Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking on an enterprise solution consisting of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to interoperate with the Charter Spectrum Business SIP Trunk service.

The Charter Spectrum Business SIP Trunking service provide customers with PSTN access via a SIP trunk between the enterprise and the service provider’s 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 the 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.
# Table of Contents

1. Introduction ........................................................................................................... 4  
2. General Test Approach and Test Results ................................................................ 4  
   2.1. Interoperability Compliance Testing ................................................................. 5  
   2.2. Test Results ......................................................................................................... 6  
   2.3. Support .............................................................................................................. 6  
3. Reference Configuration ......................................................................................... 7  
4. Equipment and Software Validated .......................................................................... 10  
5. Configure Avaya Aura® Communication Manager ......................................................... 11  
   5.1. Licensing and Capacity .................................................................................... 12  
   5.2. System Features .............................................................................................. 13  
   5.3. IP Node Names ............................................................................................... 15  
   5.4. Codecs ............................................................................................................ 16  
   5.5. IP Network Regions ....................................................................................... 17  
   5.6. Signaling Group ............................................................................................. 18  
   5.7. Trunk Group .................................................................................................... 20  
   5.8. Calling Party Information ............................................................................. 24  
   5.9. Inbound Routing ............................................................................................ 25  
   5.10. Outbound Routing ....................................................................................... 26  
6. Configure Avaya Aura® Session Manager ................................................................. 30  
   6.1. System Manager Login and Navigation ............................................................ 31  
   6.2. SIP Domain .................................................................................................... 32  
   6.3. Locations ........................................................................................................ 32  
   6.4. Adaptations ..................................................................................................... 35  
   6.5. SIP Entities ..................................................................................................... 36  
   6.6. Entity Links .................................................................................................... 40  
   6.7. Routing Policies ............................................................................................. 42  
   6.8. Dial Patterns .................................................................................................. 43  
7. Configure Avaya Session Border Controller for Enterprise ....................................... 45  
   7.1. System Access ............................................................................................... 45  
   7.2. System Management ..................................................................................... 46  
   7.3. Network Management .................................................................................. 48  
   7.4. Media Interfaces ............................................................................................ 49  
   7.5. Signaling Interfaces ....................................................................................... 51  
   7.6. Server Interworking ....................................................................................... 53  
      7.6.1. Server Interworking Profile – Enterprise ..................................................... 53  
      7.6.2. Server Interworking Profile – Service Provider ........................................ 56  
   7.7. Signaling Manipulation .................................................................................. 58  
   7.8. Server Configuration ....................................................................................... 59  
      7.8.1. Server Configuration Profile – Enterprise .................................................. 59  
      7.8.2. Server Configuration Profile – Service Provider ........................................ 61  
   7.9. Routing ........................................................................................................... 63  
      7.9.1. Routing Profile – Enterprise ................................................................... 63  

©2016 Avaya Inc. All Rights Reserved.
1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Charter Spectrum Business SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 and various Avaya endpoints, listed in Section 4.

The Charter Spectrum Business SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

Note – As a required component of the Charter Spectrum Business SIP Trunking service offering, Charter will install a Customer Premises Equipment (CPE) device at the customer premises (enterprise site). Charter will perform the initial configuration and maintenance of this device as required. The Charter managed CPE device will constitute the service demarcation point between the service provider and the enterprise site.

Throughout these Application Notes, the terms “Service Provider”, “Charter Spectrum Business” and “Charter” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Charter Spectrum Business SIP Trunking service via the Charter’s managed CPE device, and a broadband connection to the public Internet.

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.
2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP trunk static IP authentication.
- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, Avaya one-X® Communicator and Avaya Communicator for Windows softphones.
- Various call types, including: local, long distance and local directory assistant (411).
- Codec G.711MU.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Proper response/error treatment to different failure conditions.

**Note** – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

The following items are not supported or were not tested:

- The use of the SIP REFER method for network call redirection is not currently supported by Charter.
- Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.
- T.38 fax is not currently supported by Charter.
2.2. Test Results

Interoperability testing of the Charter Spectrum Business SIP Trunking service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **No matching codec on outbound calls**: If an unsupported audio codec is received by Charter on the SIP Trunk (e.g., 722), Charter will respond with “480 Temporarily Unavailable” instead of “488 Not Acceptable Here”, the user will hear re-order. This issue does not have any user impact, and should not be seen since the codecs will be matched during the installation, it is listed here simply as an observation.

- **Inbound calls to an unassigned enterprise extension**: Communication Manager sends a “404 Not Found” message to Charter when it receives calls to an unassigned extension, the user hears re-order instead of the common announcement informing the user that he/she has reached a non-working number, to please check the number and to try again. This issue is considered non service affecting and it’s being investigated by Charter, in order to apply the correct announcement to the user.

- **Conference in Avaya Communicator softclients**: The Communication Manager conference feature is not supported in the Avaya Communicator current software release 2.1.3.80. An Avaya Aura® Conferencing server is required for ad-hoc conferences. This feature should be available in the upcoming release 3.0 of Avaya Communicator.

- **SIP header optimization**: There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purposes of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charging-Vector and P-Location (Section 6.4).

2.3. Support

For support on Charter Spectrum Business SIP Trunking service visit the corporate Web page at: https://business.spectrum.com/ or call 800-314-7195.
3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Charter Spectrum Business SIP Trunking service through a public Internet WAN connection.

