



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3 and Avaya Session Border Controller for Enterprise Rel. 6.3 to support Time Warner Cable Business Class SIP Trunking Service – Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3, and Avaya Session Border Controller for Enterprise Rel. 6.3, to interoperate with Time Warner Cable Business Class SIP Trunking Service.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

Time Warner Cable Business Class SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Time Warner Cable network as an alternative to legacy analog or ISDN-PRI 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.....                                   | 4  |
| 2.2.   | Test Results .....   | 6  |
| 2.3.   | Support .....  | 6  |
| 3.     | Reference Configuration .....  | 7  |
| 4.     | Equipment and Software Validated .....                                     | 9  |
| 5.     | Configure Avaya Aura® Communication Manager.....                           | 10 |
| 5.1.   | Licensing and Capacity .....   | 11 |
| 5.2.   | System Features.....   | 12 |
| 5.3.   | IP Node Names.....   | 13 |
| 5.4.   | Codecs .....   | 14 |
| 5.5.   | IP Network Region.....   | 15 |
| 5.6.   | Signaling Group .....  | 16 |
| 5.7.   | Trunk Group.....   | 18 |
| 5.8.   | Calling Party Information.....   | 21 |
| 5.9.   | Inbound Routing.....   | 23 |
| 5.10.  | Outbound Routing .....   | 24 |
| 6.     | Configure Avaya Aura® Session Manager .....                                | 27 |
| 6.1.   | System Manager Login and Navigation.....                                   | 28 |
| 6.2.   | Specify SIP Domain .....   | 29 |
| 6.3.   | Add Location.....  | 30 |
| 6.4.   | SIP Entities .....   | 33 |
| 6.5.   | Entity Links .....   | 37 |
| 6.6.   | Routing Policies .....   | 40 |
| 6.7.   | Dial Patterns .....  | 41 |
| 6.8.   | Add/View Avaya Aura® Session Manager .....                                 | 44 |
| 7.     | Configure Avaya Session Border Controller for Enterprise (Avaya SBCE)..... | 46 |
| 7.1.   | Log in Avaya SBCE.....   | 46 |
| 7.2.   | Global Profiles.....   | 49 |
| 7.2.1. | Server Interworking - Avaya-SM .....                                       | 49 |
| 7.2.2. | Server Interworking - SP-General .....                                     | 52 |
| 7.2.3. | Server Configuration.....  | 54 |
| 7.2.4. | Routing Profiles .....   | 64 |
| 7.2.5. | Topology Hiding.....   | 67 |
| 7.2.6. | Signaling Manipulation.....  | 70 |
| 7.3.   | Domain Policies .....  | 73 |
| 7.3.1. | Application Rules.....   | 73 |
| 7.3.2. | Media Rules .....  | 74 |
| 7.3.3. | Signaling Rules .....  | 75 |
| 7.3.4. | End Point Policy Groups.....   | 81 |

|        |  |     |
|--------|--|-----|
| 7.4.   | Device Specific Settings.....  | 84  |
| 7.4.1. | Network Management.....  | 84  |
| 7.4.2. | Media Interface .....  | 86  |
| 7.4.3. | Signaling Interface .....  | 88  |
| 7.4.4. | End Point Flows.....   | 90  |
| 8.     | Time Warner Cable Business Class SIP Trunking Service Configuration..... | 94  |
| 9.     | Verification and Troubleshooting .....                                   | 95  |
| 9.1.1. | Verification Steps: .....  | 95  |
| 9.1.2. | Troubleshooting: .....   | 95  |
| 10.    | Conclusion .....   | 101 |
| 11.    | References.....  | 102 |
| 12.    | Appendix A: SigMa Script.....  | 104 |

# 1. Introduction

These Application Notes describe the steps necessary for configuring Session Initiation Protocol (SIP) trunking service between Time Warner Cable and an Avaya SIP-enabled enterprise solution.

In the sample configuration, the Avaya SIP-enabled enterprise solution consists of an Avaya Aura® Communication Manager Rel. 6.3 (hereafter referred to as Communications Manager), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.3 (hereafter referred to as Avaya SBCE), and various Avaya endpoints.

This solution does not extend to configurations without the Avaya SBCE or Session Manager.

Customers using an Avaya SIP-enabled enterprise solution with Time Warner Cable Business Class SIP Trunking service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional analog trunks and/or PSTN trunks such as ISDN-PRI. This approach generally results in lower cost for the enterprise.

The terms “service provider” or “Time Warner Cable” will be used interchangeably throughout these Application Notes.

## 2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Solution & Interoperability Test Lab by connecting Communication Manager, Session Manager and the Avaya SBCE to Time Warner Cable Business Class SIP Trunking service via the public internet, as depicted in **Figure 1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute for 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 areas were tested for compliance:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to the DID numbers assigned by Time Warner Cable. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x0 Series IP Telephones (H.323 and SIP), Avaya 96x1 Series IP Telephones (SIP), Avaya one-X® Communicator (H.323 and SIP), Avaya Communicator for Windows, Avaya 2420 Digital Telephones, and analog telephones.

- Outgoing calls to the PSTN were routed via Time Warner Cable's network to the various PSTN destinations.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 deskphones (SIP), Avaya one-X® Communicator (SIP) and Avaya Communicator for Windows (SIP).
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called party.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response from busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711MU (Time Warner Cable supported audio codec).
- No matching codecs.
- Voicemail and DTMF tone transmission per RFC 2833 (leaving and retrieving voice mail, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind and Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular call redirection).
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

**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 discussed in these Application Notes, see Reference [11].

Items not supported or not tested included the following:

- The use of the SIP REFER method for network call redirection is not currently supported by Time Warner Cable.
- Inbound toll-free calls, 911 emergency and International calls are supported but were not tested as part of the compliance test.
- Vector based Network Call Redirection (NCR) using REFER or 302 methods was not tested.
- SIP User-to-User Information (UII) was not tested.
- T.38 fax is not supported by Time Warner Cable; therefore T.38 fax was not tested.
- G.711 fax pass-through is available with Communication Manager on a "best effort" basis, it's not guaranteed that it will work; therefore G.711 fax pass-through is not recommended with this solution and was not tested.

## 2.2. Test Results

Interoperability testing of Time Warner Cable Business Class SIP Trunking service with an Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **No announcement on outbound calls to invalid PSTN numbers:** Announcement is not played to the user when the user dialed invalid PSTN numbers or numbers that have been disconnected. If a Communication Manager user dials an invalid PSTN number, or a number that has been disconnected, the user receives silence instead of an announcement informing him/her that an invalid number, or a number that has been disconnected, was dialed, to please check the number and to try again. The call is dropped after a few seconds with a “487 Request Terminated” message sent by Time Warner Cable to Communication Manager. This issue was reported to Time Warner Cable. It is expected that in Time Warner Cable production environment announcements are played to users.
- **Media shuffling:** Media shuffling allows Communication Manager to redirect media traffic directly between the inside IP of the Avaya SBCE and the enterprise endpoint, thus freeing Media Gateway resources in Communication Manager. Certain call types, such as Operator Assisted Calls (e.g. 0+10 digits), failed to complete with Media shuffling enabled in Communication Manager (**Direct IP-IP Audio Connections** set to y under the Signaling Group). Testing was done with Media shuffling disabled in Communication Manager (Refer to **Section 5.6**).
- **Re-directed and EC500 calls are rejected by Time Warner Cable with “403 Forbidden”:** Calls from the PSTN to Communication Manager that are re-directed back to the PSTN, and EC500 calls, were rejected by Time Warner Cable with a “403 Forbidden” if the Diversion header sent by Communication Manager did not contain the User Name (or the first DID number) used for SIP Trunk registration, or if the Diversion header did not contain a “+” sign in front of the 11 digits number. To solve this issue the numbering plan was changed from “private” to “public” in Communication Manager, resulting in Communication Manager adding a “+” sign to the 11 digit number included in the “From”, “Contact”, “PAI” and “Diversion” headers. With this change Time Warner Cable accepted the SIP messages with Diversion header sent by Communication Manager, allowing the call to go through their network (Refer to **Section 5.7**).

## 2.3. Support

For support on Time Warner Cable systems visit the corporate Web page at:

<http://business.timewarnercable.com/support/overview.html> or call 866-892-4249

### 3. Reference Configuration

**Figure 1** below illustrates the test configuration used. The test configuration simulates an enterprise site with an Avaya SIP-enabled enterprise solution connected to the Time Warner Cable Business Class SIP Trunking service through the public internet.

The Avaya components used to create the simulated customer site included:

- Avaya S8300 Server running Avaya Aura® Communication Manager.
- Avaya G450 Media Gateway.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- Dell R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 96x0-Series IP Telephones (H.323 and SIP).
- Avaya 96x1-Series IP Telephones (SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Communicator for Windows (SIP)
- Avaya 2420 Digital telephones.
- Analog Telephones.
- Desktop PC running various administration interfaces.

