager – Local Trunk..... | 53 |
| 6.6.3 | Entity Link for the Verizon Business IP Trunking service via the Avaya SBCE..... | 53 |
| 6.7. | Time Ranges | 54 |
| 6.8. | Routing Policies | 54 |
| 6.8.1 | Routing Policy for Verizon Inbound Calls to Avaya Aura® Communication Manager | 54 |
| 6.8.2 | Routing Policy for Outbound Calls to Verizon..... | 56 |
| 6.9. | Dial Patterns..... | 57 |
| 6.9.1 | Matching Inbound PSTN Calls to Avaya Aura® Communication Manager | 57 |
| 6.9.2 | Matching Outbound Calls to Verizon/PSTN | 59 |
| 6.10. | Verify TLS Certificates – Session Manager | 60 |
| 7. | Configure Avaya Session Border Controller for Enterprise | 62 |
| 7.1. | Device Management – Status..... | 63 |
| 7.2. | TLS Management..... | 65 |
| 7.2.1 | Verify TLS Certificates – Avaya Session Border Controller for Enterprise | 65 |
| 7.2.2 | Server Profiles..... | 66 |
| 7.2.3 | Client Profiles | 68 |
| 7.3. | Network Management..... | 70 |
| 7.4. | Media Interfaces..... | 71 |
| 7.5. | Signaling Interfaces | 72 |
| 7.6. | Server Interworking Profiles..... | 73 |
| 7.6.1 | Server Interworking Profile – Enterprise..... | 73 |
| 7.6.2 | Server Interworking Profile – Verizon | 74 |
| 7.7. | Signaling Manipulation..... | 75 |
| 7.8. | SIP Server Profiles..... | 76 |
| 7.8.1 | SIP Server Profile – Session Manager | 76 |
| 7.8.2 | SIP Server Profile – Verizon..... | 78 |
| 7.9. | Routing Profiles | 79 |
| 7.9.1 | Routing Profile – Session Manager | 80 |
| 7.9.2 | Routing Profile – Verizon | 81 |
| 7.10. | Topology Hiding Profiles | 82 |

| | | |
|--------|--|-----|
| 7.10.1 | Topology Hiding – Enterprise | 82 |
| 7.10.2 | Topology Hiding – Verizon | 83 |
| 7.11. | Application Rules..... | 83 |
| 7.12. | Media Rules | 84 |
| 7.12.1 | Enterprise – Media Rule | 84 |
| 7.12.2 | Verizon – Media Rule | 85 |
| 7.13. | Signaling Rules | 86 |
| 7.13.1 | Signaling Rule – Enterprise | 86 |
| 7.13.2 | Signaling Rule – Verizon..... | 87 |
| 7.14. | Endpoint Policy Groups..... | 87 |
| 7.14.1 | End Point Policy Group - Enterprise | 87 |
| 7.14.2 | Endpoint Policy Groups – Verizon | 88 |
| 7.15. | Endpoint Flows – Server Flows..... | 89 |
| 7.15.1 | Server Flow – Enterprise | 89 |
| 7.15.2 | Server Flow – Verizon | 90 |
| 8. | Verizon Business IP Trunking Services Suite Configuration..... | 91 |
| 8.1. | Service Access Information | 91 |
| 9. | Verification Steps..... | 92 |
| 9.1. | Avaya Aura® Communication Manager Verifications | 92 |
| 9.2. | Avaya Aura® Session Manager Verification | 94 |
| 9.3. | Avaya Session Border Controller for Enterprise Verification..... | 96 |
| 9.3.1 | Incidents..... | 96 |
| 9.3.2 | Server Status | 97 |
| 9.3.3 | Diagnostics..... | 98 |
| 9.3.4 | Tracing | 98 |
| 10. | Conclusion | 99 |
| 11. | Additional References..... | 100 |
| 11.1. | Avaya | 100 |
| 11.2. | Verizon Business | 100 |
| 12. | Appendix B – Avaya SBCE – SigMa Script File | 101 |

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.1, Avaya Aura® Communication Manager Release 8.1 and Avaya Session Border Controller for Enterprise Release 8.1 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.

Note that the terms “Verizon Business IP Trunking”, “Verizon” and “service provider” will be used interchangeably throughout these Application Notes.

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. Phone types included SIP, H.323, digital and analog telephones at the enterprise.
- Proper disconnect when the call is abandoned by the caller before it is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect for calls that are not answered.
- Proper response to busy endpoints.
- 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, Communication Manager vector digit collection steps).
- Additional PSTN numbering plans (e.g., International, operator assist, 411).
- Hold / Retrieve with music on hold.
- Blind and Consultative call transfer using two approaches
 - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to “y”)
 - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to “n”)
- Conference calls
- SIP Diversion Header for call redirection
 - Call Forwarding
 - EC500
- Long hold time calls
- Avaya Remote Worker operation (Avaya IX™ Workplace Client for Windows SIP softphone) via Avaya SBCE.

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. T.38 fax was provisioned on the Verizon Business IP Trunking production circuit used to verify these Application Notes. Still, Verizon never sent a re-Invite to transition to T.38 fax. If the **FAX Mode** field on the Communication Manager ip-codec-set form (**Section 5.6**) is set to **t.38-standard**, Communication Manager will send the 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.
When the **FAX Mode** is set to **t.38-G711-fallback**, Communication Manager will send a re-Invite to T.38 for inbound fax calls, 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 from the far end. Since Verizon never sent a T.38 re-Invite, the result is an outbound fax sent using G.711, even though the circuit is provisioned for T.38. Inbound fax calls negotiated properly to T.38.
2. 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 under investigation by the Avaya SBCE development team. A workaround is to include a SigMa script for the Verizon Server Configuration profile on the Avaya SBCE to convert “sips” to “sip” in the Diversion header. See **Section 7.7**.
3. 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 6.4.2**.
4. 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.
5. Verizon Business IP Trunking service does not support G.711A codec for domestic service (EMEA only).
6. Verizon Business IP Trunking service does not support G.729B codec.

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 6.4.2**.

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 Optimization

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 6.4.2**.

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 **Sections 7.7** and **7.8.2**.

2.5. Support

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

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

3. Reference Configuration

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

3.1. Illustrative Configuration Information

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).

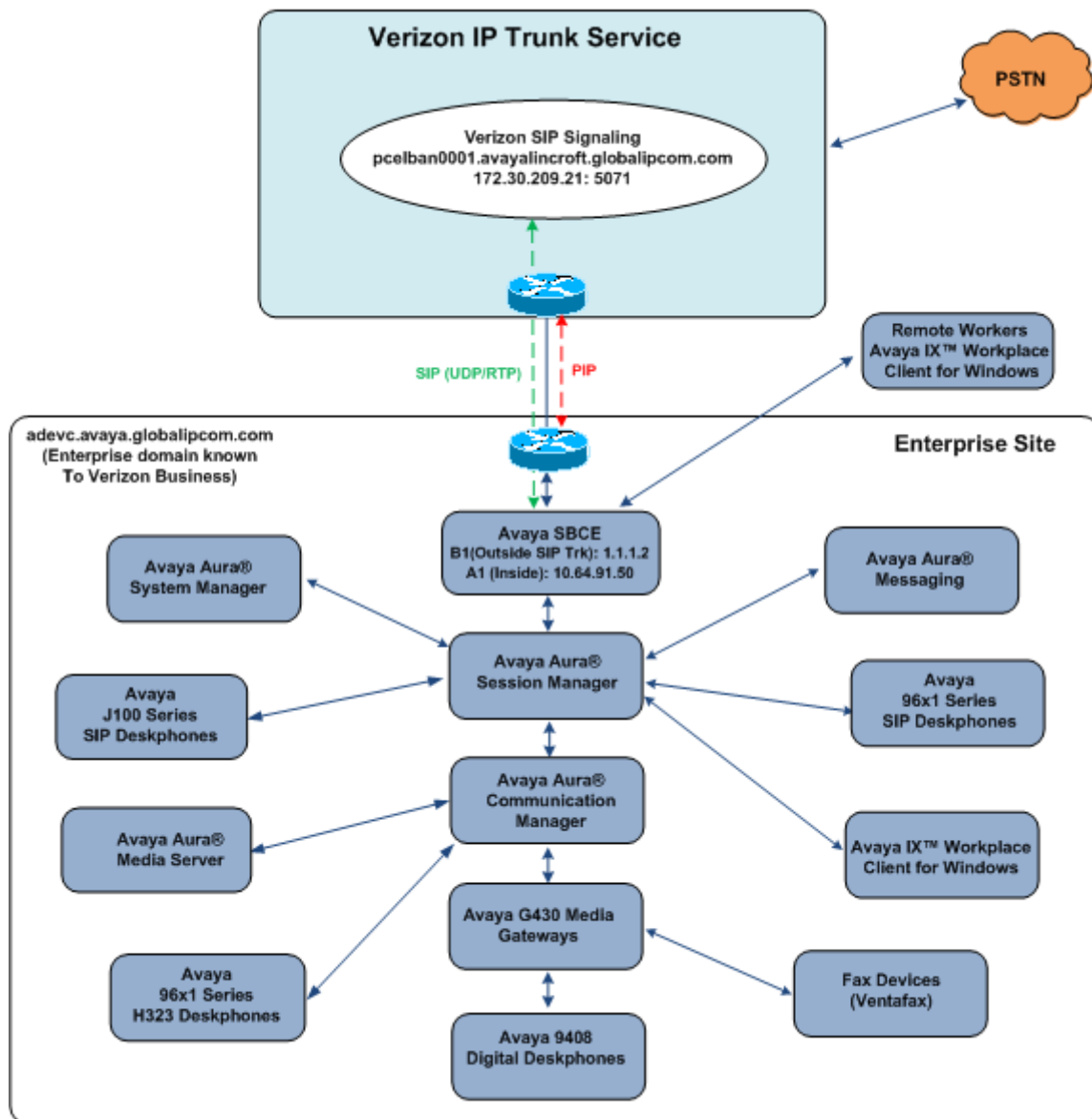


Figure 1: Avaya Interoperability Test Lab Configuration

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.

Verizon Business IP Trunking service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunking service as FQDN *adevc.avaya.globalipcom.com*. Access to the Verizon Business IP Trunking service was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, the Avaya SBCE is used to adapt the “avayalab.com” domain to the domain known to Verizon (see **Section 7.10.2**). 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 G430 Media Gateway
- Avaya Media Server
- Avaya Aura® Messaging
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle
- Avaya IX™ Workplace Client for Windows
- Avaya Digital Phones
- Ventafax fax software

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.

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

| Component | Illustrative Value in these Application Notes |
|--|---|
| Avaya Aura® Communication Manager | |
| IP Address (procr) | 10.64.91.75 |
| Avaya Aura® Session Manager | |
| IP Address | 10.64.91.81 |
| Avaya Aura® Media Server | |
| IP Address | 10.64.91.86 |
| Avaya G430 Media Gateway | |
| IPv4 Address | 10.5.5.150 |
| Avaya Session Border Controller for Enterprise (SBCE) | |
| IP Address of Inside (Private) Interface A1 | 10.64.91.50 |
| IP Address of Outside (Public) Interface | 1.1.1.2 |
| Verizon SIP Signaling | |
| IP Address | 172.30.209.21 |

Table 1: Network Values Used in these Application Notes

3.2. Call Flows

To understand how Verizon Business IP Trunking service calls are handled by the Avaya CPE environment, several basic call flows are described in this section. However, for brevity, not all possible call flows are described.

3.2.1 Inbound Call

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.

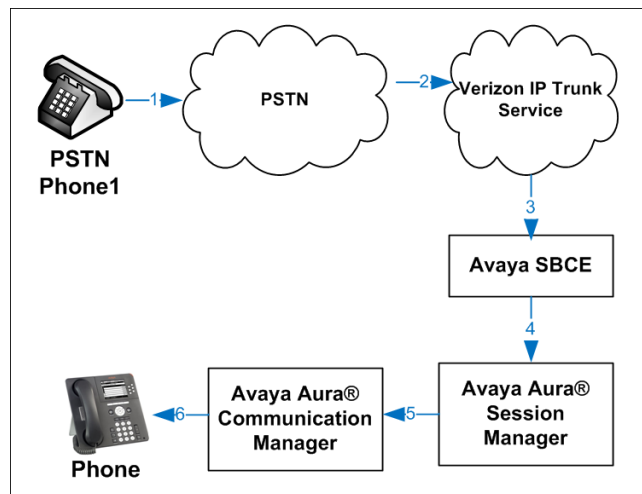


Figure 2: Inbound Verizon Call

3.2.2 Outbound Call

The call scenario illustrated below 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.

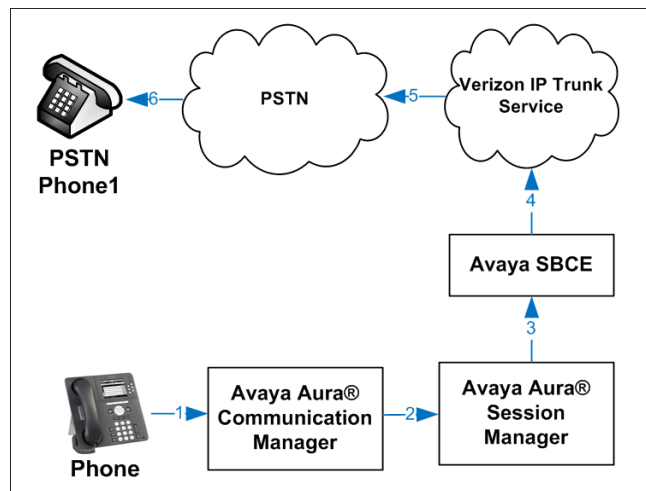


Figure 3: Outbound Verizon Call

3.2.3 Call Forward Redirection

The next call scenario 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 5.8**).

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 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.

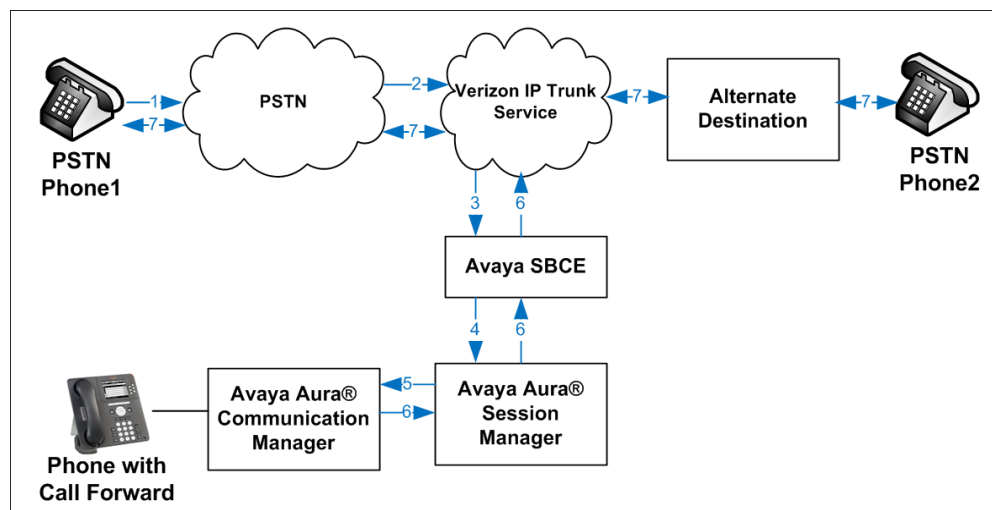


Figure 4: Station Re-directed (e.g., Call Forward) Verizon Call

3.2.4 Attended/Unattended Transfer Call Flow initiated by Communication Manager Station

The call scenario illustrated in **Figure 5** below shows an inbound call from Verizon Business IP Trunking service that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a station. The station answers the call and transfers it back to a second PSTN destination. Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and Verizon. Communication Manager completes the transfer, sending a REFER (with the Replaces parameter) to the Verizon Business IP Trunking service to connect the two active calls together.

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 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. The station answers the call and then transfers it to a new PSTN destination. Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the Verizon Business IP Trunking service. Communication Manager redirects the call using a SIP REFER message when the transfer is completed by the station. The REFER message specifies the active call to replace and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the Verizon network.
7. Verizon Business IP Trunking service replaces the call with the alternate destination specified in the REFER and connects the calling party to the alternate party directly.
8. Verizon Business IP Trunking service clears the existing calls to Communication Manager.