For security purposes, references to any public IP addresses used during the compliance test have been replaced in these Application Notes with private addresses. Also, PSTN routable phone numbers used in the test have been changed to non-routable ones.

Figure 1: Avaya SIP Enterprise Solution connected to Charter Spectrum Business SIP Trunking Service
The Avaya components used to create the simulated enterprise customer site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya G450 Media Gateway.
- Avaya 96x0 Series IP Deskphones (H.323).
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Communicator for Windows softphones (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test, using the following endpoints and protocols:

- Avaya 96x1 SIP Deskphones (using TLS and SRTP).
- Avaya Communicator for Windows (using TLS and SRTP).
- Avaya one-X® Communicator SIP (using TLS and SRTP).

For security reasons, TLS and SRTP are the recommended protocols to be used by all remote workers endpoints.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [9] in the References section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the LAN side of the Charter managed CPE device, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

The transport protocol between the public interface of the Avaya SBCE and the Charter managed CPE device was UDP. The transport protocol between the private interface of the Avaya SBCE and the enterprise Session Manager across the enterprise IP network was TCP.
For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Charter’s network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

As part of the Avaya Aura® version 7.0 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Sever (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G450 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the References section.

Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Charter Spectrum Business SIP Trunking service, they are not included in these Application Notes.
## 4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>7.0.0.2.0 (00.0.441.0-22684)</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>7.0.0.1 (7.0.0.1.700102)</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>7.0.0.1</td>
</tr>
<tr>
<td></td>
<td>Build No. 7.0.0.0.16266-7.0.9.7001011</td>
</tr>
<tr>
<td></td>
<td>Software Update Rev. No. 7.0.0.1.4212</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise</td>
<td>7.0.0-21-6602</td>
</tr>
<tr>
<td></td>
<td>Patch: sbc700-p001-20151005-7.0.0-1.x86_64.rpm</td>
</tr>
<tr>
<td>Avaya Aura® Messaging</td>
<td>6.3.3 Service Pack 3 (MSG-03.0.141.0-348_0304)</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>7.7.0.236</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>37.20.0</td>
</tr>
<tr>
<td>Avaya 96x0 Series IP Deskphone (H.323)</td>
<td>Avaya one-X® Desk phone Edition Version S3.250A</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Deskphone (SIP)</td>
<td>Avaya one-X® Deskphone SIP Version 7.0.0.39</td>
</tr>
<tr>
<td>Avaya 96x1 Series IP Deskphone (H.323)</td>
<td>Avaya one-X® Deskphone H.323 Version 6.6029</td>
</tr>
<tr>
<td>Avaya one-X® Communicator (H.323, SIP)</td>
<td>6.2.10.03-FP10</td>
</tr>
<tr>
<td>Avaya Communicator for Windows (SIP)</td>
<td>2.1.3.80</td>
</tr>
<tr>
<td>Avaya 2420 Series Digital Deskphone</td>
<td>N/A</td>
</tr>
<tr>
<td>Avaya 6210 Analog Deskphone</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Charter Spectrum Business</strong></td>
<td></td>
</tr>
<tr>
<td>Broadworks Broadsoft Application Server</td>
<td>AS_Rel_17.sp4_1.197</td>
</tr>
<tr>
<td>Acme Packet 4500 Series SBC</td>
<td>SCX6.2.0 MR-9 GA (Build 1014)</td>
</tr>
<tr>
<td>Adtran NetVanta 3430 Modular Access Router</td>
<td>R10.3.0.V</td>
</tr>
</tbody>
</table>

**Note** – The Adtran NetVanta 3430 Modular Access Router shown on the table above was installed at the enterprise site, and it is referenced throughout this document as “Charter managed CPE device”.

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Servers and Media Gateway platforms running similar versions of Communication Manager and Session Manager.
**Note** – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 5.5) platforms. Consult the installation documentation on the References section for more information.

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

This section describes the procedure for configuring Communication Manager to work with the Charter Spectrum Business SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and the Avaya Aura® Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens captures will show the use of the `change` command instead of the `add` command, since the configuration used for the testing was previously added.
5.1. Licensing and Capacity

Use the `display system-parameters customer-options` command to verify that the **Maximum Administered SIP Trunks** value on Page 2 is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **122** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

<table>
<thead>
<tr>
<th>IP PORT CAPACITIES</th>
<th>USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Administered H.323 Trunks:</td>
<td>12000</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations:</td>
<td>18000</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks:</td>
<td>12000</td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations:</td>
<td>18000</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons:</td>
<td>414</td>
</tr>
<tr>
<td>Max Concur Registered Unauthenticated H.323 Stations:</td>
<td>100</td>
</tr>
<tr>
<td>Maximum Video Capable Stations:</td>
<td>41000</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones:</td>
<td>18000</td>
</tr>
<tr>
<td><strong>Maximum Administered SIP Trunks:</strong></td>
<td><strong>24000</strong></td>
</tr>
<tr>
<td>Maximum Administered Ad-hoc Video Conferencing Ports:</td>
<td><strong>24000</strong></td>
</tr>
<tr>
<td>Maximum Number of DS1 Boards with Echo Cancellation:</td>
<td><strong>522</strong></td>
</tr>
</tbody>
</table>

*(NOTE: You must logoff & login to effect the permission changes.)*
5.2. System Features

Use the `change system-parameters features` command to set the **Trunk-to-Trunk Transfer** field to *all* to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to *none*.

