Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.1, Avaya Aura® Communication Manager Release 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise Release 8.0 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. History Info and Diversion Headers .......................................................................... 7

2.3. SIP Header Removal ............................................................................................... 8

2.5. Support ...................................................................................................................... 9

3. Reference Configuration ............................................................................................ 10

3.1. Illustrative Configuration Information .................................................................... 10

3.2. Call Flows ................................................................................................................ 12

3.2.1 Communication Manager .................................................................................... 12

3.2.2 Experience Portal ................................................................................................ 15

4. Equipment and Software Validated .......................................................................... 18

5. Configure Avaya Aura® Communication Manager .................................................... 19

5.1. Verify Licensed Features ......................................................................................... 19

5.2. System-Parameters Features .................................................................................. 21

5.3. Dial Plan .................................................................................................................. 22

5.4. Node Names ............................................................................................................ 22

5.5. Processor Ethernet Configuration .......................................................................... 23

5.6. IP Codec Sets .......................................................................................................... 24

5.6.1 Codecs for IP Network Region 1 (calls within the CPE) .................................. 24

5.6.2 Codecs for IP Network Region 2 (calls to/from Verizon) .................................. 25

5.7. Network Regions .................................................................................................... 26

5.7.1 IP Network Region 1 – Local CPE Region ......................................................... 26

5.7.2 IP Network Region 2 – Verizon Trunk Region .................................................. 27

5.8. SIP Trunks ............................................................................................................... 28

5.8.1 SIP Trunk for Inbound/Outbound Verizon calls .............................................. 28

5.8.2 Local SIP Trunk (Avaya SIP Telephones, Messaging Access, etc.) .................. 32

5.9. Public Numbering ................................................................................................... 33

5.10. Private Numbering ............................................................................................... 34

5.11. Route Patterns ....................................................................................................... 34

5.11.1 Route Pattern for National Calls to Verizon ..................................................... 34

5.11.2 Route Pattern for International Calls to Verizon ............................................. 35

5.11.3 Route Pattern for Service Calls to Verizon ..................................................... 36

5.11.4 Route Pattern for Calls within the CPE ............................................................ 36

5.12. Automatic Route Selection (ARS) Dialing ............................................................ 37

5.13. Automatic Alternate Routing (AAR) Dialing ......................................................... 37


5.15. Avaya Aura® Media Server Provisioning ............................................................... 39

5.16. Save Translations .................................................................................................. 40

5.17. Verify TLS Certificates – Communication Manager ............................................. 41

6. Configure Avaya Aura® Session Manager ................................................................. 42

6.1. System Manager Login and Navigation ................................................................. 43

6.2. SIP Domain ............................................................................................................ 44

6.3. Locations ............................................................................................................... 44
8.6. Server Interworking Profiles .......................................................... 84
8.6.1 Server Interworking Profile – Enterprise ........................................... 84
8.6.2 Server Interworking Profile – Verizon ............................................... 85
8.7. Signaling Manipulation ................................................................. 86
8.8. SIP Server Profiles ................................................................. 87
8.8.1 SIP Server Profile – Session Manager ........................................... 87
8.8.2 SIP Server Profile – Verizon ....................................................... 89
8.9. Routing Profiles ............................................................................ 90
8.9.1 Routing Profile – Session Manager ............................................... 91
8.9.2 Routing Profile – Verizon ............................................................. 92
8.10. Topology Hiding Profiles ........................................................... 93
8.10.1 Topology Hiding – Enterprise ..................................................... 93
8.10.2 Topology Hiding – Verizon ......................................................... 94
8.11. Application Rules ............................................................... 94
8.12. Media Rules ................................................................................. 95
8.12.1 Enterprise – Media Rule ............................................................ 95
8.12.2 Verizon – Media Rule ............................................................... 96
8.13. Signaling Rules ............................................................... 97
8.13.1 Signaling Rule – Enterprise ....................................................... 97
8.13.2 Signaling Rule – Verizon ........................................................... 98
8.14.1 End Point Policy Group - Enterprise ........................................... 98
8.15. Endpoint Flows – Server Flows .................................................. 100
8.15.1 Server Flow – Enterprise ......................................................... 100
8.15.2 Server Flow – Verizon ............................................................. 101
9.1. Service Access Information ....................................................... 102
10. Verification Steps ............................................................................ 103
10.1. Avaya Aura® Communication Manager Verifications ...................... 103
10.2. Avaya Aura® Session Manager Verification .................................. 105
10.3. Avaya Session Border Controller for Enterprise Verification ............ 107
10.3.1 Incidents .................................................................................. 107
10.3.2 Server Status ............................................................................ 108
10.3.3 Diagnostics ............................................................................. 109
10.3.4 Tracing .................................................................................... 109
11. Conclusion .................................................................................... 110
12. Additional References .................................................................... 111
12.1. Avaya ......................................................................................... 111
12.2. Verizon Business ......................................................................... 111
13. Appendix A – Avaya SBCE – Refer Handling .................................. 112
14. Appendix B – Avaya SBCE – SigMa Script File .................................. 114
1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 8.1, Avaya Aura® Communication Manager Release 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise Release 8.0 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, Experience Portal, 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
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements and/or music on hold) and Automatic Speech Recognition.
- Experience Portal use of SIP REFER to redirect inbound calls, via the Avaya SBCE, to the appropriate Communication Manager agent extension
- Call and two-way talk path establishment between callers and Communication Manager agents following redirection from Experience Portal
- Inbound calls to a self-service Experience Portal application which forwards the call to 8YY or any other PSTN number over Verizon IPT service using SIP REFER
- Long hold time calls
- Avaya Remote Worker operation (Avaya Equinox 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. Even though T.38 fax was provisioned on the Verizon Business IP Trunking production circuit used to verify these Application Notes, 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 currently under investigation by the Avaya SBCE development team. A workaround is to include a SigMa script for the Verizon Server Configuration profile on the Avaya SBCE to convert “sips” to “sip” in the Diversion header. See Section 8.7.

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. The Experience Portal test application used for compliance testing performs consultative call transfers using SIP INVITE with the original calling party number in the From and P-Asserted Identity headers, it does not include a Diversion header. Verizon requires a Diversion header for this scenario. This caused consultative call transfers out the Verizon Business IP Trunking service to fail. However, blind transfers out to Verizon using SIP REFER were successful. Also, consultative and blind transfers from Experience Portal to Communication Manager were successful as well.
5. Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested; therefore, it is the customer’s responsibility to ensure proper operation with its equipment/software vendor.