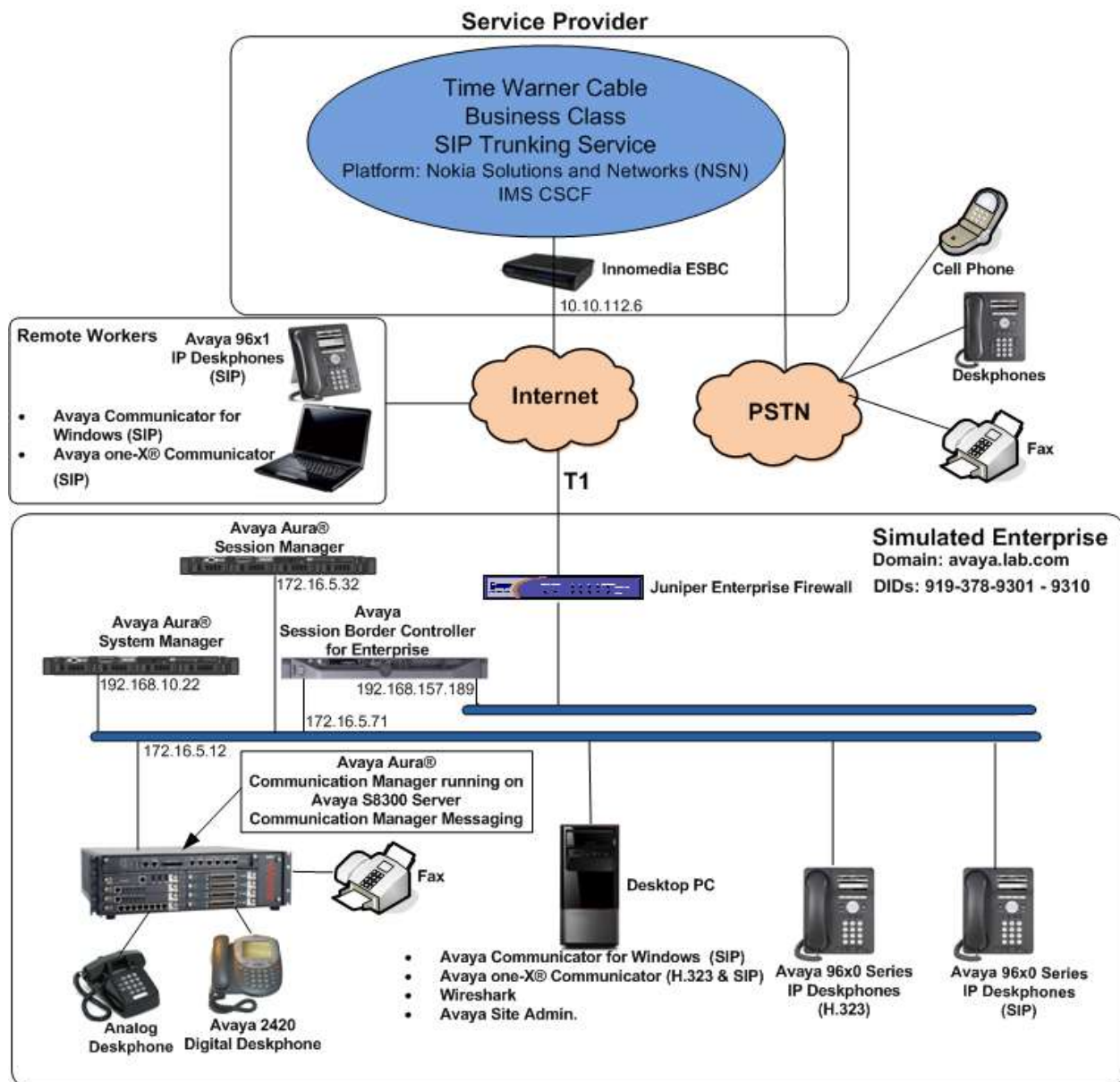
Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flow through the Avaya SBCE. This way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Time Warner Cable across the public Internet is SIP over UDP. The transport protocol between the Avaya SBCE and Session Manager across the enterprise network is SIP over TCP. The transport protocol between Session Manager and Communication Manager across the enterprise network is SIP over TLS. Note that for ease of troubleshooting during the testing, the compliance test was conducted with the transport protocol set to **tcp** between Session Manager and Communication Manager.

One SIP trunk group was created between Communication Manager and Session Manager to carry the traffic to and from the service provider (two-way trunk group). To separate the codec settings required by the service provider from the codec used by the telephones, two IP network regions were created, each with a dedicated signaling group.

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 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 translations and class of service restrictions are performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as Automatic Route Selection (ARS) and Class of Service restrictions.

Once Communication Manager selected the proper SIP trunk; the call is routed to Session Manager. Session Manager once again used the configured dial patterns and routing policies to determine the route to the Avaya SBCE for egress to Time Warner Cable's network.



**Figure 1: Avaya SIP-enabled Enterprise Solution and Time Warner Cable Business Class SIP Trunking Service**



## 4. Equipment and Software Validated

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

| Equipment/Software  | Release/Version  |
|---|--|
| <b>Avaya</b>  |  |
| Avaya Aura® Communication Manager running on an Avaya S8300 Server.             | 6.3.9 (Service Pack 9)<br>(03.0.124.0-21971)   |
| Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.          | 6.3.9 (Service Pack 9)<br>(6.3.9.0.639011)   |
| Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.           | 6.3.9 (Service Pack 9)<br>Build No. 6.3.0.8.5682-6.3.8.4414<br>Software Update Rev. No. 6.3.9.1.2482 |
| G450 Gateway  | 36.12.0  |
| Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server | 6.3.000-19-4338  |
| Avaya Aura® Integrated Management Site Administrator                            | 6.0.07   |
| Avaya Aura® Communication Manager Messaging (CMM)                               | CMM 6.3 (Service Pack 4)<br>(03.0.124.0-0402)  |
| Avaya Communicator for Windows  | 2.1.0.69   |
| Avaya one-X® Communicator (SIP & H.323)   | 6.2.4.07-FP4   |
| Avaya 96x0 Series IP Deskphones (H.323)   | Avaya one-X® Deskphone Edition<br>Version S3.230A  |
| Avaya 96x0 Series IP Telephones (SIP)   | Avaya one-X® Deskphone SIP<br>Version 2.6.13.1   |
| Avaya 96x1 Series IP Deskphones (SIP)   | Avaya one-X® Deskphone SIP<br>Version 6.4.1.25   |
| Avaya 2420 Series Digital Deskphones  | --   |
| Lucent Analog Deskphones  | --   |
| <b>Time Warner Cable</b>  |  |
| Nokia Solutions and Networks (NSN) IMS CSCF                                     | 8.2EP2   |
| Innomedia ESBC  | 2.0.13.0   |

**Table 2 – Hardware and Software Components Tested**

The specific configuration above was used for the compliance testing. Note that this solution is compatible with other Avaya Servers and Media Gateway platforms running similar versions of Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Time Warner Cable. It is assumed that the general installation of Communication Manager, the Avaya G450 Media Gateway and Session Manager has been previously completed.

In configuring Communication Manager, various components such as ip-network-regions, signaling groups, trunk groups, etc. need to be selected or created for use with the SIP connection to the service provider. Unless specifically stated otherwise, any unused ip-network-region, signaling group, trunk group, etc. can be used for this purpose.

Note that in some of the screenshots that follow the ‘Change’ command, instead of the ‘Add’ command may have been used since the Communication Manager configuration shown was previously added.

The Communication Manager configuration was performed using the Avaya Integrated Management Site Administrator. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

## 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 SIP trunks to the service provider. The example below shows one license with a capacity of **4000** trunks are available and **22** 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 to add additional capacity.

| display system-parameters customer-options                        |      | Page 2 of 11 |
|---|------|--------------|
| OPTIONAL FEATURES   |      |              |
| IP PORT CAPACITIES  |      | USED         |
| Maximum Administered H.323 Trunks:                                | 4000 | 10           |
| Maximum Concurrently Registered IP Stations:                      | 2400 | 2            |
| Maximum Administered Remote Office Trunks:                        | 4000 | 0            |
| Maximum Concurrently Registered Remote Office Stations:           | 2400 | 0            |
| Maximum Concurrently Registered IP eCons:                         | 68   | 0            |
| Max Concur Registered Unauthenticated H.323 Stations:             | 100  | 0            |
| Maximum Video Capable Stations:                                   | 2400 | 0            |
| Maximum Video Capable IP Softphones:                              | 2400 | 2            |
| Maximum Administered SIP Trunks:                                  | 4000 | 22           |
| Maximum Administered Ad-hoc Video Conferencing Ports:             | 4000 | 0            |
| Maximum Number of DS1 Boards with Echo Cancellation:              | 80   | 0            |
| Maximum TN2501 VAL Boards:  | 10   | 0            |
| Maximum Media Gateway VAL Sources:                                | 50   | 1            |
| Maximum TN2602 Boards with 80 VoIP Channels:                      | 128  | 0            |
| Maximum TN2602 Boards with 320 VoIP Channels:                     | 128  | 0            |
| Maximum Number of Expanded Meet-me Conference Ports:              | 300  | 0            |
| (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 this field set to ***none***.

```
change system-parameters features                               Page 1 of 20
FEATURE-RELATED SYSTEM PARAMETERS
  Self Station Display Enabled? n
    Trunk-to-Trunk Transfer: all
  Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
  Call Park Timeout Interval (minutes): 10
  Off-Premises Tone Detect Timeout Interval (seconds): 20
  AAR/ARS Dial Tone Required? y

  Music (or Silence) on Transferred Trunk Calls? no
  DID/Tie/ISDN/SIP Intercept Treatment: attendant
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
  Automatic Circuit Assurance (ACA) Enabled? n

  Abbreviated Dial Programming by Assigned Lists? n
  Auto Abbreviated/Delayed Transition Interval (rings): 2
  Protocol for Caller ID Analog Terminals: Bellcore
Display Calling Number for Room to Room Caller ID Calls? n
```

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.

| change system-parameters features  |  | Page 9 of 20                             |
|--|--|--|
| <b>FEATURE-RELATED SYSTEM PARAMETERS</b>   |  |  |
| <b>CPN/ANI/ICLID PARAMETERS</b>  |  |  |
| <div style="border: 1px solid red; padding: 2px;"> CPN/ANI/ICLID Replacement for Restricted Calls: <u>restricted</u><br/> CPN/ANI/ICLID Replacement for Unavailable Calls: <u>unavailable</u> </div> |  |  |
| <b>DISPLAY TEXT</b>  |  |  |
|  |  | Identity When Bridging: <u>principal</u> |
|  |  | User Guidance Display? <u>n</u>          |
| Extension only label for Team button on 96xx H.323 terminals? <u>n</u>   |  |  |
| <b>INTERNATIONAL CALL ROUTING PARAMETERS</b>   |  |  |
|  |  | Local Country Code: <u>      </u>        |
|  |  | International Access Code: <u>      </u> |
| <b>SCCAN PARAMETERS</b>  |  |  |
| Enable Enbloc Dialing without ARS FAC? <u>n</u>  |  |  |
| <b>CALLER ID ON CALL WAITING PARAMETERS</b>  |  |  |
| Caller ID on Call Waiting Delay Timer (msec): <u>200</u>   |  |  |