<table>
<thead>
<tr>
<th>Feature-related System Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Station Display Enabled?</td>
<td>n</td>
</tr>
<tr>
<td><strong>Trunk-to-Trunk Transfer:</strong> all</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback with Called Party Queuing?</td>
<td>n</td>
</tr>
<tr>
<td>Automatic Callback - No Answer Timeout Interval (rings):</td>
<td>2</td>
</tr>
<tr>
<td>Call Park Timeout Interval (minutes):</td>
<td>10</td>
</tr>
<tr>
<td>Off-Premises Tone Detect Timeout Interval (seconds):</td>
<td>20</td>
</tr>
<tr>
<td>AAR/ARS Dial Tone Required?</td>
<td>y</td>
</tr>
<tr>
<td>Music (or Silence) on Transferred Trunk Calls?</td>
<td>all</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:</td>
<td>transferred</td>
</tr>
<tr>
<td>Automatic Circuit Assurance (ACA) Enabled?</td>
<td>n</td>
</tr>
<tr>
<td>Abbreviated Dial Programming by Assigned Lists?</td>
<td>n</td>
</tr>
<tr>
<td>Auto Abbreviated/Delayed Transition Interval (rings):</td>
<td>2</td>
</tr>
<tr>
<td>Protocol for Caller ID Analog Terminals: Bellscore</td>
<td></td>
</tr>
<tr>
<td>Display Calling Number for Room to Room Caller ID Calls?</td>
<td>n</td>
</tr>
</tbody>
</table>
On Page 9 verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of restricted for restricted calls and unavailable for unavailable calls.
5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (proc) and the Session Manager security module (Lab-HG-SM). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASBCE 41</td>
<td>172.16.5.71</td>
</tr>
<tr>
<td>Lab-HG-SH</td>
<td>172.16.5.82</td>
</tr>
<tr>
<td>HA-CM</td>
<td>192.168.10.12</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>media_server</td>
<td>192.168.10.46</td>
</tr>
<tr>
<td>msgserver</td>
<td>172.16.5.12</td>
</tr>
<tr>
<td>proc</td>
<td>172.16.5.261</td>
</tr>
<tr>
<td>proc6</td>
<td>::</td>
</tr>
</tbody>
</table>

(8 of 8 administered node-names were displayed)

Use `list node-names` command to see all the administered node-names

Use `change node-names ip xxx` to change a node-name `xxx` or add a node-name
5.4. Codecs

Use the `change ip-codec-set` command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, `ip-codec-set 2` was used for this purpose. Charter only used codec G.711MU on the SIP trunk. Enter the corresponding codec in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