6. Verizon Business IP Trunking service does not support G.711A codec for domestic service (EMEA only).


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

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

If Communication Manager sends the History Info header, Session Manager can convert the History Info header into the Diversion header. This is performed by specifying the “VerizonAdapter” adaptation in Session Manager. See Section 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 Removal
To support advanced SIP telephony features in the Avaya Aura® enterprise environment, certain proprietary headers may be included in the SIP message sent toward Verizon. These extra headers can cause the SIP message to become larger than the specified Maximum Transmission Unit (MTU) and create fragmented UDP packets. These fragmented packets may not be re-assembled properly on the far-end by Verizon’s equipment, for instance, when packets arrive out of order. To prevent fragmented packets, any unnecessary or proprietary headers should be removed from the SIP message before being sent to Verizon. Session Manager can remove these headers by specifying the “eRHdrs” parameter within the “VerizonAdapter” adaptation. See Section 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 8.7 and 8.8.2.

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

3.1. Illustrative Configuration Information

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

The Avaya SBCE receives traffic from the Verizon Business IP Trunking service on port 5060 and sends traffic to the Verizon Business IP Trunking service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunking service).

![Diagram of Avaya Interoperability Test Lab Configuration](image-url)
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 8.10.2). 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 Aura® Experience Portal
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- J100 Series IP Deskphones using the SIP software bundle
- Avaya Equinox™ for Windows
- Avaya Digital Phones
- Ventafax fax software
3.2. Call Flows
To understand how Verizon Business IP Trunking service calls are handled by the Avaya CPE environment, several call flows are described in this section.

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

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

![Figure 2: Inbound Verizon Call](image-url)
The second call scenario illustrated is an outbound call initiated on Communication Manager, routed to Session Manager, and is subsequently sent to the Avaya SBCE for delivery to the Verizon Business IP Trunking service.

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

Figure 3: Outbound Verizon Call
The third call scenario illustrated is an inbound Verizon Business IP Trunking service call that arrives at the Avaya SBCE, to Session Manager, and subsequently Communication Manager. Communication Manager routes the call to a destination station; however, the station has set Call Forward to an alternate destination. Without answering the call, Communication Manager redirects the call back to the Verizon Business IP Trunking service for routing to the alternate destination.

**Note** – In cases where calls are forwarded to an alternate destination such as an 8xx numbers, the Verizon Business IP Trunking service requires the use of SIP Diversion Header for the redirected call to complete (see Section 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. Communication Manager routes the call to a station.
7. 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.
8. 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.

![Diagram](image-url)

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

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

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

Figure 5: Inbound Call Handling Entirely by Avaya Aura® Experience Portal
The second call scenario illustrated below is an inbound call arriving on Experience Portal and transferred to Communication Manager without determining whether an agent is available or not.

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

![Diagram showing the call flow from PSTN to Avaya Aura® Experience Portal, Avaya SBCE, Communication Manager, and Agent](image)

Figure 6: Avaya Aura® Experience Portal Transfers Call to Avaya Aura® Communication Manager
The third call scenario illustrated below is an inbound call arriving on Experience Portal and forwarded to an 8YY number or any other PSTN number over the Verizon network.