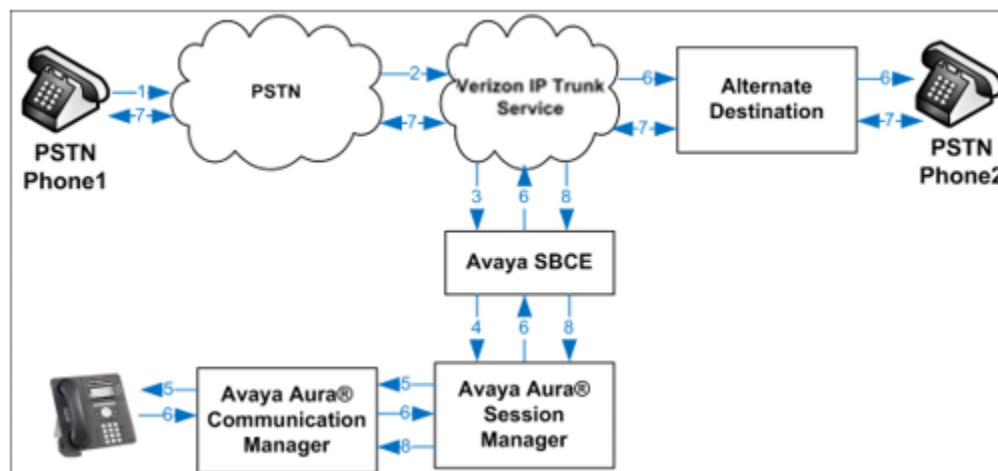


Figure 5: Attended/Unattended Transfer Using REFER

4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|--|----------------------------------|
| Avaya Aura® System Manager | 8.1.2.0.0611097 (Feature Pack 2) |
| Avaya Aura® Session Manager | 8.1.2.0.812039 |
| Avaya Aura® Communication Manager | 8.1.2.0.0-FP2 (patch 26095) |
| Avaya Session Border Controller for Enterprise | 8.1.0.0.14-18490 |
| Avaya Aura® Messaging | 7.1.Service Pack 2 |
| Avaya Aura® Media Server | 8.0.2.93 |
| G430 Gateway | 41.24.0 |
| Avaya 96X1 Series IP Deskphone (SIP) | 6.8304 |
| Avaya 96X1 Series IP Deskphone (H.323) | 7.1.8.0.9 |
| Avaya J100 Series IP Deskphone(SIP) | 4.0.4.0.10 |
| Avaya IX™ Workplace Client for Windows | 3.8.2.20.6 |
| Avaya 9408 Digital Deskphone | 20.06 |
| Fax device | Ventafax 7.10 |

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager

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.

5.1. 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: | 1000 | 0 | | |
| Maximum Administered Remote Office Trunks: | 4000 | 0 | | |
| Max Concurrently Registered Remote Office Stations: | 1000 | 0 | | |
| Maximum Concurrently Registered IP eCons: | 68 | 0 | | |
| Max Concur Reg Unauthenticated H.323 Stations: | 100 | 0 | | |
| Maximum Video Capable Stations: | 2400 | 0 | | |
| Maximum Video Capable IP Softphones: | 1000 | 5 | | |
| Maximum Administered SIP Trunks: | 4000 | 95 | | |
| Max Administered Ad-hoc Video Conferencing Ports: | 4000 | 0 | | |
| Max Number of DS1 Boards with Echo Cancellation: | 80 | 0 | | |

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

| display system-parameters customer-options | | Page 4 of 12 |
|--|-------------------------------------|--------------|
| OPTIONAL FEATURES | | |
| Abbreviated Dialing Enhanced List? y | Audible Message Waiting? y | |
| Access Security Gateway (ASG)? n | Authorization Codes? y | |
| Analog Trunk Incoming Call ID? y | CAS Branch? n | |
| A/D Grp/Sys List Dialing Start at 01? y | CAS Main? n | |
| Answer Supervision by Call Classifier? y | Change COR by FAC? n | |
| ARS? y | Computer Telephony Adjunct Links? y | |
| ARS/AAR Partitioning? y | Cvg Of Calls Redirected Off-net? y | |
| ARS/AAR Dialing without FAC? n | DCS (Basic)? y | |
| ASAI Link Core Capabilities? n | DCS Call Coverage? y | |
| ASAI Link Plus Capabilities? n | DCS with Rerouting? y | |
| Async. Transfer Mode (ATM) PNC? n | | |
| Async. Transfer Mode (ATM) Trunking? n | Digital Loss Plan Modification? y | |
| ATM WAN Spare Processor? n | DS1 MSP? y | |
| ATMS? y | DS1 Echo Cancellation? y | |
| Attendant Vectoring? y | | |

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

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

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

| display system-parameters customer-options | | Page 6 of 12 |
|--|------------------------------------|--------------|
| OPTIONAL FEATURES | | |
| Multinational Locations? n | Station and Trunk MSP? y | |
| Multiple Level Precedence & Preemption? n | Station as Virtual Extension? y | |
| Multiple Locations? n | | |
| 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 | |
| Private Networking? y | Usage Allocation Enhancements? y | |
| Processor and System MSP? y | | |
| Processor Ethernet? y | Wideband Switching? y | |
| | Wireless? n | |
| Remote Office? y | | |
| Restrict Call Forward Off Net? y | | |
| Secondary Data Module? y | | |

5.2. System-Parameters Features

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

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

5.3. 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 5.8**.

| change dialplan analysis | | | | | | Page 1 of 12 | | | |
|--------------------------|---------------|--------------|-----------|---------------|--------------|-----------------|---------------|--------------|-----------|
| DIAL PLAN ANALYSIS TABLE | | | | | | | | | |
| Location: all | | | | | | Percent Full: 1 | | | |
| | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type |
| 1 | | 5 | ext | | | | | | |
| 2 | | 5 | ext | | | | | | |
| 3 | | 5 | ext | | | | | | |
| 4 | | 5 | ext | | | | | | |
| 5 | | 5 | ext | | | | | | |
| 60 | | 3 | ext | | | | | | |
| 66 | | 2 | fac | | | | | | |
| 7 | | 5 | ext | | | | | | |
| 8 | | 5 | ext | | | | | | |
| 9 | | 1 | fac | | | | | | |
| * | | 3 | dac | | | | | | |

5.4. 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 6.5**

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., **AMS801** and **10.64.91.86**). 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 | | | |
| AMS801 | 10.64.91.86 | | | |
| SM | 10.64.91.81 | | | |
| default | 0.0.0.0 | | | |
| procr | 10.64.91.75 | | | |
| procr6 | :: | | | |

5.5. Processor Ethernet Configuration

The **change 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 | | |

5.6. IP Codec Sets

Use the **change ip-codec-set** command to define a list of codecs to use for calls within the enterprise, and for calls between the enterprise and the service provider.

5.6.1 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 Codec | Silence Suppression | Frames Per Pkt | Packet Size (ms) | | |
| 1: G.722-64K | | 2 | 20 | | |
| 2: G.711MU | n | 2 | 20 | | |
| 3: G.729A | n | 2 | 20 | | |
| Media Encryption | | | | Encrypted SRTCP: enforce-unenc-srtcp | |
| 1: 1-srtp-aescm128-hmac80 | | | | | |
| 2: none | | | | | |

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

| | | | | | |
|---|----------------------|-----------------|--------|---------------------|--|
| change ip-codec-set 1 | | | | Page 2 of 2 | |
| IP MEDIA PARAMETERS | | | | | |
| Allow Direct-IP Multimedia? y | | | | | |
| Maximum Call Rate for Direct-IP Multimedia : 15360:Kbits | | | | | |
| Maximum Call Rate for Priority Direct-IP Multimedia : 15360:Kbits | | | | | |
| | Mode | Redun- dancy | ECM: y | Packet Size (ms) | |
| FAX | t.38-standard | 0 | | | |
| Modem | off | 0 | | | |
| TDD/TTY | US | 3 | | | |
| H.323 Clear-channel | n | 0 | | | |
| SIP 64K Data | n | 0 | | 20 | |
| Media Connection IP Address Type Preferences | | | | | |
| 1: IPv4 | | | | | |
| 2: | | | | | |

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

This IP codec set will be used for Verizon Business IP Trunking calls. Repeat the steps in **Section 5.6.1** with the following changes:

On **Page 1**, provision the codecs in the order shown below.

change ip-codec-set 2Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 2

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

Media Encryption

Encrypted SRTP: enforce-unenc-srtpc

| |
|---------------------------|
| 1: 1-srtp-aescm128-hmac80 |
| 2: none |

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

change ip-codec-set 2Page 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

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

Media Connection IP Address Type Preferences

1: IPv4

5.7. Network Regions

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G430 Media Gateway and Avaya Media Server are in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Verizon testing.

5.7.1 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.
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.

| change ip-network-region 1 | | Page 1 of 20 |
|---------------------------------------|--------------------------------------|-----------------|
| IP NETWORK REGION | | |
| Region: 1 | | |
| Location: 1 | Authoritative Domain: avayalab.com | |
| Name: Enterprise | Stub Network Region: n | |
| MEDIA PARAMETERS | | |
| 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 4** of the form:

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

| change ip-network-region 1 | | | | | | | | | | Page | 4 | of | 20 |
|----------------------------|-------|--|---------------|-------|-------|-------------|-----|---------|-----|------|-----|----|----|
| Source Region: 1 | | Inter Network Region Connection Management | | | | | | | | I | | M | |
| | | | | | | | | | | G | A | t | |
| dst | codec | direct | WAN-BW-limits | | Video | Intervening | | Dyn | A | G | c | | |
| rgn | set | WAN | Units | Total | Norm | Prio | Shr | Regions | CAC | R | L | e | |
| 1 | 1 | | | | | | | | | | all | | |
| 2 | 2 | y | NoLimit | | | | | | n | | t | | |

5.7.2 IP Network Region 2 – Verizon Trunk Region

Repeat the steps in **Section 5.7.1** 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 | codec | direct | WAN-BW-limits | | Video | Intervening | | Dyn | A | G | c | | |
| rgn | set | WAN | Units | Total | Norm | Prio | Shr | Regions | CAC | R | L | e | |
| 1 | 2 | y | NoLimit | | | | | | | | | | |
| 2 | 2 | | | | | | | | | | all | | |
| 3 | | | | | | | | | | | | | |

5.8. 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. This trunk will use TLS port 5081.
- Internal CPE access (e.g., Avaya SIP telephones, Messaging, etc.) – SIP Trunk 3. This trunk will use TLS port 5061.

Note that different ports are assigned to each trunk. This is necessary so Session Manager can distinguish the traffic on the service provider trunk, from the traffic on the trunk used for other enterprise SIP traffic.

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 6.5** regarding the use of TLS transport protocols in the CPE.

5.8.1 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 Group 1 is defined. This trunk corresponds to the **CM-TG1** SIP Entity defined later in **Section 6.5.2**.

5.8.1.1 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 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (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 5.6.2**.
- **Far-end Domain** – Enter **avayalab.com**.
- **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 the default value **n**.
- **H.323 Station Outgoing Direct Media** is set to the default value **n**.

| | | |
|---|------------------------------------|--------------|
| 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 | |

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

5.8.1.2 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 5.8.1.1** (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**.

| | |
|--------------------------------|----------------------------------|
| add trunk-group 1 | Page 3 of 21 |
| TRUNK FEATURES | |
| ACA Assignment? n | Measured: none |
| | Maintenance Tests? y |
| Suppress # Outpulsing? n | Numbering Format: public |
| | 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**.

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 6.4.2**). Alternatively, History Info may be disabled here with the Diversion Header enabled.

```
add trunk-group 1                                     Page 4 of 21
                                                    PROTOCOL VARIATIONS

                                                    Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                                    Send Transferring Party Information? n
                                                    Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n
                                                    Send Diversion Header? n
                                                    Support Request History? y
                                                    Telephone Event Payload Type: 101
                                                    Shuffling with SDP? n

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

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

5.8.2 Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.)

Trunk Group 3 corresponds to the **CM-TG3** SIP Entity defined later in **Section 6.5.3**

5.8.2.1 Signaling Group 3

Repeat the steps in **Section 5.8.1.1** 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 5.7.1**.

5.8.2.2 Trunk Group 3

Repeat the steps in **Section 5.8.1.2** 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 5.8.2.1** (e.g., **3**).

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

- Same as **Section 5.8.1.2**

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.

5.9. Public Numbering

In the reference configuration, the public-unknown-numbering form, (used in conjunction with the **Numbering Format: public** setting in **Section 5.8.1.2**), is used to convert Communication Manager local extensions to Verizon public numbers, for inclusion in any origination 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., **12001**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **1**).
- **Private Prefix** – Enter the corresponding Verizon DNIS number (e.g., **17329450231**).
- **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 | |

5.10. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 5.8.2.2**), 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 5.3** (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 | |

5.11. Route Patterns

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

5.11.1 Route Pattern for National Calls to Verizon

This form defines the public SIP trunk, based on the route-pattern selected by the ARS table later in **Section 5.12**. 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/ QSIG | IXC | |
| 1: 1 | 0 | | 1 | | | | p | n | user | |
| 2: | | | | | | | | n | user | |
| 3: | | | | | | | | n | user | |
| BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbering LAR | | | | | | | | | | |
| 0 1 2 M 4 W Request Dgts Format | | | | | | | | | | |
| 1: y | y | y | y | y | n | n | rest | | | none |

5.11.2 Route Pattern for International Calls to Verizon

Repeat the steps in **Section 5.11.1** 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 No | FRL | NPA | Pfx Mrk | Hop Lmt | Toll List | No. Del | Inserted Digits | DCS/ QSIG | IXC | |
| 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 |

5.11.3 Route Pattern for Service Calls to Verizon

Repeat the steps in **Section 5.11.1** 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
                                           Intw
1: 1      0
2:
3:
                                           n   user
                                           n   user
                                           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
```

5.11.4 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 5.13** (e.g., calls to Avaya SIP telephone extensions or Messaging).

Step 1 - Repeat the steps in **Section 5.11.1** 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
2:
3:
                                           n   user
                                           n   user
                                           n   user

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

5.12. 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 0**. 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 5.11**).

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 17xxxxxxxx.
- 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 | | Route | Call | Node | ANI |
| | | Min | Max | Pattern | Type | Num | Reqd |
| | 1720 | 11 | 11 | 1 | fnpa | | n |
| | 18 | 11 | 11 | 1 | fnpa | | n |
| | 19 | 11 | 11 | 1 | fnpa | | n |
| | 1900 | 11 | 11 | deny | fnpa | | n |
| | 1900555 | 11 | 11 | deny | fnpa | | n |
| | 1xxx976 | 11 | 11 | deny | fnpa | | n |
| | 311 | 3 | 3 | 4 | svcl | | n |
| | 011 | 10 | 18 | 2 | intl | | n |
| | 411 | 3 | 3 | 4 | svcl | | n |
| | 5 | 10 | 10 | 1 | fnpa | | n |

5.13. 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 | Total | | Route | Call | Node | ANI | |
| | String | Min | Max | Pattern | Type | Num | Reqd | |
| 50 | | 5 | 5 | 3 | lev0 | | n | |

5.14. Avaya G430 Media Gateway Provisioning

In the reference configuration, an Avaya G430 Media Gateway is provisioned. The G430 is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below. For additional information for the provisioning of the Medias Gateway see Error! Reference source not found..

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

Step 2 - Enter the **show system** command and copy down the G430 serial number.

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 5.5**).

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

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

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

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

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

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

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

                                     Type: g430
                                     Name: G430-1
                                     Serial No: 11IS31439520
Link Encryption Type: any-ptls/tls      Enable CF? n
Network Region: 1                      Location: 1
Use for IP Sync? n                     Site Data:
Recovery Rule: none

Registered? y
FW Version/HW Vintage: 41 .24 .0 /1
MGP IPV4 Address: 10.64.91.91
MGP IPV6 Address:
Controller IP Address: 10.64.91.75
MAC Address: 00:1b:4f:53:37:69

Mutual Authentication? optional
```

5.15. Avaya Aura® Media Server Provisioning

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

Note – Only the Media Server provisioning associated with Communication Manager is shown below. See Error! Reference source not found. and Error! Reference source not found. 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 5.4**) 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., **80**), 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 5.4**.
 - **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 5.4** (e.g., **AMS801**).
 - **Near-end Listen Port** and **Far-end Listen Port** – The default ports **9061** and **5061** are used. These ports may be changed to other values if desired.
 - **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.7.1**.
 - **Far-end Domain** – Automatically populated with the IP address of the Media Server.

```
add signaling-group 80                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 80                Group Type: sip
                                Transport Method: tls

Peer Detection Enabled? n  Peer Server: AMS

Near-end Node Name: procr                Far-end Node Name: AMS801
Near-end Listen Port: 9061              Far-end Listen Port: 5061
                                Far-end Network Region: 1

Far-end Domain: 10.64.91.86
```

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., **80**).
- **Voip Channel License Limit** – Enter the number of VoIP channels for this Media Server (based on licensing) (e.g., **300**).
- **Dedicated Voip Channel Licenses** – Enter the number of VoIP channels licensed to this Media Server (e.g., **300**).
- Remaining fields are automatically populated based on the signaling group provisioning for the Media Server.

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

Media Server ID: 1

    Signaling Group: 80
    Voip Channel License Limit: 300
    Dedicated Voip Channel Licenses: 300

Node Name: AMS801
Network Region: 1
Location: 1
Announcement Storage Area: ANNC-be99ad1a-1f39-41e5-ba04-000c29f8f3f3
```

5.16. Save Translations

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

5.17. 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. Follow the steps below 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 Certificates** 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) for server cm8. The left sidebar contains navigation links: Alarms, SNMP, Diagnostics, and Server. The main content area is titled "Trusted Certificates" and includes a description, a legend for Trusted Repositories (A, C, W, R, F), and a table of certificates.

| 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_sseca_root.crt | SCCAN Server Root CA | SCCAN Server Root CA | Sun Dec 04 2033 | C |
| <input type="radio"/> sip_product_root.crt | SIP Product Certificate Authority | SIP Product Certificate Authority | Tue Aug 17 2027 | C W R |

Buttons at the bottom: Display, Add, Remove, Copy, Help.