On Page 2, set the **Fax Mode** to **off**. Charter does not support T.38 fax.
5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunk. Use the `change ip-network-region 2` command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is `avaya.lab.com` as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in Section 5.4.
- Default values may be used for all other fields.

```
change ip-network-region 2
Region: 2
Location: 1
Name: IP Region
Authoritative Domain: avaya.lab.com
Stub Network Region: n
IP Network Region

MEDIA PARAMETERS
Codec Set: 2
UDP Port Min: 2048
UDP Port Max: 3349

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 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

©2016 Avaya Inc. All Rights Reserved.

CharterCMSMSBC7
On Page 4, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the codec set column of the row with destination region (dst rgn) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

<table>
<thead>
<tr>
<th>Source Region: 2</th>
<th>Inter Network Region Connection Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst codec direct</td>
<td>WAN-BW-limits Video Intervening Dyn A G c</td>
</tr>
<tr>
<td>rgn set WAN Units Total Norm Prio Shr Regions CAC R L e</td>
<td></td>
</tr>
<tr>
<td>1 2 y NoLimit</td>
<td>all</td>
</tr>
</tbody>
</table>

5.6. Signaling Group

Use the `add signaling-group` command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, *tcp* was used.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to *SM* once Communication Manager detects its peer is a Session Manager.

**Note:** Once the **Peer-Server** field is updated to *SM*, the system changes the default values of the following fields, setting them to display–only:

- **Prepend ‘+’ to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to *y*.
- Remove ‘+’ from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? is changed to n.
- Set the Near-end Node Name to procr. This node name maps to the IP address of the Communication Manager as defined in Section 5.3.
- Set the Far-end Node Name to Lab-HG-SM. This node name maps to the IP address of Session Manager, as defined in Section 5.3.

<table>
<thead>
<tr>
<th>SIGNALING GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Number:</strong> 2</td>
</tr>
<tr>
<td><strong>Group Type:</strong> sip</td>
</tr>
<tr>
<td><strong>IMS Enabled?</strong> y</td>
</tr>
<tr>
<td><strong>Q-SIP?</strong> n</td>
</tr>
<tr>
<td><strong>Transport Method:</strong> tcp</td>
</tr>
<tr>
<td><strong>Enforce SIPS URI For SRTP?</strong> y</td>
</tr>
<tr>
<td><strong>IP Video?</strong> y</td>
</tr>
<tr>
<td><strong>Peer Detection Enabled?</strong> y</td>
</tr>
<tr>
<td><strong>Peer Server:</strong> SM</td>
</tr>
<tr>
<td><strong>Prepend ‘+’ to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?</strong> y</td>
</tr>
<tr>
<td><strong>Remove ‘+’ from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?</strong> n</td>
</tr>
<tr>
<td><strong>Alert Incoming SIP Crisis Calls?</strong> n</td>
</tr>
<tr>
<td><strong>Near-end Node Name:</strong> procr</td>
</tr>
<tr>
<td><strong>Near-end Listen Port:</strong> 5078</td>
</tr>
<tr>
<td><strong>Far-end Node Name:</strong> Lab-HG-SM</td>
</tr>
<tr>
<td><strong>Far-end Listen Port:</strong> 5070</td>
</tr>
<tr>
<td><strong>Far-end Network Region:</strong> 2</td>
</tr>
<tr>
<td><strong>Far-end Domain:</strong> avaya.lab.com</td>
</tr>
<tr>
<td><strong>Incoming Dialog Loopbacks:</strong> eliminate</td>
</tr>
<tr>
<td><strong>Bypass If IP Threshold Exceeded?</strong> n</td>
</tr>
<tr>
<td><strong>RFC 3089 Comfort Noise?</strong> n</td>
</tr>
<tr>
<td><strong>DTMF over IP:</strong> rtp-payload</td>
</tr>
<tr>
<td><strong>Direct IP-IP Audio Connections?</strong> y</td>
</tr>
<tr>
<td><strong>Session Establishment Timer(min):</strong> 3</td>
</tr>
<tr>
<td><strong>IP Audio Hairpinning?</strong> n</td>
</tr>
<tr>
<td><strong>Enable Layer 3 Test?</strong> n</td>
</tr>
<tr>
<td><strong>Initial IP-IP Direct Media?</strong> n</td>
</tr>
<tr>
<td><strong>H.323 Station Outgoing Direct Media?</strong> n</td>
</tr>
<tr>
<td><strong>Alternate Route Timer(sec):</strong> 6</td>
</tr>
</tbody>
</table>

- Set the Near-end Listen Port and Far-end Listen Port to a valid unused port instead of the default well-known port value. (For TCP, the well-known port value is 5060). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the Near-end Listen Port and Far-end Listen Port were set to 5070.
- Set the Far-end Network Region to the IP network region defined for the service provider in Section 5.5.
- Set the Far-end Domain to the domain of the enterprise.
- Set the DTMF over IP field to rtp-payload. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set Direct IP-IP Audio Connections to y. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to n, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.
5.7. Trunk Group

Use the `add trunk-group` command to create a trunk group for the signaling group created in Section 5.6. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to `sip`.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to `public-ntwrk`.
- Set the **Signaling Group** to the signaling group shown in the previous section.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.
On **Page 2**, 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. The default value of **600** seconds was used.
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. When *public* format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. To keep uniformity with the format used by Charter, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (see **Section 5.10**). 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 has enabled CPN block.
On Page 4, set the **Network Call Redirection** field to *n*. With this setting, Communication Manager will not use the REFER method, which is not supported by Charter, for the redirection of PSTN calls that are transferred back to the SIP trunk. Set the **Send Diversion Header** field to *y* and **Support Request History** to *n*. Set the **Telephone Event Payload Type** to **101**, the value preferred by Charter. Set **Identity for Calling Party Display** to **P-Asserted-Identity**. Default values were used for all other fields.
5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (Section 5.7), use the `change private-numbering` command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs). In the example below, three DID numbers were assigned by the service provider for testing. These DID numbers were used as the outbound calling party information on the service provider trunk when calls were originated from the mapped extensions.

<table>
<thead>
<tr>
<th>Ext Len</th>
<th>Ext Code</th>
<th>Trk Grp(s)</th>
<th>Private Prefix</th>
<th>Total Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
<td>3031231273</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>3044</td>
<td>2</td>
<td>3031231275</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>3047</td>