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

Figure 7: Inbound Call forwarded by Experience Portal to another PSTN number
4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>8.1.0.1.1 (Service Pack 1.1)</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>8.1.0.0.079880</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>8.1.0.0.810007</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise</td>
<td>8.0.0.19</td>
</tr>
<tr>
<td>Avaya Aura® Messaging</td>
<td>7.1 SP 1</td>
</tr>
<tr>
<td>Avaya Aura® Experience Portal</td>
<td>7.2.2.0.2118</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>8.0.0.205</td>
</tr>
<tr>
<td>G430 Gateway</td>
<td>41.9.0</td>
</tr>
<tr>
<td>Avaya 96X1 Series IP Deskphone (SIP)</td>
<td>7.1.5.0.11</td>
</tr>
<tr>
<td>Avaya 96X1 Series IP Deskphone (H.323)</td>
<td>6.8102</td>
</tr>
<tr>
<td>Avaya J100 Series IP Deskphone (SIP)</td>
<td>4.0.1.0.11</td>
</tr>
<tr>
<td>Avaya Equinox™ for Windows</td>
<td>3.5.7.30.1</td>
</tr>
<tr>
<td>Avaya 9408 Digital Deskphone</td>
<td>2.00</td>
</tr>
<tr>
<td>Fax device</td>
<td>Ventafax 7.10</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th></th>
<th>Page 2 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP PORT CAPACITIES</td>
<td>USED</td>
</tr>
<tr>
<td>Maximum Administered H.323 Trunks:</td>
<td>4000</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations:</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks:</td>
<td>4000</td>
</tr>
<tr>
<td>Max Concurrently Registered Remote Office Stations:</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons:</td>
<td>68</td>
</tr>
<tr>
<td>Max Concur Reg Unauthenticated H.323 Stations:</td>
<td>100</td>
</tr>
<tr>
<td>Maximum Video Capable Stations:</td>
<td>2400</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones:</td>
<td>1000</td>
</tr>
<tr>
<td><strong>Maximum Administered SIP Trunks</strong>:</td>
<td><strong>4000</strong></td>
</tr>
<tr>
<td>Max Administered Ad-hoc Video Conferencing Ports:</td>
<td>4000</td>
</tr>
<tr>
<td>Max Number of DS1 Boards with Echo Cancellation:</td>
<td>80</td>
</tr>
</tbody>
</table>
Step 2 - On Page 4 of the form, verify that ARS is enabled.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>Page 4 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTIONAL FEATURES</td>
<td></td>
</tr>
<tr>
<td>Access Security Gateway (ASG)? n</td>
<td>Authorization Codes? y</td>
</tr>
<tr>
<td>Analog Trunk Incoming Call ID? y</td>
<td>CAS Branch? n</td>
</tr>
<tr>
<td>A/D Grp/Sys List Dialing Start at 01? y</td>
<td>CAS Main? n</td>
</tr>
<tr>
<td>Answer Supervision by Call Classifier? y</td>
<td>Change COR by FAC? n</td>
</tr>
<tr>
<td>ARS? y</td>
<td>Computer Telephony Adjunct Links? y</td>
</tr>
<tr>
<td>ARS/AAR Partitioning? y</td>
<td>Cvg Of Calls Redirected Off-net? y</td>
</tr>
<tr>
<td>ARS/AAR Dialing without FAC? n</td>
<td>DCS (Basic)? y</td>
</tr>
<tr>
<td>ASAI Link Core Capabilities? n</td>
<td>DCS Call Coverage? y</td>
</tr>
<tr>
<td>ASAI Link Plus Capabilities? n</td>
<td>DCS with Rerouting? y</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) PNC? n</td>
<td></td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) Trunking? n</td>
<td></td>
</tr>
<tr>
<td>ATM WAN Spare Processor? n</td>
<td></td>
</tr>
<tr>
<td>ATMS? y</td>
<td></td>
</tr>
<tr>
<td>Attendant Vectoring? y</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>Page 5 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTIONAL FEATURES</td>
<td></td>
</tr>
<tr>
<td>Enhanced EC500? y</td>
<td></td>
</tr>
<tr>
<td>Enterprise Servicable Server? n</td>
<td></td>
</tr>
<tr>
<td>Enterprise Wide Licensing? n</td>
<td></td>
</tr>
<tr>
<td>ESS Administration? y</td>
<td></td>
</tr>
<tr>
<td>Extended Cvg/Fwd Admin? y</td>
<td></td>
</tr>
<tr>
<td>External Device Alarm Admin? y</td>
<td></td>
</tr>
<tr>
<td>Five Port Networks Max Per MCC? n</td>
<td></td>
</tr>
<tr>
<td>Flexible Billing? n</td>
<td></td>
</tr>
<tr>
<td>Forced Entry of Account Codes? y</td>
<td></td>
</tr>
<tr>
<td>Global Call Classification? y</td>
<td></td>
</tr>
<tr>
<td>Hospitality (Basic)? y</td>
<td></td>
</tr>
<tr>
<td>Hospitality (G3V3 Enhancements)? y</td>
<td></td>
</tr>
<tr>
<td>IP Trunks? y</td>
<td></td>
</tr>
<tr>
<td>IP Attendant Consoles? y</td>
<td></td>
</tr>
<tr>
<td>Emergency Access to Attendant? y</td>
<td>ISDN Feature Plus? n</td>
</tr>
<tr>
<td>Enable 'dadmin' Login? y</td>
<td>ISDN/BRI Trunks? y</td>
</tr>
<tr>
<td>Enhanced Conferencing? y</td>
<td>ISDN-PRI? y</td>
</tr>
<tr>
<td>ISDN/SIP Network Call Redirection? y</td>
<td>Local Survivable Processor? n</td>
</tr>
<tr>
<td>Multifrequency Signaling? y</td>
<td>Malicious Call Trace? y</td>
</tr>
<tr>
<td>Flexible Billing? n</td>
<td></td>
</tr>
<tr>
<td>Global Call Classification? y</td>
<td></td>
</tr>
<tr>
<td>Hospitality (Basic)? y</td>
<td></td>
</tr>
<tr>
<td>Hospitality (G3V3 Enhancements)? y</td>
<td></td>
</tr>
<tr>
<td>IP Trunks? y</td>
<td></td>
</tr>
</tbody>
</table>
Step 4 - On Page 6 of the form, verify that the Processor Ethernet field is set to y.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>OPTIONAL FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multinational Locations? n</td>
<td>Station and Trunk MSP? y</td>
</tr>
<tr>
<td>Multiple Level Precedence &amp; Preemption?</td>
<td>Station as Virtual Extension? y</td>
</tr>
<tr>
<td>Multiple Locations? n</td>
<td>System Management Data Transfer? n</td>
</tr>
<tr>
<td>Personal Station Access (PSA)? y</td>
<td>Tenant Partitioning? y</td>
</tr>
<tr>
<td>PNC Duplication? n</td>
<td>Terminal Trans. Init. (TTI)? y</td>
</tr>
<tr>
<td>Posted Messages? y</td>
<td>TN2501 VAL Maximum Capacity? y</td>
</tr>
<tr>
<td>Private Networking? y</td>
<td>Uniform Dialing Plan? y</td>
</tr>
<tr>
<td>Processor and System MSP? y</td>
<td>Usage Allocation Enhancements? y</td>
</tr>
<tr>
<td>Processor Ethernet? y</td>
<td>Wideband Switching? y</td>
</tr>
<tr>
<td></td>
<td>Wireless? n</td>
</tr>
<tr>
<td>Remote Office? y</td>
<td></td>
</tr>
<tr>
<td>Restrict Call Forward Off Net? y</td>
<td></td>
</tr>
<tr>
<td>Secondary Data Module? y</td>
<td></td>
</tr>
</tbody>
</table>

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.

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

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Call Length Type</th>
<th>Dialed String</th>
<th>Total Call Length Type</th>
<th>Dialed String</th>
<th>Total Call Length Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>2</td>
<td>ext</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>60</td>
<td>3</td>
<td>66</td>
<td>2</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>*</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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., **AMS** and **10.64.91.80**). The Media Server node name is only needed if a Media Server is present.
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

IP INTERFACES

  Type: PROCR
  Target socket load: 4800

  Enable Interface? y
  Allow H.323 Endpoints? y
  Allow H.248 Gateways? y
  Network Region: 1
  Gatekeeper Priority: 5

IPV4 PARAMETERS

  Node Name: procr
  IP Address: 10.64.91.75
  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` 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.

<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Silence Suppression</th>
<th>Frames Per Pkt</th>
<th>Packet Size(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: G.722-64K</td>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2: G.711MU</td>
<td>n</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3: G.729A</td>
<td>n</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

Media Encryption

- Encrypted SRTCP: enforce-unenc-srtcp

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

<table>
<thead>
<tr>
<th>FAX Mode</th>
<th>Redundancy</th>
<th>Packet Size(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>t.38-standard</td>
<td>0</td>
<td>ECM: y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mode</th>
<th>Redundancy</th>
<th>Packet Size(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem off</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TDD/TTY US</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>H.323 Clear-channel n</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SIP 64K Data n</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Codec</th>
<th>Audio Codec</th>
<th>Silence Suppression</th>
<th>Frames Per Pkt</th>
<th>Packet Size(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: G.729A</td>
<td>n</td>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2: G.711MU</td>
<td>n</td>
<td>2</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Media Encryption
1: 1-srtp-aescm128-hmac80
2: none

Encrypted SRTCP: enforce-unenc-srtcp

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.