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

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) for server cm8. The left sidebar contains navigation links: Alarms, SNMP, Diagnostics, and Server. The main content area is titled "Server/Application Certificates" and includes a description, a legend for Certificate Repositories (A, C, W, R, F), and a table of certificates.

| 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 | SIP Product Certificate Authority | Tue Jan 28 2025 | W |

Buttons at the bottom: Display, Add, Remove, Copy, Help.

6. Configure Avaya Aura® Session Manager

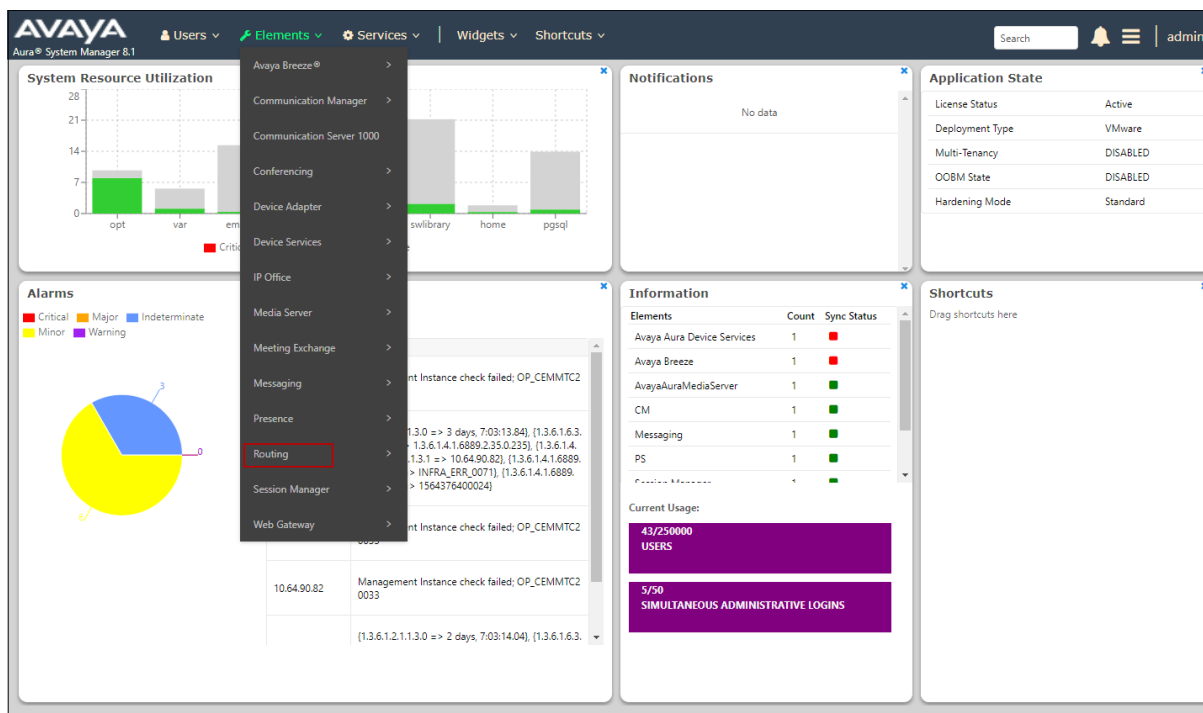
This section provides the procedures for configuring Session Manager to process inbound and outbound calls between Communication Manager and the Avaya SBCE. In the reference configuration, all Session Manager provisioning is performed via System Manager.

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

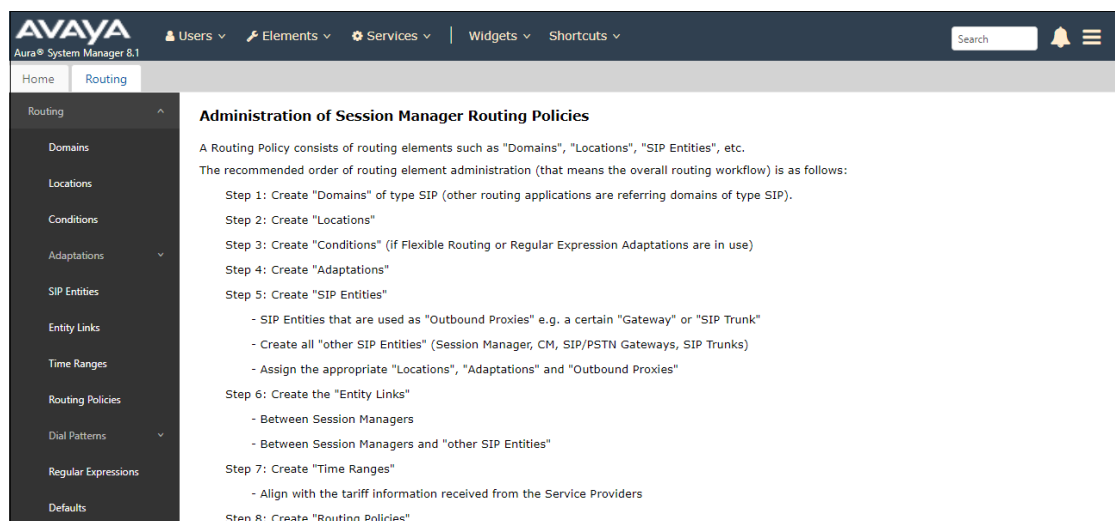
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1]- [4] in the Additional References section for further details.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading, select **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** element shown below.



6.2. 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.



6.3. 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-SBCs** – Avaya SBCE.

6.3.1 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

Add Remove

0 Items Filter: Enable

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

6.3.2 Common-SBCs Location

To configure the Avaya SBCE Location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

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

6.4. 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 6.4.1**) - 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 6.4.2**) - 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**).

6.4.1 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 the enterprise domain “avayalab.com”. For example, for inbound PSTN calls from Verizon to Communication Manager, the PAI header will contain “avayalab.com”.

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

The screenshot shows the 'Adaptation Details' configuration page. The left sidebar has a menu with 'Routing' selected, and 'Adaptations' is highlighted. The main area is titled 'Adaptation Details' and has a 'General' tab. At the top right are 'Commit' and 'Cancel' buttons. The configuration fields are as follows:

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

Below these is a table for parameters:

| Name | Value |
|--------|--------------|
| fromto | true |
| osrcd | avayalab.com |

At the bottom, there are fields for 'Egress URI Parameters' (empty) and 'Notes' (CM - Vz - IPT). A 'Select : All, None' dropdown is also present.

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

Add Remove

4 Items Filter: 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

Commit Cancel

6.4.2 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 6.4.1** 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 5.8.1**) and replace them with Diversion headers.

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

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

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

The screenshot shows the 'Adaptation Details' page in a web application. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations (selected), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. At the top right of the main area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The form contains the following fields and values:

- Adaptation Name:** SBC1-Adaptation for Verizon
- Module Name:** VerizonAdapter (selected from a dropdown)
- Module Parameter Type:** Name-Value Parameter (selected from a dropdown)

Below these fields is a table for Name-Value Parameters:

| 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 |

Below the table is a 'Select : All, None' dropdown. At the bottom of the form are two more fields:

- Egress URI Parameters:** (empty)
- 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 3**, the E.164 formatted numbers sent by Communication Manager's public-unknown numbering table (**Section 5.9**) on the outbound origination headers, need to be converted to 10 digit numbers expected by Verizon.
 - Enter + in the **Matching Pattern** column.
 - Enter **12** in the **Min/Max** columns.
 - Enter **2** in the **Delete Digits** column.
 - Specify that this should be applied to the SIP **origination** headers in the **Address to modify** column.
 - Enter any desired notes

| Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Adaptation Data | Notes |
|------------------|-----|-----|---------------|---------------|---------------|-------------------|-----------------|--|
| + | 12 | 12 | | 2 | | origination | | E.164 to 10 digit Calling Party Number |

Select : All, None

Commit Cancel

6.5. SIP Entities

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

- Session Manager (**Section 6.5.1**).
- Communication Manager for Verizon trunk access (**Section 6.5.2**) – 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 6.5.3**) – 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 6.5.4**) – 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.

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 ports 5060 and 5071 per Verizon requirements.

6.5.1 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., **Session Manager**).

Note – the **IP Address Family** in the SIP Entity form only needs to be specified if both IPv4 and IPv6 addresses have been enabled in Session Manager. If only IPv4 is enabled, the **IP Address Family** field is not present, and the **IPv4 Address** field is renamed as **IP Address**.

- **IP Address Family** – Select **IPv4**.
- **IPv4 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 6.3.1**).
- **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 in the Avaya Aura Session Manager interface. The left-hand navigation pane shows the 'SIP Entities' option selected under the 'Routing' category. The main configuration area is split into two sections: 'General' and 'Monitoring'. In the 'General' section, the 'Name' is set to 'Session Manager', 'IP Address Family' is 'IPv4', 'IPv4 Address' is '10.64.91.81', 'SIP FQDN' is empty, 'Type' is 'Session Manager', 'Location' is 'Main', 'Outbound Proxy' is empty, 'Time Zone' is 'America/Denver', 'Minimum TLS Version' is 'Use Global Setting', and 'Credential name' is empty. In the 'Monitoring' section, both 'SIP Link Monitoring' and 'CRLF Keep Alive Monitoring' are set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the configuration area.

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 6.6**. Click on **Add** and provision entries as follows:

- **Port** – Enter **5061**.
- **Protocol** – Select **TLS**.
- **Default Domain** – Select a SIP domain administered in **Section 6.26.2** (e.g., **avayalab.com**).

Step 5 - Enter any notes as desired and leave all other fields on the page blank/default.

Step 6 - Click on **Commit**.

The screenshot shows the 'Listen Ports' section of a configuration page. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '1 Item' with a refresh icon and a 'Filter: Enable' link. A table lists the configured ports:

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

At the bottom left, it says 'Select : All, None'.

Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 6.6**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.

6.5.2 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**).
- **IP Address Family** – Select **IPv4**.
- **FQDN or IPv4 Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 5.5** (e.g., **10.64.91.75**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM-TG1-VzIPT** administered in **Section 6.4.1**.
- **Location** – Select a Location **Main** administered in **Section 6.3.1**.
- **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

General

* Name:

* IP Address Family: Tolerance: ☐

* FQDN or IPv4 Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

* SIP Timer B/F (in seconds):

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

6.5.3 Avaya Aura® Communication Manager SIP Entity – Local Trunk

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **CM-TG3**).
- **Adaptations** – Leave this field blank.

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** CM-TG3
- IP Address Family:** IPv4
- Tolerance:** ☐
- FQDN or IPv4 Address:** 10.64.91.75
- Type:** CM
- Notes:** Trunk Group 3 - CM to Enterprise
- Adaptation:** (empty dropdown)
- Location:** Main
- Time Zone:** America/Denver

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

6.5.4 Avaya Session Border Controller for Enterprise SIP Entity

Repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **SBC1**).
- **FQDN or IPv4 Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.64.91.50**, see **Section 7.5**).
- **Type** – Select **SIP Trunk**.
- **Adaptations** – Select Adaptation **SBC1-Adaptation for Verizon** (**Section 6.4.2**).
- **Location** – Select Location **Common-SBCs** administered in **Section 6.3.2**.

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** SBC1
- IP Address Family:** IPv4
- Tolerance:** ☐
- FQDN or IPv4 Address:** 10.64.91.50
- Type:** SIP Trunk
- Notes:** Avaya SBC-1 to PSTN
- Adaptation:** SBC1-Adaptation for Verizon
- Location:** Common-SBCs
- Time Zone:** America/Denver

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

6.6. Entity Links

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

- Session Manager to Communication Manager Public trunk (**Section 6.6.1**).
- Session Manager to Communication Manager Local trunk (**Section 6.6.2**).
- Session Manager to Avaya SBCE (**Section 6.6.3**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.5**.

Note – See the information in **Section 6.5** regarding the transport protocols and ports used in the reference configuration.

6.6.1 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 6.5.1** for Session Manager (e.g., **Session Manager**).
- **Protocol** – Select **TLS** (see **Section 5.8.1**).
- **SIP Entity 1 Port** – Enter **5081**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public entity (e.g., **CM-TG1**).
- **SIP Entity 2 Port** – Enter **5081** (see **Section 5.8.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.

Step 3 - Click on **Commit**.

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | IP Address Family | DNS Override | Connection Policy | Deny New Service |
|----------------|-------------------|----------|--------|--------------|--------|-------------------|--------------------------|-------------------|--------------------------|
| * SM to CM TG1 | * Session Manager | TLS | * 5081 | * CM-TG1 | * 5081 | IPv4 | <input type="checkbox"/> | trusted | <input type="checkbox"/> |

Select : All, None

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

To configure this Entity Link, repeat the steps in **Section 6.6.1**, 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 6.5.3** for the Communication Manager local entity (e.g., **CM-TG3**).
- **SIP Entity 2 Port** – Enter **5061** (see **Section 5.8.12**).

The screenshot shows the 'Entity Links' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (selected). The main area has a title 'Entity Links' and 'Commit' and 'Cancel' buttons. Below is a table with 1 item. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, Connection Policy, and Deny New Service. The row contains: Name: SM to CM TG3, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5061, SIP Entity 2: CM-TG3, Port: 5061, IP Address Family: IPv4, DNS Override: (unchecked), Connection Policy: trusted, Deny New Service: (unchecked). Below the table is a 'Select: All, None' dropdown.

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | IP Address Family | DNS Override | Connection Policy | Deny New Service |
|--------------|-----------------|----------|------|--------------|------|-------------------|--------------------------|-------------------|--------------------------|
| SM to CM TG3 | Session Manager | TLS | 5061 | CM-TG3 | 5061 | IPv4 | <input type="checkbox"/> | trusted | <input type="checkbox"/> |

6.6.3 Entity Link for the Verizon Business IP Trunking service via the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.6.1**, 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 6.5.4** for the Avaya SBCE entity (e.g., **SBC1**).
- **SIP Entity 2 Port** – Enter **5061**.

The screenshot shows the 'Entity Links' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (selected). The main area has a title 'Entity Links' and 'Commit' and 'Cancel' buttons. Below is a table with 1 item. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, IP Address Family, DNS Override, Connection Policy, and Deny New Service. The row contains: Name: SM to SBC1, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5061, SIP Entity 2: SBC1, Port: 5061, IP Address Family: IPv4, DNS Override: (unchecked), Connection Policy: trusted, Deny New Service: (unchecked). Below the table is a 'Select: All, None' dropdown.

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | IP Address Family | DNS Override | Connection Policy | Deny New Service |
|------------|-----------------|----------|------|--------------|------|-------------------|--------------------------|-------------------|--------------------------|
| SM to SBC1 | Session Manager | TLS | 5061 | SBC1 | 5061 | IPv4 | <input type="checkbox"/> | trusted | <input type="checkbox"/> |

6.7. 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.

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

6.8. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (**Section 6.8.1**).
- Outbound calls to Verizon/PSTN (**Section 6.8.22**).

6.8.1 Routing Policy for Verizon Inbound Calls 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.

| Name | IP Address Family | FQDN or IPv4 Address | FQDN or IPv6 Address | Type | Notes |
|------|-------------------|----------------------|----------------------|------|-------|
|------|-------------------|----------------------|----------------------|------|-------|

Step 4 - In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.2** for the Communication Manager public SIP Entity (**CM-TG1**), and click on **Select**.

SIP Entities Select Cancel Help ?