### 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 the Avaya S8300D server running Communication Manager (**procr**), and for Session Manager (**Lab-HG-SM**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

| change node-names ip |               | Page 1 of 2 |
|----------------------|---------------|-------------|
| <b>IP NODE NAMES</b> |               |             |
| Name                 | IP Address    |             |
| ASBCE A1             | 172.16.5.71   |             |
| Lab-HG-SM            | 172.16.5.32   |             |
| MA-CM                | 192.168.10.12 |             |
| default              | 0.0.0.0       |             |
| msgserver            | 172.16.5.12   |             |
| procr                | 172.16.5.12   |             |
| procr6               | ::            |             |

## 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. Time Warner Cable Business Class SIP Trunking only supports G.711MU. Thus, this codec was included in this set. Enter **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

```
change ip-codec-set 2                                     Page 1 of 2
```

IP CODEC SET

Codec Set: 2

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

Media Encryption

1: none

2:

3:

On **Page 2**, set the **Fax Mode** to *off* (T.38 fax is not supported by Time Warner Cable).

```
change ip-codec-set 2                                     Page 2 of 2
```

IP Codec Set

Allow Direct-IP Multimedia? n

|               | Mode | Redundancy |
|---------------|------|------------|
| FAX           | off  | 0          |
| Modem         | off  | 0          |
| TDD/TTY       | US   | 3          |
| Clear-channel | n    | 0          |

## 5.5. IP Network Region

Create a separate IP network region for the service provider trunk. 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*. This name appears in the “From” header of SIP messages 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 Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to *yes*. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

| change ip-network-region 2             |   | Page 1 of 20           |
|--|---|------------------------|
| IP NETWORK REGION                      |   |                        |
| Region: 2                              |   |                        |
| Location: <u>1</u>                     | Authoritative Domain: <u>avaya.lab.com</u>  |                        |
| Name: <u>SP Region</u>                 | Stub Network Region: <u>n</u>               |                        |
| MEDIA PARAMETERS                       |   |                        |
| Codec Set: <u>2</u>                    | Intra-region IP-IP Direct Audio: <u>yes</u> |                        |
|  | Inter-region IP-IP Direct Audio: <u>yes</u> |                        |
| UDP Port Min: <u>2048</u>              | IP Audio Hairpinning? <u>n</u>              |                        |
| UDP Port Max: <u>3349</u>              |   |                        |
| DIFFSERV/TOS PARAMETERS                |   |                        |
| Call Control PHB Value: <u>46</u>      |   |                        |
| Audio PHB Value: <u>46</u>             |   |                        |
| Video PHB Value: <u>26</u>             |   |                        |
| 802.1P/Q PARAMETERS                    |   |                        |
| Call Control 802.1p Priority: <u>6</u> |   |                        |
| Audio 802.1p Priority: <u>6</u>        |   |                        |
| Video 802.1p Priority: <u>5</u>        |   |                        |
| AUDIO RESOURCE RESERVATION PARAMETERS  |   |                        |
| H.323 IP ENDPOINTS                     |   | RSVP Enabled? <u>n</u> |
| H.323 Link Bounce Recovery? <u>y</u>   |   |                        |
| Idle Traffic Interval (sec): <u>20</u> |   |                        |
| Keep-Alive Interval (sec): <u>5</u>    |   |                        |
| Keep-Alive Count: <u>5</u>             |   |                        |

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. 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 example below 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).

| change ip-network-region 2 |       |  |               |            |             |     |   |     |   | Page | 4 of 20 |
|----------------------------|-------|--|---------------|------------|-------------|-----|---|-----|---|------|---------|
| Source Region: 2           |       | Inter Network Region Connection Management |               |            |             |     |   |     |   | I    | M       |
| dst                        | codec | direct                                     | WAN-BW-limits | Video      | Intervening | Dyn | G | A   | t |      |         |
| rgn                        | set   | WAN  | Units         | Total Norm | Prio Shr    | CAC | R | L   | e |      |         |
| 1                          | 2     | y  | NoLimit       |            |             |     | n |     | t |      |         |
| 2                          | 2     |  |               |            |             |     |   | all |   |      |         |
| 3                          |       |  |               |            |             |     |   |     |   |      |         |

## 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 SIP 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 for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). Note that for ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to *tcp*. The transport method specified here is used between Communication Manager and Session Manager. The transport method used between Session Manager and the Avaya SBCE is specified as TCP in **Sections 6.5**. Lastly, the transport method between the Avaya SBCE and Time Warner Cable is UDP. This is defined in **Section 7.2.3**.
- 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 TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to *5070*. (For TCP, the well-known port value for SIP is 5060).
- 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 as Session Manager.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Avaya S8300D Server running 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**.



- 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 **Direct IP-IP Audio Connections** to *n*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the inside IP of the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Testing was done with this field disabled (set to *n*), refer to **Section 2.2**.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

| change signaling-group 2   |   | Page 1 of 2                         |
|--|---|-------------------------------------|
| <b>SIGNALING GROUP</b>   |   |                                     |
| Group Number: 2  | Group Type: sip                           |                                     |
| IMS Enabled? <u>n</u>  | Transport Method: <u>tcp</u>              |                                     |
| Q-SIP? <u>n</u>  |   |                                     |
| IP Video? <u>n</u>   |   | Enforce SIPS URI for SRTP? <u>y</u> |
| Peer Detection Enabled? <u>y</u>   | Peer Server: SM                           |                                     |
| Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <u>y</u>  |   |                                     |
| Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <u>n</u> |   |                                     |
| Alert Incoming SIP Crisis Calls? <u>n</u>  |   |                                     |
| Near-end Node Name: <u>procr</u>   | Far-end Node Name: <u>Lab-HG-SM</u>       |                                     |
| Near-end Listen Port: <u>5070</u>  | Far-end Listen Port: <u>5070</u>          |                                     |
|  | Far-end Network Region: <u>2</u>          |                                     |
| Far-end Domain: <u>avaya.lab.com</u>   |   |                                     |
| Incoming Dialog Loopbacks: <u>eliminate</u>  | Bypass If IP Threshold Exceeded? <u>n</u> |                                     |
| DTMF over IP: <u>rtp-payload</u>   | RFC 3389 Comfort Noise? <u>n</u>          |                                     |
| Session Establishment Timer(min): <u>3</u>   | Direct IP-IP Audio Connections? <u>n</u>  |                                     |
| Enable Layer 3 Test? <u>n</u>  | IP Audio Hairpinning? <u>n</u>            |                                     |
|  | Alternate Route Timer(sec): <u>6</u>      |                                     |

## 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 step.
- 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.

```
change trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2      Group Type: sip      CDR Reports: y
Group Name: Service Provider      COR: 1      TN: 1      TAC: 602
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service:
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 2
                                     Number of Members: 10
```

