Application Notes for AT&T SIP Trunking Service with Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Aura® Communication Manager Release 7.0 and Avaya Aura® Session Manager 7.0 with SIP Trunks to the Avaya Session Border Controller for Enterprise 7.0 (Avaya SBCE) when used to connect the AT&T SIP Trunking Service available from AT&T (Australia).

AT&T SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the AT&T network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

AT&T is a member of the Avaya DevConnect Service Provider program. 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.
Table of Contents

1. Introduction ............................................................................................................. 4
2. General Test Approach and Test Results ............................................................... 4
   2.1 Interoperability Compliance Testing .................................................................. 4
2.2 Test Results ........................................................................................................... 5
2.3 Support .................................................................................................................. 6
3. Reference Configuration ......................................................................................... 6
4. Equipment and Software Validated ....................................................................... 8
5. Configure Avaya Aura® Communication Manager .................................................. 9
   5.1 System-Parameters Customer-Options ............................................................... 9
   5.2 System-Parameters Features ............................................................................ 10
   5.3 Dial Plan ............................................................................................................ 11
   5.4 IP Node Names .................................................................................................. 12
   5.5 IP Interface for Procrs ...................................................................................... 12
   5.6 IP Network Regions .......................................................................................... 13
   5.7 IP Codec Parameters ....................................................................................... 15
   5.8 SIP Trunks ......................................................................................................... 16
      5.8.1 Signaling Group .......................................................................................... 16
      5.8.2 Trunk Group .............................................................................................. 17
   5.9 Calling Party Information ................................................................................. 20
   5.10 Incoming Call Handling Treatment .................................................................. 20
   5.11 Outbound Routing ........................................................................................... 21
   5.12 Avaya G430 Media Gateway Provisioning ....................................................... 23
   5.13 Avaya Aura® Media Server Provisioning ......................................................... 24
      5.13.1 Signaling Group for Media Server ............................................................ 24
      5.13.2 Adding Media Server ............................................................................... 25
   5.14 Save Communication Manager Translations .................................................. 25
6. Configure Avaya Aura® Session Manager ............................................................... 26
   6.1 Configure SIP Domain ....................................................................................... 27
6.2 Configure Locations ............................................................................................. 27
   6.3 Configure SIP Entities ....................................................................................... 27
      6.3.1 Configure Session Manager SIP Entity ...................................................... 28
      6.3.2 Configure Communication Manager SIP Entity ....................................... 28
      6.3.3 Configure Avaya SBCE SIP Entity ............................................................. 30
   6.4 Configure Entity Links ...................................................................................... 30
      6.4.1 Configure Entity Link to Communication Manager ..................................... 31
      6.4.2 Configure Entity Link for Avaya SBCE ...................................................... 32
6.5 Configure Routing Policies .................................................................................. 32
   6.5.1 Configure Routing Policy for Communication Manager ............................. 32
   6.5.2 Configure Routing Policy for Avaya SBCE .................................................. 33
   6.6 Configure Dial Patterns ..................................................................................... 33
7. Configure Avaya Session Border Controller for Enterprise .......................................................... 37
7.1 System Management – Status ......................................................................................................... 38
7.2 Global Profiles ............................................................................................................................. 39
  7.2.1 Uniform Resource Identifier (URI) Groups ............................................................................. 39
  7.2.2 Server Interworking – Session Manager .............................................................................. 40
  7.2.3 Server Interworking – AT&T ................................................................................................. 43
  7.2.4 Server Configuration – Session Manager ............................................................................. 45
  7.2.5 Server Configuration – AT&T ............................................................................................... 47
  7.2.6 Routing – To Session Manager ............................................................................................. 49
  7.2.7 Routing – To AT&T ................................................................................................................ 50
  7.2.8 Topology Hiding – Session Manager .................................................................................... 51
  7.2.9 Topology Hiding – AT&T ....................................................................................................... 51
  7.2.10 Domain Policies ..................................................................................................................... 52
  7.2.11 Application Rules ................................................................................................................. 52
  7.2.12 Border Rules ........................................................................................................................ 52
  7.2.13 Media Rules .......................................................................................................................... 53
  7.2.14 Signaling Rules ..................................................................................................................... 54
  7.2.15 Endpoint Policy Groups ....................................................................................................... 54
7.3 Device Specific Settings ................................................................................................................... 54
  7.3.1 Network Management ............................................................................................................ 54
  7.3.2 Media Interfaces ..................................................................................................................... 55
  7.3.3 Signaling Interface ................................................................................................................ 56
  7.3.4 Endpoint Flows – For Session Manager ............................................................................... 57
  7.3.5 Endpoint Flows – For AT&T ................................................................................................. 58
8. Verification Steps ............................................................................................................................ 59
  8.1 Avaya Session Border Controller for Enterprise ................................................................. 59
  8.2 Avaya Aura® Communication Manager ................................................................................. 61
  8.3 Avaya Aura® Session Manager Status .................................................................................... 62
  8.4 Telephony Services .................................................................................................................... 63
9. Conclusion ........................................................................................................................................ 63
10. Additional References ...................................................................................................................... 63
1. Introduction

These Application Notes illustrate a sample configuration Avaya Aura® Communication Manager Release 7.0 and Avaya Aura® Session Manager 7.0 with SIP Trunks to the Avaya Session Border Controller for Enterprise 7.0 (Avaya SBCE) when used to connect to the AT&T SIP Trunking Service available from AT&T (Australia).

Avaya Aura® Session Manager 7.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 7.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya SBCE 7.0 is the point of connection between Avaya Aura® Session Manager and the AT&T SIP Trunking Service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The SIP Trunking Service available from AT&T is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The AT&T SIP Trunking Service allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise’s sites.

2. General Test Approach and Test Results

The general test approach was to make calls through the Avaya SBCE while DoS policies are in place using various codec settings and exercising common and advanced PBX features.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising 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.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, the Avaya SBCE, and the AT&T SIP Trunking Service.

The compliance testing was based on the standard Avaya GSSCP test plan. The testing covered functionality required for compliance as a solution supported on the AT&T SIP Trunk network. Calls were made to and from the PSTN across the AT&T network. The following standard features were tested as part of this effort:
Inbound PSTN calls to various phone types including H.323, SIP and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.

Outbound PSTN calls from various phone types including H.323, SIP and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.

Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) and Avaya Communicator for Windows soft phones. Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested.

Dialing plans including local, long distance, international, outbound toll-free, calls etc.

Calling Party Name presentation and Calling Party Name restriction.

Codecs G.711A, G.711MU and G.729A.

Media and Early Media transmissions.

Incoming and outgoing fax using T.38-standard.

DTMF tone transmissions as out-of-band RTP events as per RFC2833.

Voicemail navigation for inbound and outbound calls.

User features such as hold and resume, transfer, forward and conference.

Off-net call forward with Diversion method.

EC500 mobility (extension to cellular) with Diversion method.

Routing inbound vector call to call center agent queues.

Response to OPTIONS heartbeat.

Response to incomplete call attempts and trunk errors.