SIP Entities

19 Items Filter: Enable

| | Name | IP Address Family | FQDN or IPv4 Address | FQDN or IPv6 Address | Type | Notes |
|-----------------------|------------------|-------------------|----------------------|------------------------|-------------------|--------------------------------------|
| <input type="radio"/> | Aura Messaging | IPv4 | 10.64.91.84 | | Messaging | Aura Messaging |
| <input type="radio"/> | Breeze | IPv4 | 10.64.91.18 | | Avaya Breeze | |
| <input type="radio"/> | CM-TG1 | IPv4 | 10.64.91.75 | | CM | Trunk Group 1 - CM to Vz-IPT |
| <input type="radio"/> | CM-TG2 | IPv4 | 10.64.91.75 | | CM | Trunk Group 2 - Vz-Toll-Free inbound |
| <input type="radio"/> | CM-TG3 | IPv4 | 10.64.91.75 | | CM | Trunk Group 3 - CM to Enterprise |
| <input type="radio"/> | CM-TG4 | IPv4 | 10.64.91.75 | | CM | Trunk Group 4 - ATT IPTF |
| <input type="radio"/> | CM-TG5 | IPv4 | 10.64.91.75 | | CM | Trunk Group 5 - ATT IPFR |
| <input type="radio"/> | CM-TG6 | IPv6 | | fd22:305b:b390:14e6::5 | CM | CM IPv6 trunk for AT&T TF |
| <input type="radio"/> | CM-TG7 | IPv6 | | fd22:305b:b390:14e6::5 | CM | CM IPv6 trunk for AT&T IPFR |
| <input type="radio"/> | CM-TG9 | IPv4 | 10.64.91.75 | | CM | Masergy |
| <input type="radio"/> | ExperiencePortal | IPv4 | 10.64.91.90 | | Voice Portal | |
| <input type="radio"/> | Presence | IPv4 | 10.64.91.18 | | Presence Services | |
| <input type="radio"/> | SBC1 | IPv4 | 10.64.91.50 | | SIP Trunk | Avaya SBC-1 to PSTN |
| <input type="radio"/> | SBC2-100 | IPv4 | 10.64.91.100 | | SIP Trunk | Avaya SBC-2 to PSTN |
| <input type="radio"/> | SBC2-101 | IPv4 | 10.64.91.101 | | SIP Trunk | SBCE Masergy |

Select : None Page 1 of 2

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 6.7**, 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 6.9**) 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 | IP Address Family | FQDN or IPv4 Address | FQDN or IPv6 Address | Type | Notes |
|--------|-------------------|----------------------|----------------------|------|------------------------------|
| CM-TG1 | IPv4 | 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 |
|----------------------------|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-------|
| <input type="checkbox"/> 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

6.8.2 Routing Policy for Outbound Calls to Verizon

This Routing Policy is used for outbound calls to Verizon. Repeat the steps in **Section 6.8.1** 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**).
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.4** for the Avaya SBCE SIP Entity (e.g., **SBC1**).

The screenshot shows the 'Routing Policy Details' configuration page. The left sidebar contains a navigation menu with options: Domains, Locations, Conditions, Adaptations, SIP Entities, Entry Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. At the top right of the main area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The 'General' section contains the following fields:

- Name:** To SBC1
- Disabled:** ☐
- Retries:** 0
- Notes:** (empty text area)

Below the 'General' section is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

| Name | IP Address Family | FQDN or IPv4 Address | FQDN or IPv6 Address | Type | Notes |
|------|-------------------|----------------------|----------------------|-----------|---------------------|
| SBC1 | IPv4 | 10.64.91.50 | | SIP Trunk | Avaya SBC-1 to PSTN |

Below the 'SIP Entity as Destination' section is the 'Time of Day' section, which includes an 'Add' button, a 'Remove' button, and a 'View Gaps/Overlaps' button. It also features a 'Filter: Enable' link. The 'Time of Day' section contains a table with the following data:

| 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 | |

At the bottom of the 'Time of Day' section is a 'Select : All, None' dropdown menu.

6.9. 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 6.9.1).
- Outbound calls to Verizon/PSTN (Section 6.9.2).

6.9.1 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 **7329450**. Note – The Adaptation defined for Communication Manager in Section 6.4.1 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, Origination Dial Pattern Sets, and Routing Policies

Add Remove

0 Items Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Origination Dial Pattern Set Name | Origination Dial Pattern Set Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|-----------------------------------|------------------------------------|---------------------|------|-------------------------|----------------------------|----------------------|
|--------------------------|---------------------------|----------------------------|-----------------------------------|------------------------------------|---------------------|------|-------------------------|----------------------------|----------------------|

Step 3 - Scroll down to the **Originating Locations, Origination Dial Patterns 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-SBCs**.

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 6.8.1** (e.g., **To CM TG1**) and click on **Select**.

Originating Location

Help ?

SelectCancel

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-SBCs | SBC to PSTN |
| <input type="checkbox"/> | Main | Avaya SIL |
| <input type="checkbox"/> | RemoteAccess | Remote Access from SBCE1 |

Select : All, None

Origination Dial Pattern Sets

0 Items

Filter: Enable

| Name | Notes |
|------|-------|
|------|-------|

Routing Policies

14 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 |

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.

6.9.2 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 6.9.1**, 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, Origination Dial Patterns 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 6.8.2** (e.g., **To SBC1**).

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: +

* Min: 10

* Max: 36

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: E.164 Public Numbers

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

Add Remove

7 Items Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Origination Dial Pattern Set Name | Origination Dial Pattern Set Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|-----------------------------------|------------------------------------|---------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | Main | Avaya SIL | | | To SBC1 | 0 | <input type="checkbox"/> | SBC1 | |

Select : All, None

Denied Originating Locations and Origination Dial Pattern Sets

Add Remove

0 Items

| <input type="checkbox"/> | Originating Location | Notes | Origination Dial Pattern Set Name | Origination Dial Pattern Set Notes |
|--------------------------|----------------------|-------|-----------------------------------|------------------------------------|
|--------------------------|----------------------|-------|-----------------------------------|------------------------------------|

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

Dial Patterns Help ?

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 |

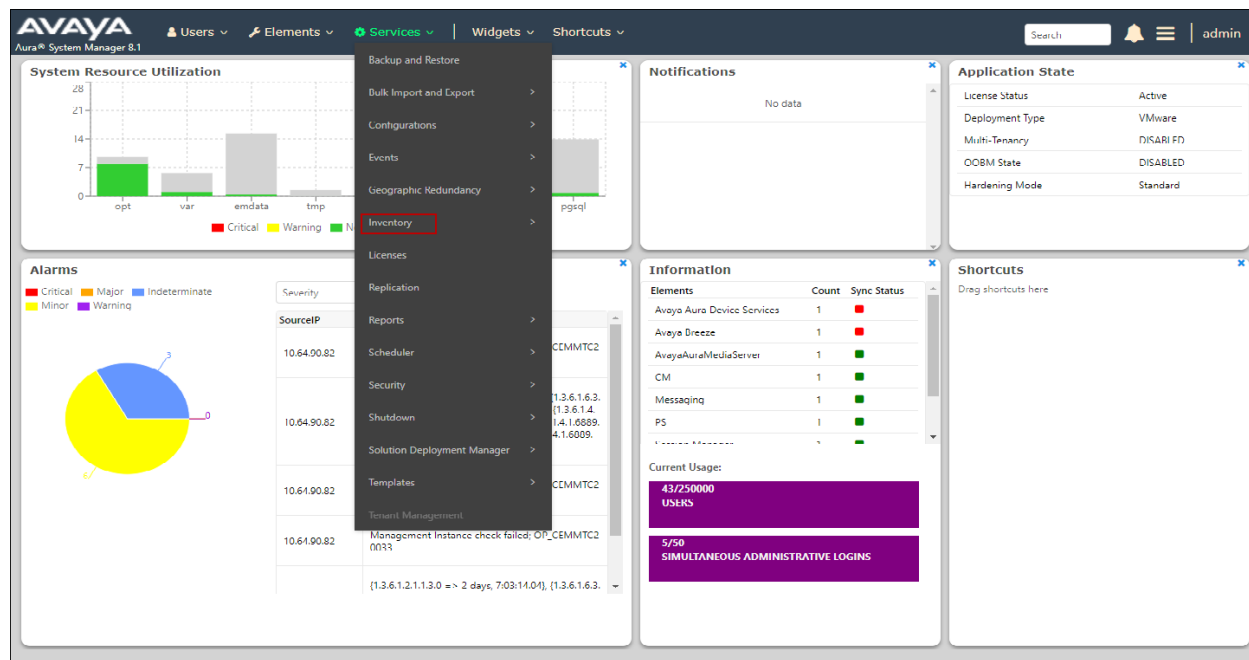
Select : All, None

6.10. Verify TLS Certificates – Session Manager

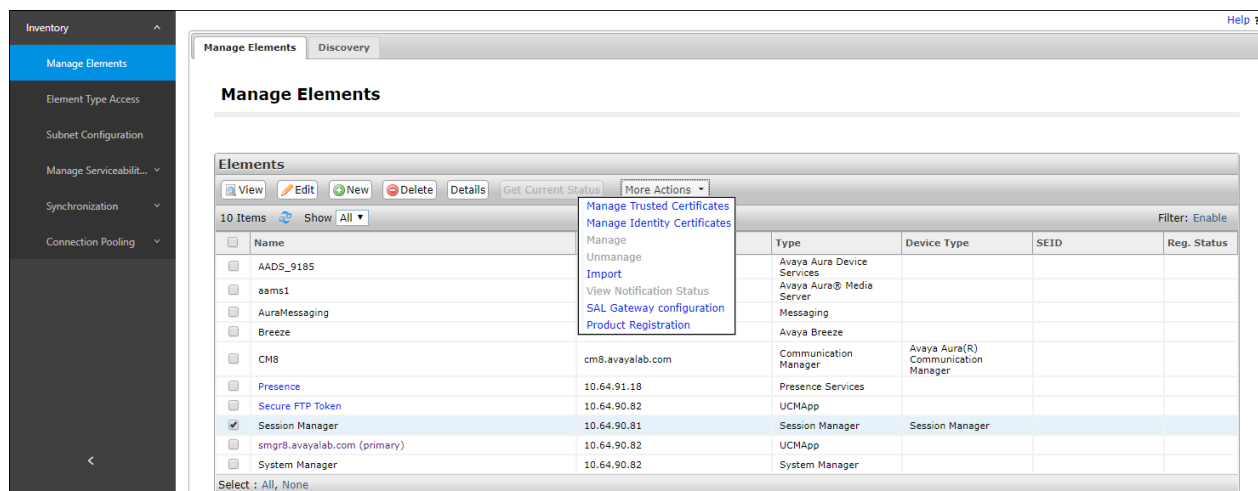
Note – Testing was done with System Manager signed identity certificates. The procedure to obtain and install certificates is outside the scope of these Application Notes.

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

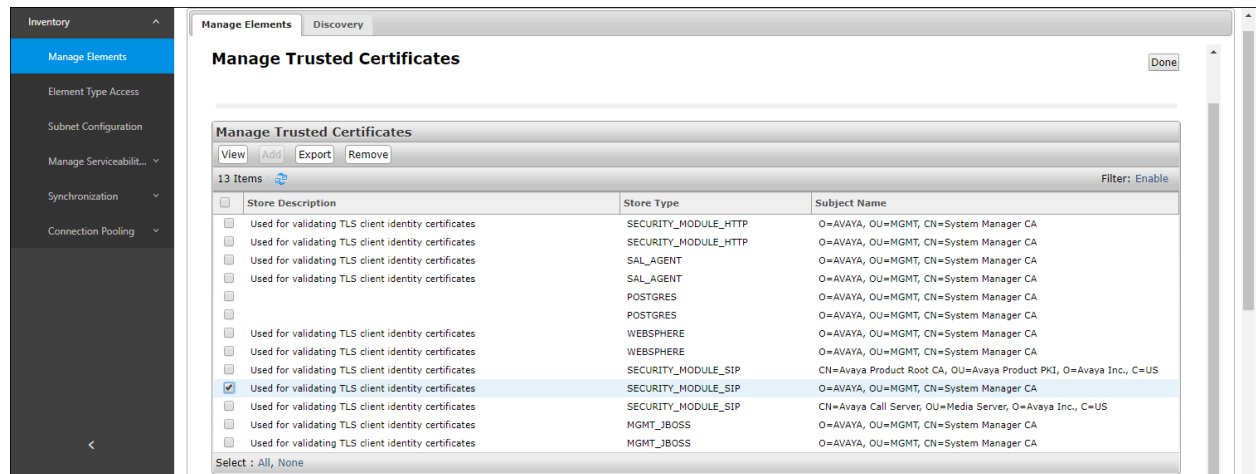
Step 1 - From the **Home** screen, under the **Services** heading, select **Inventory**.



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

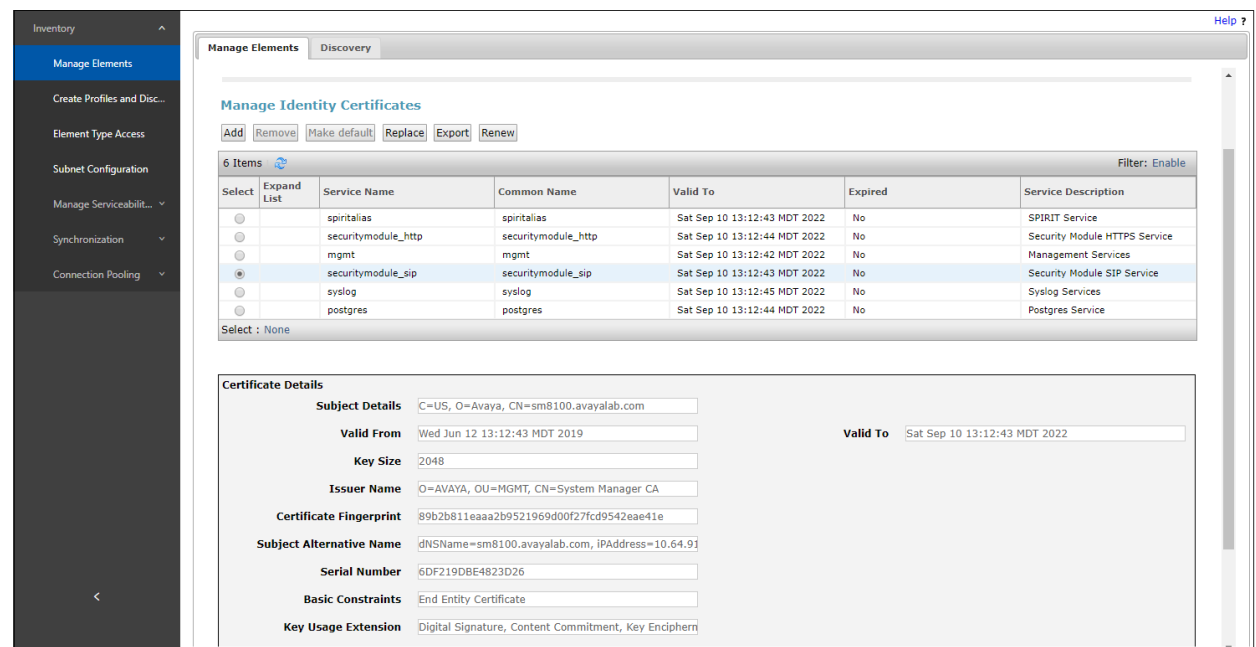


Step 3 - Verify the **System Manager** Certificate Authority certificate is listed in the trusted store, **SECURITY_MODULE_SIP**. Click **Done** to return to the previous screen.



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).



7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the initial provisioning of the Avaya SBCE, including the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

Use a WEB browser to access the Element Management Server (EMS) web interface, and enter `https://ipaddress/sbc` in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE. Log in using the appropriate credentials.



The login page features the Avaya logo on the left and a 'Log In' section on the right. The 'Log In' section includes fields for 'Username' (containing 'ucsec') and 'Password' (masked with dots), followed by a 'Log In' button. Below the login fields, there is a 'WELCOME TO AVAYA SBC' message, a disclaimer about unauthorized access, a consent statement, and a copyright notice for 2011-2019 Avaya Inc.

AVAYA

Session Border Controller for Enterprise

Log In

Username:

Password:

WELCOME TO AVAYA SBC

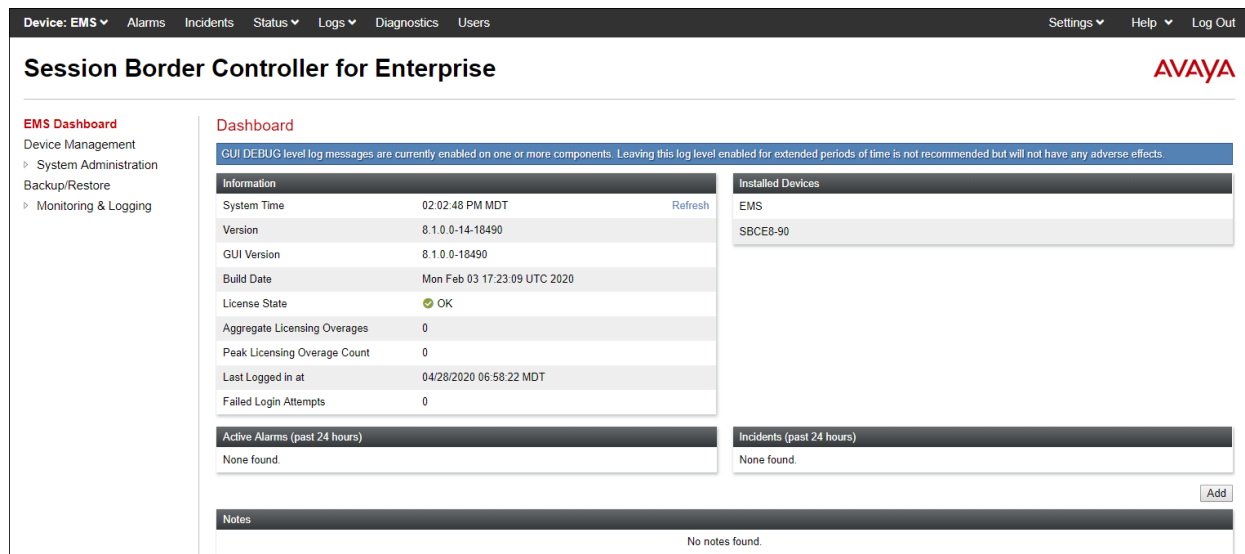
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

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.