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. For the compliance test, the value of **600** seconds was used.

```
change trunk-group 2                                     Page 2 of 21
      Group Type: sip
TRUNK PARAMETERS
      Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
      SCCAN? n      Digital Loss Group: 18
      Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
      XOIP Treatment: auto      Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to *public*. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP “From”, “Contact”, “P-Asserted Identity” and “Diversion” headers. The addition of the + sign to the 11 digit number included in the Diversion header for re-directed calls to the PSTN and for EC500 calls was required by Time Warner Cable. Thus, the **Numbering Format** was set to *public* (Refer to **Section 2.2**).

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. Default values were used for all other fields.

| change trunk-group 2                    |                       | Page 3 of 21                           |
|---|-----------------------|--|
| TRUNK FEATURES                          |                       |  |
| ACA Assignment? <u>n</u>                | Measured: <u>none</u> | Maintenance Tests? <u>y</u>            |
| <br>                                    |                       |  |
| Numbering Format: <u>public</u>         |                       | UII Treatment: <u>service-provider</u> |
|   |                       | Replace Restricted Numbers? <u>y</u>   |
|   |                       | Replace Unavailable Numbers? <u>y</u>  |
| <br>                                    |                       |  |
| Modify Tandem Calling Number: <u>no</u> |                       |  |
| <br>                                    |                       |  |
| Show ANSWERED BY on Display? <u>y</u>   |                       |  |
| <br>                                    |                       |  |

On **Page 4**, set **Network Call Redirection** field to *n* to direct Communication Manager not to use the SIP REFER message for transferring calls off-net to the PSTN (Refer to **Section 2.2**). Set the **Send Diversion Header** field to *y*. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to *n*. Set the **Telephone Event Payload Type** to *101*, the value preferred by Time Warner Cable. Set **Convert 180 to 183 for Early Media** to *y*.

| change trunk-group 2   | Page 4 of 21               |
|--|----------------------------|
| PROTOCOL VARIATIONS  |                            |
| Mark Users as Phone?   | <u>n</u>                   |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number?                  | <u>n</u>                   |
| Send Transferring Party Information?   | <u>n</u>                   |
| Network Call Redirection?  | <u>n</u>                   |
| Send Diversion Header?   | <u>y</u>                   |
| Support Request History?   | <u>n</u>                   |
| Telephone Event Payload Type:  | <u>101</u>                 |
| Convert 180 to 183 for Early Media?  | <u>y</u>                   |
| Always Use re-INVITE for Display Updates?                                    | <u>n</u>                   |
| Identity for Calling Party Display:  | <u>P-Asserted-Identity</u> |
| Block Sending Calling Party Location in INVITE?                              | <u>n</u>                   |
| Accept Redirect to Blank User Destination?                                   | <u>n</u>                   |
| Enable Q-SIP?  | <u>n</u>                   |
| Interworking of ISDN Clearing with In-Band Tones: <u>keep-channel-active</u> |                            |

## 5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are assigned by the SIP service provider. It is used to authenticate the caller. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs).

The screen below shows DID numbers assigned for testing. Shown below are DID numbers mapped to enterprise extensions. These 11-digit numbers were used for the outbound calling party information on the service provider trunk when calls were originated from these extensions. Since public numbering plan was used, Communication Manager automatically inserts a “+” sign to the 11-digit numbers in the “From”, “Contact”, “PAI”, and “Diversion” headers.

| change public-unknown-numbering 1 |          |            |             |               | Page 1 of 2   |
|-----------------------------------|----------|------------|-------------|---------------|---|
| NUMBERING - PUBLIC/UNKNOWN FORMAT |          |            |             |               |   |
| Ext Len                           | Ext Code | Trk Grp(s) | CPN Prefix  | Total CPN Len |   |
| 4                                 | 3        |            |             | 4             | Total Administered: 11  |
| 4                                 | 5        |            |             | 4             | Maximum Entries: 240  |
| 4                                 | 3040     | 2          | 19193781301 | 11            | Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number. |
| 4                                 | 3041     | 2          | 19193781302 | 11            |   |
| 4                                 | 3042     | 2          | 19193781307 | 11            |   |
| 4                                 | 3045     | 2          | 19193781306 | 11            |   |
| 4                                 | 3046     | 2          | 19193781305 | 11            |   |
| 4                                 | 3047     | 2          | 19193781303 | 11            |   |
| 4                                 | 3048     | 2          | 19193781304 | 11            |   |
| 4                                 | 5013     | 2          | 19193781308 | 11            |   |
| 4                                 | 5016     | 2          | 19193781309 | 11            | Communication Manager automatically inserts a '+' digit in this case.   |
| —                                 | —        | —          | —           | —             |   |
| —                                 | —        | —          | —           | —             |   |
| —                                 | —        | —          | —           | —             |   |

[illegible]

## 5.9. Inbound Routing

DID numbers received from Time Warner Cable were mapped to extensions 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 number.

| change inc-call-handling-trmt trunk-group 2 |               |                  |     |        | Page 1 of 3 |
|---|---------------|------------------|-----|--------|-------------|
| INCOMING CALL HANDLING TREATMENT            |               |                  |     |        |             |
| Service/<br>Feature                         | Number<br>Len | Number<br>Digits | Del | Insert |             |
| public-ntwrk                                | 11            | 19193781301      | 11  | 3040   |             |
| public-ntwrk                                | 11            | 19193781302      | 11  | 3041   |             |
| public-ntwrk                                | 11            | 19193781303      | 11  | 3047   |             |
| public-ntwrk                                | 11            | 19193781304      | 11  | 3048   |             |
| public-ntwrk                                | 11            | 19193781305      | 11  | 3046   |             |
| public-ntwrk                                | 11            | 19193781306      | 11  | 3045   |             |
| public-ntwrk                                | 11            | 19193781307      | 11  | 3042   |             |
| public-ntwrk                                | 11            | 19193781308      | 11  | 5013   |             |
| public-ntwrk                                | 11            | 19193781309      | 11  | 5016   |             |
| public-ntwrk                                | 11            | 19193781310      | 11  | 3051   |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |

In a real customer environment, where DID numbers are usually comprised of a local extension plus a prefix, a single entry can be applied for all extensions, like in the example shown below.

| change inc-call-handling-trmt trunk-group 2 |               |                  |     |        | Page 1 of 3 |
|---|---------------|------------------|-----|--------|-------------|
| INCOMING CALL HANDLING TREATMENT            |               |                  |     |        |             |
| Service/<br>Feature                         | Number<br>Len | Number<br>Digits | Del | Insert |             |
| public-ntwrk                                | 11            | 1919378          | 7   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |
| public-ntwrk                                | —             | —                | —   | —      |             |

## 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**).

| change dialplan analysis |              |           | DIAL PLAN ANALYSIS TABLE |              |           |                 |              |           | Page 1 of 12 |
|--------------------------|--------------|-----------|--------------------------|--------------|-----------|-----------------|--------------|-----------|--------------|
|                          |              |           | Location: all            |              |           | Percent Full: 2 |              |           |              |
| Dialed String            | Total Length | Call Type | Dialed String            | Total Length | Call Type | Dialed String   | Total Length | Call Type |              |
| 0                        | 13           | udp       |                          |              |           |                 |              |           |              |
| 1                        | 4            | dac       |                          |              |           |                 |              |           |              |
| 2                        | 4            | ext       |                          |              |           |                 |              |           |              |
| 3                        | 4            | ext       |                          |              |           |                 |              |           |              |
| 4                        | 4            | udp       |                          |              |           |                 |              |           |              |
| 5                        | 4            | ext       |                          |              |           |                 |              |           |              |
| 6                        | 3            | dac       |                          |              |           |                 |              |           |              |
| 7                        | 4            | ext       |                          |              |           |                 |              |           |              |
| 8                        | 4            | ext       |                          |              |           |                 |              |           |              |
| 9                        | 1            | fac       |                          |              |           |                 |              |           |              |
| *                        | 3            | dac       |                          |              |           |                 |              |           |              |
| #                        | 2            | dac       |                          |              |           |                 |              |           |              |



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

```

change feature-access-codes                                     Page 1 of 10
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: #7
Answer Back Access Code: ____
Attendant Access Code: ____
Auto Alternate Routing (AAR) Access Code: *01
Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2: ____
Automatic Callback Activation: ____ Deactivation: ____
Call Forwarding Activation Busy/DA: ____ All: ____ Deactivation: ____
Call Forwarding Enhanced Status: ____ Act: ____ Deactivation: ____
Call Park Access Code: ____
Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
CDR Account Code Access Code: ____
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 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 to the service provider (as defined next).

| change ars analysis 17   |           |           |               |           |          |           | Page 1 of 2     |
|--------------------------|-----------|-----------|---------------|-----------|----------|-----------|-----------------|
| ARS DIGIT ANALYSIS TABLE |           |           |               |           |          |           |                 |
| Location: all            |           |           |               |           |          |           | Percent Full: 2 |
| Dialed String            | Total Min | Total Max | Route Pattern | Call Type | Node Num | ANI Req'd |                 |
| 170                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 1700                     | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 171                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 172                      | 11        | 11        | 2             | fnpa      | ____     | n         |                 |
| 173                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 174                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 175                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 176                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 177                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 178                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 1786                     | 11        | 11        | 2             | fnpa      | ____     | n         |                 |
| 179                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 180                      | 11        | 11        | deny          | fnpa      | ____     | n         |                 |
| 1800                     | 11        | 11        | 2             | fnpa      | ____     | n         |                 |
| 1800555                  | 11        | 11        | deny          | fnpa      | ____     | n         |                 |

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 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **2** 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.
- **Pfx Mrk:** **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNP 10 digit numbers are left unchanged.

```
change route-pattern 2
```

Page 1 of 3

Pattern Number: 2      Pattern Name: Serv. Provider

SCCAN? n      Secure SIP? n

| Grp No | FRL      | NPA      | Pfx Mrk  | Hop Lmt | Toll List | No. Del | Inserted Dgts | DCS/ QSIG Intw | IXC         |
|--------|----------|----------|----------|---------|-----------|---------|---------------|----------------|-------------|
| 1:     | <u>2</u> | <u>0</u> | <u>1</u> |         |           |         |               | <u>n</u>       | <u>user</u> |
| 2:     |          |          |          |         |           |         |               | <u>n</u>       | <u>user</u> |
| 3:     |          |          |          |         |           |         |               | <u>n</u>       | <u>user</u> |
| 4:     |          |          |          |         |           |         |               | <u>n</u>       | <u>user</u> |
| 5:     |          |          |          |         |           |         |               | <u>n</u>       | <u>user</u> |
| 6:     |          |          |          |         |           |         |               | <u>n</u>       | <u>user</u> |

| BCC | VALUE    | TSC      | CA-TSC   | ITC      | BCIE     | Service/Feature | PARM     | No. Dgts | Numbering Format | LAR         |
|-----|----------|----------|----------|----------|----------|-----------------|----------|----------|------------------|-------------|
| 0   | 1        | 2        | M        | 4        | W        |                 |          |          |                  |             |
| 1:  | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>n</u>        | <u>n</u> |          | <u>rest</u>      | <u>none</u> |
| 2:  | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>n</u>        | <u>n</u> |          | <u>rest</u>      | <u>none</u> |
| 3:  | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>n</u>        | <u>n</u> |          | <u>rest</u>      | <u>none</u> |
| 4:  | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>n</u>        | <u>n</u> |          | <u>rest</u>      | <u>none</u> |
| 5:  | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>n</u>        | <u>n</u> |          | <u>rest</u>      | <u>none</u> |
| 6:  | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>y</u> | <u>n</u>        | <u>n</u> |          | <u>rest</u>      | <u>none</u> |