Session Timers implementation.

Network Call Redirection.

Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

2.2 Test Results

Interoperability testing of AT&T SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Inbound call** – It was observed that in the inbound call from PSTN phones to Avaya SIP IP phones, Avaya Aura® Session Manager responded back with SIP 500 “Server Internal Error” to the SIP INVITE message sent from AT&T Sip Trunk. This was found to be caused by low value of Max-forwards header value (i.e. 10) in the SIP INVITE message to Avaya SBCE. Resolution of the issue was done by AT&T Engineer by increasing the value of Max-forwards header of SIP message at AT&T’s Session Border Controller to 50.
2.3 Support

- **Avaya**: Avaya customers may obtain documentation and support for Avaya products by visiting [http://support.avaya.com](http://support.avaya.com).
- **AT&T Australia**: Customers should contact their AT&T Business representative or follow the support links available on [http://www.corp.att.com/ap/about/where/australia/](http://www.corp.att.com/ap/about/where/australia/).

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya Aura® Communication Manager running on VMware ESXi 5.5.
- Avaya Aura® Session Manager running on VMware ESXi 5.5.
- Avaya Aura® System Manager running on VMware ESXi 5.5.
- Avaya Aura® Messaging running on VMware ESXi 5.5.
- Avaya G430 Media Gateway.
- Avaya Aura® Media Server running on VMware ESXi 5.5. The Media Server can act as a media gateway Gxxx series in providing tones, announcements or music on hold.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running H.323/SIP software.
- Avaya one-X® Communicator 6.2.
- Avaya Communicator for Windows 2.1.
- The Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the AT&T SIP Trunking Service and the enterprise internal network.

All IP addresses shown in the diagram are private IP addresses.
Figure 1: Network Components as Tested
## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avaya</strong></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura Communication Manager 7.0</td>
<td>7.0.0.3.1.441.22947</td>
</tr>
<tr>
<td>Avaya Aura Session Manager 7.0 SP2</td>
<td>7.0.0.2.700201</td>
</tr>
<tr>
<td>Avaya Aura System Manager 7.0 SP2</td>
<td>Build No. - 7.0.0.0.16266-7.0.9.7002010</td>
</tr>
<tr>
<td></td>
<td>Software Update Revision No: 7.0.0.2.4416</td>
</tr>
<tr>
<td>Avaya Aura Messaging 6.3.3</td>
<td>6.3.3.0.11348</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise 7.0</td>
<td>7.00-21-6602</td>
</tr>
<tr>
<td>Avaya Media Gateway G430</td>
<td>g430_sw_37_21_0</td>
</tr>
<tr>
<td>Avaya Aura Media Server 7.7</td>
<td>7.7.0.281</td>
</tr>
<tr>
<td>Avaya One-X Communicator 6.2</td>
<td>6.2.11.03</td>
</tr>
<tr>
<td>Avaya Communicator for Windows 2.1</td>
<td>2.1.3.80</td>
</tr>
<tr>
<td>Avaya One-X Agent H323 2.5.8</td>
<td>2.5.58020.0</td>
</tr>
<tr>
<td>Avaya 96x1 series – SIP phone</td>
<td>7.0.1.0.46</td>
</tr>
<tr>
<td>Avaya 96xx series – H.323 phone</td>
<td>6.6115</td>
</tr>
<tr>
<td><strong>Service Provider</strong></td>
<td></td>
</tr>
<tr>
<td>AT&amp;T SIP Trunking Service</td>
<td>Genband</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these Application Notes. Other parameter values may or may not match based on local configurations.

5.1 System-Parameters Customer-Options

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

NOTE - For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.

Follow the steps shown below:

1. Enter the **display system-parameters customer-options** command. On Page 2 of the form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

```
display system-parameters customer-options

OPTIONAL FEATURES

IP PORT CAPACITIES

| Maximum Administered H.323 Trunks: 12000 | 0 |
| Maximum Concurrently Registered IP Stations: 18000 | 4 |
| Maximum Administered Remote Office Trunks: 12000 | 0 |
| Maximum Concurrently Registered Remote Office Stations: 18000 | 0 |
| Maximum Concurrently Registered IP eCons: 0 | 0 |
| Max Concur Registered Unauthenticated H.323 Stations: 0 | 0 |
| Maximum Video Capable Stations: 41000 | 1 |
| Maximum Video Capable IP Softphones: 1000 | 2 |
| **Maximum Administered SIP Trunks:** 24000 | 70 |
| Maximum Administered Ad-hoc Video Conferencing Ports: 24000 | 0 |
| Maximum Number of DS1 Boards with Echo Calculated: 522 | 0 |
```
2. On **Page 6** of the form, verify that the **Private Networking** and **Processor Ethernet** fields are set to *y*.

<table>
<thead>
<tr>
<th>display system-parameters customer-options</th>
<th>Page 6 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPTIONAL FEATURES</strong></td>
<td></td>
</tr>
<tr>
<td>Multinational Locations? n</td>
<td>Station and Trunk MSP? y</td>
</tr>
<tr>
<td>Multiple Level Precedence &amp; Preemption? y</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><strong>Private Networking? y</strong></td>
<td>Uniform Dialing Plan? y</td>
</tr>
<tr>
<td><strong>Processor Ethernet? y</strong></td>
<td>Usage Allocation Enhancements? y</td>
</tr>
<tr>
<td>Remote Office? y</td>
<td>Wideband Switching? y</td>
</tr>
<tr>
<td>Restrict Call Forward Off Net? y</td>
<td>Wireless? n</td>
</tr>
<tr>
<td>Secondary Data Module? y</td>
<td></td>
</tr>
</tbody>
</table>

5.2 **System-Parameters Features**

Follow the steps shown below:

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>display system-parameters features</th>
<th>Page 1 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE-RELATED SYSTEM PARAMETERS</strong></td>
<td></td>
</tr>
<tr>
<td>Self Station Display Enabled? n</td>
<td></td>
</tr>
<tr>
<td><strong>Trunk-to-Trunk Transfer:</strong> all</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback with Called Party Queuing? n</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback - No Answer Timeout Interval (rings): 3</td>
<td></td>
</tr>
<tr>
<td>Call Park Timeout Interval (minutes): 1</td>
<td></td>
</tr>
<tr>
<td>Off-Premises Tone Detect Timeout Interval (seconds): 20</td>
<td></td>
</tr>
<tr>
<td>AAR/ARS Dial Tone Required? y</td>
<td></td>
</tr>
<tr>
<td>Music (or Silence) on Transferred Trunk Calls? no</td>
<td></td>
</tr>
<tr>
<td>DID/Tie/ISDN/SIP Intercept Treatment: attendant</td>
<td></td>
</tr>
<tr>
<td>Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred</td>
<td></td>
</tr>
<tr>
<td>Automatic Circuit Assurance (ACA) Enabled? n</td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dial Programming by Assigned Lists? n</td>
<td></td>
</tr>
<tr>
<td>Auto Abbreviated/Delayed Transition Interval (rings): 2</td>
<td></td>
</tr>
<tr>
<td>Protocol for Caller ID Analog Terminals: Bellcore</td>
<td></td>
</tr>
<tr>
<td>Display Calling Number for Room to Room Caller ID Calls? n</td>
<td></td>
</tr>
</tbody>
</table>
2. On Page 9 verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the value of Restricted for restricted calls and Unavailable for unavailable calls.

```
<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Call Length</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>fac</td>
</tr>
<tr>
<td>847</td>
<td>4</td>
<td>ext</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>fac</td>
</tr>
<tr>
<td>*</td>
<td>3</td>
<td>dac</td>
</tr>
<tr>
<td>#</td>
<td>4</td>
<td>fac</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.

Follow the steps shown below:

- Enter the `change dialplan analysis` command to provision the following dial plan.
  - 4-digit extensions with a Call Type of `ext` beginning with `847` (which is a subset of DID numbers (028059847x) assigned by AT&T).
  - 3-digit dial access code (indicated with a Call Type of `dac`), e.g., access code `*` for SIP Trunk Access Codes (TAC).
5.4 IP 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 6.3.2.

Follow the steps shown below:

- Enter the `change node-names ip` command, and add node names and IP addresses for the following:
  - Session Manager SIP signaling interface (e.g., ve3-sm and 192.168.1.11).
  - Media Server (e.g., ve4-ams and 192.168.1.15).

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ve3-sm</td>
<td>192.168.1.11</td>
</tr>
<tr>
<td>ve4-ams</td>
<td>192.168.1.15</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>procr</td>
<td>192.168.1.12</td>
</tr>
<tr>
<td>procr6</td>
<td>::</td>
</tr>
</tbody>
</table>

5.5 IP Interface for Procr
The `display ip-interface procr` command can be used to verify the Processor Ethernet (procr) parameters defined during installation.

- Verify that Enable Interface?, Allow H.323 Endpoints?, and Allow H248 Gateways? fields are set to y.
- In the reference configuration the procr is assigned to Network Region: 1.
- The default values are used for the remaining parameters.
5.6 IP Network Regions

For the compliance testing, ip-network-region 1 was created by the `change ip-network-region 1` command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is `sipinterop.net`. This domain name appears in the “From” header of SIP message originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to **yes**. Shuffling can be further restricted at the trunk level under the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.7**.
- Default values can be used for all other fields.

```
display ip-network-region 1
```

<table>
<thead>
<tr>
<th>IP NETWORK REGION</th>
<th>Page 1 of 20</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Region</strong>: 1</td>
<td><strong>Authoritative Domain</strong>: sipinterop.net</td>
</tr>
<tr>
<td><strong>Location</strong>: 1</td>
<td><strong>Stub Network Region</strong>: n</td>
</tr>
<tr>
<td><strong>Name</strong>: 123ER</td>
<td><strong>Intra-region IP-IP Direct Audio</strong>: yes</td>
</tr>
<tr>
<td><strong>Codec Set</strong>: 1</td>
<td><strong>Inter-region IP-IP Direct Audio</strong>: yes</td>
</tr>
<tr>
<td><strong>UDP Port Min</strong>: 16384</td>
<td><strong>IP Audio Hairpinning?</strong>: n</td>
</tr>
<tr>
<td><strong>UDP Port Max</strong>: 53999</td>
<td></td>
</tr>
<tr>
<td><strong>DIFFSERV/TOS PARAMETERS</strong></td>
<td><strong>AUDIO RESOURCE RESERVATION PARAMETERS</strong></td>
</tr>
<tr>
<td><strong>Call Control PHB Value</strong>: 34</td>
<td><strong>RSVP Enabled?</strong>: n</td>
</tr>
<tr>
<td><strong>Audio PHB Value</strong>: 46</td>
<td><strong>Audio PHB Value</strong>: 46</td>
</tr>
<tr>
<td><strong>Video PHB Value</strong>: 26</td>
<td><strong>Video PHB Value</strong>: 26</td>
</tr>
<tr>
<td><strong>802.1P/Q PARAMETERS</strong></td>
<td><strong>H.323 IP ENDPOINTS</strong></td>
</tr>
<tr>
<td><strong>Call Control 802.1p Priority</strong>: 6</td>
<td><strong>H.323 Link Bounce Recovery?</strong>: y</td>
</tr>
<tr>
<td><strong>Audio 802.1p Priority</strong>: 6</td>
<td><strong>Idle Traffic Interval (sec)</strong>: 20</td>
</tr>
<tr>
<td><strong>Video 802.1p Priority</strong>: 5</td>
<td><strong>Keep-Alive Interval (sec)</strong>: 5</td>
</tr>
<tr>
<td></td>
<td><strong>Keep-Alive Count</strong>: 5</td>
</tr>
<tr>
<td></td>
<td><strong>Subnet Mask</strong>: /24</td>
</tr>
</tbody>
</table>
On Page 4, define the IP codec set to be used for traffic in region 1. In the compliance testing, Communication Manager, the Avaya G430 Media Gateway, IP/SIP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the *codec set* column of the table with appropriate destination region (*dst rgn*). Default values may be used for all other fields.

![Codec Table](image)

Non-IP telephones (e.g., analog, digital) derive their network region from the IP interface of the Avaya G430 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use the `change ip-interface procr` command as shown in the following screen.

![IP Interface Screen](image)
To define network region 1 for the Avaya G430 Media Gateway, use the `change media-gateway` command as shown in the following screen.

```
change media-gateway 1
MEDIA GATEWAY 1

    Type: g430
    Name: g430
    Serial No: 10IS2xxxxxxx
    Link Encryption Type: any-pts/tls
    Network Region: 1
    Location: 1
    Site Data: 1

    Recovery Rule: none

    Registered? y
    FW Version/HW Vintage: 37.21.0 /1
    MGP IPV4 Address: 192.168.1.13
    MGP IPV6 Address: 00:1b:4f:3f:14:48
    Controller IP Address: 192.168.1.12

Mutual Authentication? optional
```

### 5.7 IP Codec Parameters

Follow the steps shown below:

1. Enter the `change ip-codec-set x` command, where `x` is the number of the IP codec set specified in Section 5.6. On Page 1 of the ip-codec-set form, ensure that G.711A, G.711MU and G.729A are included in the codec list. Note that the packet interval size will default to 20ms.