<table>
<thead>
<tr>
<th>FAX</th>
<th>t.38-G711-fallback 0</th>
<th>ECM: y FB-Timer: 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem</td>
<td>off</td>
<td>0</td>
</tr>
<tr>
<td>TDD/TTY</td>
<td>US</td>
<td>3</td>
</tr>
<tr>
<td>H.323 Clear-channel</td>
<td>n</td>
<td>0</td>
</tr>
<tr>
<td>SIP 64K Data</td>
<td>n</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Region: 1</th>
<th>Authoritative Domain: avayalab.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location: 1</td>
<td>Stub Network Region: n</td>
</tr>
<tr>
<td>Name: Enterprise</td>
<td>Intra-region IP-IP Direct Audio: yes</td>
</tr>
<tr>
<td>MEDIA PARAMETERS</td>
<td>Inter-region IP-IP Direct Audio: yes</td>
</tr>
<tr>
<td>Codec Set: 1</td>
<td>IP Audio Hairpinning? n</td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td></td>
</tr>
<tr>
<td>UDP Port Max: 3329</td>
<td></td>
</tr>
</tbody>
</table>

**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**
- 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.

<table>
<thead>
<tr>
<th>change ip-network-region 1</th>
<th>Page 4 of 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Region: 1</td>
<td>Inter Network Region Connection Management</td>
</tr>
<tr>
<td>var</td>
<td>I M</td>
</tr>
<tr>
<td>dst codec</td>
<td>direct</td>
</tr>
<tr>
<td>rgn set</td>
<td>WAN BW-limits</td>
</tr>
<tr>
<td></td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td>Intervening</td>
</tr>
<tr>
<td></td>
<td>Dyn</td>
</tr>
<tr>
<td></td>
<td>A G C</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>NoLimit</td>
</tr>
<tr>
<td></td>
<td>n</td>
</tr>
<tr>
<td></td>
<td>t</td>
</tr>
</tbody>
</table>

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).

<table>
<thead>
<tr>
<th>change ip-network-region 2</th>
<th>Page 4 of 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Region: 2</td>
<td>Inter Network Region Connection Management</td>
</tr>
<tr>
<td>var</td>
<td>I M</td>
</tr>
<tr>
<td>dst codec</td>
<td>direct</td>
</tr>
<tr>
<td>rgn set</td>
<td>WAN BW-limits</td>
</tr>
<tr>
<td></td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td>Intervening</td>
</tr>
<tr>
<td></td>
<td>Dyn</td>
</tr>
<tr>
<td></td>
<td>A G C</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>NoLimit</td>
</tr>
<tr>
<td></td>
<td>n</td>
</tr>
<tr>
<td></td>
<td>t</td>
</tr>
<tr>
<td></td>
<td>all</td>
</tr>
</tbody>
</table>
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 **proc** 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`.
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).
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
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

TRUNK FEATURES
ACA Assignment? n
Measured: none

Maintenance Tests? y
Suppress # Outpulsing? n
Numbering Format: public
UUI Treatment: service-provider
Replace Restricted Numbers? y
Replace Unavailable Numbers? y
Hold/Unhold Notifications? y
Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```
Step 4 - On Page 4 of the Trunk Group form:

- Verify **Network Call Redirection** is set to y.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by Verizon (e.g., 101).
- Set **Convert 180 to 183 for Early Media** to y.

**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

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).

<table>
<thead>
<tr>
<th>Ext Len</th>
<th>Ext Code</th>
<th>Trk Grp(s)</th>
<th>CPN</th>
<th>Total Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>12001</td>
<td>1</td>
<td>17329450231</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>14006</td>
<td>1</td>
<td>17329450236</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>14007</td>
<td>1</td>
<td>17329450237</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>14008</td>
<td>1</td>
<td>17329450238</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>50</td>
<td>1</td>
<td>173294</td>
<td>11</td>
</tr>
</tbody>
</table>

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.
5.10. 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).

<table>
<thead>
<tr>
<th>Ext Ext Len</th>
<th>Code</th>
<th>Trk Grp(s)</th>
<th>Private Prefix</th>
<th>Total Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>11</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td>3</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td>3</td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

Maximum Entries: 540
Total Administered: 11

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.

<table>
<thead>
<tr>
<th>Grp No</th>
<th>FRL</th>
<th>NPA</th>
<th>Pfx Mrk</th>
<th>Hop Toll No.</th>
<th>Inserted Digits</th>
<th>DCS/IXC</th>
<th>QSIG</th>
<th>Intw</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td>p</td>
<td>n</td>
<td>user</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Grp No</th>
<th>FRL</th>
<th>NPA</th>
<th>Pfx Mrk</th>
<th>Hop Toll No.</th>
<th>Inserted Digits</th>
<th>DCS/IXC</th>
<th>QSIG</th>
<th>Intw</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td></td>
<td>p</td>
<td>n</td>
<td>user</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE</th>
<th>TSC CA-TSC</th>
<th>ITC BCIE Service/Feature SUB PARM Sub</th>
<th>Numbering</th>
<th>LAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 4 5 6</td>
<td>Request</td>
<td></td>
<td>Dgts Format</td>
<td>none</td>
</tr>
</tbody>
</table>
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).

<table>
<thead>
<tr>
<th>Grp FRL NPA Pfx Hop Toll No. Inserted Digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: 0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Grp FRL NPA Pfx Hop Toll No. Inserted Digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>3: 0</td>
</tr>
</tbody>
</table>

change route-pattern 3

<table>
<thead>
<tr>
<th>Pattern Number: 3 Pattern Name: ToSM Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCAN? n Secure SIP? n Used for SIP stations? y</td>
</tr>
<tr>
<td>Primary SM: SM Secondary SM:</td>
</tr>
<tr>
<td>Grp FRL NPA Pfx Hop Toll No. Inserted Digits</td>
</tr>
<tr>
<td>3: 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbering LAR Dgts Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 M 4 W Request lev0-pvt none</td>
</tr>
</tbody>
</table>
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 5.3. The access code is removed and the ARS table matches the remaining outbound dialed digits and sends them to the designated route-pattern (see Section 5.11).

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

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

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

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Total Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node</th>
<th>ANI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1720</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>11</td>
<td>11</td>
<td>1</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>1900</td>
<td>11</td>
<td>11</td>
<td>deny</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>1900555</td>
<td>11</td>
<td>11</td>
<td>deny</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>lxxx976</td>
<td>11</td>
<td>11</td>
<td>deny</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>311</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>svcl</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>011</td>
<td>10</td>
<td>18</td>
<td>2</td>
<td>Intl</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>411</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>svcl</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>fnpa</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

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:

- **Dialled 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).

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 Media Gateway see [7].

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

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

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-pts1/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.