**Note:** To save all Communication Manager provisioning changes, enter the command **save translations**.

## 6. Configure Avaya Aura® Session Manager

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

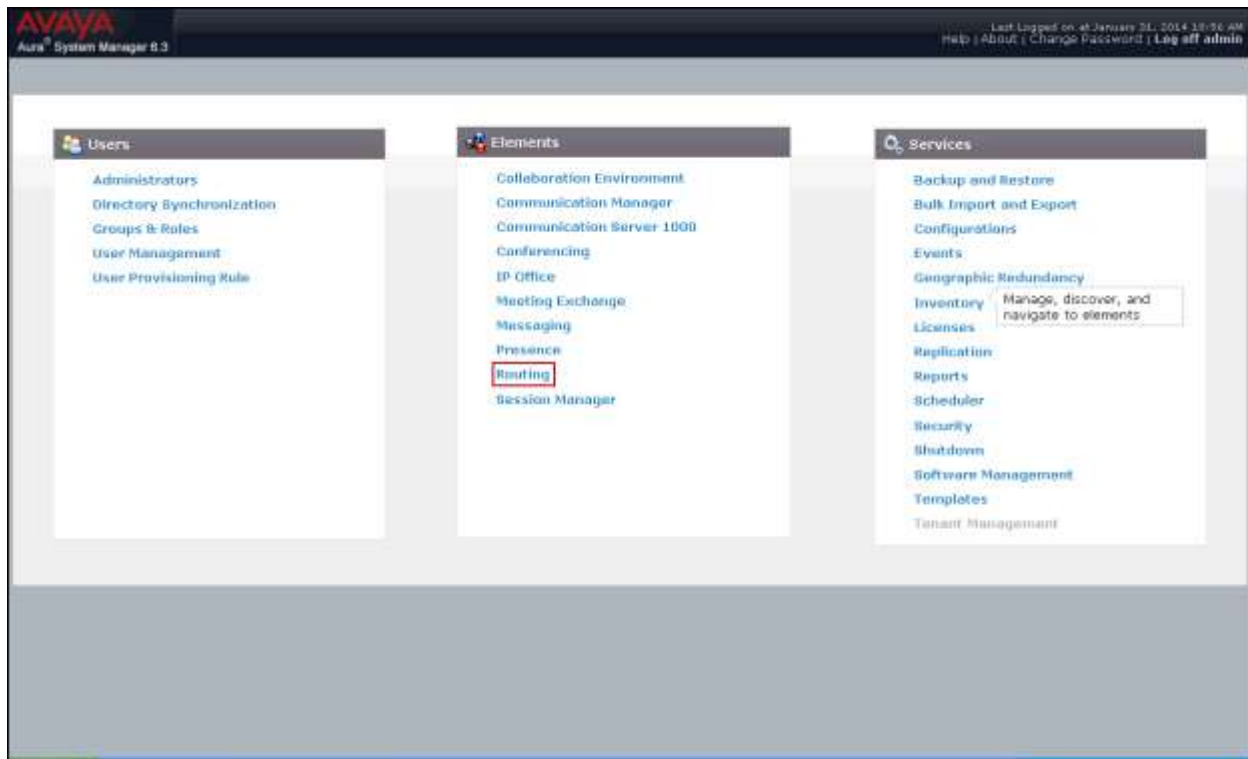
- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager 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
- Regular Expressions, which also can be used to route calls
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

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

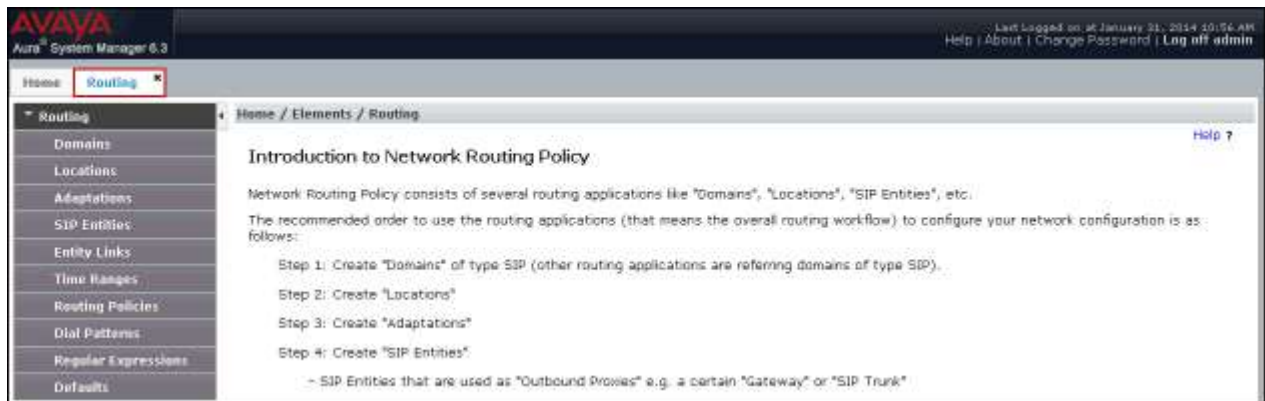
|  |
|--|
| <b>Note:</b> Some of the default information in the screenshots that follow may have been cut out (not included) for brevity |
|--|

## 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 (not shown). The screen shown below is then displayed. Click on **Routing**.



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



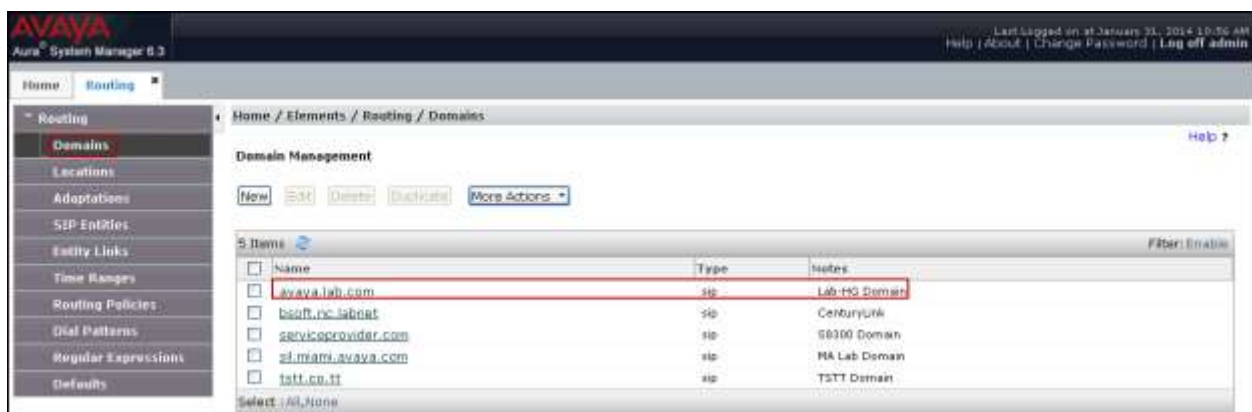
## 6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, the enterprise domain **avaya.lab.com** was used.

To add a domain 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 (not show).

The screen below shows the entry for the enterprise domain **avaya.lab.com**.



### 6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management and call admission control. 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. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save.

The screen below shows the **HG Session Manager** location. This location will be assigned later to the SIP Entity corresponding to Session Manager.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations'. The 'Location Details' section includes a 'General' tab. The 'Name' field is populated with 'HG Session Manager' and is highlighted with a red box. The 'Notes' field is empty. Below this, the 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox that is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'kbit/sec', with 'Total Bandwidth' and 'Multimedia Bandwidth' fields empty. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked. The 'Per-Call Bandwidth Parameters' section shows 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)' both set to '1000 Kbit/Sec', 'Minimum Multimedia Bandwidth' set to '64 Kbit/Sec', and 'Default Audio Bandwidth' set to '80 Kbit/Sec'. The 'Alarm Threshold' section shows 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' both set to '80 %', with 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' both set to '5 Minutes'. The 'Location Pattern' section at the bottom shows '0 Items' and a table with one row for 'IP Address Pattern'. The 'Commit' and 'Cancel' buttons are visible at the bottom right.

The following screen shows the **HG Communication Manager** location. This location will be assigned later to the SIP Entity corresponding to Communication Manager.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left sidebar shows the navigation menu with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations'. The 'Location Details' section includes a 'Name' field set to 'HG Communication Manager' and a 'Notes' field. Below this is the 'Dial Plan Transparency in Survivable Mode' section with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section contains fields for 'Managed Bandwidth Units' (set to Kbit/sec), 'Total Bandwidth', and 'Multimedia Bandwidth', along with a checked 'Audio Calls Can Take Multimedia Bandwidth' checkbox. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'. The 'Alarm Threshold' section has fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', and latency before alarm triggers. The 'Location Pattern' section at the bottom shows a table with one entry: 'IP Address Pattern'.

AVAYA  
Aura® System Manager 6.3

Home / Elements / Routing / Locations

Location Details

General

\* Name: HG Communication Manager

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

\* Minimum Multimedia Bandwidth: 64 Kbit/Sec

\* Default Audio Bandwidth: 80 Kbit/Sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

\* Latency before Overall Alarm Trigger: 5 Minutes

\* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

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

Commit Cancel

The following screen shows the **HG ASBCE** location. This location will be assigned later to the SIP Entity corresponding to the Avaya SBCE.

AVAYA  
Aura® System Manager 6.3

Home / Elements / Routing / Locations

Location Details

General

\* Name: HG ASBCE

Notes: HG Avaya SBCE

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

\* Minimum Multimedia Bandwidth: 64 Kbit/Sec

\* Default Audio Bandwidth: 00 Kbit/Sec

Alarm Threshold

Overall Alarm Threshold: 00 %

Multimedia Alarm Threshold: 00 %

\* Latency before Overall Alarm Trigger: 5 Minutes

\* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

Filter: Enable

IP Address Pattern

Notes

Commit Cancel



## 6.4. 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-hand 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 interface that is used for SIP signaling.
- **Type:** Enter *Session Manager* for Session Manager, *CM* for Communication Manager and *Other* for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name**.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which the Session Manager will listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.
- Click **Commit** to save.

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to the Avaya SBCE.
- **5070** with **TCP** for connecting to Communication Manager.

The following screen shows the addition of the Session Manager SIP entity. The name ***HG Session Manager***, the IP address of the Session Manager signaling interface and the Location ***HG Session Manager*** created in **Section 6.3** was used.