<td>2</td>
<td>3031231274</td>
<td>10</td>
</tr>
</tbody>
</table>

Total Administered: 5
Maximum Entries: 540
5.9. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Charter is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the `change inc-call-handling-trmt` command to create an entry for each DID.

<table>
<thead>
<tr>
<th>Service/Feature</th>
<th>Number</th>
<th>Len</th>
<th>Digits</th>
<th>Del Insert</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-network</td>
<td>10 303123473</td>
<td>10</td>
<td>3042</td>
<td></td>
</tr>
<tr>
<td>public-network</td>
<td>10 303123474</td>
<td>10</td>
<td>3047</td>
<td></td>
</tr>
<tr>
<td>public-network</td>
<td>10 303123475</td>
<td>10</td>
<td>3044</td>
<td></td>
</tr>
</tbody>
</table>
5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the `change dialplan analysis` command to define a dialed string beginning with 9 of length 1, as a feature access code (`fac`).

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Length</th>
<th>Call Type</th>
<th>Dialed String</th>
<th>Total Length</th>
<th>Call Type</th>
<th>Dialed String</th>
<th>Total Length</th>
<th>Call Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>13</td>
<td>udp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>dac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>ext</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>ext</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>udp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>ext</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>dac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>ext</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>fac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>fac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>3</td>
<td>dac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>2</td>
<td>dac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Length</th>
<th>Call Type</th>
<th>Dialed String</th>
<th>Total Length</th>
<th>Call Type</th>
<th>Dialed String</th>
<th>Total Length</th>
<th>Call Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use the `change feature-access-codes` command to configure 9 as the **Auto Route Selection (ARS) – Access Code 1**.

<table>
<thead>
<tr>
<th>change feature-access-codes</th>
<th>FEATURE ACCESS CODE (FAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviated Dialing List1 Access Code:</td>
<td>1</td>
</tr>
<tr>
<td>Abbreviated Dialing List2 Access Code:</td>
<td>2</td>
</tr>
<tr>
<td>Abbreviated Dialing List3 Access Code:</td>
<td>3</td>
</tr>
<tr>
<td>Abbreviated Dial – Prgn Group List Access Code:</td>
<td></td>
</tr>
<tr>
<td>Announcement Access Code:</td>
<td>#7</td>
</tr>
<tr>
<td>Answer Back Access Code:</td>
<td></td>
</tr>
<tr>
<td>Attendant Access Code:</td>
<td></td>
</tr>
<tr>
<td>Auto Alternate Routing (AAR) Access Code:</td>
<td>8</td>
</tr>
<tr>
<td><strong>Auto Route Selection (ARS) – Access Code 1: 9</strong></td>
<td></td>
</tr>
<tr>
<td>Automatic Callback Activation:</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding Activation Busy/DA:</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding Enhanced Status:</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding All:</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding Act:</td>
<td></td>
</tr>
<tr>
<td>Call Park Access Code:</td>
<td></td>
</tr>
<tr>
<td>Call Pickup Access Code:</td>
<td>*44</td>
</tr>
<tr>
<td>CAS Remote Hold/Answer Hold-Unhold Access Code:</td>
<td></td>
</tr>
<tr>
<td>CDR Account Code Access Code:</td>
<td></td>
</tr>
<tr>
<td>Change COR Access Code:</td>
<td></td>
</tr>
<tr>
<td>Change Coverage Access Code:</td>
<td></td>
</tr>
<tr>
<td>Conditional Call Extend Activation:</td>
<td></td>
</tr>
<tr>
<td>Contact Closure Open Code:</td>
<td></td>
</tr>
<tr>
<td>Close Code:</td>
<td></td>
</tr>
</tbody>
</table>
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 test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

<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 Num</th>
<th>ANI Reqd</th>
</tr>
</thead>
<tbody>
<tr>
<td>170</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1700</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>171</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>172</td>
<td>11</td>
<td>11</td>
<td>2 fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>173</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>174</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>175</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>176</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>177</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>178</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1786</td>
<td>11</td>
<td>11</td>
<td>2 fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>179</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>180</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1800</td>
<td>11</td>
<td>11</td>
<td>2 fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1800555</td>
<td>11</td>
<td>11</td>
<td>deny fnpa</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the `change route-pattern` command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 in the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider.
- **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.
- **Pfx Mrk**: Set to 1 to ensure 1 + 10 digits are sent to the service provider for long distance numbers in the North American Numbering Plan (NANP).
- **Numbering Format**: Set to `unk-unk`. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form in Section 5.7.

<table>
<thead>
<tr>
<th>Pattern Number: 2</th>
<th>Pattern Name: Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp No</td>
<td>Secure SIP?</td>
</tr>
<tr>
<td>1:</td>
<td>n</td>
</tr>
<tr>
<td>2:</td>
<td>n</td>
</tr>
<tr>
<td>3:</td>
<td>n</td>
</tr>
<tr>
<td>4:</td>
<td>n</td>
</tr>
<tr>
<td>5:</td>
<td>n</td>
</tr>
<tr>
<td>6:</td>
<td>n</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE</th>
<th>TSC</th>
<th>CA-TSC</th>
<th>ITC</th>
<th>BCIE</th>
<th>Service/Feature</th>
<th>PARM</th>
<th>Sub Dgts</th>
<th>Numbering Format</th>
<th>LAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 M 4 W</td>
<td>Request</td>
<td>ITC</td>
<td>BCIE</td>
<td>Service/Feature</td>
<td>PARM</td>
<td>Sub Dgts</td>
<td>Numbering Format</td>
<td>LAR</td>
<td></td>
</tr>
<tr>
<td>1: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>unk-unk</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>2: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>3: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>4: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>5: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>6: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**Note** - Enter the `save translation` command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.