```
change ip-codec-set 1
IP CODEC SET

Codec Set: 1

Audio Codec       Silence Suppression Frames Per Pkt Packet Size(ms)
1: G.711A         n         2        20
2: G.711MU        n         2        20
3: G.729A         n         2        20
4:                
5:                
6:                
7:                

Media Encryption  Encrypted SRTCP: enforce-unenc-srtcp
1: none
2:                
3:                
4:                
5:                
```
2. On Page 2 of the ip-codec-set form, set FAX Mode to \texttt{t.38-standard}.

<table>
<thead>
<tr>
<th></th>
<th>Mode</th>
<th>Redundancy</th>
<th>ECM</th>
<th>Size (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FAX</strong></td>
<td>\texttt{t.38-standard}</td>
<td>0</td>
<td>y</td>
<td>20</td>
</tr>
<tr>
<td>Modem</td>
<td>off</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TDD/TTY</td>
<td>US</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 Clear-channel</td>
<td>n</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP 64K Data</td>
<td>n</td>
<td>0</td>
<td></td>
<td></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.

#### 5.8.1 Signaling Group

This section describes the steps for administering the SIP trunk to Session Manager. This trunk corresponds to the \texttt{ve3-cm} SIP Entity defined in Section 6.3.2.

Enter the \texttt{add signaling-group x} command, where \texttt{x} is the number of an unused signaling group (e.g., 3), and provision the following:

- **Group Type** – Set to \texttt{sip}.
- **Transport Method** – Set to \texttt{tls}.
- **Verify that IMS Enabled?** is set to \texttt{n}.
- **Verify that IP Video?** is set to \texttt{n}
- **Verify that Peer Detection Enabled?** is set to \texttt{y}. The systems will auto detect and set the Peer Server to SM.
- **Near-end Node Name** – Set to the node name of the \texttt{procr} noted in Section 5.4.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in Section 5.4 (e.g., \texttt{ve3-sm}).
- **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 5.6.
- **Far-end Domain** – Enter \texttt{sipinterop.net}. This is the domain provisioned for Session Manager in Section 6.1.
- **DTMF over IP** – Set to \texttt{rtp-payload} to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to \texttt{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** – Set to y.
• **Enable Layer 3 Test** – Set to y. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
• Default values may be used for all other fields.

```
display signaling-group 3
SIGNALING GROUP

Group Number: 3  Group Type: sip
IMS Enabled? n  Transport Method: tls
Q-SIP? n  
IP Video? n  Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y  Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr  Far-end Node Name: ve3-sm
Near-end Listen Port: 5061  Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain: sipinterop.net
Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload  Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3  IP Audio Hairpinning? n
Enable Layer 3 Test? y  Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n  Alternate Route Timer(sec): 30
```

### 5.8.2 Trunk Group

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, provision the following:

- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., *03).
- **Direction** – Set to two-way.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **5.8.1** (e.g., 3).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., 10).

```
display trunk-group 3
TRUNK GROUP

Group Number: 3  Group Type: sip  CDR Reports: y
Group Name: TO-SM  COR: 1  TN: 1  TAC: *03
Direction: two-way  Outgoing Display? y
Dial Access? n  
Queue Length: 0
Service Type: public-ntwrk  Auth Code? n
Member Assignment Method: auto
  Signaling Group: 3
  Number of Members: 10
```
On Page 2, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval (in milliseconds) should be equal to the time interval defined by the **Alternate Route Timer** on the signaling group form described in Section 5.8.1.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

<table>
<thead>
<tr>
<th>display trunk-group 3</th>
<th>Page 2 of 22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type: sip</td>
<td></td>
</tr>
<tr>
<td><strong>TRUNK PARAMETERS</strong></td>
<td></td>
</tr>
<tr>
<td>Unicode Name: auto</td>
<td>Redirect On OPTIM Failure: 30000</td>
</tr>
<tr>
<td>SCCAN? n</td>
<td>Digital Loss Group: 18</td>
</tr>
<tr>
<td>Preferred Minimum Session Refresh Interval (sec): 600</td>
<td></td>
</tr>
<tr>
<td>Disconnect Supervision - In? y Out? y</td>
<td></td>
</tr>
<tr>
<td>XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n</td>
<td></td>
</tr>
</tbody>
</table>

On Page 3, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in Section 5.2, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

<table>
<thead>
<tr>
<th>display trunk-group 3</th>
<th>Page 3 of 22</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUNK FEATURES</td>
<td></td>
</tr>
<tr>
<td>ACA Assignment? n</td>
<td>Measured: none</td>
</tr>
<tr>
<td>Numbering Format: private</td>
<td>Maintenance Tests? y</td>
</tr>
<tr>
<td>SCCAN? n</td>
<td></td>
</tr>
<tr>
<td>Digital Loss Group: 18</td>
<td></td>
</tr>
<tr>
<td>SCCAN? n</td>
<td>Digital Loss Group: 18</td>
</tr>
<tr>
<td>Preferred Minimum Session Refresh Interval (sec): 600</td>
<td></td>
</tr>
<tr>
<td>Disconnect Supervision - In? y Out? y</td>
<td></td>
</tr>
<tr>
<td>XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n</td>
<td></td>
</tr>
<tr>
<td>wrists</td>
<td></td>
</tr>
</tbody>
</table>
On Page 5, the **Network Call Redirection** field may be set to **n** or **y**, both approaches are supported in this solution. Setting the **Network Call Redirection** flag to **y** enables the use of the SIP REFERENCE message for call transfer; otherwise the SIP INVITE message will be used for call transfer.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These header modifications are needed to support the call display for call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

**Setting n for Network Call Redirection:**

<table>
<thead>
<tr>
<th>add trunk-group 3</th>
<th>Page 5 of 21</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PROTOCOL VARIATIONS</td>
</tr>
<tr>
<td></td>
<td>Mark Users as Phone? n</td>
</tr>
<tr>
<td></td>
<td>Prepend '+' to Calling/Alerting/Diverting/Connected Number? n</td>
</tr>
<tr>
<td></td>
<td><strong>Send Transferring Party Information? y</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Network Call Redirection? n</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Send Diversion Header? y</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Support Request History? n</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Telephone Event Payload Type: 101</strong></td>
</tr>
<tr>
<td></td>
<td>Convert 180 to 183 for Early Media? n</td>
</tr>
<tr>
<td></td>
<td>Always Use re-INVITE for Display Updates? n</td>
</tr>
<tr>
<td></td>
<td>Identity for Calling Party Display: P-Asserted-Identity</td>
</tr>
<tr>
<td></td>
<td>Block Sending Calling Party Location in INVITE? n</td>
</tr>
<tr>
<td></td>
<td>Accept Redirect to Blank User Destination? y</td>
</tr>
<tr>
<td></td>
<td>Enable Q-SIP? n</td>
</tr>
</tbody>
</table>

**Setting y for Network Call Redirection:**

<table>
<thead>
<tr>
<th>add trunk-group 3</th>
<th>Page 5 of 21</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PROTOCOL VARIATIONS</td>
</tr>
<tr>
<td></td>
<td>Mark Users as Phone? n</td>
</tr>
<tr>
<td></td>
<td>Prepend '+' to Calling/Alerting/Diverting/Connected Number? n</td>
</tr>
<tr>
<td></td>
<td><strong>Send Transferring Party Information? y</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Network Call Redirection? y</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Build Refer-To URI of REFER From Contact For NCR? y</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Send Diversion Header? y</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Support Request History? n</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Telephone Event Payload Type: 101</strong></td>
</tr>
<tr>
<td></td>
<td>Convert 180 to 183 for Early Media? n</td>
</tr>
<tr>
<td></td>
<td>Always Use re-INVITE for Display Updates? n</td>
</tr>
<tr>
<td></td>
<td>Identity for Calling Party Display: P-Asserted-Identity</td>
</tr>
<tr>
<td></td>
<td>Block Sending Calling Party Location in INVITE? n</td>
</tr>
<tr>
<td></td>
<td>Accept Redirect to Blank User Destination? y</td>
</tr>
<tr>
<td></td>
<td>Enable Q-SIP? n</td>
</tr>
</tbody>
</table>
5.9 Calling Party Information
The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Use the change public-unknown-numbering command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, the 028059847x DID numbers provided for testing were assigned to the extensions 847x. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

<table>
<thead>
<tr>
<th>Ext Ext Len Code</th>
<th>Trk Grp(s)</th>
<th>CPN Prefix</th>
<th>Total CPN Len</th>
<th>Total Administered: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 847</td>
<td>3</td>
<td>028059</td>
<td>10</td>
<td>Maximum Entries: 9999</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.

Communication Manager automatically inserts a '+' digit in this case.

Repeat the same in private-numbering table:

<table>
<thead>
<tr>
<th>Ext Ext Len Code</th>
<th>Trk Grp(s)</th>
<th>Private Prefix</th>
<th>Total Len</th>
<th>Total Administered: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 847</td>
<td>3</td>
<td>028059</td>
<td>10</td>
<td>Maximum Entries: 540</td>
</tr>
</tbody>
</table>

5.10 Incoming Call Handling Treatment
In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by AT&T can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the change inc-call-handling-trmt trunk-group command to create an entry for each DID.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Service/ Call Handling Treatment</th>
<th>Number Len</th>
<th>Number Digits</th>
<th>Del Insert</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ntwrk</td>
<td>INCOMING CALL HANDLING TREATMENT</td>
<td>10</td>
<td>028059</td>
<td>6</td>
</tr>
<tr>
<td>public-ntwrk</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.11 Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route an outbound call via the SIP trunk to the service provider. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (fac) 9, use the change dialplan analysis command as shown below.