© 2011 - 2019 Avaya Inc. All rights reserved.

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

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



The dashboard shows system information, installed devices, active alarms, incidents, and notes. The 'Information' table lists system time, version, GUI version, build date, license state (OK), and licensing overages. The 'Installed Devices' table lists EMS and SBCE8-90. The 'Active Alarms' and 'Incidents' sections show 'None found'. The 'Notes' section also shows 'No notes found'.

Device: EMS | Alarms | Incidents | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
 - System Administration
 - Backup/Restore
 - Monitoring & Logging

Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

| Information | |
|------------------------------|------------------------------|
| System Time | 02:02:48 PM MDT |
| Version | 8.1.0.0-14-18490 |
| GUI Version | 8.1.0.0-18490 |
| Build Date | Mon Feb 03 17:23:09 UTC 2020 |
| License State | OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 04/28/2020 06:58:22 MDT |
| Failed Login Attempts | 0 |

| Installed Devices |
|-------------------|
| EMS |
| SBCE8-90 |

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

Notes

No notes found.

7.1. Device Management – Status

Select **Device Management** on the left-hand menu. A list of installed devices is shown on the **Devices** tab on the right pane. In the case of the sample configuration, a single device named **SBCE8-90** is shown. Verify that the **Status** column shows **Commissioned**. If not, contact your Avaya representative. To view the configuration of this device, click **View** on the screen below.

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

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: EMS, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left sidebar shows the EMS Dashboard with the following menu items: EMS Dashboard, Device Management (selected), System Administration, Backup/Restore, and Monitoring & Logging. The main content area is titled 'Session Border Controller for Enterprise' and features the Avaya logo. The 'Device Management' section is active, showing a table of installed devices. The table has columns for Device Name, Management IP, Version, and Status. A single device, SBCE8-90, is listed with a Management IP of 10.64.90.90, Version 8.1.0.0-14-18490, and Status Commissioned. Action links for Reboot, Shutdown, Restart Application, View, Edit, and Uninstall are available for this device.

| Device Name | Management IP | Version | Status | Actions |
|-------------|---------------|------------------|--------------|---|
| SBCE8-90 | 10.64.90.90 | 8.1.0.0-14-18490 | Commissioned | Reboot Shutdown Restart Application View Edit Uninstall |

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation, corresponding to **Figure 1**. 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 interfaces **A1** and **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: SBCE8-90

General Configuration

Appliance Name

SBCE8-90

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

Dynamic License Allocation

| | Min License Allocation | Max License Allocation |
|-----------------------|--|------------------------|
| Standard Sessions | 10 | 100 |
| Advanced Sessions | 10 | 100 |
| Scopia Video Sessions | 10 | 100 |
| CES Sessions | 10 | 100 |
| Transcoding Sessions | 10 | 100 |
| CLID | --- | |
| Encryption | Available: Yes <input checked="" type="checkbox"/> | |

Network Configuration

| IP | Public IP | Network Prefix or Subnet Mask | Gateway | Interface |
|-------------|-------------|-------------------------------|------------|-----------|
| 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 |
| 1.1.1.2 | 1.1.1.2 | 255.255.255.0 | 1.1.1.1 | B1 |
| | | 255.255.255.128 | | B2 |
| | | 255.255.255.128 | | B2 |

DNS Configuration

Primary DNS

172.30.209.4

Secondary DNS

DNS Location

DMZ

DNS Client IP

1.1.1.2

Management IP(s)

IP #1 (IPv4)

10.64.90.90

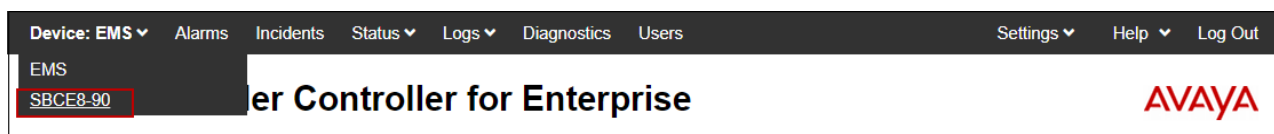
7.2. TLS Management

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

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

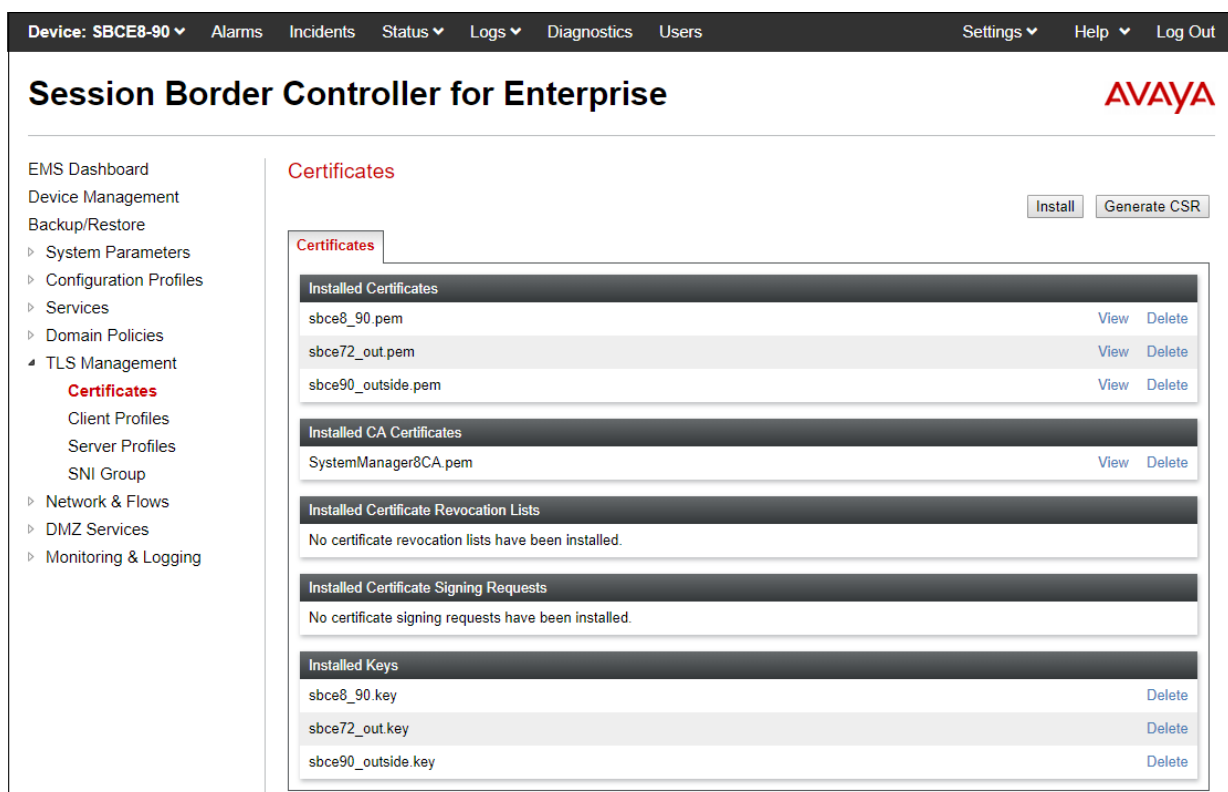
7.2.1 Verify TLS Certificates – Avaya Session Border Controller for Enterprise

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.



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

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



7.2.2 Server Profiles

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


- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_90.pem**, from pull down menu.
- **Peer Verification** = **None**.
- Click **Next**.

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

The screenshot shows a dialog box 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 dialog is divided into two main sections. The first section, "TLS Profile", contains four fields: "Profile Name" with the value "Inside_Server", "Certificate" with a dropdown menu showing "sbce8_90.pem", "SNI Options" with a dropdown menu showing "None", and "SNI Group" with a dropdown menu showing "None". The second section, "Certificate Verification", contains four fields: "Peer Verification" with a dropdown menu showing "None", "Peer Certificate Authorities" with a text box containing "SystemManager8CA.pem", "Peer Certificate Revocation Lists" with an empty text box, and "Verification Depth" with a text box containing "0". At the bottom right of the dialog, there is a "Next" button.

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

Session Border Controller for Enterprise



EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

- Certificates
- Client Profiles
- Server Profiles**
- SNI Group

Network & Flows

DMZ Services

Monitoring & Logging

Server Profiles: Inside_Server

Add

Delete

Server Profiles

Inside_Server

Outside_Server

Click here to add a description.

Server Profile

TLS Profile

Profile Name

Inside_Server

Certificate

sbce8_90.pem

SNI Options

None

Certificate Verification

Peer Verification

None

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0

Ciphers

☒ Default ☐ FIPS ☐ Custom

Value

HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

7.2.3 Client Profiles

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

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **sbce8_90.pem**, 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., **SystemManager8CA.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 red warning box with the text: "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 form is divided into two main sections: "TLS Profile" and "Certificate Verification".

TLS Profile

- Profile Name:** A text input field containing "Inside_Client".
- Certificate:** A dropdown menu showing "sbce8_90.pem".
- SNI:** A checkbox labeled "Enabled" which is currently unchecked.


Certificate Verification

- Peer Verification:** A label with the value "Required" next to it.
- Peer Certificate Authorities:** A list box containing "SystemManager8CA.pem".
- Peer Certificate Revocation Lists:** An empty list box.
- Verification Depth:** A text input field containing the number "1".
- Extended Hostname Verification:** A checkbox which is currently unchecked.
- Server Hostname:** An empty text input field.

At the bottom right of the form, there is a "Next" button.

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

Session Border Controller for Enterprise



EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

- Certificates
- Client Profiles**
- Server Profiles
- SNI Group

Network & Flows

DMZ Services

Monitoring & Logging

Client Profiles: Inside_Client

Add

Delete

Client Profiles

Inside_Client

Outside_Client

Click here to add a description.

Client Profile

TLS Profile

Profile NameInside_Client

Certificatesbce8_90.pem

SNI☐ Enabled

Certificate Verification

Peer VerificationRequired

Peer Certificate AuthoritiesSystemManager8CA.pem

Peer Certificate Revocation Lists---

Verification Depth1

Extended Hostname Verification☐

Renegotiation Parameters

Renegotiation Time0

Renegotiation Byte Count0

Handshake Options

Version☒ TLS 1.2☐ TLS 1.1☐ TLS 1.0

Ciphers☒ Default☐ FIPS☐ Custom

ValueHIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

7.3. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Step 1 - Select **Networks & Flows** → **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 and B1 are used.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Network Management' section active. The 'Interfaces' tab is selected, displaying a table of network interfaces. The table has three columns: 'Interface Name', 'VLAN Tag', and 'Status'. The interfaces listed are A1 (Enabled), A2 (Disabled), B1 (Enabled), and B2 (Enabled). There is an 'Add VLAN' button in the top right corner of the table area. The left sidebar shows the navigation menu with 'Network Management' highlighted under 'Network & Flows'.

| 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.

- **A1: 10.64.91.50** – “Inside” IP address, toward Session Manager.
- **B1: 1.1.1.2** – “Outside” IP address toward the Verizon SIP trunk. This address is known to Verizon.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Network Management' section active. The 'Networks' tab is selected, displaying a table of network configurations. The table has five columns: 'Name', 'Gateway', 'Subnet Mask / Prefix Length', 'Interface', and 'IP Address'. The configurations listed are 'Inside A1' (Gateway: 10.64.91.1, Subnet: 255.255.255.0, Interface: A1, IP: 10.64.91.48, 10.64.91.49, 10.64.91.50), 'Verizon B1' (Gateway: 1.1.1.1, Subnet: 255.255.255.0, Interface: B1, IP: 1.1.1.2), and 'Public B2' (Gateway: [redacted], Subnet: 255.255.255.128, Interface: B2, IP: [redacted]). Each row has 'Edit' and 'Delete' buttons. There is an 'Add' button in the top right corner of the table area. The left sidebar shows the navigation menu with 'Network Management' highlighted under 'Network & Flows'.

| Name | Gateway | Subnet Mask / Prefix Length | Interface | IP Address | |
|------------|------------|-----------------------------|-----------|---|-------------|
| 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 |
| Verizon B1 | 1.1.1.1 | 255.255.255.0 | B1 | 1.1.1.2 | Edit Delete |
| Public B2 | [redacted] | 255.255.255.128 | B2 | [redacted] | Edit Delete |

7.4. Media Interfaces

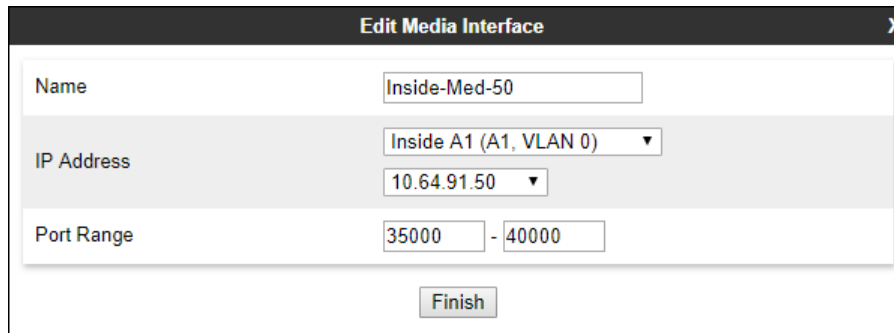
Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which the SBCE will accept media from the connected server. Create a SIP Media Interface for both the inside and outside IP interfaces.

Step 1 - Select **Network & Flows** → **Media Interface** from the menu on the left-hand side.

Step 2 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Enter an appropriate name (e.g., **Inside-Med-50**).
- **IP Address:** Select **Inside-A1 (A1,VLAN0)** and **10.64.91.50** from the drop-down menus.
- **Port Range:** **35000 – 40000**.

Step 3 - Click **Finish**.



The screenshot shows the 'Edit Media Interface' window with the following configuration:

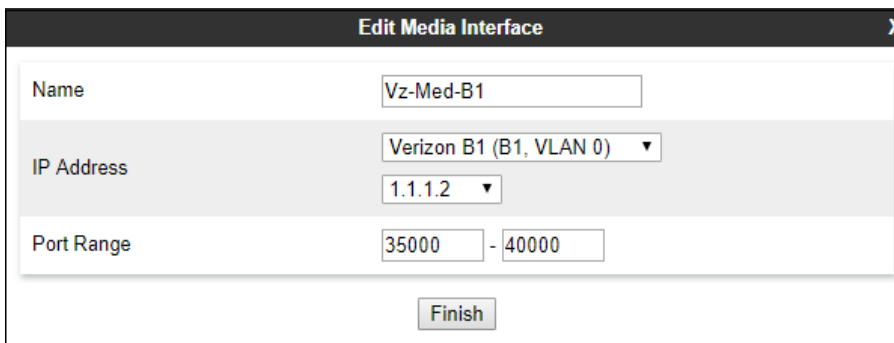
| Field | Value |
|------------|--------------------------------------|
| Name | Inside-Med-50 |
| IP Address | Inside A1 (A1, VLAN 0) / 10.64.91.50 |
| Port Range | 35000 - 40000 |

A 'Finish' button is located at the bottom center of the window.

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

- **Name:** Enter an appropriate name (e.g., **Vz-Med-B1**).
- **IP Address:** Select **Verizon-B1 (B1,VLAN0)** and **1.1.1.2** from the drop-down menus.
- **Port Range:** **35000 – 40000**.

Step 5 - Click **Finish**.



The screenshot shows the 'Edit Media Interface' window with the following configuration:

| Field | Value |
|------------|-----------------------------------|
| Name | Vz-Med-B1 |
| IP Address | Verizon B1 (B1, VLAN 0) / 1.1.1.2 |
| Port Range | 35000 - 40000 |

A 'Finish' button is located at the bottom center of the window.

7.5. Signaling Interfaces

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 **Network & Flows** → **Signaling Interface** from the menu on the left-hand side.

Step 2 - Select **Add** (not shown) and enter the following:

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

Step 3 - Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' dialog box with the following fields and values:

| Field | Value |
|-----------------------|---|
| Name | Inside-Sig-50 |
| IP Address | Inside A1 (A1, VLAN 0) (dropdown) 10.64.91.50 (dropdown) |
| TCP Port | (empty) |
| UDP Port | (empty) |
| TLS Port | 5061 |
| TLS Profile | Inside_Server (dropdown) |
| Enable Shared Control | <input type="checkbox"/> |
| Shared Control Port | (empty) |

Finish button is at the bottom right.

Step 4 - Select **Add** (not shown), and enter the following:

- **Name:** Enter an appropriate name (e.g., **Vz-Sig-B1**).
- **IP Address:** Select **Verizon B1 (B1,VLAN0)** and **1.1.1.2**.
- **UDP Port:** **5060**.

Step 5 - Click **Finish**.