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 Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- 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.

The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.
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). The screen shown below is then displayed; click on Routing under Elements.

![System Manager Login](image)

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 link shown below.

![Routing Tree](image)

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like “Domains”, “Locations”, “SIP Entities”, etc. The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

1. Step 1: Create “Domains” of type SIP (other routing applications are referring domains of type SIP).
2. Step 2: Create “Locations”
3. Step 3: Create “Adaptations”
4. Step 4: Create “SIP Entities”

   - SIP Entities that are used as "Outbound Prefixes" e.g. a certain "Gateway" or "SIP Trunk"
6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, *avaya.lab.com*. Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select *sip* from the pull-down menu.
- **Notes:** Add a brief description (optional).
- **Click Commit** to save.

The screen below shows the entry for the enterprise domain.

![Enterprise Domain Entry](image)

6.3. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).
- **Click Commit** to save.
The following screen shows the location details for the location named **HG Session Manager**. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Default values were used for all parameters.
The following screen shows the location details for the location named **HG Communication Manager**. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The following screen shows the location details for the location named **HG ASBCE**. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.
6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.0 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named *CM_Outbound_Header_Removal* was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

Navigate to **Routing ➔ Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name**: Enter an appropriate name.
- **Module Name**: Select the *DigitConversionAdapter* option.
- **Module Parameter Type**: Select *Name-Value Parameter*.

Click **Add** to add the name and value parameters.

- **Name**: Enter *eRHdrs*. This parameter will remove the specified headers from messages in the egress direction.
- **Value**: Enter “Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View”
- **Click Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left at their default values.
6.5. 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 the Avaya SBCE. Navigate to Routing → SIP Entities in the left navigation pane and click on the New button in the right pane (not shown). In the General section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *SIP Trunk* (or *Other*) for the Avaya SBCE.
- **Adaptation:** This field is only present if Type is not set to *Session Manager*.
  If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in Section 6.3.
- **Time Zone:** Select the time zone for the location above.
- **Click Commit** to save.
The following screen shows the addition of the **HG Session Manager** SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.
The following screen shows the addition of the **HG CM Trunk 2** SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “procr” interface in Communication Manager, as seen in **Section 5.3**.
The following screen shows the addition of the **HG ASBCE** SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). On the **Adaptation** field, the adaptation module **CM_Outbound_Header_Removal** previously defined in **Section 6.4** was selected.
6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to Routing → Entity Links in the left navigation pane and click on 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 from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- **Click Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in Section 5.6.
The Entity Link to the Avaya SBCE is shown below. TCP and port 5060 were used.
6.7. Routing Policies
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in Section 6.5. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to Routing → Routing Policies in the left navigation pane and click on the New button in the right pane (not shown). The following screen is displayed. In the General section, enter a descriptive Name and add a brief description under Notes (optional).

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

The following screens show the Routing Policies for Communication Manager and the Avaya SBCE.
6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route 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 on the New button in the right pane (not shown). Fill in the following, as shown in the screens below:

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, or select "ALL" to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).
- **Click Commit to save.**

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 (not shown).

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with 303, the area code assigned to the DID numbers provided by Charter, arriving from location HG ASBCE, used route policy To HG CM trunk 2 to Communication Manager.
Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows the 11 digit dialed numbers for outbound calls, beginning with 1, arriving from the HG Communication Manager location, will use route policy To HG ASBCE, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP Trunk. The SIP Domain was set to –ALL– since dial pattern 1 is shared among multiple SIP Domains in the Avaya lab, SIP Domain Avaya.lab.com could have been used instead.

Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider’s network via the Avaya SBCE.
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, 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 initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the Additional References section.

7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL https://<ip-address>, where <ip-address> is the management IP address configured at installation. Log in using the appropriate credentials.

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the License State field is OK, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.
7.2. System Management

To view current system information, select System Management on the left navigation pane. A list of installed devices is shown in the Devices tab on the right pane. In the reference configuration, a single device named Avaya SBCE is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the Status is Commissioned, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.
To view the network configuration assigned to the Avaya SBCE, click **View** on the screen in the previous page. The **System Information** window is displayed, containing the current device configuration and network settings.