The screenshot displays the Avaya Aura System Manager 8.3 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration fields are as follows:

- Name:** HG Session Manager
- FQDN or IP Address:** 172.16.5.32
- Type:** Session Manager
- Notes:** HG Session Manager
- Location:** HG Session Manager
- Outbound Proxy:** (empty)
- Time Zone:** America/New\_York
- Credential name:** (empty)

Below the configuration fields, there is a 'SIP Link Monitoring' section with a checkbox labeled 'Use Session Manager Configuration' which is checked. Under the 'Port' section, there are input fields for 'TCP Fallback port' and 'TLS Fallback port', both of which are empty. Below these are 'Add' and 'Remove' buttons.

A table lists the ports and protocols for the SIP entity:

| Port | Protocol | Default Domain | Notes |
|------|----------|----------------|-------|
| 5060 | TCP      | avaya.lab.com  |       |
| 5060 | UDP      | avaya.lab.com  |       |
| 5061 | TLS      | avaya.lab.com  |       |
| 5062 | TCP      | avaya.lab.com  |       |
| 5070 | TCP      | avaya.lab.com  |       |
| 5090 | TCP      | avaya.lab.com  |       |
| 5091 | TCP      | avaya.lab.com  |       |
| 5095 | UDP      | avaya.lab.com  |       |
| 5096 | TCP      | avaya.lab.com  |       |

Below the table, there is a 'SIP Responses to an OPTIONS Request' section with 'Add' and 'Remove' buttons. A table for these responses is shown at the bottom, with columns for 'Response Code & Reason Phrase', 'Mark Entity Up/Down', and 'Notes'. The table is currently empty.

At the bottom right of the configuration area, there are 'Commit' and 'Cancel' buttons.

The following screen shows the addition of the Communication Manager SIP Entity.

A separate SIP entity for Communication Manager is required in order to route traffic from Communication Manager to the Service Provider.

The name ***HG CM Trunk 2***, the IP of the Avaya S8300D Server running Communication Manager and the location ***HG Communication Manager*** created in **Section 6.3** was used.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows a tree structure with 'Routing' expanded, and 'SIP Entities' highlighted. The main content area is titled 'Home / Elements / Routing / SIP Entities' and contains the 'SIP Entity Details' form. The 'General' tab is active. The form includes the following fields: 'Name' (set to 'HG CM Trunk 2'), 'FQDN or IP Address' (set to '172.16.5.12'), 'Type' (set to 'CH'), 'Notes' (set to 'CM SIP Trunk 2'), 'Adaptation' (a dropdown menu), 'Location' (set to 'HG Communication Manager'), 'Time Zone' (set to 'America/New\_York'), 'SIP Timer B/F (in seconds)' (set to '4'), 'Credential name' (an empty text field), 'Call Detail Recording' (set to 'none'), 'Loop Detection Mode' (set to 'Off'), and 'SIP Link Monitoring' (set to 'Use Session Manager Configuration'). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

The following screen shows the addition of the SIP entity for the Avaya SBCE.

The name **HG ASBCE**, the inside IP address of the Avaya SBCE and the location **HG ASBCE** created in **Section 6.3** was used.

AVAYA  
Aura System Manager 6.3

Home / Routing / SIP Entities

SIP Entity Details

General

Name: HG ASBCE

FQDN or IP Address: 172.16.5.71

Type: Other

Notes: HG ASBCE

Adaptation:

Location: HG ASBCE

Time Zone: America/New\_York

SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

## 6.5. 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 Communication Manager and one to the Avaya SBCE, to be used only for service provider traffic. To add an entity link, navigate to **Routing → Entity Links** in the left-hand 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.
- **Protocol:** Select the transport protocol used for this link.
- **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 signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system will receive SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted** (not shown).
- Click **Commit** to save.

The following screens illustrate the entity links to Communication Manager and to the Avaya SBCE. It should be noted that in a customer environment the entity link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic is not encrypted.

The following screen shows the entity link to Communication Manager:

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, **Entity Links** (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Entity Links'. It features a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. A single row is displayed, representing a link between 'HG Session Manager' and 'HG CM Trunk 2'. The 'Connection Policy' is set to 'trusted'. Below the table, there are 'Commit' and 'Cancel' buttons.

| Name                 | SIP Entity 1         | Protocol | Port   | SIP Entity 2    | DNS Override | Port   | Connection Policy | Deny New Service | Notes |
|----------------------|----------------------|----------|--------|-----------------|--------------|--------|-------------------|------------------|-------|
| * HG Session Manager | * HG Session Manager | TCP      | * 5070 | * HG CM Trunk 2 |              | * 5070 | trusted           |                  |       |

The following screen shows the entity link to the Avaya SBCE:

The screenshot shows the Avaya Aura System Manager 6.3 interface, similar to the previous one, but with the 'Entity Links' menu item highlighted. The main content area is titled 'Home / Elements / Routing / Entity Links'. The table below shows a link between 'HG Session Manager' and 'HG ASBCE'. The 'Connection Policy' is set to 'trusted'. Below the table, there are 'Commit' and 'Cancel' buttons.

| Name                 | SIP Entity 1         | Protocol | Port   | SIP Entity 2 | DNS Override | Port   | Connection Policy | Deny New Service | Notes |
|----------------------|----------------------|----------|--------|--------------|--------------|--------|-------------------|------------------|-------|
| * HG Session Manager | * HG Session Manager | TCP      | * 5060 | * HG ASBCE   |              | * 5060 | trusted           |                  |       |

The following screen shows the list of the newly added entity links. Note that only the highlighted entity links were created for the compliance test, and are the ones relevant to these Application Notes.

| <input type="checkbox"/> | Name                                      | SIP Entity 1       | Protocol | Port | SIP Entity 2     | DNS Override             | Port | Connection Policy | Deny New Service         | Notes           |
|--------------------------|---|--------------------|----------|------|------------------|--------------------------|------|-------------------|--------------------------|-----------------|
| <input type="checkbox"/> | HG Session Manager AAC 5060 TCP           | HG Session Manager | TCP      | 5060 | AAC              | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> | AAC Entity Link |
| <input type="checkbox"/> | HG Session Manager sip1 5060 TCP          | HG Session Manager | TCP      | 5060 | Acme Packet sip1 | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |                 |
| <input type="checkbox"/> | HG Session Manager CS1K7.6 5085 UDP       | HG Session Manager | UDP      | 5085 | CS1K7.6          | <input type="checkbox"/> | 5085 | trusted           | <input type="checkbox"/> |                 |
| <input type="checkbox"/> | HG Session Manager SBC 5060 UDP           | HG Session Manager | UDP      | 5060 | EdgeHarc SBC     | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |                 |
| <input type="checkbox"/> | HG Session Manager HG AA-SBC 5060 TCP     | HG Session Manager | TCP      | 5060 | HG AA-SBC        | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |                 |
| <input type="checkbox"/> | HG Session Manager HG ASBCE 5060 TCP      | HG Session Manager | TCP      | 5060 | HG ASBCE         | <input type="checkbox"/> | 5060 | trusted           | <input type="checkbox"/> |                 |
| <input type="checkbox"/> | HG Session Manager HG CM Trunk 1 5080 TCP | HG Session Manager | TLS      | 5061 | HG CM Trunk 1    | <input type="checkbox"/> | 5061 | trusted           | <input type="checkbox"/> |                 |
| <input type="checkbox"/> | HG Session Manager HG CM Trunk 2 5070 TCP | HG Session Manager | TCP      | 5070 | HG CM Trunk 2    | <input type="checkbox"/> | 5070 | trusted           | <input type="checkbox"/> |                 |

## 6.6. Routing Policies

Routing Policies describe the conditions under which calls are routed to the SIP entities specified in **Section 6.4**. Two routing policies must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **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 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 screen shows the routing policy for Communication Manager:

AVAYA  
Avaya System Manager 6.3

Home / Elements / Routing / Routing Policies

Routing Policy Details

General

\* Name: To HG CM Trunk 2

Disabled: ☐

\* Retries: 0

Notes: Inbound calls to HG CM Trunk 2

SIP Entity as Destination

Select

| Name          | FQDN or IP Address | Type | Notes          |
|---------------|--------------------|------|----------------|
| HG CM Trunk 2 | 172.16.5.12        | CM   | CM SIP Trunk 2 |



The following screen shows the routing policy for the Avaya SBCE:

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' highlighted. The main content area is titled 'Home / Elements / Routing / Routing Policies' and shows the 'Routing Policy Details' for a policy named 'HG ASBCE'. The 'General' tab is active, showing fields for 'Name' (To HG ASBCE), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (Outbound calls via ASBCE). Below this, the 'SIP Entity as Destination' section has a 'Select' button. At the bottom, a table lists the SIP entities:

| Name     | FQDN or IP Address | Type  | Notes    |
|----------|--------------------|-------|----------|
| HG ASBCE | 172.16.5.71        | Other | HG ASBCE |

## 6.7. Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Time Warner Cable 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-hand 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. Use default values for all remaining fields:

- **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**.

- Click **Commit** to save.

Examples of dial patterns used for the compliance testing are shown below.

The first example shows dial pattern **1**, with destination SIP Domain of **-ALL-**, Originating Location Name **HG Communication Manager** and Routing Policy name **To HG ASBCE**. This dial pattern was used for outbound calls to the PSTN.

**Note:** The SIP Domain was set to **-ALL-** since dial pattern 1 is shared among multiple SIP Domains in the Avaya lab.