The screenshot shows the 'Edit Signaling Interface' dialog box with the following fields and values:

| Field | Value |
|-----------------------|--|
| Name | Vz-Sig-B1 |
| IP Address | Verizon B1 (B1, VLAN 0) (dropdown) 1.1.1.2 (dropdown) |
| TCP Port | (empty) |
| UDP Port | 5060 |
| TLS Port | (empty) |
| TLS Profile | None (dropdown) |
| Enable Shared Control | <input type="checkbox"/> |
| Shared Control Port | (empty) |

Finish button is at the bottom right.

7.6. Server Interworking Profiles

The Server Interworking Profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below. Create separate Server Interworking Profiles for the enterprise and the service provider.

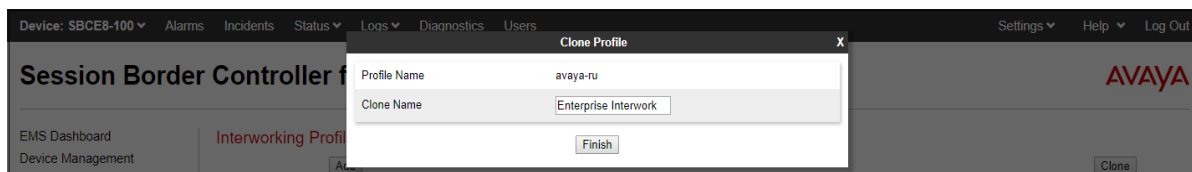
7.6.1 Server Interworking Profile – Enterprise

In the sample configuration, the enterprise Server Interworking profile was cloned from the default **avaya-ru** profile and then modified.

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

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

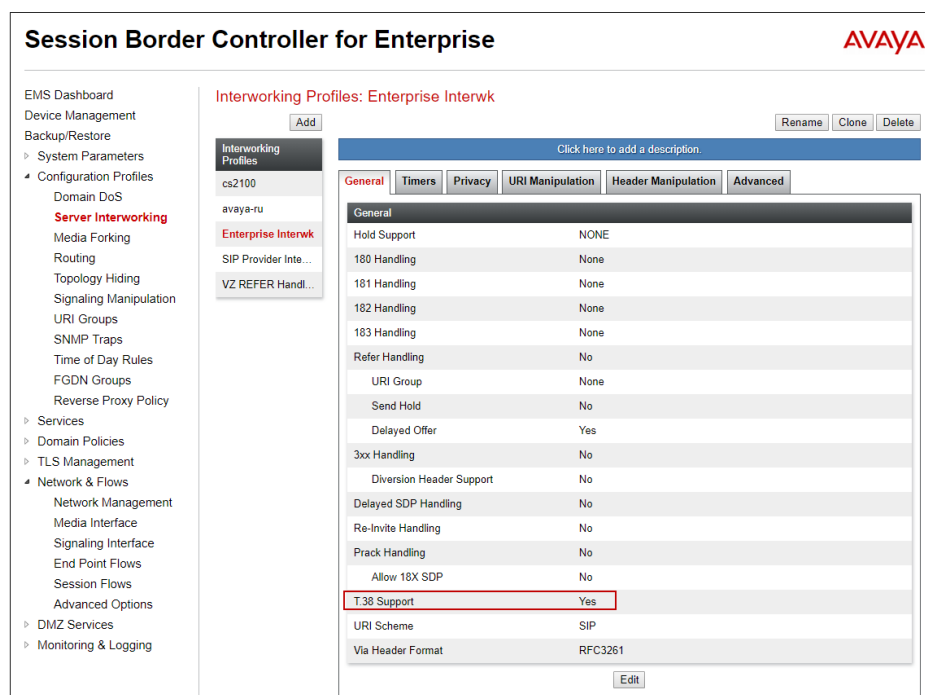
Step 3 - Enter profile name: (e.g., **Enterprise Interwork**), and click **Finish** to continue.



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

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

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



7.6.2 Server Interworking Profile – Verizon

In the sample configuration, the Server Interworking profile for Verizon was created by adding a new profile.

Step 1 - Select **Add Profile** 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** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The left sidebar shows the navigation menu with 'Configuration Profiles' expanded, and 'Server Interworking' selected. The main area shows the 'Interworking Profiles: SIP Provider Interwk' configuration page. The 'Advanced' tab is active, showing the following settings:

| Field | Value |
|---|------------|
| Record Routes | Both Sides |
| Include End Point IP for Context Lookup | No |
| Extensions | None |
| Diversion Manipulation | No |
| Has Remote SBC | Yes |
| Route Response on Via Port | No |
| Relay INVITE Replace for SIPREC | No |
| MOBX Re-INVITE Handling | No |

Below the Advanced tab, the DTMF section is visible:

| Field | Value |
|--------------|-------|
| DTMF Support | None |

The interface includes an 'Add' button for creating new profiles and 'Rename', 'Clone', and 'Delete' buttons for existing ones. The 'Edit' button is located at the bottom right of the configuration area.

7.7. 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 Server Interworking Profiles (**Section 7.6**) or Signaling Rules (**Section 7.13**) does not meet the desired result. Refer to Additional References Error! Reference source not found. for information on the Avaya SBCE scripting language.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor.

A Sigma script was created during the compliance test to correct the following interoperability issues:

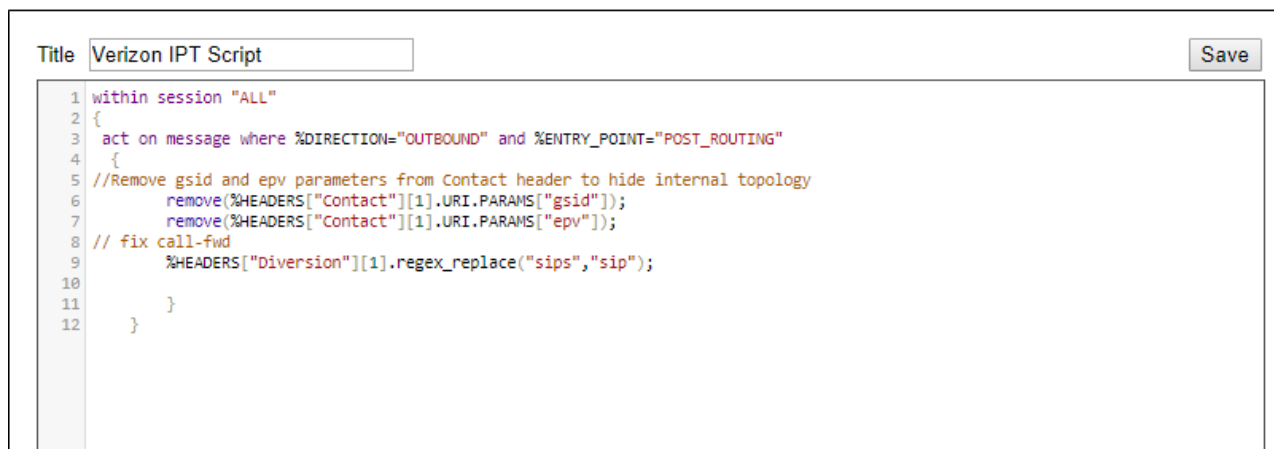
- Remove the gsid and epv parameters from the outbound Contact header. See **Section 2.4**
- Change the Diversion header scheme from SIPS to SIP towards Verizon. See **Section 2.2**

The details of the script appear on **Section 02**.

Step 1 - Select **Configuration Profiles → Signaling Manipulation** from the menu on the left.

Step 2 - Click **Add Script** (not shown) and the script editor window will open.

- Enter a name for the script in the **Title** box (e.g., **Verizon IPT script**).
- Copy and paste the script from **Section 02**.



The screenshot shows a script editor window with a title bar containing a text box with 'Verizon IPT Script' and a 'Save' button. The script content is as follows:

```
1 within session "ALL"
2 {
3   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4   {
5     //Remove gsid and epv parameters from Contact header to hide internal topology
6     remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
7     remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
8     // fix call-fwd
9     %HEADERS["Diversion"][1].regex_replace("sips","sip");
10
11   }
12 }
```

Step 3 - Click on **Save**. The script editor will test for any errors, and the window will close. This script will later be applied to the Verizon Server Configuration profile in **Section 0**.

7.8. SIP Server Profiles

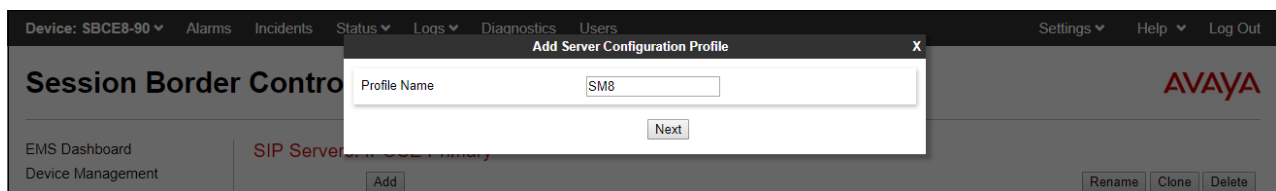
The **SIP Server Profile** contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

7.8.1 SIP Server Profile – Session Manager

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

Step 1 - Select **Services** → **SIP Servers** from the left-hand menu.

Step 2 - Select **Add** 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 7.2.3** (e.g., **Inside_Client**).
- **IP Address**: **10.64.91.81** (Session Manager Security Module IP address).
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 10.64.91.81 | 5061 | TLS |

Step 4 - Default values can be used on the **Authentication** tab.

Step 5 - On the **Heartbeat** tab, check the **Enable Heartbeat** box to have the Avaya SBCE source “heartbeats” toward Session Manager. This configuration is optional.

- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward Session Manager.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.

The screenshot shows the 'Edit SIP Server Profile - Heartbeat' window. It contains the following fields and values:

| Field | Value |
|------------------|-------------------------------------|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method | OPTIONS |
| Frequency | 120 seconds |
| From URI | SBC@avayalab.com |
| To URI | SM@avayalab.com |

A 'Finish' button is located at the bottom right of the form.

Step 6 - Default values are used on the **Registration** and **Ping** tabs.

Step 7 - On the **Advanced** tab:

- Select the **Enterprise Interwk** (created in **Section 7.6**), for **Interworking Profile**.
- Since TLS transport is specified in **Step 3**, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.

The screenshot shows the 'Edit SIP Server Profile - Advanced' window. It contains the following fields and values:

| Field | Value |
|-------------------------------|-------------------------------------|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input checked="" type="checkbox"/> |
| Interworking Profile | Enterprise Interwk |
| Signaling Manipulation Script | None |
| Securable | <input type="checkbox"/> |
| Enable FGDN | <input type="checkbox"/> |
| TCP Failover Port | |
| TLS Failover Port | |
| Tolerant | <input type="checkbox"/> |
| URI Group | None |

A 'Finish' button is located at the bottom right of the form.

7.8.2 SIP Server Profile – Verizon

Repeat the steps in **Section 7.8.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Verizon.

Note - 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).

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).
- Select **Port: 5071**, **Transport: UDP**, as specified by Verizon.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 172.30.209.21 | 5071 | UDP |

Step 4 - Default values are used on the **Authentication** tab.

Step 5 - On the **Heartbeat** tab, check the **Enable Heartbeat** box to optionally have the Avaya SBCE source “heartbeats” toward Verizon. The screen below shows the values used in the reference configuration.

| | |
|------------------|--|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method | OPTIONS |
| Frequency | 60 seconds |
| From URI | SBC1@adec.avaya.globalipcom.com |
| To URI | Vz@pcelban0001.avayalincroft.globalipcom.com |

Step 6 - Default values are used on the **Registration** and **Ping** tabs.

Step 7 - On the **Advanced** window, enter the following:

- **Enable Grooming** is not used for UDP connections and is left unchecked.
- Select the **SIP Provider Interwk** (created in **Section 7.6.2**), for **Interworking Profile**.
- Select the **Verizon IPT Script** (created in **Section 7.7**) for **Signaling Manipulation Script**.
- Select **Finish**.

| Edit SIP Server Profile - Advanced | |
|------------------------------------|--------------------------|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input type="checkbox"/> |
| Interworking Profile | SIP Provider Interwk ▼ |
| Signaling Manipulation Script | Verizon IPT Script ▼ |
| Securable | <input type="checkbox"/> |
| Enable FGDN | <input type="checkbox"/> |
| TCP Failover Port | <input type="text"/> |
| TLS Failover Port | <input type="text"/> |
| Tolerant | <input type="checkbox"/> |
| URI Group | None ▼ |
| <div>Finish</div> | |

7.9. Routing Profiles

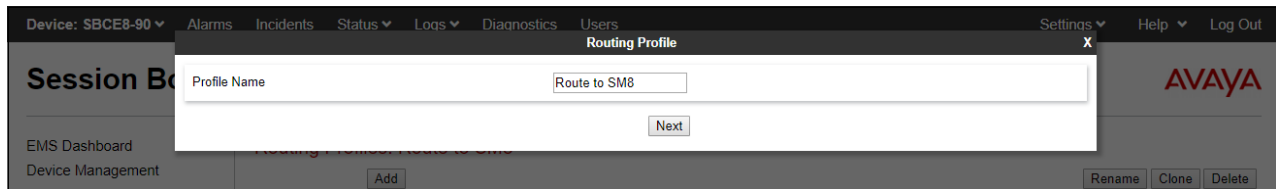
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types. Separate Routing Profiles were created in the reference configuration for Session Manager and Verizon.

7.9.1 Routing Profile – Session Manager

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

Step 1 - Select **Configuration Profiles → Routing** from the left-hand menu, and select **Add**.

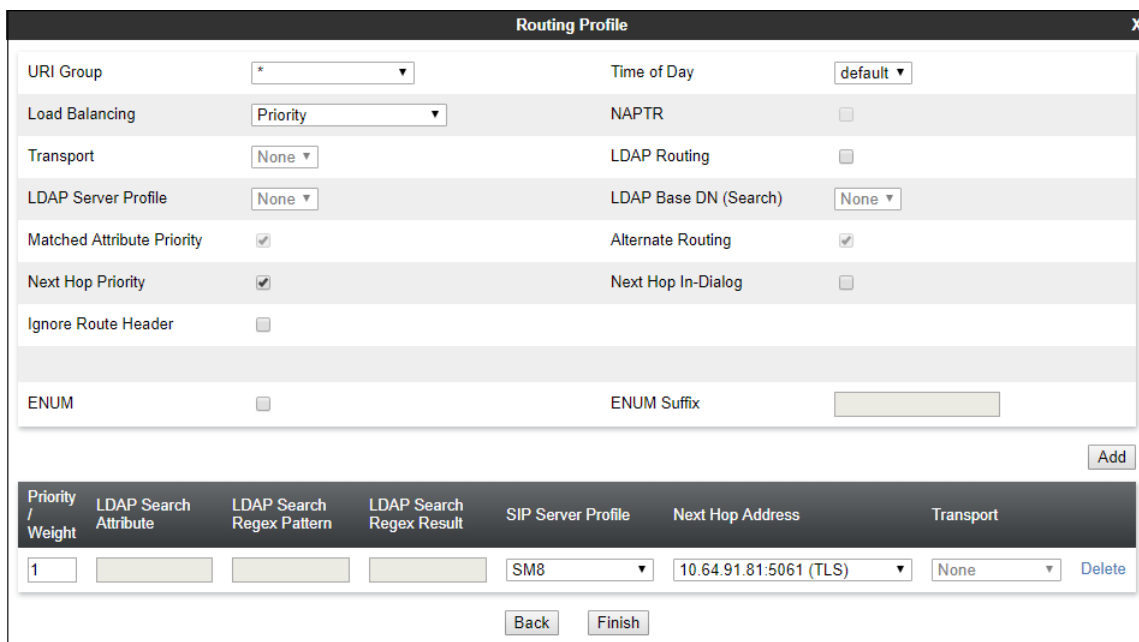
Step 2 - Enter a **Profile Name**: (e.g., **Route to SM8**) and click **Next**.



Step 3 - The Routing Profile window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button.

Step 4 - The **Next-Hop Address** section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight** = 1
- **SIP Server Profile** = SM8 (from Section 7.8.1).
- **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**.



7.9.2 Routing Profile – Verizon

Repeat the steps in **Section 7.9.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Verizon.

Step 1 - On the **Configuration Profiles → Routing** screen, select **Add** and 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**
- **SIP Server Profile = Verizon IPT** (from **Section 7.8.2**).
- **Next Hop Address:** Verify that **172.30.209.21:5071 (UDP)** is selected.

Step 3 - Click **Finish**.

| URI Group | Time of Day |
|---|--|
| * | default |
| Load Balancing: Priority | NAPTR: <input type="checkbox"/> |
| Transport: None | LDAP Routing: <input type="checkbox"/> |
| LDAP Server Profile: None | LDAP Base DN (Search): None |
| Matched Attribute Priority: <input checked="" type="checkbox"/> | Alternate Routing: <input checked="" type="checkbox"/> |
| Next Hop Priority: <input checked="" type="checkbox"/> | Next Hop In-Dialog: <input type="checkbox"/> |
| Ignore Route Header: <input type="checkbox"/> | |
| ENUM: <input type="checkbox"/> | ENUM Suffix: |

Add

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address | Transport | |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|--------------------------|-----------|--------|
| 1 | | | | Verizon IPT | 172.30.209.21:5071 (UDP) | None | Delete |

Back Finish

7.10. Topology Hiding Profiles

The **Topology Hiding** profile manages 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.