<table>
<thead>
<tr>
<th>display media-gateway 1</th>
<th>Page 1 of 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIA GATEWAY 1</td>
<td></td>
</tr>
<tr>
<td>Type: g430</td>
<td></td>
</tr>
<tr>
<td>Name: G430-1</td>
<td></td>
</tr>
<tr>
<td>Serial No: 11IS31439520</td>
<td></td>
</tr>
<tr>
<td>Link Encryption Type: any-pts1/tls</td>
<td>Enable CF? n</td>
</tr>
<tr>
<td>Network Region: 1</td>
<td>Location: 1</td>
</tr>
<tr>
<td>Use for IP Sync? n</td>
<td>Site Data:</td>
</tr>
<tr>
<td>Recovery Rule: none</td>
<td></td>
</tr>
<tr>
<td>Registered? y</td>
<td></td>
</tr>
<tr>
<td>FW Version/HW Vintage: 41.9.0 /1</td>
<td></td>
</tr>
<tr>
<td>MGP IPV4 Address: 10.64.91.91</td>
<td></td>
</tr>
<tr>
<td>MGP IPV6 Address:</td>
<td></td>
</tr>
<tr>
<td>Controller IP Address: 10.64.91.75</td>
<td></td>
</tr>
<tr>
<td>MAC Address: 00:1b:4f:53:37:69</td>
<td></td>
</tr>
<tr>
<td>Mutual Authentication? optional</td>
<td></td>
</tr>
</tbody>
</table>
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 [8] and [9] for additional information.

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

Step 2 - On the Media Server Element Manager, navigate to Home → System Configuration → Signaling Protocols → SIP → Node and Routes and add the Communication Manager Procr interface IP address (e.g., 10.64.91.75, see Section 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., 60), and provision the following:

- Group Type – Set to sip.
- Transport Method – Set to tls
- Verify that Peer Detection Enabled? – Set to n.
- Peer Server to AMS.
- Near-end Node Name – Set to the node name of the procr noted in Section 5.4.
- Far-end Node Name – Set to the node name of Media Server as administered in Section 5.4 (e.g., AMS).
- Near-end Listen Port and Far-end Listen Port – Set to 5061.
- Far-end Network Region – Set the IP network region to 1, as set in Section 5.7.1.
- Far-end Domain – Automatically populated with the IP address of the Media Server.

add signaling-group 60

<table>
<thead>
<tr>
<th>SIGNALING GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number: 60</td>
</tr>
<tr>
<td>Transport Method: tls</td>
</tr>
</tbody>
</table>

Peer Detection Enabled? n  Peer Server: AMS

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

Far-end Domain: 10.64.91.80
Step 4 - On Communication Manager, enter the **add media-server x** command where x is an available Media Server identifier (e.g., 1). Enter the following parameters:

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

<table>
<thead>
<tr>
<th>add media-server 1</th>
<th>Page 1 of 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIA SERVER</td>
<td></td>
</tr>
<tr>
<td>Media Server ID: 1</td>
<td></td>
</tr>
<tr>
<td>Signaling Group: 60</td>
<td></td>
</tr>
<tr>
<td>Voip Channel License Limit: 300</td>
<td></td>
</tr>
<tr>
<td>Dedicated Voip Channel Licenses: 300</td>
<td></td>
</tr>
<tr>
<td>Node Name: AMS</td>
<td></td>
</tr>
<tr>
<td>Network Region: 1</td>
<td></td>
</tr>
<tr>
<td>Location: 1</td>
<td></td>
</tr>
<tr>
<td>Announcement Storage Area: ANNC-be99ad1a-1f39-41e5-ba04-000c29f8f3f3</td>
<td></td>
</tr>
</tbody>
</table>

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 Certificate and verify the System Manager CA certificate is present in the Communication Manager trusted repository.
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 a Location for 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, the Avaya SBCE, Messaging and Experience Portal.
- Define Entity Links describing the SIP trunks between Session Manager, Communication Manager, Messaging and Experience Portal, as well as the SIP trunks between the Session Manager and the Avaya SBCE.
- Define Routing Policies associated with the Communication Manager, Messaging, Experience Portal 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.

![Diagram of System Manager GUI]

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.

![Diagram of Session Manager Routing Policies]

Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as “Domains”, “Locations”, “SIP Entities”, etc. The recommended order of routing element administration (that means the overall routing workflow) is as follows:

1. Create “Domain” of type SIP (other routing applications are referring domains of type SIP).
2. Create “Locations”.
3. Create “SIP Entities” if Handset Routing or Regular Expression Adaptors are in use.
4. Create “Adaptations”.
5. Create “SIP Entities” if SIP Entities that are used as “Outbound Processor” e.g. a certain “Gateway” or SIP Trunk.
6. Create all other SIP Entities (Session Managers, CH, SIP/PGTN Gateways, SIP Trunks).
7. Assign the appropriate Locations, Adaptations and “Outbound Processor”.
8. Create the “Entity Links”.
10. Between Session Managers and other SIP Entities.
11. Align with the bxml information received from the Service Providers.
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.
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.
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.
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”
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

![Digit Conversion for Outgoing Calls from SM](image)

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

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.
- Messaging (Section 6.5.5) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Messaging.
- Experience Portal (Section 6.5.6) – This entity, and its associated Entity Link (using TLS and port 5061), is for calls to/from Experience Portal.
Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5061 and 5081), and to the Avaya SBCE (port 5061). The connection between the Avaya SBCE and the Verizon Business IP Trunking service uses UDP/5071 per Verizon requirements.

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., SessionManager).
- **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, *(not the management interface), provisioned during installation (e.g., 10.64.91.81).*
- **Type** – Verify Session Manager is selected.
- **Location** – Select location Main (Section 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.
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 - Repeat Step 4 to provision entries for any other listening ports used by Session Manager, for example:

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

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

Step 7 - Click on **Commit**.

---

**Note** – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in Section 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).
- **FQDN or IP 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:
  - **Use Session Manager Configuration** for SIP Link Monitoring field and use the default values for the remaining parameters.

Step 3 - Click on Commit.
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.

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 IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., 10.64.91.50, see *Section 8.5*).
- **Type** – Select SIP Trunk.
- **Adaptations** – Select Adaptation SBC1-Adaptation for Verizon (Section 6.4.2).

6.5.5 **Avaya Aura® Messaging SIP Entity**

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

- **Name** – Enter a descriptive name (e.g., Aura Messaging).
- **FQDN or IP Address** – Enter the IP address of Messaging (e.g., 10.64.91.54).
- **Type** – Select Messaging.
- **Adaptations** – Leave this field blank.