**Avaya Aura System Manager 6.3**

Home / Routing / Dial Patterns

**Dial Pattern Details**

Commit Cancel

**General**

\* Pattern: 1

\* Min: 1

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

6 Items Filter: Stable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name   | Risk | Routing Policy Disabled             | Routing Policy Destination | Routing Policy Notes     |
|--------------------------|---------------------------|----------------------------|-----------------------|------|-------------------------------------|----------------------------|--------------------------|
| <input type="checkbox"/> | CS1k Node                 | CS1K7.6                    | Outbound to MA ASBCE  | 0    | <input type="checkbox"/>            | MA_SBCE                    | Outbound to MA_SBCE      |
| <input type="checkbox"/> | CS1k Node                 | CS1K7.6                    | To EdgeHarc           | 0    | <input checked="" type="checkbox"/> | EdgeHarc SBC               |                          |
| <input type="checkbox"/> | HG Communication Manager  |                            | To HG ASBCE           | 0    | <input type="checkbox"/>            | HG ASBCE                   | Outbound calls via ASBCE |
| <input type="checkbox"/> | MA Communication Manager  | HP DL360                   | Outbound to MA AA-SBC | 0    | <input checked="" type="checkbox"/> | MA_AA-SBC                  |                          |
| <input type="checkbox"/> | MA Communication Manager  | HP DL360                   | Outbound to MA ASBCE  | 0    | <input type="checkbox"/>            | MA_SBCE                    | Outbound to MA_SBCE      |
| <input type="checkbox"/> | SIL Lab Others            |                            | Outbound to MA ASBCE  | 0    | <input type="checkbox"/>            | MA_SBCE                    | Outbound to MA_SBCE      |

Select: All, None

The following dial pattern used for the compliance testing was for inbound calls to the enterprise. For calls that begin with **1919**, are between **4** and **11** digits in length, have a SIP Domain of **avaya.lab.com** and an Originating Location Name of **HG ASBCE**, Routing Policy **To HG CM Trunk 2** will be used.

**AVAYA**  
Aura® System Manager 6.3

Last Logged in as January 30, 2015 8:23 AM  
Log off admin

Home: **Routing**

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** [Commit] [Cancel] [Help]

**General**

\* Pattern: 1919  
 \* Min: 4  
 \* Max: 11

Emergency Call: ☐  
 Emergency Priority: 1  
 Emergency Type: SIP Domain: avaya.lab.com  
 Notes:

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item

| Originating Location Name         | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled             | Routing Policy Destination | Routing Policy Notes           |
|-----------------------------------|----------------------------|---------------------|------|-------------------------------------|----------------------------|--------------------------------|
| <input type="checkbox"/> HG ASBCE | HG Avaya SBCE              | To HG CM Trunk 2    | 0    | <input checked="" type="checkbox"/> | HG CM Trunk 2              | Inbound calls to HG CM Trunk 2 |

Select: All, None

The same procedure should be followed to add other required dial patterns, such as: **011** for International calls, **411** for Directory Assistance calls, **911** for Emergency calls, etc.

## 6.8. Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of the Session Manager signaling interface.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields.

- Click **Save** (not shown).

The screen below shows the Session Manager values used for the compliance test.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header shows the Avaya logo and the text "Aura® System Manager 6.3". On the right, it indicates "Last Logged on at January 21, 2014 4:45 PM" and provides links for "Home", "About", "Change Password", and "Log off admin".

The left sidebar contains a navigation menu with the following items: "Session Manager", "Dashboard", "Session Manager", "Administration", "Communication Profile", "Editor", "Network Configuration", "Device and Location", "Configuration", "Application", "Configuration", "System Status", "System Tools", and "Performance".

The main content area is titled "View Session Manager" and includes a "Return" button. Below the title, there is a breadcrumb trail: "Home / Elements / Session Manager / Session Manager Administration".

The configuration is organized into two main sections:

- General**:
  - SIP Entity Name:
  - Description:
  - Management Access Point Host Name/IP:
  - Direct Routing to Endpoints: ☒
  - VMware Virtual Machine: ☐
- Security Module**:
  - SIP Entity IP Address:
  - Network Mask:
  - Default Gateway:
  - Call Control PHB:
  - QoS Priority:
  - Speed & Duplex:
  - VLAN ID:

## 7. Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).

This section describes the required configuration of the Avaya SBCE to connect to Time Warner Cable Business Class SIP Trunking Service.

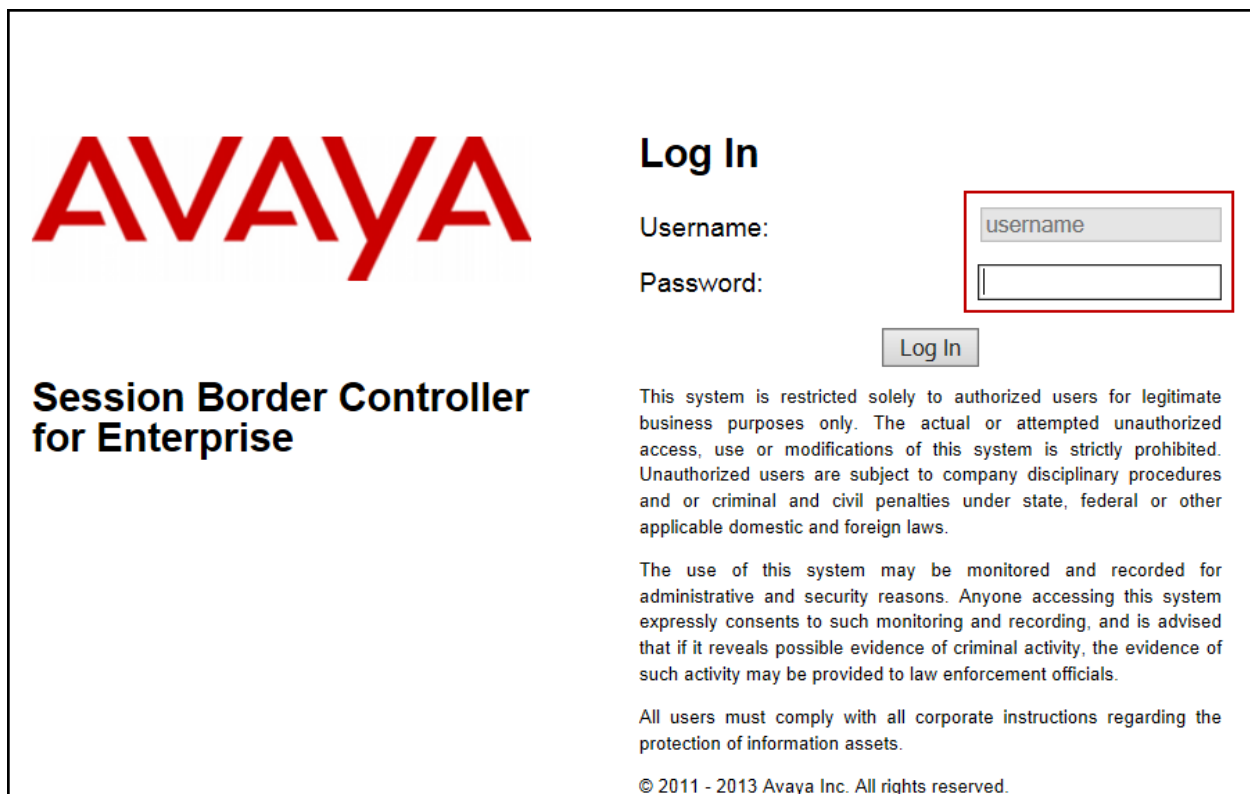
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

**Note:** In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

### 7.1. Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.



**AVAYA**

### Log In

Username:

Password:

**Session Border Controller  
for Enterprise**

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The **Dashboard** main page will appear as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The left sidebar contains a navigation menu with 'Dashboard' highlighted. The main content area is divided into three sections: 'Information', 'Installed Devices', and 'Alarms (past 24 hours)'. The 'Information' section displays system details like time, version, and license state. The 'Installed Devices' section lists 'EMS' and 'Avaya SBCE'. The 'Alarms' section shows a list of incidents, all with the message 'Avaya SBCE: No Server Flow Matched for Incoming Message'.

| Information                  |   |
|------------------------------|---|
| System Time                  | 09:25:34 PM CST <a href="#">Refresh</a> |
| Version                      | 6.3.000-19-4338                         |
| Build Date                   | Fri Sep 26 09:14:23 EDT 2014            |
| License State                | OK                                      |
| Aggregate Licensing Overages | 0                                       |
| Peak Licensing Overage Count | 0                                       |

| Installed Devices |
|-------------------|
| EMS               |
| Avaya SBCE        |

| Alarms (past 24 hours) |
|------------------------|
| None found.            |

| Incidents (past 24 hours)                               |
|---|
| Avaya SBCE: No Server Flow Matched for Incoming Message |
| Avaya SBCE: No Server Flow Matched for Incoming Message |
| Avaya SBCE: No Server Flow Matched for Incoming Message |
| Avaya SBCE: No Server Flow Matched for Incoming Message |
| Avaya SBCE: No Server Flow Matched for Incoming Message |

Notes: No notes found.

To view the system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.