```
<table>
<thead>
<tr>
<th>Appliance Name</th>
<th>Avaya SBCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box Type</td>
<td>SIP</td>
</tr>
<tr>
<td>Deployment Mode</td>
<td>Proxy</td>
</tr>
</tbody>
</table>

**System Information: Avaya SBCE**

**Device Configuration**

- HA Mode: No
- Two Bypass Mode: No

**License Allocation**

- Standard Sessions: 2000
  - Requested: 2000
- Advanced Sessions: 2000
  - Requested: 2000
- Scopia Video Sessions: 500
  - Requested: 500
- CES Sessions: 0
  - Requested: 0
- Encryption: On

**Network Configuration**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Public IP</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.5.71</td>
<td>172.16.5.71</td>
<td>255.255.255.0</td>
<td>172.16.5.254</td>
<td>A1</td>
</tr>
<tr>
<td>172.16.5.94</td>
<td>172.16.5.94</td>
<td>255.255.255.0</td>
<td>172.16.5.254</td>
<td>A1</td>
</tr>
</tbody>
</table>

**DNS Configuration**

- Primary DNS: [IP Address]
- Secondary DNS: [IP Address]
- DNS Location: DMZ
- DNS Client IP: [IP Address]

**Management IP(s)**

- IP: [IP Address]
```
The highlighted IP addresses in the **System Information** screen are the ones used for the SIP trunk to Charter, and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (172.16.5.71) was used to connect to the enterprise network, while its public interface (174.16.5.94) was used to connect to the LAN interface of the Charter managed CPE device (172.16.5.185). The WAN interface of the Charter managed CPE device was used to connect to the public network. See Figure 1. Note that Charter is responsible for the configuration of the Charter managed CPE device; hence the configuration tasks for this device are not covered in these Application Notes.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

### 7.3. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, **Avaya_SBCE** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (172.16.5.71) and public (172.16.5.94) sides of the Avaya SBCE were both assigned to interface **A1**.
On the Interfaces tab, verify the Administrative Status is Enabled for the A1 interface. Click the buttons under the Status column if necessary to enable the interface.

7.4. Media Interfaces

Media Interfaces were 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 it will accept media from the Call Server or the Trunk Server.

To add the Media Interface in the enterprise direction, select Media Interface from the Device Specific Settings menu on the left-hand side, select the device being managed and click the Add button (not shown). On the Add Media Interface screen, enter an appropriate Name for the Media Interface. Under IP Address, select from the drop-down menus the network and IP address to be associated with this interface. The Port Range was left at the default values of 35000-40000. Click Finish.
A Media Interface facing the public side was similarly created with the name `Public_med`, as shown below. Under **IP Address**, the network and IP address to be associated with this interface was selected. The **Port Range** was left at the default values. Click **Finish**.

![Add Media Interface](image)

**Name**: Public_med

**IP Address**: Network_A1 (A1, VLAN 0) 172.16.5.94

**Port Range**: 35000 - 40000

**Finish**
7.5. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select Signaling Interface from the Device Specific Settings menu on the left-hand side, select the device being managed and click the Add button (not shown). On the Add Signaling Interface screen, enter an appropriate Name for the interface. Under IP Address, select from the drop-down menus the network and IP address to be associated with this interface. Enter 5060 for TCP Port, since TCP port 5060 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in Section 6.6. Click Finish.
A second Signaling Interface with the name `Public_sig` was similarly created in the service provider’s direction. Under IP Address, select from the drop-down menus the network and IP address to be associated with this interface. Enter 5060 for UDP Port, since this is the protocol and port used by the Avaya SBCE to listen to the service provider’s SIP traffic. Click Finish.
7.6. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.6.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select Global Profiles → Server Interworking on the left navigation pane. Under Interworking Profiles, select avaya-ru from the list of pre-defined profiles. Click Clone.

Enter a descriptive name for the cloned profile. Click Finish.
On the newly cloned *Avaya-SM* interworking profile, on the **General** tab all parameters retain their default values, as shown on the screen below.

![Session Border Controller for Enterprise](image)
The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries. The **Advanced** tab settings are shown on the screen below:
7.6.2. **Server Interworking Profile – Service Provider**

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles ➔ Server Interworking** on the left navigation pane and click **Add** (not shown). Enter a descriptive name for the new profile. Click **Next**.

On the **General** screen, all parameters retain their default values. Click **Next**.
Click **Next** on the **SIP Timers** and **Privacy** tabs (not shown). On the **Advanced/DTMF** tab, select **Both Sides** under **Record Routes**. Accept the defaults settings for all other fields. Click **Finish**.
7.7. Signaling Manipulation

Music on hold: When calls from/to the PSTN were placed on hold by Communication Manager users, the PSTN users did not hear Music while on hold. A SigMa script was created to remove the “sendonly” message Communication Manager includes in the SDP of re-INVITEs when calls from/to the PSTN are placed on hold, this allowed the PSTN users to hear Music while on hold. The script was latter applied to the Service Provider side of the server configuration profile (refer to Section 7.8.2). The script was included under the Remove_Sendonly script shown below.

To add a Signaling Manipulation script, from the Global Profiles menu on the left panel, select Signaling Manipulation. Click Add to open the SigMa Editor screen, where the text of the script can be entered or copied.

The details of the script used can be found in Appendix A in this document.
7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and the Charter managed CPE device (Trunk Server).

7.8.1. Server Configuration Profile – Enterprise

From the Global Profiles menu on the left-hand navigation pane, select Server Configuration and click the Add button (not shown) to add a new profile for the Call Server. Enter an appropriate Profile Name similar to the screen below. Click Next.

On the Add Server Configuration Profile Tab select Call Server from the drop down menu under the Server Type. On the IP Addresses / FQDN field, enter the IP address of the Session Manager Security Module (Section 6.5). Enter 5060 under Port and select TCP for Transport. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously in Section 6.6. Click Next.
Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select **Avaya-SM** from the **Interworking Profile** drop down menu. Click **Finish**.
7.8.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the Add button on the Server Configuration screen (not shown). Enter an appropriate Profile Name similar to the screen below. Click Next.

![Add Server Configuration Profile](image)

On the Add Server Configuration Profile Tab select Trunk Server from the drop down menu for the Server Type. On the IP Addresses / FQDN field, enter the IP address of the LAN interface of the Charter managed CPE device. Enter 5060 under Port, and select UDP for Transport. Click Next.

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

Click Next on the Authentication and Heartbeat tab (not shown).
On the **Advanced** tab, select **SP-General** from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the **Remove_Sendonly** script created in **Section 7.7**. Click **Finish**.
7.9. Routing
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

7.9.1. Routing Profile – Enterprise