```
change dialplan analysis
DIAL PLAN ANALYSIS TABLE

<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>6</td>
<td>1</td>
<td>fac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B47</td>
<td>4</td>
<td>ext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>fac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>3</td>
<td>dac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>4</td>
<td>fac</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Use the change feature-access-codes command to define 9 as the Auto Route Selection (ARS) – Access Code 1.

```
display feature-access-codes
FEATURE ACCESS CODE (FAC)

Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial – Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code:
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code:
Auto Route Selection (ARS) – Access Code 1: 9 Access Code 2: 6
Automatic Callback Activation: #002 Deactivation: #003
Call Forwarding Activation Busy/DA: #004 All: #005 Deactivation: #006
Call Forwarding Enhanced Status: #007 Act: #008 Deactivation: #009
Call Park Access Code: #010
Call Pickup Access Code: #011
CAS Remote Hold/Answer Hold-Unhold Access Code: #012
CDR Account Code Access Code: #013
Change COR Access Code:
Change Coverage Access Code:
Conditional Call Extend Activation: Deactivation:
Contact Closure Open Code: Close Code:
```
Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance testing. All dialed strings are mapped to route pattern 3 for an outbound call which contains the SIP trunk to the service provider (as defined next).

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node Num</th>
<th>Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>10</td>
<td>10</td>
<td>3</td>
<td>pubu</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>04</td>
<td>10</td>
<td>10</td>
<td>3</td>
<td>pubu</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>0011</td>
<td>12</td>
<td>20</td>
<td>3</td>
<td>pubu</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>emer</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern 3 in the following manner.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group 3 was used.
- **FRL**: Set the Facility Restriction Level (FRL) field to a level that allows access to this trunk for all users that require it. The value of 0 is the least restrictive level.
- **Numbering Format**: unk-unk. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.9**.
5.12 Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateways 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.

1. SSH 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)#).
2. Enter the show system command and note the G430 serial number (e.g., 10IS2xxxxxxx).
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., 192.168.1.12).
4. Enter the copy run copy start command to save the G430 configuration.
5. On Communication Manager, enter the add media-gateway x command where x is an available Media Gateway identifier (e.g., 1). The Media Gateway form will open (not shown).

Enter the following parameters:
- Set **Type** = G430.
- Set **Name** = Enter a descriptive name (e.g., g430).
- Set **Serial Number** = Enter the serial number copied from **Step 2** (e.g., 10IS2xxxxxxx).
- Set the **Encrypt Link** parameter as desired (n was used in the reference configuration).
- Set **Network Region** = 1.

When the Media Gateway registers, the SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., g430-001(super)#).

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

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

  MEDIA GATEWAY 1

    Type:  g430
    Name:  g430
  Serial No:  10IS2xxxxxxx
    Link Encryption Type:  any-pts/pts
    Network Region:  1
       Enable CF?: n
       Location:  1
       Site Data:  1
    Recovery Rule:  none

    Registered?: y
    FW Version/HW Vintage:  37.21.0 /1
    MGP IPV4 Address:  192.168.1.12
    MGP IPV6 Address:  
    Controller IP Address:  192.168.1.13
    MAC Address:  00:1b:4f:3f:14:48

  Mutual Authentication?: optional
```
5.13 Avaya Aura® Media Server Provisioning

Starting from release 7.0 of Avaya Aura®, Media Server can be used as VOIP resources for tones, announcements and music on hold in conjunction with Avaya Aura® Communication Manager.

5.13.1 Signaling Group for Media Server

This section describes the steps for administering the SIP connection to Media Server.

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 **Peer Detection Enabled?** is set to **n**. Set the **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 the Media Server as administered in Section 5.4 (e.g., ve4-ams).
- **Near-end Listen Port** – Set to 5061.
- **Far-end Listen Port** – Set to 5061.
- **Far-end Network Region** – Set to 1.

```
add signaling-group 1

SIGNALING GROUP

Group Number: 1 Group Type: sip
Transport Method: tls
Peer Detection Enabled? n Peer Server: AMS
Near-end Node Name: procr
Near-end Listen Port: 5061
Far-end Node Name: ve4-ams
Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain: 192.168.1.15
```
5.13.2 Adding Media Server

Enter the add media-server x command, where x is the number of an unused media server (e.g., 1), and provision the following:

- **Signaling Group** – Set to signaling group administered in Section 5.13.1 (e.g., 1).
- **Voip Channel License Limit** – Set to 10.
- **Dedicated Voip Channel Licenses** – Set to 10.
- **Network Region** – Set to the network region administered in Section 5.6 (e.g., 1).