Topology Hiding can also be used as an interoperability tool to adapt the host portion of the SIP headers, to the IP addresses or domains expected on the service provider and the enterprise networks.

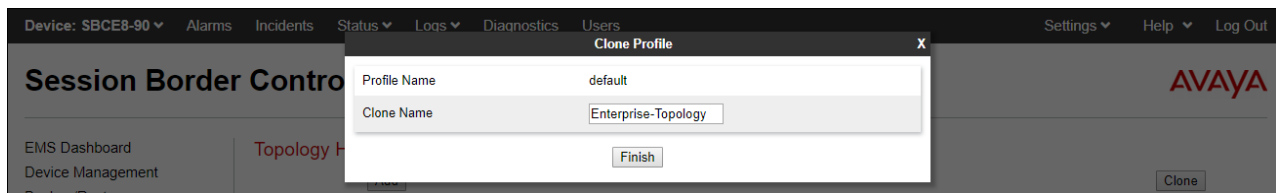
7.10.1 Topology Hiding – Enterprise

In the sample configuration, the enterprise Topology Hiding Profile was cloned from the **default** profile and then modified.

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

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

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



Step 4 - Edit the newly created **Enterprise-Topology** profile.

Step 5 - For the **Request-Line**, **To** and **From** headers select **Overwrite** under the **Replace Action** column. Enter the domain of the enterprise (e.g., **avayalab.com**) on the **Overwrite Value** field.

Step 6 - Click **Finish**.

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

Finish

7.10.2 Topology Hiding – Verizon

Repeat the steps in **Section 7.10.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Verizon.

- Enter a Profile Name (e.g., **VZ IPT Topology**).
- Overwrite the headers as shown below with the FQDNs known by Verizon.

Topology Hiding Profiles: VZ IPT Topology

Add Rename Clone Delete

Topology Hiding Profiles

- default
- cisco_th_profile
- IPOSE-Topology
- Vz IPCC Topology
- Enterprise-Topology
- VZ IPT Topology**

Click here to add a description.

Topology Hiding

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

Edit

7.11. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

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

Step 2 - Select the **default-trunk** rule.

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

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
 - Application Rules**
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - Charging Rules
 - End Point Policy
 - Groups
 - Session Policies

Application Rules: sip-trunk

Add 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 | Off |
| RTCP Keep-Alive | No |

Edit

7.12. Media Rules

Media Rules define packet parameters for the RTP media, such as encryption techniques and QoS settings. Separate media rules are created for Verizon and Session Manager.

7.12.1 Enterprise – Media Rule

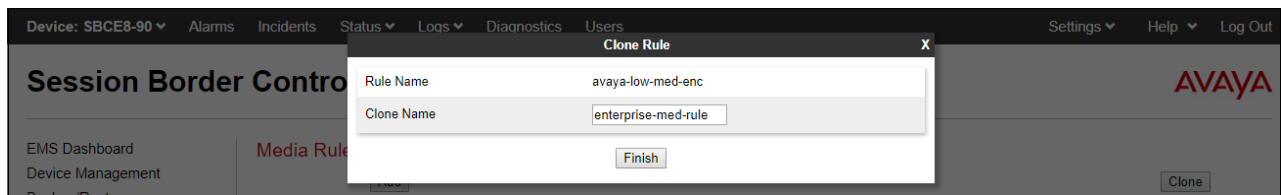
In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

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, and the **Clone Rule** window will open.

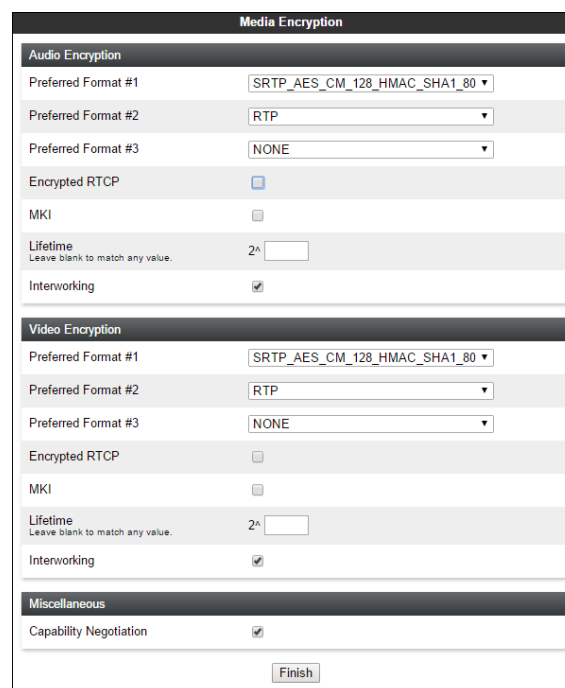
- In the **Clone Name** field enter the new Media Rule name (e.g., **enterprise-med-rule**)
- Click **Finish**. The newly created rule will be displayed.



Step 4 - On the **enterprise med rule** just created, select the **Encryption** tab.

- Click the **Edit** button and the **Media Encryption** window will open.
- In the **Audio Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Video Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Miscellaneous** section, select **Capability Negotiation**.

Step 5 - Click **Finish**.



The completed **enterprise-med-rule** is shown on the screen below.

The screenshot displays the 'Media Rules: enterprise-med-rule' configuration page. On the left is a navigation menu with categories like EMS Dashboard, Device Management, Backup/Restore, and Domain Policies. The 'Media Rules' section is expanded, showing a list of rules including 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', 'enterprise-med-rule' (highlighted in red), 'rw-med-rule', and 'Vz-trk-med-rule'. The main content area has a title bar with 'Add', 'Rename', 'Clone', and 'Delete' buttons. Below the title bar is a description field. The configuration is divided into four tabs: 'Encryption' (selected), 'Codec Prioritization', 'Advanced', and 'QoS'. The 'Encryption' tab contains sections for 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'. Under 'Audio Encryption', 'Preferred Formats' is set to 'SRTP_AES_CM_128_HMAC_SHA1_80 RTP', 'Encrypted RTCP' is unchecked, 'MKI' is unchecked, 'Lifetime' is 'Any', and 'Interworking' is checked. The 'Video Encryption' section has identical settings. The 'Miscellaneous' section has 'Capability Negotiation' checked. An 'Edit' button is at the bottom right.

7.12.2 Verizon – Media Rule

Repeat the steps in **Section 7.12.1**, 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 the new Media Rule name (e.g., **Vz-trk-med-rule**).

The completed **Vz-trk-med-rule** is shown on the screen below.

The screenshot displays the 'Media Rules: Vz-trk-med-rule' configuration page. The navigation menu is the same as in the previous screenshot. The 'Media Rules' list now includes 'Vz-trk-med-rule' at the bottom, highlighted in red. The main content area shows the configuration for this rule. The 'Encryption' tab is selected. Under 'Audio Encryption', 'Preferred Formats' is set to 'RTP', 'Interworking' is checked, and 'Encrypted RTCP' and 'MKI' are unchecked. The 'Video Encryption' section has 'Preferred Formats' set to 'RTP' and 'Interworking' checked. The 'Miscellaneous' section has 'Capability Negotiation' unchecked. An 'Edit' button is at the bottom right.

7.13. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. In the reference configuration, Signaling Rules are used to define QoS parameters for the SIP signaling packets.

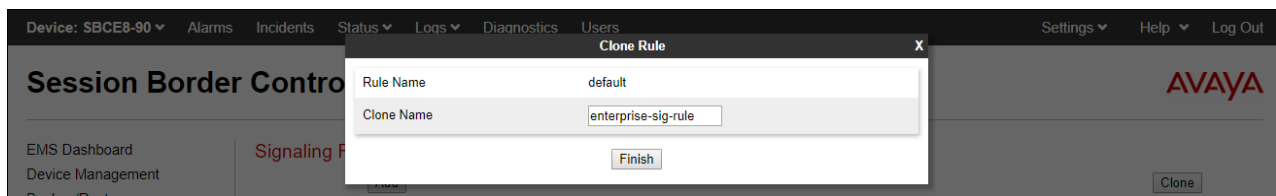
7.13.1 Signaling Rule – Enterprise

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

Step 2 - From the Signaling Rules menu, select the **default** rule.

Step 3 - Select the **Clone** button and the **Clone Rule** window will open.

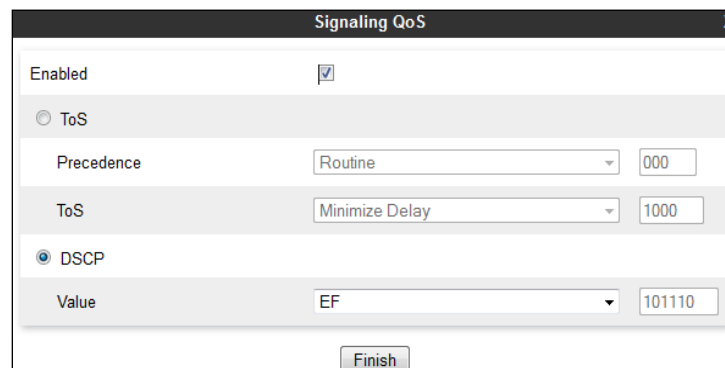
- In the **Rule Name** field enter the new Signaling Rule name (e.g., **enterprise-sig-rule**)
- Click **Finish**. The newly created rule will be displayed.



Step 4 – On the **enterprise-sig-rule** newly created, select the **Signaling QoS** tab and enter the following:

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

Step 5 - Click **Finish**.



7.13.2 Signaling Rule – Verizon

Repeat the steps in **Section 7.13.1**, with the following changes, to create a Media Rule for Verizon.

- Clone the **default** rule.
- In the **Clone Name** field enter the new Media Rule name (e.g., **Vz-trk-sig-rule**).
- On the **Signaling QoS** tab select **Value = AF32**. This value was specified by Verizon.

The completed **Vz-trk-sig-rule** is shown on the screen below.

The screenshot shows the 'Signaling Rules: Vz-trk-sig-rule' configuration page. On the left is a navigation menu with 'Domain Policies' expanded, showing 'Signaling Rules' as the selected option. The main area has a tabbed interface with 'Signaling QoS' selected. The 'Signaling QoS' tab shows a table with two rows: 'QoS Type' with value 'DSCP' and 'DSCP' with value 'AF32'. There are 'Add', 'Rename', 'Clone', and 'Delete' buttons at the top right. An 'Edit' button is at the bottom right of the table.

| QoS Type | DSCP |
|----------|------|
| DSCP | AF32 |

7.14. Endpoint Policy Groups

The rules created under the Domain Policy are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.15**.

7.14.1 End Point Policy Group - Enterprise

Step 1 - Select **Domain Policies** → **End Point Policy Groups** from the left-hand side menu.

Step 2 - Select **Add**.

- **Name:** enterpr-trk-policy.
- Click **Next**.

The screenshot shows a 'Policy Group' dialog box with a 'Group Name' field containing 'enterpr-trk-policy' and a 'Next' button. The background shows the 'Session Border Control' configuration page with the 'Policy Groups' tab selected.

Step 3 – On the **Policy Group** window (not shown), select the following.

- **Application Rule:** sip-trunk (created in **Section 7.11**).
- **Border Rule:** default.
- **Media Rule:** enterprise-med-rule (created in **Section 7.12.1**).
- **Security Rule:** default-low.
- **Signaling Rule:** enterprise-sig-rule (created in **Section 7.13.1**).

Step 4 - Select **Finish**.

The completed Policy Group **enterprise-trk-policy** is shown on the screen below.

The screenshot shows the 'Policy Groups: enterpr-trk-policy' window. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area shows a list of policy groups on the left and a detailed view of the 'enterprise-trk-policy' group on the right. The detailed view includes a table with the following data:

| Order | Application | Border | Media | Security | Signaling | Charging | RTCP Mon Gen | |
|-------|-------------|---------|---------------------|-------------|---------------------|----------|--------------|------|
| 1 | sip-trunk | default | enterprise-med-rule | default-low | enterprise-sig-rule | None | Off | Edit |

7.14.2 Endpoint Policy Groups – Verizon

Step 1 - Repeat steps 1 through 4 from **Section 7.14.1** with the following changes:

- **Group Name:** Vz-policy-grp.
- **Media Rule:** Vz-trk-med-rule (created in **Section 7.12.2**).
- **Signaling Rule:** Vz-trk-sig-rule (created in **Section 7.13.2**).

The completed Policy Group **Vz-policy-grp** is shown on the screen below.

The screenshot shows the 'Policy Groups: Vz-policy-grp' window. On the left is a navigation menu with 'End Point Policy Groups' highlighted. The main area shows a list of policy groups on the left and a detailed view of the 'Vz-policy-grp' group on the right. The detailed view includes a table with the following data:

| Order | Application | Border | Media | Security | Signaling | Charging | RTCP Mon Gen | |
|-------|-------------|---------|-----------------|-------------|-----------------|----------|--------------|------|
| 1 | sip-trunk | default | Vz-trk-med-rule | default-low | Vz-trk-sig-rule | None | Off | Edit |

7.15. Endpoint Flows – Server Flows

Server Flows combine the interfaces, policies, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBCE, the content of the packet (IP addresses, SIP URIs, etc.) is used to determine which flow it matches, so that the appropriate policies can be applied. Create separate Server Flows for the enterprise and the Verizon IP Trunking Service.

7.15.1 Server Flow – Enterprise

Step 1 - Select **Network and Flows** → **Endpoint Flows** from the menu on the left-hand side (not shown). Select the **Server Flows** tab (not shown).

Step 2 - Select **Add**, (not shown) and enter the following:

- **Flow Name:** Enter a name for the flow, e.g., **SM8 Flow (for Vz IPT)**.
- **Server Configuration:** **SM8** (Section 7.8.1).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** **Vz-Sig-B1** (Section 7.5).
- **Signaling Interface:** **Inside-Sig-50** (Section 7.5).
- **Media Interface:** **Inside-Med-50** (Section 7.4).
- **End Point Policy Group:** **enterpr-trk-policy** (Section 7.14.1).
- **Routing Profile:** **Route to VZ IPT** (Section 7.9.2).
- **Topology Hiding Profile:** **Enterprise-Topology** (Section 7.10.1).
- Let other fields at the default values.

Step 3 - Click **Finish** (not shown).

| View Flow: SM8 Flow (for Vz IPT) | | Profile | |
|----------------------------------|-----------------------|-------------------------------|--------------------------|
| Flow Name | SM8 Flow (for Vz IPT) | Signaling Interface | Inside-Sig-50 |
| Server Configuration | SM8 | Media Interface | Inside-Med-50 |
| URI Group | * | Secondary Media Interface | None |
| Transport | * | End Point Policy Group | enterpr-trk-policy |
| Remote Subnet | * | Routing Profile | Route to VZ IPT |
| Received Interface | Vz-Sig-B1 | Topology Hiding Profile | Enterprise-Topology |
| | | Signaling Manipulation Script | None |
| | | Remote Branch Office | Any |
| | | Link Monitoring from Peer | <input type="checkbox"/> |

7.15.2 Server Flow – Verizon

Step 1 - Repeat steps **1** through **3** from **Section 7.15.1**, with the following changes:

- **Flow Name:** Enter a name for the flow, e.g., **Verizon IPT Flow (for SM)**.
- **Server Configuration:** **Verizon IPT** (Section 7.8.2).
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** **Inside-Sig-50** (Section 7.5).
- **Signaling Interface:** **Vz-Sig-B1** (Section 7.5).
- **Media Interface:** **Vz-Med-B1** (Section 7.4).
- **End Point Policy Group:** **Vz-policy-grp** (Section 7.14.2).
- **Routing Profile:** **Route to SM8** (Section 7.9.1).
- **Topology Hiding Profile:** **VZ IPT Topology** (Section 7.10.2).

View Flow: Verizon IPT Flow (for SM) X

Criteria

| | |
|----------------------|---------------------------|
| Flow Name | Verizon IPT Flow (for SM) |
| Server Configuration | Verizon IPT |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Inside-Sig-50 |

Profile

| | |
|-------------------------------|--------------------------|
| Signaling Interface | Vz-Sig-B1 |
| Media Interface | Vz-Med-B1 |
| Secondary Media Interface | None |
| End Point Policy Group | Vz-policy-grp |
| Routing Profile | Route to SM8 |
| Topology Hiding Profile | VZ IPT Topology |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |
| Link Monitoring from Peer | <input type="checkbox"/> |

The screen below shows the completed **Server Flows** tab as configured in the shared test environment is shown below.

| SIP Server: SM8 | | | | | | | |
|-----------------|-----------------------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| Update | | | | | | | |
| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile | |
| 1 | SM8 Flow (for Vz IPT) | * | Vz-Sig-B1 | Inside-Sig-50 | enterpr-trk-policy | Route to VZ IPT | View Clone Edit Delete |

| SIP Server: Verizon IPT | | | | | | | |
|-------------------------|---------------------------|-----------|--------------------|---------------------|------------------------|-----------------|--|
| Update | | | | | | | |
| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile | |
| 1 | Verizon IPT Flow (for SM) | * | Inside-Sig-50 | Vz-Sig-B1 | Vz-policy-grp | Route to SM8 | View Clone Edit Delete |

8. Verizon Business IP Trunking Services Suite Configuration

Information regarding the Verizon Business IP Trunking Services suite offer can be found at <https://enterprise.verizon.com/products/business-communications/voip-and-voice-services/voip-ip-trunking/> or by contacting a Verizon Business sales representative.