6.5.6 **Avaya Aura® Experience Portal SIP Entity**

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

- **Name** – Enter a descriptive name (e.g., ExperiencePortal).
- **FQDN or IP Address** – Enter the IP address of Experience Portal (e.g., 10.64.91.90).
- **Type** – Select Voice Portal.
- **Adaptations** – Leave this field blank.
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).
- Session Manager to Messaging (Section 6.6.4).
- Session Manager to Experience Portal (Section 6.6.5).

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.
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).

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.

6.6.4 Entity Link to Avaya Aura® Messaging
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 Messaging (e.g., SM to AAM).
- **SIP Entity 1 Port** – Enter 5061.
- **SIP Entity 2** – Select the SIP Entity administered in Section 6.5.5 for the Aura® Messaging entity (e.g., Aura Messaging).
- **SIP Entity 2 Port** – Enter 5061.

6.6.5 Entity Link to Avaya Aura® Experience Portal
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 Messaging (e.g., SM to ExperiencePortal).
- **SIP Entity 1 Port** – Enter 5061.
- **SIP Entity 2** – Select the SIP Entity administered in Section 6.5.6 for the Experience Portal entity (e.g., ExperiencePortal).
- **SIP Entity 2 Port** – Enter 5061.
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.

6.8. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions (Section 6.8.1).
- Inbound calls to Messaging (Section 6.8.2).
- Inbound calls to Experience Portal (Section 6.8.3).
- Outbound calls to Verizon/PSTN (Section 6.8.4).

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.
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.

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.
6.8.2 Routing Policy for Inbound Calls to Avaya Aura® Messaging
This routing policy is for inbound calls to Aura® Messaging for message retrieval. Repeat the steps in Section 6.8.1 with the following differences:

- Enter a descriptive Name (e.g., To AAM), and ensure that the Disabled checkbox is unchecked to activate this Routing Policy.
- In the SIP Entities list page, select the SIP Entity administered in Section 6.5.5 for Aura® Messaging (e.g., AAM).

6.8.3 Routing Policy for Inbound Calls to Experience Portal
This routing policy is for inbound calls to Experience Portal. Repeat the steps in Section 6.8.1 with the following differences:

- Enter a descriptive Name (e.g., To Experience Portal), and ensure that the Disabled checkbox is unchecked to activate this Routing Policy.
- In the SIP Entities list page, select the SIP Entity administered in Section 6.5.6 for Experience Portal (e.g., ExperiencePortal).

6.8.4 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), and ensure that the Disabled checkbox is unchecked to activate this Routing Policy.
- In the SIP Entities list page, select the SIP Entity administered in Section 6.5.4 for the Avaya SBCE SIP Entity (e.g., SBC1).
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).

Note: Session Manager release 8.1 incorporates new functionality with the addition of Origination Dial Pattern sets. This configuration is optional. Origination Dial Pattern sets can be created to include digits patterns, that can be matched by Session Manager to make more granular routing decisions, like the use of alternate routes or call restriction for calls arriving to Session Manager from the same Originating Location. This is done by matching the number present on the From header of the call. More information can be found on [2] on the References section.

Origination Dial Patterns were not used in the reference configuration.

If Origination Dial Patterns are to be used in the customer configuration, **Enable Flexible Routing** needs to be checked under **Elements → Session Manager → Global Settings**.
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 732-945-0xx numbers into their corresponding Communication Manager extensions.
- Min and Max – Enter 10.
- SIP Domain – Select the enterprise SIP domain, e.g., avayalab.com.

**Step 3** - 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**.

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 6.8.4** (e.g., **To SBC1**).

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

![Image of AVAYA System Manager dashboard](image)

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

![Manage Elements screen](image)
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. Avaya Aura® Experience Portal

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

7.1. Background

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

References to the Voice XML and/or Call Control XML applications are administered on Experience Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Experience Portal, the called party DNIS number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match is found, Experience Portal informs the caller that the call cannot be handled, and disconnects the call\(^1\).

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

\(^1\) An application may be configured with “inbound default” as the called number, to process all inbound calls that do not match any other application references.
7.2. Logging In and Licensing

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

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

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

**Step 2** - In the left pane, navigate to **Security**→**Licensing**. On the **Licensing** page, verify that Experience Portal is properly licensed. If required licenses are not enabled, contact an authorized Avaya account representative to obtain the licenses.
7.3. VoIP Connection
This section defines a SIP trunk between Experience Portal and Session Manager.

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

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

Step 2 - Configure a SIP connection as follows:
- **Name** – Set to a descriptive name (e.g., SM8).
- **Enable** – Set to Yes.
- **Proxy Server Transport** – Set to TLS.
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = 10.64.91.81 (the IP address of the Session Manager signaling interface defined in Section 6.5.1).
  - **Port** = 5061
  - **Priority** = 0 (default)
  - **Weight** = 0 (default)
- **Listener Port** – Set to 5061.
- **SIP Domain** – Set to avayalab.com (see Section 6.2).
- **Consultative Transfer** – Select REFER.
- **SIP Reject Response Code** – Select ASM (503).
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of 10 was used.
- Select **All Calls can be either inbound or outbound**.
- **SRTP Enable** = Yes
- **Encryption Algorithm** = AES_CM_128
- **Authentication Algorithm** = HMAC_SHA1_80
- **RTCP Encryption Enabled** = No
- **RTP Authentication Enabled** = Yes
- Use default values for all other fields.
- Click Save.
7.4. Speech Servers

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

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

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

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

![Image of Change Application page](image-url)
### 7.6. MPP Servers and VoIP Settings

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

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

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

**Step 3** - The certificate page will open. Check the **Trust this certificate** box (not shown). Once complete, click **Save**.
Step 4 - Click VoIP Settings tab on the screen displayed in Step 1, and the following screen is displayed.

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

![VoIP Settings Screen](image)

- In the Codecs section set:
  - Set Packet Time to 20.
  - Verify the G729 Codec is enabled.
  - Set G729 Discontinuous Transmission to No (G.729A).
  - Set the Offer Order to the preferred codec. In the sample configuration, G729 is the first codec, followed by G711ulaw, then G711aLaw.

- Use default values for all other fields.

Step 5 - Click on Save.
7.7. Configuring RFC2833 Event Value Offered by Experience Portal

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

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

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

- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

After saving the file with the change, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the Restart button available via the Experience Portal GUI at System Management → MPP Manager. Note that the State column shows when the MPP is running after the restart.
8. 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.

Enter the Username and click on Continue.

![Log In](image)

Enter the password and click on Log In.
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.