```
add media-server 1
```

```
MEDIA SERVER

Media Server ID: 1
Signaling Group: 1
Voip Channel License Limit: 10
Dedicated Voip Channel Licenses: 10

Node Name: ve4-ams
Network Region: 1
Location: 1
Announcement Storage Area: ANNC-638363a6-f0d7-41e5-913d-000c29d72adf
```

5.14 Save Communication Manager Translations

After the Communication Manager provisioning is completed, enter the command save translation.
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location that can be used by SIP Entities.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

It may not be necessary to configure all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

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

Follow the steps shown below:

1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.net** was defined.
2. Click **New** (not shown). Enter the following values and use default values for remaining fields.
   - **Name**: Enter the enterprise SIP Domain Name. In the sample screen below, **sipinterop.net** is shown.
   - **Type**: Verify **sip** is selected.
   - **Notes**: Add a brief description.
3. Click **Commit** to save (not shown).

![Image of Domain Management](image)

6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **123ER** is configured.

Follow the steps shown below:

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., **123ER**).
   - **Notes**: Add a brief description.
2. Click **Commit** to save.

![Image of Location Management](image)

6.3 Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE.
6.3.1 Configure Session Manager SIP Entity

Follow the steps shown below:

1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name** – Enter a descriptive name (e.g., `ve3-sm`).
   - **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, *(not the management interface)*, provisioned during installation (e.g., `192.168.1.11`).
   - **Type** – Verify **Session Manager** is selected.
   - **Location** – Select location **123ER**.
   - **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.
3. In the **SIP 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.

![SIP Entity Details](image)

6.3.2 Configure Communication Manager SIP Entity

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name** – Enter a descriptive name (e.g. `ve3-cm`).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) (e.g. 192.168.1.12).
- **Type** – Select CM.
- **Location** – Select a Location 123ER administered in Section 6.2.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.

3. Click on **Commit**.

![SIP Entity Details](image)

- **Name**: ve3-cm
- **FQDN or IP Address**: 192.168.1.12
- **Type**: CM
- **Location**: 123ER
- **Time Zone**: Australia/Sydney
- **SIP Timer B/F (in seconds)**: 4
- **Call Detail Recording**: none
- **Loop Detection Mode**: On
- **Loop Count Threshold**: 5
- **Loop Detection Interval (in msec)**: 200
- **SIP Link Monitoring**: Use Session Manager Configuration
6.3.3 Configure Avaya SBCE SIP Entity

Repeat the steps in Section 6.3.2 with the following changes:

- **Name** – Enter a descriptive name (e.g., `sbce_A1`).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., `192.168.1.16`).
- **Type** – Verify **SIP Trunk** is selected.
- **Location** – Select location 123ER (Section 6.2).

![SIP Entity Details](image)

6.4 Configure Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and another one for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name**: Enter a descriptive name.
• **SIP Entity 1**: Select the Session Manager defined in Section 6.3.1.
• **Protocol**: Select the transport protocol used for this link, TLS for the Entity Link to Communication Manager and TLS for the Entity Link to the Avaya SBCE.
• **Port**: Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the Far-end Listen Port defined on the Communication Manager.
• **SIP Entity 2**: Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in Section 6.3.2. For Avaya SBCE, select Avaya SBCE SIP Entity defined in Section 6.3.3.
• **Port**: Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the Near-end Listen Port defined on the Communication Manager.
• **Connection Policy**: Select Trusted.
• Click Commit to save.

### 6.4.1 Configure Entity Link to Communication Manager

Follow the steps shown below:

1. In the left pane under Routing, click on Entity Links, then click on New (not shown).
2. Continuing in the Entity Links page, provision the following:
   - **Name** – Enter a descriptive name (or have it created automatically) for this link to Communication Manager (e.g., ve3-sm_ve3-cm_5061_TLS).
   - **SIP Entity 1** – Select the SIP Entity administered in Section 6.3.1 for Session Manager (e.g., ve3-sm).
   - **SIP Entity 1 Port** – Enter 5061.
   - **Protocol** – Select TLS.
   - **SIP Entity 2** – Select the SIP Entity administered in Section 6.3.2 for the Communication Manager internal entity (e.g., ve3-cm).
   - **SIP Entity 2 Port** – Enter 5061.
   - **Connection Policy** – Select Trusted.
3. Click on Commit.
6.4.2 Configure Entity Link for Avaya SBCE

To configure this Entity Link, repeat the steps in Section 6.4.1, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., `ve3-sm_sbce_A1_5061_TLS`).
- **SIP Entity 2** – Select the SIP Entity administered in Section 6.3.3 for the Avaya SBCE entity (e.g., `sbce_A1`).

![Configuration Interface](image)

6.5 Configure Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in Section 6.4. Two routing policies were added, one for Communication Manager and another for Avaya SBCE. To add a routing policy, navigate to Routing → Routing Policies in the left navigation pane and click the New button in the right pane (not shown). The following screen is displayed.

In the **General** section, enter the following values:

- **Name**: Enter a descriptive name.
- **Notes**: Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

6.5.1 Configure Routing Policy for Communication Manager

This Routing Policy is used for inbound calls from AT&T.

1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page, click on **New** (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., `ve3-cm`), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
4. In the **SIP Entity List** page, select the SIP Entity administered in Section 6.3.2 for the Communication Manager SIP Entity (ve3-cm), and click on **Select**.
5. Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.

6. No **Regular Expressions** were used in the reference configuration.

7. Click on **Commit**.

---

**6.5.2 Configure Routing Policy for Avaya SBCE**

This Routing Policy is used for outbound calls to the service provider. Repeat the steps in **Section 6.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sbce**).
- **SIP Entity List** – Select the SIP Entity administered in **Section 6.3.3** for the Avaya SBCE entity (e.g., **sbce_A1**).

---

**6.6 Configure Dial Patterns**

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to AT&T and vice versa. Dial Patterns define which routing policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click **New** button in the right pane (not shown).

In the **General** section, enter the following values:
• **Pattern:** Enter a dial string that will be matched against the “Request-URI” of the call.
• **Min:** Enter a minimum length used in the match criteria.
• **Max:** Enter a maximum length used in the match criteria.
• **SIP Domain:** Enter the destination domain used in the match criteria.
• **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Three examples of the dial patterns used for the compliance testing were shown below, one for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise and another one for Avaya SIP extension.

The first example shows that 10-digit dialed numbers that has a destination domain of “sipinterop.net” uses route policy to Avaya SBCE as defined in **Section 6.5.2**.

![Dial Pattern Details](image-url)
The second example shows that outbound 12-digit to 20-digit numbers that start with 0011 uses route policy to Avaya SBCE as defined in Section 6.5.2 for PSTN International calls.

The third example shows that 10-digit pattern that start with 028059 is used for inbound calls from AT&T to DID numbers on Avaya Aura® Communication Manager.
The fourth example shows that 000 dialed number is used for emergency service in Australia.

### Dial Pattern Details

**General**

- **Pattern**: 000
- **Min**: 3
- **Max**: 3
- **Emergency Call**: Y
- **Emergency Priority**: 1
- **Emergency Type**: all
- **SIP Domain**: sipinterop.net

**Notes:**

### Originating Locations and Routing Policies

<table>
<thead>
<tr>
<th>Originating Location Name</th>
<th>Originating Location Notes</th>
<th>Routing Policy</th>
<th>Rank</th>
<th>Routing Policy Disabled</th>
<th>Routing Policy Destination</th>
<th>Routing Policy Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>123ER</td>
<td></td>
<td>sbce</td>
<td>0</td>
<td></td>
<td></td>
<td>sbce_A1</td>
</tr>
</tbody>
</table>

Select: All, None
7. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

As described in Section 3, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (192.168.1.16), with access to the 123ER location. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 10.240.249.130). The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

1. Access the web interface by typing “https://x.x.x.x” (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the Username and click on Continue.
3. Enter the password and click on Log In.
The main menu window will open. 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.

![Dashboard](image.png)

![Installed Devices](image2.png)

**7.1 System Management – Status**

1. Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.

![System Management](image3.png)
2. Click on View (shown above) to display the System Information screen.

### 7.2 Global Profiles

#### 7.2.1 Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.
7.2.2 Server Interworking – Session Manager

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

1. Select **Global Profiles → Server Interworking** from the left-hand menu.
2. Click the **Add** button.
3. Enter profile name: (e.g., **Session Manager**), and click **Next**.
4. The **General** screen will open.
   - Check **T38 Support**.
   - All other options can be left with default values, and click **Next**.