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

8.1. Service Access Information

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

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

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

9. Verification Steps

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

9.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

The following edited Communication Manager **list trace tac** trace output shows an incoming call received on trunk group 1, member 1. The PSTN telephone dialed 732-945-0231. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x50231).

```
list trace tac *01                                     Page 1

LIST TRACE

time      data
12:50:49  TRACE STARTED 04/29/2020 CM Release String cold-01.0.890.0-26095
12:50:59  SIP<INVITE sips:50231@avayalab.com SIP/2.0
12:50:59  Call-ID: 4dbc357a7268f620762b29717637fe5a
12:50:59  active trunk-group 1 member 1      cid 0xd95
12:50:59  SIP>SIP/2.0 183 Session Progress
12:50:59  Call-ID: 4dbc357a7268f620762b29717637fe5a
12:50:59  dial 50231
12:50:59  ring station      50231 cid 0xd95
12:50:59  Alerting party uses public-unknown-numbering
12:50:59  G729 ss:off ps:20
12:50:59  rgn:2 [10.64.91.50]:35072
12:50:59  rgn:1 [10.64.91.86]:6092
12:50:59  G72264K ss:off ps:20
12:50:59  rgn:1 [10.5.5.211]:25152
12:50:59  rgn:1 [10.64.91.86]:6094
12:51:02  SIP>SIP/2.0 200 OK
12:51:02  Call-ID: 4dbc357a7268f620762b29717637fe5a
12:51:02  active station      50231 cid 0xd95
12:51:02  Connected party uses public-unknown-numbering
```

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

The following screen shows **Page 2** of the output of the **status trunk 1/x** command (where x is the trunk group member active on the call, **1** in the example) 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 (**10.5.5.211**) 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: 10.5.5.211                               : 25152
  Far-end:  10.64.91.50                               : 35074

```

The screen below shows **Page 3** of the output of the **status trunk 1/1** command pertaining to this same call. Note that codec G.729 and SRTP is used.

```

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

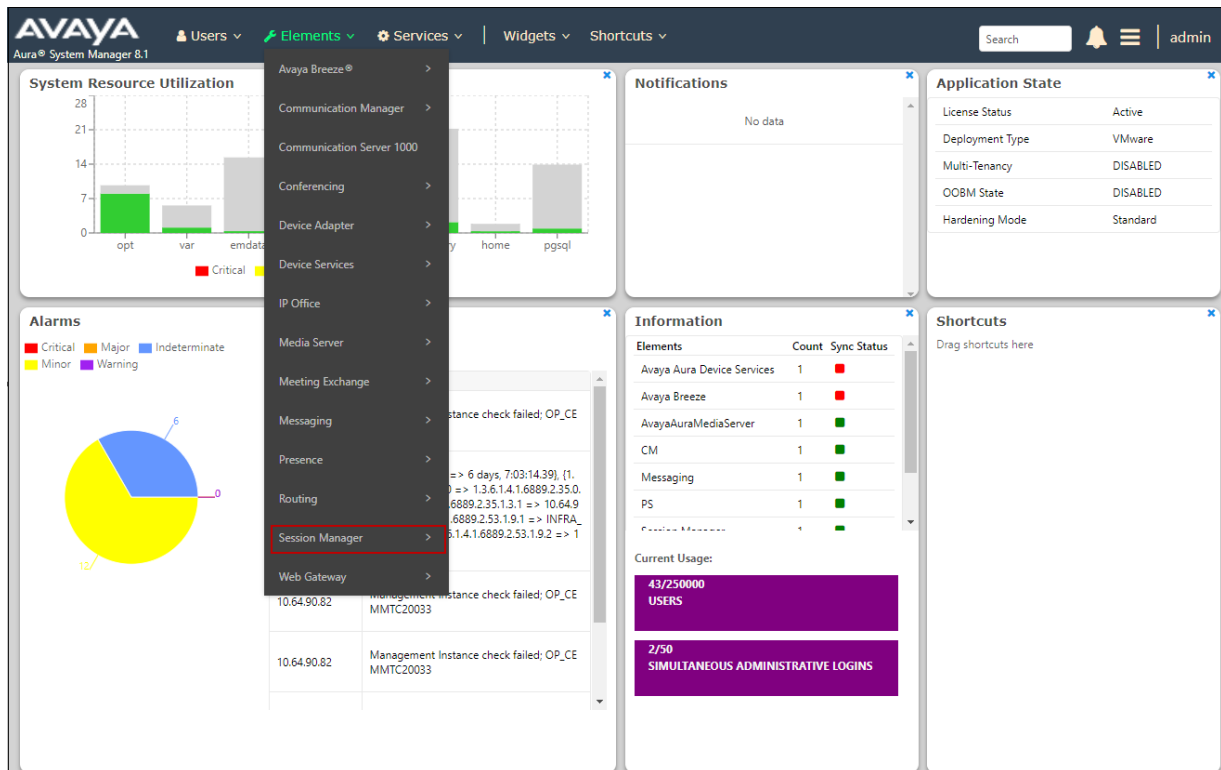
src port: T00001
T000001:TX:10.64.91.50:35074/g729/20ms/1-srtp-aescm128-hmac80
S000598:RX:10.5.5.211:25152/g729/20ms/1-srtp-aescm128-hmac80

```

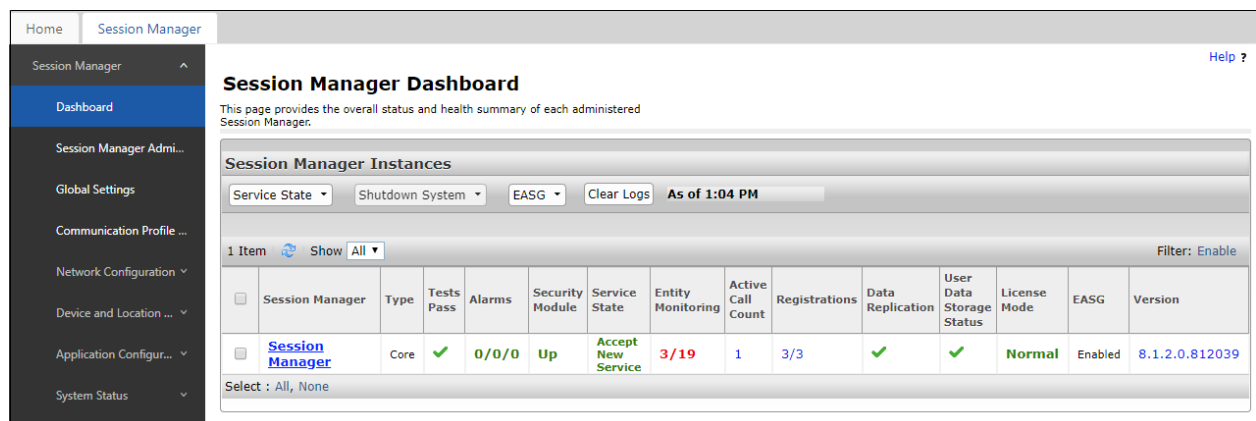
9.2. Avaya Aura® Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



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



In the example, the entry **3/19** under the **Entity Monitoring** column shows that there are alarms on 3 out of the 19 Entities being monitored by Session Manager. Clicking the entry under the **Entity Monitoring** column brings up the **Session Manager Entity Link Connection Status** page. Verify that the state of the Session Manager links of interest, to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

19 Items Filter: Enable

| | SIP Entity Name | Session Manager IP Address Family | SIP Entity Resolved IP | Port | Proto. | Deny | Conn. Status | Reason Code | Link Status |
|----------------------------------|----------------------------------|-----------------------------------|------------------------|------|--------|-------|--------------|--|-------------|
| <input type="radio"/> | Aura Messaging | IPv4 | 10.64.91.84 | 5061 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | Breeze | IPv4 | 10.64.91.18 | 5061 | TLS | FALSE | DOWN | 500 Server Internal Error: Destination Unreachable | DOWN |
| <input checked="" type="radio"/> | CM-TG1 | IPv4 | 10.64.91.75 | 5081 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG2 | IPv4 | 10.64.91.75 | 5071 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG3 | IPv4 | 10.64.91.75 | 5061 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG4 | IPv4 | 10.64.91.75 | 5064 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG5 | IPv4 | 10.64.91.75 | 5065 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG6 | IPv6 | fd22:305b:b390:14e6::5 | 5066 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG7 | IPv6 | fd22:305b:b390:14e6::5 | 5067 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | CM-TG9 | IPv4 | 10.64.91.75 | 5069 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | ExperiencePortal | IPv4 | 10.64.91.90 | 5061 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | Presence | IPv4 | 10.64.91.18 | 5061 | TLS | FALSE | DOWN | 500 Server Internal Error: Destination Unreachable | DOWN |
| <input checked="" type="radio"/> | SBC1 | IPv4 | 10.64.91.50 | 5061 | TLS | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | SBC2-100 | IPv4 | 10.64.91.100 | 5060 | TCP | FALSE | UP | 200 OK | UP |
| <input type="radio"/> | SBC2-101 | IPv4 | 10.64.91.101 | 5061 | TLS | FALSE | DOWN | 500 Server Internal Error | DOWN |

Select : None Page 1 of 2

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

9.3. Avaya Session Border Controller for Enterprise Verification

This section provides verification steps that may be performed with the Avaya SBCE.

9.3.1 Incidents

The Incident Viewer can be accessed from the Avaya top navigation menu as highlighted in the screenshot below.

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

| Information | |
|------------------------------|---|
| System Time | 07:00:36 AM MDT Refresh |
| Version | 8.1.0.0-14-18490 |
| GUI Version | 8.1.0.0-18490 |
| Build Date | Mon Feb 03 17:23:09 UTC 2020 |
| License State | OK |
| Aggregate Licensing Overages | 0 |
| Peak Licensing Overage Count | 0 |
| Last Logged in at | 04/29/2020 15:00:45 MDT |
| Failed Login Attempts | 0 |

Installed Devices

| |
|----------|
| EMS |
| SBCE8-90 |

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

| |
|--|
| SBCE8-90: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number |
| SBCE8-90: Heartbeat Successful, Server is UP |

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures.

Incident Viewer

Device: Category: [Clear Filters](#) [Refresh](#) [Generate Report](#)

Displaying results 1 to 15 out of 2000.

| ID | Device | Date & Time | Category | Type | Cause |
|-----------------|----------|---------------------------|----------------------|------------------------------|--|
| 794123251623179 | SBCE8-90 | Apr 30, 2020, 5:35:03 AM | TLS Certificate | TLS Handshake Failed | error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number |
| 794096209987550 | SBCE8-90 | Apr 29, 2020, 2:33:39 PM | Policy | Server Heartbeat | Heartbeat Successful, Server is UP |
| 794096209959351 | SBCE8-90 | Apr 29, 2020, 2:33:39 PM | Policy | Server Heartbeat | Heartbeat Successful, Server is UP |
| 794096209923173 | SBCE8-90 | Apr 29, 2020, 2:33:39 PM | Policy | Server Heartbeat | Heartbeat Successful, Server is UP |
| 794096209922952 | SBCE8-90 | Apr 29, 2020, 2:33:39 PM | Policy | Server Heartbeat | Heartbeat Successful, Server is UP |
| 794089588242798 | SBCE8-90 | Apr 29, 2020, 10:52:56 AM | Protocol Discrepancy | NOTIFY Message Out of Dialog | General Method not allowed Out-Of-Dialog |

Further Information can be obtained by clicking on a specific incident in the incident viewer above.

9.3.2 Server Status

The **Server Status** can be accessed from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **Server Status**.

Device: SBCE8-90 Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller Enterprise

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Dashboard

GUI DEBUG level log messages are currently enabled on one or more components. Leaving this log level enabled for extended periods of time is not recommended but will not have any adverse effects.

| Information | |
|------------------------------|---|
| System Time | 07:11:29 AM MDT Refresh |
| Version | 8.1.0.0-14-18490 |
| GUI Version | 8.1.0.0-18490 |
| Build Date | Mon Feb 03 17:23:09 UTC 2020 |
| License State | OK |
| Aggregate Licensing Overages | 0 |

| Installed Devices | |
|-------------------|--|
| EMS | |
| SBCE8-90 | |

The **Server Status** screen provides information about the condition of the connection to the connected SIP Servers. This functionality requires Heartbeat to be enabled on the SIP Server Configuration profiles, as configured in **Section 7.8**.

Device: SBCE8-90 Help

Status

Server Status

| Server Profile | Server FQDN | Server IP | Server Port | Server Transport | Heartbeat Status | Registration Status | TimeStamp |
|----------------|---------------|---------------|-------------|------------------|------------------|---------------------|-------------------------|
| SM8 | 10.64.91.81 | 10.64.91.81 | 5061 | TLS | UP | UNKNOWN | 04/30/2020 07:11:40 MDT |
| Verizon IPT | 172.30.209.21 | 172.30.209.21 | 5071 | UDP | UP | UNKNOWN | 04/30/2020 07:12:40 MDT |

9.3.3 Diagnostics

This screen provides a **Full Diagnostics** tool to verify the link of each interface and ping the configured next-hop gateways and DNS servers. The **Ping Test** tool can be used to ping specific devices from any Avaya SBCE interface.

| Task Description | Status |
|--|--------|
| EMS Link Check | Failed |
| SBC Link Check: A1 | Failed |
| SBC Link Check: B1 | Failed |
| SBC Link Check: B2 | Failed |
| Ping: SBC (A1) to Gateway (10.64.91.1) | Failed |
| Ping: SBC (A1) to Primary DNS (172.30.209.4) | Failed |
| Ping: SBC (B1) to Gateway (1.1.1.1) | Failed |
| Ping: SBC (B1) to Primary DNS (172.30.209.4) | Failed |

9.3.4 Tracing

To take a call trace, navigate to **Monitoring & Logging → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.

Session Border Controller for Enterprise

Trace: SBCE8-90

Packet Capture Configuration

| | |
|---|-----------|
| Status | Ready |
| Interface | Any |
| Local Address <small>[IP:Port]</small> | All : |
| Remote Address <small>*, *:Port, IP, IP:Port</small> | * |
| Protocol | All |
| Maximum Number of Packets to Capture | 10000 |
| Capture Filename <small>Using the name of an existing capture will overwrite it.</small> | Test.pcap |

Start Capture 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.

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging
 - SNMP
 - Syslog Management
 - Debugging
 - Trace**
 - Log Collection
 - DoS Learning
 - CDR Adjunct

Trace: SBCE8-90

Packet Capture Captures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

Status In Progress

Interface Any

Local Address IP:Port All

Remote Address *Port, IP, IP:Port *

Protocol All

Maximum Number of Packets to Capture 10000

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

Stop Capture

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.

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging
 - SNMP
 - Syslog Management
 - Debugging
 - Trace**

Trace: SBCE8-90

Packet Capture Captures

Refresh

| File Name | File Size (bytes) | Last Modified |
|--------------------------|-------------------|-------------------------------|
| Test_20190801093220.pcap | 2,558,166 | August 1, 2019 9:32:58 AM MDT |

Delete

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.1 can be configured to interoperate successfully with Verizon Business IP Trunking service, within the constraints described in **Section** Error! Reference source not found..

The reference configuration shown in these Application Notes is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

11. Additional References

11.1. Avaya

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

Avaya Aura® Session Manager/System Manager

- [1] *Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment*, Release 8.1.x, Issue 3, March 2020
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 3, March 2020
- [3] *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2020
- [4] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 5, March 2020

Avaya Aura® Communication Manager

- [5] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 8.1.x, Issue 4, March 2020
- [6] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020
- [7] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1.x, Issue 6, March 2020
- [8] *Administering Avaya G430 Branch Gateway*, Release 8.1.x, Issue 3, March 2020
- [9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.2, Issue 9, December 2019
- [10] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, Issue 1.1, June 2018

Avaya Session Border Controller for Enterprise

- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1, Issue 1, February 2020
- [12] *Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment*, Release 8.1, Issue 1, February 2020
- [13] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 8.1, Issue 1, February 2020

Avaya Aura® Messaging

- [14] *Administering Avaya Aura® Messaging*, Release 7.1.0, Issue 9, April 2020

11.2. 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)*

12. Appendix B – Avaya SBCE – SigMa Script File

Details of the Signaling Manipulation script used in the configuration of the Avaya SBCE, in **Section 7.7**.

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    //Remove gsid and epv parameters from Contact header to hide internal topology
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
    // fix call-fwd
    %HEADERS["Diversion"][1].regex_replace("sips","sip");

  }
}
```

©2020 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.