To create the inbound route, select the Routing tab from the Global Profiles menu on the left-hand side and select Add (not shown). Enter an appropriate Profile Name similar to the example below. Click Next.

On the Routing Profile tab, click the Add button to enter the next-hop address. Enter 1 under Priority/Weight. Under Server Configuration, select Session Manager. The Next Hop Address field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in Section 7.8.1. Defaults were used for all other parameters. Click Finish.
7.9.2. Routing Profile – Service Provider

Back at the Routing tab, select Add (not shown) to repeat the process in order to create the outbound route. Enter an appropriate Profile Name similar to the example below. Click Next.

On the Routing Profile tab, click the Add button to enter the next-hop address. Enter 1 under Priority/Weight. Under Server Configuration, select Service Provider. The Next Hop Address field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in Section 7.8.2. Defaults were used for all other parameters. Click Finish.
7.10. Topology Hiding
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.10.1. Topology Hiding Profile – Enterprise
To add the Topology Hiding Profile in the enterprise direction, select Topology Hiding from the Global Profiles menu on the left-hand side, select default from the list of pre-defined profiles and click the Clone button (not shown). Enter a Clone Name such as the one shown below. Click Finish.

![Clone Profile](image)

On the newly cloned Session_Manager profile screen, click the Edit button (not shown).
For the, **From, To and Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **avaya.lab.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**. Default values were used for all other fields. Click **Finish**.

7.10.2. Topology Hiding Profile – Service Provider

A Topology Hiding profile named **Service_Provider** was similarly created in the direction of the SIP trunk to the service provider. During the compliance test, IP addresses and not domains names were used in all SIP messages between the service provider and the Avaya SBCE. Note that since the default action of **Auto** implies the insertion of IP addresses in the host portion of these headers, it was not necessary to modify any of the headers sent to the service provider. The screen below shows the **Service_Provider** profile once the configuration was completed.
7.11. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. In the reference configuration, the End Point Policy Groups used default sets of rules already pre-defined in the configuration. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule. Also note that even though the End Point Policy Groups for both the Enterprise and the Service Provider used the same set of rules, they were still separately defined, to allow for future changes to be made in one direction if needed, without affecting the other direction.

7.11.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select End Point Policy Groups under the Domain Policies menu and select Add (not shown).

Enter an appropriate name in the Group Name field. Click Next.

In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration. Click Finish.
7.11.2. End Point Policy Group – Service Provider

A second End Point Policy Group was created for the service provider, repeating the steps previously described. In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration.

The screen below shows the End Point Policy Group named *Service Provider* after the configuration was completed.
7.12. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

7.12.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the Device Specific menu, select End Point Flows, then select the Server Flows tab. Click Add (not shown). The screen below shows the flow named Session_Manager_Flow created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the Routing Profile selection is the profile created for the Service Provider in Section 7.9.2, which is the reverse route of the flow. Click Finish.
7.12.2. End Point Flow – Service Provider

A second Server Flow with the name *SIP_Trunk_Flow* was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in Section 7.9.1, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Since the script created in Section 7.7 was previously applied to the service provider’s Server Configuration Profile in Section 7.8.2, it is not necessary to make a selection here. Click **Finish**.

![Edit Flow: SIP_Trunk_Flow](image)

Click **Finish**.

The service provider is responsible for the configuration of the SIP Trunking service, including the provisioning of the Charter managed CPE device in the customer’s network. Charter will require from the customer the information needed to configure the service, which includes:

- IP addresses, subnet mask and default gateway to be assigned to the Charter managed CPE device interfaces (LAN and WAN), in order to be inserted at the edge of the enterprise site.
- IP address, protocol and port used to reach the Avaya SBCE at the enterprise.

Charter will provide the customer the necessary information to configure the SIP trunk connection from the enterprise site to the network, including:

- IP address, protocol and port used to reach the Charter managed CPE device.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

This information is used to complete the configuration of Communication Manager, Session Manager and the Avaya SBCE discussed in the previous sections.

9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of commands that can be used to troubleshoot the solution.

9.1. General Verification Steps

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- list trace station <extension number>
  Traces calls to and from a specific station.
- list trace tac <trunk access code number>
Trace calls over a specific trunk group.

- **status signaling-group** <signaling group number>
  Displays signaling group service state.

- **status trunk** <trunk group number>
  Displays trunk group service state.

- **status station** <extension number>
  Displays signaling and media information for an active call on a specific station.

### 9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager → System Status → SIP Entity Monitoring**. Click the Session Manager instance (**HG Session Manager** in the example below).
Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is *UP*, like shown on the screen below.

![Session Manager Entity Link Connection Status](image)

Other Session Manager useful verification and troubleshooting tools include:

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

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

**Alarms**: This screen provides information about the health of the SBC.

![Session Border Controller for Enterprise](image)

The following screen shows the **Alarm Viewer** page.

![Alarm Viewer](image)
**Incidents**: Provides detailed reports of anomalies, errors, policies violations, etc.

The following screen shows the **Incident Viewer** page.
**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

![Session Border Controller for Enterprise](image)

The following screen shows the Diagnostics page with the results of a ping test.

![Diagnostics](image)
Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings → Troubleshooting → Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.
Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.
10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to connect to the Charter Spectrum Business SIP Trunking service, as shown in Figure 1.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in Section 2.2.

11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

12. Appendix A: SigMa Script

Following is the Signaling Manipulation scripts that was used in the configuration of the Avaya SBCE, Section 7.8.2. When adding these scripts as instructed in Section 7.7 enter a name for the script in the Title (e.g., Remove_Sendonly) and copy/paste the scripts as shown below.

```bash
within session "INVITE" {
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        //Removes the a=sendonly from the re-INVITE messages.
        %BODY[1].regex_replace("a=sendonly\r\n","");
    }
}
```