```
<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold Support</td>
</tr>
<tr>
<td>RFC2543 - c=0.0.0.0</td>
</tr>
<tr>
<td>RFC3224 - a=sendonly</td>
</tr>
<tr>
<td>180 Handling</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>SDP</td>
</tr>
<tr>
<td>No SDP</td>
</tr>
<tr>
<td>181 Handling</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>SDP</td>
</tr>
<tr>
<td>No SDP</td>
</tr>
<tr>
<td>182 Handling</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>SDP</td>
</tr>
<tr>
<td>No SDP</td>
</tr>
<tr>
<td>183 Handling</td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td>SDP</td>
</tr>
<tr>
<td>No SDP</td>
</tr>
<tr>
<td>Refer Handling</td>
</tr>
<tr>
<td>URI Group</td>
</tr>
<tr>
<td>Send Hold</td>
</tr>
<tr>
<td>Delayed Offer</td>
</tr>
<tr>
<td>3ox Handling</td>
</tr>
<tr>
<td>Diversion Header Support</td>
</tr>
<tr>
<td>Delayed SDP Handling</td>
</tr>
<tr>
<td>Re-Invite Handling</td>
</tr>
<tr>
<td>Prack Handling</td>
</tr>
<tr>
<td>Allow 18X SDP</td>
</tr>
<tr>
<td>T.38 Support</td>
</tr>
<tr>
<td>URI Scheme</td>
</tr>
<tr>
<td>SIP</td>
</tr>
<tr>
<td>TEL</td>
</tr>
<tr>
<td>ANY</td>
</tr>
<tr>
<td>Via Header Format</td>
</tr>
<tr>
<td>RFC3224</td>
</tr>
<tr>
<td>RFC2543</td>
</tr>
</tbody>
</table>
```
5. On the **Timers** and **Privacy** windows, select **Next** to accept default values.
6. On the **Advanced** window, configure as below while other field left as default:
   - Record Routes: choose **None**.
   - Include End Point IP for Context Lookup: choose **Yes**.
   - Extension: choose **Avaya**.
   - Has Remote SBC: choose **Yes**.
7.2.3 Server Interworking – AT&T

Repeat the steps shown in Section 7.2.2 to add an Interworking Profile for the connection to AT&T via the VPN network, with the following changes:

1. Click Add to add a new profile, enter ATT then click Next (not shown)
2. The General screen will open:
   - Check T38 Support.
   - All other options can be left as default.
   - Click Next.
   - The Timers then Privacy screens will open (not shown), accept default values for all the screens by clicking Next.
Advanced window is configured as below, click Finish to save the profile:

- **Record Routes**: choose None
- **Extensions**: choose Nortel
- **Check Has Remote SBC**
7.2.4 Server Configuration – Session Manager

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

1. Select Global Profiles → Server Configuration from the left-hand menu.
2. Select Add Profile and the Profile Name window will open. Enter a Profile Name (e.g., Session Manager) and click Next.

   ![Add Server Configuration Profile](image)

3. The Add Server Configuration Profile window will open.
   - Select Server Type: Call Server.
   - IP Address / FQDN: 192.168.1.11 (Session Manager signaling IP Address).
   - Transport: Select TLS.
   - Port: 5061.
   - Select Next.

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

4. The Authentication window will open (not shown).
   - Select Next to accept default values.
5. The **Heartbeat** window will open.
   - Check to **Enable Heartbeat**
   - **Method**: select **OPTIONS**
   - **Frequency**: enter 30 (or more)
   - **From URI** and **To URI**: enter `ping@sipinterop.net`

![Heartbeat Window](image1)

6. The **Advanced** window will open.
   - Check to **Enable Grooming**
   - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.
   - **TLS Client Profile**: select proper provisioned profile (please refer to *Administering Avaya Session Border Controller for Enterprise* document for TLS management). In this example select **SMclient2**.
   - Select **Finish**.

![Advanced Window](image2)
7.2.5 Server Configuration – AT&T

Repeat the steps in Section 7.2.4, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

1. Select Add Profile and enter a Profile Name (e.g., ATT) and select Next.
2. On the General window (not shown), enter the following.
   - Select Server Type: Trunk Server.
   - IP Address / FQDN: 10.56.65.242 (AT&T’s SBC IP address)
   - Transport: Select TLS.
   - Port: 5061.
   - Select Next (not shown).

3. Just select Next under Authentication window (not shown).
4. Under **Heartbeat** window:
   - Select **Enable Heartbeat**.
   - **Method**: choose **OPTIONS**.
   - **Frequency**: enter 30 (or more).
   - **From URI** and **To URI**: enter ping@10.56.65.242.

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

5. Under **Advanced** window:
   - Select **ATT** for **Interworking Profile**.
   - Select **ATTClient** for **TLS Client Profile**.

   ![Edit Server Configuration Profile - Advanced](image)
7.2.6 Routing – To Session Manager

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

1. Select Global Profiles → Routing from the left-hand menu, and select Add (not shown).
2. Enter a Profile Name: (e.g., Session Manager) and click Next.
3. The Routing Profile window will open. Using the default values shown, click on Add.
4. The Next-Hop Address window will open. Populate the following fields:
   - Priority/Weight = 1.
   - Server Configuration = Session Manager.
   - Next Hop Address: Verify that the 192.168.1.11:5061 (TLS) entry from the drop down menu is selected (Session Manager IP address). Also note that the Transport field is grayed out.
   - Click on Finish.
7.2.7 Routing – To AT&T

Repeat the steps in Section 7.2.6, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

1. On the Global Profiles ➔ Routing window (not shown), enter a Profile Name: (e.g., ATT).
2. On the Next-Hop Address window (not shown), populate the following fields:
   - Server Configuration = ATT.
   - Next Hop Address: Verify that the 10.56.65.242:5061 entry from the drop down menu is selected.
   - Use default values for the rest of the parameters.
3. Click Finish.
7.2.8 Topology Hiding – Session Manager

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

1. Select **Global Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name**: (e.g., **Session Manager**), and click **Next**.
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until **Via** header is added.
4. Populate the fields as shown below, and click **Finish**. Note that **sipinterop.net** is the domain used.

![Topology Hiding Profiles: Session Manager](image)

7.2.9 Topology Hiding – AT&T

Repeat the steps in **Section 7.2.8**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

1. Enter a **Profile Name**: (e.g., **ATT**).
2. Click on the **Add Header** button repeatedly until **Refer-By** header is added.
3. Populate the fields as shown below, and click **Finish**.

![Topology Hiding Profiles: ATT](image)
7.2.10 Domain Policies
The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.2.11 Application Rules
Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 100 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.

7.2.12 Border Rules
The Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses.
7.2.13 Media Rules