8.1. 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 **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.

<table>
<thead>
<tr>
<th>General Configuration</th>
<th>Device Configuration</th>
<th>Dynamic License Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance Name: SBC8-90</td>
<td>HA Mode: No</td>
<td>Min License Allocation</td>
</tr>
<tr>
<td>Box Type: SIP</td>
<td>Two Bypass Mode: No</td>
<td>Standard Sessions: 10</td>
</tr>
<tr>
<td>Deployment Mode: Proxy</td>
<td></td>
<td>Advanced Sessions: 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scopia Video Sessions: 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CES Sessions: 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transcoding Sessions: 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLID: ---</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption: NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Configuration</th>
<th>Management IP(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Public IP</td>
</tr>
<tr>
<td>10.64.91.48</td>
<td>10.64.91.48</td>
</tr>
<tr>
<td>10.64.91.49</td>
<td>10.64.91.49</td>
</tr>
<tr>
<td>10.64.91.50</td>
<td>10.64.91.50</td>
</tr>
<tr>
<td>1.1.1.2</td>
<td>1.1.1.2</td>
</tr>
</tbody>
</table>

| DNS Configuration | IP #1 (IPv4) | 10.64.99.90 |
|------------------|-------------|
| Primary DNS: 172.39.269.4 | | |
| Secondary DNS | | |
| DNS Location: DAI | | |
| DNS Client IP: 1.1.1.2 | | |
8.2. TLS Management

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

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

8.2.1 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.
8.2.2 Server Profiles

Step 1 - Select TLS Management → Server Profiles and click on Add. Enter the following:
- **Profile Name**: enter descriptive name.
- **Certificate**: select the identity certificate, e.g., **Inside-Server**, from pull down menu.
- **Peer Verification = None**.
- Click Next.

Step 2 - Accept default values for the next screen (not shown) and click **Finish**.
The following screen shows the completed TLS **Server Profile** form:
8.2.3 Client Profiles

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

- **Profile Name**: enter descriptive name.
- **Certificate**: select the identity certificate, e.g., **Inside-Client**, from pull down menu.
- **Peer Verification = Required**.
- **Peer Certificate Authorities**: select the CA certificate used to verify the certificate received from Session Manager, e.g., **SystemManager8CA.pem**.
- **Verification Depth**: enter 1.
- Click Next.

Step 2 - Accept default values for the next screen (not shown) and click Finish.
The following screen shows the completed TLS Client Profile form:
8.3. 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.

**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.
8.4. 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**.

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**.
8.5. 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 8.2.2 (e.g., Inside_Server)

Step 3 - Click Finish.

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.
8.6. 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.

8.6.1 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.
8.6.2 Server Interworking Profile – Verizon

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

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

**Step 1** - Select **Add Profile** 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).
8.7. 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 8.6) or Signaling Rules (Section 8.13) does not meet the desired result. Refer to Additional References [10] 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 14.

**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 14.

![Sigma Script Example](image)

**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.
8.8. 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.

8.8.1 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 8.2.3 (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.
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.

![Edit SIP Server Profile - Heartbeat](image)

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 8.6), 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.

![Edit SIP Server Profile - Advanced](image)
8.8.2 SIP Server Profile – Verizon

Repeat the steps in Section 8.8.1, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Verizon.

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

**Step 2** - On the General window, enter the following:
- **Server Type**: Select Trunk Server.
- **IP Address**: 172.30.209.21 (Verizon-provided IP address).
- **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.

![Edit SIP Server Profile - General](image)

**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.

![Heartbeat Settings](image)
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 8.6.2), for Interworking Profile.
- Select the Verizon IPT Script (created in Section 8.7) for Signaling Manipulation Script.
- Select Finish.

![Edit SIP Server Profile Advanced](image)

8.9. 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.
8.9.1 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 8.8.1).
- 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.
8.9.2 Routing Profile – Verizon

Repeat the steps in Section 8.9.1, 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 8.8.2).
- Next Hop Address: Verify that 172.30.209.21:5071 (UDP) is selected.

Step 3 - Click Finish.
8.10. 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.

8.10.1 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**.
8.10.2 Topology Hiding – Verizon

Repeat the steps in Section 8.10.1, 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.

8.11. 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.
8.12. 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.

8.12.1 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.

![Media Rules: enterprise-med-rule](image1)

**8.12.2 Verizon – Media Rule**

Repeat the steps in **Section 8.12.1**, 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.

![Media Rules: Vz-trk-med-rule](image2)
8.13. 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.

8.13.1 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.
8.13.2 Signaling Rule – Verizon
Repeat the steps in Section 8.13.1, 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.

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

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 8.15.

8.14.1 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: enterprise-trk-policy.
- Click Next.
Step 3 – On the Policy Group window (not shown), select the following.
  - Application Rule: sip-trunk (created in Section 8.11).
  - Border Rule: default.
  - Media Rule: enterprise-med-rule (created in Section 8.12.1).
  - Signaling Rule: enterprise-sig-rule (created in Section 8.13.1).

Step 4 - Select Finish.

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

8.14.2 Endpoint Policy Groups – Verizon

Step 1 - Repeat steps 1 through 4 from Section 8.14.1 with the following changes:
  - Group Name: Vz-policy-grp.
  - Media Rule: Vz-trk-med-rule (created in Section 8.12.2).
  - Signaling Rule: Vz-trk-sig-rule (created in Section 8.13.2).

The completed Policy Group Vz-policy-grp is shown on the screen below.
8.15. 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.

8.15.1 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 8.8.1).
- URI Group: *
- Transport: *
- Remote Subnet: *
- Received Interface: Vz-Sig-B1 (Section 8.5).
- Signaling Interface: Inside-Sig-50 (Section 8.5).
- Media Interface: Inside-Med-50 (Section 8.4).
- End Point Policy Group: enterprise-trk-policy (Section 8.14.1).
- Routing Profile: Route to VZ IPT (Section 8.9.2).
- Topology Hiding Profile: Enterprise-Topology (Section 8.10.1).
- Let other fields at the default values.

Step 3 - Click Finish (not shown).
8.15.2 Server Flow – Verizon

Step 1 - Repeat steps 1 through 3 from Section 8.15.1, with the following changes:

- **Flow Name**: Enter a name for the flow, e.g., *Verizon IPT Flow (for SM).*
- **Server Configuration**: Verizon IPT (Section 8.8.2).
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: Inside-Sig-50 (Section 8.5).
- **Signaling Interface**: Vz-Sig-B1 (Section 8.5).
- **Media Interface**: Vz-Med-B1 (Section 8.4).
- **End Point Policy Group**: Vz-policy-grp (Section 8.14.2).
- **Routing Profile**: Route to SM8 (Section 8.9.1).
- **Topology Hiding Profile**: VZ IPT Topology (Section 8.10.2).