This Media Rule will be applied to both directions and therefore, only one rule is needed.
In the solution as tested, the `default-low-med` rule was utilized. No customization was required.
7.2.14 Signaling Rules
The default Signaling Rule was utilized. No customization was required.

![Signaling Rules](image)

7.2.15 Endpoint Policy Groups
In the solution as tested, the default-low rule was utilized. This rule incorporated the media and Signaling Rules specified above, as well as other policies.

![Endpoint Policy Groups](image)

7.3 Device Specific Settings
The Device Specific Settings feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

7.3.1 Network Management
1. Select Device Specific Settings → Network Management from the menu on the left-hand side.
2. The Interfaces tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
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.

Note: B1 has two IP Addresses configured for each interface. One is used for SIP trunking, another one is used for Remote worker. Configuration for Remote worker is out of scope of this document.

7.3.2 Media Interfaces

1. Select Device Specific Settings from the menu on the left-hand side (not shown).
2. Select Media Interface.
3. Select Add (not shown). The Add Media Interface window will open. Enter the following:
   - Name: Media_A1.
   - IP Address: 192.168.1.16 (Avaya SBCE A1 address).
   - Port Range: 35000-40000.
4. Click Finish (not shown).
5. Select Add (not shown). The Add Media Interface window will open. Enter the following:
   - Name: Media_B1_trunking.
   - IP Address: 10.240.249.130 (Avaya SBCE B1 address).
   - Port Range: 35000-40000.
6. Click Finish (not shown). Note that changes to these values require an application restart. The completed Media Interface screen is shown below.
7.3.3 Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
   - **Name**: Sig_A1.
   - **IP Address**: 192.168.1.16 (Avaya SBCE A1 address).
   - **TLS Port**: 5061.
   - **TCP Port**: 5060.
   - **TLS Profile**: SMserver2.
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
   - **Name**: Sig_B1_trunking.
   - **IP Address**: 10.240.249.130 (Avaya SBCE B1 address).
   - **TLS Port**: 5061.
   - **TLS Profile**: ATTserver.
6. Click **Finish** (not shown). Note that changes to these values require an application restart.
7.3.4 Endpoint Flows – For Session Manager

1. Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
   - **Name**: Session Manager.
   - **Server Configuration**: Session Manager.
   - **URI Group**: *
   - **Transport**: TLS.
   - **Remote Subnet**: *
   - **Received Interface**: Sig_B1_trunking.
   - **Signaling Interface**: Sig_A1.
   - **Media Interface**: Med_A1.
   - **End Point Policy Group**: default-low.
   - **Routing Profile**: ATT.
   - **Topology Hiding Profile**: Session Manager.
   - Let other values default.
4. Click **Finish**.
7.3.5 Endpoint Flows – For AT&T

Repeat step 1 through 4 from Section 7.3.4, with the following changes:

- **Name**: ATT.
- **Server Configuration**: ATT.
- **Received Interface**: Sig_A1.
- **Signaling Interface**: Sig_B1_trunking.
- **Media Interface**: Med_B1_trunking.
- **Routing Profile**: Session Manager.
- **Topology Hiding Profile**: ATT.

![Edit Flow: ATT](image)

<table>
<thead>
<tr>
<th>Flow Name</th>
<th>ATT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Configuration</td>
<td>ATT</td>
</tr>
<tr>
<td>URI Group</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>Remote Subnet</td>
<td></td>
</tr>
<tr>
<td>Received Interface</td>
<td>Sig_A1</td>
</tr>
<tr>
<td>Signaling Interface</td>
<td>Sig_B1_trunking</td>
</tr>
<tr>
<td>Media Interface</td>
<td>Media_B1_trunking</td>
</tr>
<tr>
<td>End Point Policy Group</td>
<td>default-low</td>
</tr>
<tr>
<td>Routing Profile</td>
<td>Session Manager</td>
</tr>
<tr>
<td>Topology Hiding Profile</td>
<td>ATT</td>
</tr>
<tr>
<td>Signaling Manipulation Script</td>
<td>None</td>
</tr>
<tr>
<td>Remote Branch Office</td>
<td>Any</td>
</tr>
<tr>
<td>Finish</td>
<td></td>
</tr>
</tbody>
</table>
8. Verification Steps
The following steps may be used to verify the configuration.

8.1 Avaya Session Border Controller for Enterprise
Log into the Avaya SBCE as shown in Section 7. Across the top of the display are options to display Alarms, Incidents, Logs, and Diagnostics. In addition, the most recent Incidents are listed in the lower right of the screen.

Protocol Traces
The Avaya SBCE can take internal traces of specified interfaces.
1. Navigate to Device Specific Settings → Troubleshooting → Trace.
2. Select the Packet Capture tab and select the following:
   • Select the desired Interface from the drop down menu (e.g., All).
   • Specify the Maximum Number of Packets to Capture (e.g., 5000).
   • Specify a Capture Filename (e.g., TEST.pcap).
   • Unless specific values are required, the default values may be used for the Local Address, Remote Address, and Protocol fields.
   • Click Start Capture to begin the trace.

The capture process will initialize and then display the following In Progress status window:
3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a `.pcap` file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the VNGS SIP Trunk Service and the customer SIP PABX is the customer SBC. On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the AT&T network gateway.
- Ping from the SBC to the Session Manager.
- Ping from the AT&T network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.
8.2 Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager.

- Verify signaling status, trunk status.
### 8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

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

2. The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status. In the **Entity Monitoring Column**, Session Manager shows that there are 0 (zero) alarms out of the 3 Entities defined.

3. Clicking on the 0/3 entry in the **Entity Monitoring** column, results in the following display:
Options messages between Avaya SBCE and Session Manager:

![Options messages between Avaya SBCE and Session Manager](image)

### 8.4 Telephony Services
1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Confirm that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

### 9. Conclusion
As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Control for Enterprise 7.0 can be configured to interoperate successfully with AT&T SIP Trunking Service. This solution allows enterprise users access to the PSTN using the AT&T SIP Trunking Service connection. Please refer to Section 2.2 for exceptions.

### 10. Additional References
This section references the documentation relevant to these Application Notes. Avaya product documentation is available at [http://support.avaya.com](http://support.avaya.com).

[18] Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3. Issue 1.

Product documentation for AT&T SIP Trunking service is available from AT&T.