![Server Flow Tab](image)

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

![Server Flows Tab](image)


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

9.1. Service Access Information

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

<table>
<thead>
<tr>
<th>CPE (Avaya)</th>
<th>Verizon Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>adevc.avaya.globalipcom.com</td>
<td>pcelban0001.avayalincroft.globalipcom.com</td>
</tr>
<tr>
<td>UDP port 5060</td>
<td>UDP Port 5071</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP DID Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>732-945-0231</td>
</tr>
<tr>
<td>732-945-0232</td>
</tr>
<tr>
<td>732-945-0233</td>
</tr>
<tr>
<td>732-945-0234</td>
</tr>
<tr>
<td>732-945-0235</td>
</tr>
<tr>
<td>732-945-0236</td>
</tr>
<tr>
<td>732-945-0237</td>
</tr>
<tr>
<td>732-945-0238</td>
</tr>
<tr>
<td>732-945-0239</td>
</tr>
</tbody>
</table>
10. Verification Steps
This section provides example verifications of the Avaya configuration with Verizon Business IP Trunk service.

10.1. Avaya Aura® Communication Manager Verifications
This section illustrates verifications from Communication Manager.

The following edited Communication Manager list trace tac trace output shows 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

LIST TRACE

07:33:03 TRACE STARTED 08/01/2019 CM Release String cold-01.0.890.0-25517
07:33:09 SIP<INVITE sips:50231@avayalab.com SIP/2.0
07:33:09 Call-ID: 7d190449a90cb62d5249c61df2a3da78
07:33:09 active trunk-group 1 member 1 cid 0x139
07:33:09 Call-ID: 7d190449a90cb62d5249c61df2a3da78
07:33:09 dial 50231
07:33:09 ring station 50231 cid 0x139
07:33:09 Alerting party uses public-unknown-numbering
07:33:09 G711MU ss:off ps:20
07:33:09 G711MU rgp:1 [10.5.3.211]:25458
07:33:09 G711MU rgp:1 [10.64.91.91]:16400
07:33:09 G729 ss:off ps:20
07:33:09 G729 rgp:2 [10.64.91.50]:35104
07:33:09 G729 rgp:1 [10.64.91.91]:16390
07:33:09 xoip options: fax:T38 modem:off tty:US uid:0x500001
07:33:09 xoip ip: [10.64.91.91]:16390
07:33:15 SIP>SIP/2.0 200 OK
07:33:15 Call-ID: 7d190449a90cb62d5249c61df2a3da78
07:33:15 active station 50231 cid 0x139
```
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.

<table>
<thead>
<tr>
<th>status trunk 1/1</th>
<th>CALL CONTROL SIGNALING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near-end Signaling Loc: PROCR</td>
<td></td>
</tr>
<tr>
<td>Signaling IP Address                     Port</td>
<td></td>
</tr>
<tr>
<td>Near-end: 10.64.91.75               : 5081</td>
<td></td>
</tr>
<tr>
<td>Far-end: 10.64.91.81              : 5081</td>
<td></td>
</tr>
<tr>
<td>H.245 Near:</td>
<td></td>
</tr>
<tr>
<td>H.245 Far:</td>
<td></td>
</tr>
<tr>
<td>H.245 Signaling Loc:                  H.245 Tunneled in Q.931? no</td>
<td></td>
</tr>
<tr>
<td>Audio Connection Type: ip-direct       Authentication Type: None</td>
<td></td>
</tr>
<tr>
<td>Near-end Audio Loc:                   Codec Type: G.729</td>
<td></td>
</tr>
<tr>
<td>Audio IP Address                      Port</td>
<td></td>
</tr>
<tr>
<td>Near-end: 10.5.5.211                : 25458</td>
<td></td>
</tr>
<tr>
<td>Far-end: 10.64.91.50               : 35110</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>status trunk 1/1</th>
<th>SRC PORT TO DEST PORT TALKPATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>src port: T00001</td>
<td></td>
</tr>
<tr>
<td>T00001:TX:10.64.91.50:35938/g729/20ms/1-srtp-aescm128-hmac80</td>
<td></td>
</tr>
<tr>
<td>T00028:RX:10.64.91.154:5004/g729/20ms/1-srtp-aescm128-hmac80</td>
<td></td>
</tr>
</tbody>
</table>
10.2. 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 3/16 under the **Entity Monitoring** column shows that there are alarms on 3 out of the 16 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.

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.
10.3. Avaya Session Border Controller for Enterprise Verification

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

10.3.1 Incidents

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

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

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

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

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 8.8.
10.3.3 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.

10.3.4 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.
When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, click the Stop Capture button at the bottom.

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

11. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, Avaya Aura® Experience Portal 7.2 and Avaya Session Border Controller for Enterprise 8.0 can be configured to interoperate successfully with Verizon Business IP Trunking service. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users access to the PSTN using a Verizon Business IP Trunking public SIP trunk service connection.
12. Additional References

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

**Avaya Aura® Session Manager/System Manager**
- [1] Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment, Release 8.1, Issue 1, June 2019

**Avaya Aura® Communication Manager**
- [9] 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**

**Avaya Aura® Messaging**

**Avaya Aura® Experience Portal**
- [14] Implementing Avaya Aura® Experience Portal on a single server, Release 7.2.2, Issue 1, March 2019

12.2. Verizon Business
The following documents may be obtained by contacting a Verizon Business Account Representative.
- [15] Retail VoIP Interoperability Test Plan
- [16] Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)
13. Appendix A – Avaya SBCE – Refer Handling

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

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

Create a URI Group for numbers intended for Communication Manager.

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

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

**Step 3** - Enter the following:

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

![Edit URI](image)
Step 4 - For additional entries, select Add on the right-hand side of the URI Group tab and repeat Step 3.

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

Step 1 - Select Configuration Profiles → Server Interworking from the left-hand menu
Step 2 - Select the Verizon Server Interworking Profile created in Section 8.6.2 and click Edit
  - Check Refer Handling.
  - URI Group: internal-extensions
  - Select Finish.
14. Appendix B – Avaya SBCE – SigMa Script File

Details of the Signaling Manipulation script used in the configuration of the Avaya SBCE, in Section 8.7.

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");
  }
}
©2019 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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