The screenshot shows the 'System Management' page. The left sidebar has 'System Management' highlighted. The main content area has tabs for 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is active, displaying a table of installed devices. The table has columns for Device Name, Management IP, Version, and Status. The device 'Avaya SBCE' is listed with Management IP 172.18.5.70 and Version 6.3.000-19-4338. The status is 'Commissioned'. Action buttons for 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Uninstall' are shown for this device.

| Device Name | Management IP | Version         | Status       |
|-------------|---------------|-----------------|--------------|
| Avaya SBCE  | 172.18.5.70   | 6.3.000-19-4338 | Commissioned |

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

**System Information: Avaya SBCE**

| General Configuration |            | Device Configuration |    | License Allocation    |                                     |
|-----------------------|------------|----------------------|----|-----------------------|-------------------------------------|
| Appliance Name        | Avaya SBCE | HA Mode              | No | Standard Sessions     | 2000                                |
| Box Type              | SIP        | Two Bypass Mode      | No | Advanced Sessions     | 2000                                |
| Deployment Mode       | Proxy      |                      |    | Scopia Video Sessions | 500                                 |
|                       |            |                      |    | Requested: 500        |                                     |
|                       |            |                      |    | Encryption            | <input checked="" type="checkbox"/> |

| Network Configuration |                 |                 |              |           |
|-----------------------|-----------------|-----------------|--------------|-----------|
| IP                    | Public IP       | Netmask         | Gateway      | Interface |
| 172.16.5.71           | 172.16.5.71     | 255.255.255.0   | 172.16.5.254 | A1        |
| 192.168.157.189       | 192.168.157.189 | 255.255.255.192 | .157.129     | B1        |
| [Blurred]             | [Blurred]       | [Blurred]       | [Blurred]    | [Blurred] |
| [Blurred]             | [Blurred]       | [Blurred]       | [Blurred]    | [Blurred] |
| [Blurred]             | [Blurred]       | [Blurred]       | [Blurred]    | [Blurred] |

| DNS Configuration |              | Management IP(s) |           |
|-------------------|--------------|------------------|-----------|
| Primary DNS       | 172.16.5.102 | IP               | [Blurred] |
| Secondary DNS     |              |                  |           |
| DNS Location      | DMZ          |                  |           |
| DNS Client IP     | 172.16.5.71  |                  |           |

On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE, respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to Time Warner Cable. Other IP addresses assigned to these interfaces are used to support other functionalities not discussed in this document, these IP addresses have been blurred out. The management IP has also been blurred out for security reasons.

**IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled “M1”) 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).**



## 7.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

### 7.2.1. Server Interworking - Avaya-SM

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since directly modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or “cloned”. If needed, the profile can then be modified to meet specific requirements for the enterprise SIP-enabled solution. For Time Warner Cable, this profile was left with the **avaya-ru** default values.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** on top right of the screen.

Enter the new profile name in the **Clone Name** field, the name of **Avaya-SM** was chosen in this example. Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Avaya-SM** Server Interworking Profile.

Alarms 1 Incidents Status Logs Diagnostics Users

## Session Border Controller for Enterprise

Dashboard  
Administration  
Backup/Restore  
System Management  
Global Parameters  
Global Profiles  
Domain DoS  
Fingerprint  
Server Interworking  
Phone Interworking  
Media Forking  
Routing  
Server Configuration  
Topology Hiding  
Signaling Manipulation  
URI Groups  
PPM Services  
Domain Policies  
TLS Management  
Device Specific Settings

Interworking Profiles: Avaya-SM

Add

| Interworking Profiles |
|-----------------------|
| ca2100                |
| avaya-nu              |
| OCS-Edge-Server       |
| cisco-cm              |
| cups                  |
| Sipera-Halo           |
| OCS-FrontEnd-Server   |
| Avaya-SM              |
| SP-General            |
| Avaya-CS1000          |
| Avaya-IPD             |
| Avaya-CM              |

Click here to add a description

General Timers URI Manipulation Header Manipulation Advanced

General

|                          |         |
|--------------------------|---------|
| Hold Support             | NONE    |
| 180 Handling             | None    |
| 181 Handling             | None    |
| 182 Handling             | None    |
| 183 Handling             | None    |
| Refer Handling           | No      |
| URI Group                | None    |
| Send Hold                | No      |
| 3xx Handling             | No      |
| Diversion Header Support | No      |
| Delayed SDP Handling     | No      |
| Re-Invite Handling       | No      |
| T.38 Support             | No      |
| URI Scheme               | SIP     |
| Via Header Format        | RFC3261 |

Privacy

|                      |    |
|----------------------|----|
| Privacy Enabled      | No |
| User Name            |    |
| P-Asserted-Identity  | No |
| P-Preferred-Identity | No |
| Privacy Header       |    |

DTMF

|              |      |
|--------------|------|
| DTMF Support | None |
|--------------|------|

Edit

The following screen capture shows the **Advanced** tab of the newly created **Avaya-SM** Server Interworking Profile.

Alarms 1 Incidents Status Logs Diagnostics Users

## Session Border Controller for Enterprise

Dashboard  
Administration  
Backup/Restore  
System Management  
Global Parameters  
Global Profiles  
Domain DoS  
Fingerprint  
Server Interworking  
Phone Interworking  
Media Forking  
Routing  
Server Configuration  
Topology Hiding  
Signaling Manipulation  
URI Groups  
PPM Services  
Domain Policies  
TLS Management  
Device Specific Settings

Interworking Profiles: Avaya-SM

Add

| Interworking Profiles |
|-----------------------|
| ca2105                |
| avaya-fu              |
| OCS-Edge-Server       |
| cisco-com             |
| cupb                  |
| Sigera-Hals           |
| OCS-FrontEnd-Server   |
| <b>Avaya-SM</b>       |
| SP-General            |
| Avaya-CS1000          |
| Avaya-IP0             |
| Avaya-CM              |

Click here to add a description

| General                                 | Timers | URI Manipulation | Header Manipulation | Advanced |
|---|--------|------------------|---------------------|----------|
| Record Routes                           |        |                  |                     | Both     |
| Topology Hiding: Change Call-ID         |        |                  |                     | No       |
| Call-Info NAT                           |        |                  |                     | No       |
| Change Max Forwards                     |        |                  |                     | Yes      |
| Include End Point IP for Context Lookup |        |                  |                     | Yes      |
| OCS Extensions                          |        |                  |                     | No       |
| AVAYA Extensions                        |        |                  |                     | Yes      |
| NORTEL Extensions                       |        |                  |                     | No       |
| Diversion Manipulation                  |        |                  |                     | No       |
| Metaswitch Extensions                   |        |                  |                     | No       |
| Reset on Talk Spurt                     |        |                  |                     | No       |
| Reset SRTP Context on Session Refresh   |        |                  |                     | No       |
| Has Remote SBC                          |        |                  |                     | Yes      |
| Route Response on Via Port              |        |                  |                     | No       |
| Cisco Extensions                        |        |                  | No                  |          |

Edit

### 7.2.2. Server Interworking - SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add** (note that **Add** is being used to create the SP-General profile instead of cloning the avaya-ru profile).

Enter the new profile name, the name of **SP-General** was chosen in this example. Accept the default values for all fields by clicking **Next** and then click **Finish**.

The following screen capture shows the **General** tab of the newly created **SP-General** Server Interworking Profile.

The screenshot displays the 'Session Border Controller for Enterprise' management interface. On the left, a navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), and various sub-profiles. Under 'Global Profiles', 'Server Interworking' is selected, and 'SP-General' is highlighted in the 'Interworking Profiles' list. The main area shows the configuration for 'SP-General' with tabs for General, Timers, URI Manipulation, Header Manipulation, and Advanced. The 'General' tab is active, showing a table of settings.

| General                  |         |
|--------------------------|---------|
| Hold Support             | NONE    |
| 180 Handling             | None    |
| 181 Handling             | None    |
| 182 Handling             | None    |
| 183 Handling             | None    |
| Refer Handling           | No      |
| URI Group                | None    |
| Send Hold                | No      |
| 3xx Handling             | No      |
| Diversion Header Support | No      |
| Delayed SDP Handling     | No      |
| Re-Invite Handling       | No      |
| T.38 Support             | No      |
| URI Scheme               | SIP     |
| Via Header Format        | RFC3261 |

| Privacy              |    |
|----------------------|----|
| Privacy Enabled      | No |
| User Name            |    |
| P-Asserted-Identity  | No |
| P-Preferred-Identity | No |
| Privacy Header       |    |

| DTMF         |      |
|--------------|------|
| DTMF Support | None |

An 'Edit' button is located at the bottom right of the configuration area.

The following screen capture shows the **Advanced** tab of the newly created **SP-General** Server Interworking Profile.

The screenshot displays the 'Session Border Controller for Enterprise' management interface. On the left is a navigation menu with categories like Dashboard, Administration, and System Management. Under 'System Management', 'Global Profiles' is expanded, and 'Server Interworking' is selected. The main area is titled 'Interworking Profiles: SP-General' and features a list of profiles on the left, including 'cs2100', 'avaya-nu', 'OCS-Edge-Server', 'cisco-com', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-CS1000', 'Avaya-IPO', and 'Avaya-CM'. An 'Add' button is present above the list. The right pane shows the configuration for the 'SP-General' profile, with tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (selected). The 'Advanced' tab contains a table of settings:

| Setting                                 | Value |
|---|-------|
| Record Routes                           | Both  |
| Topology Hiding: Change Call-ID         | Yes   |
| Call-info NAT                           | No    |
| Change Max Forwards                     | Yes   |
| Include End Point IP for Context Lookup | No    |
| OCS Extensions                          | No    |
| AVAYA Extensions                        | No    |
| NORTEL Extensions                       | No    |
| Diversion Manipulation                  | No    |
| Metaswitch Extensions                   | No    |
| Reset on Talk Start                     | No    |
| Reset SRTP Context on Session Refresh   | No    |
| Has Remote SBC                          | Yes   |
| Route Response on Via Port              | No    |
| Cisco Extensions                        | No    |

An 'Edit' button is located at the bottom right of the configuration pane.

### 7.2.3. Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name: ***Session Manager***.

On the **Add Server Configuration Profile - General** window:

- **Server Type:** Select ***Call Server***.
- **IP Address / FQDN:** ***172.16.5.32*** (IP Address of Session Manager Security Module).
- **Port:** ***5060*** (This port must match the port number defined in **Section 6.5**).
- **Transports:** Select ***TCP***.
- Click **Next**.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 172.16.5.32       | 5060 | TCP       |

- Click **Next** on the **Authentication** window.
- Click **Next** on the **Heartbeat** window.

On the **Advanced** tab:

- Check **Enable Grooming**.
- Select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

**Add Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya-SM

Signaling Manipulation Script None

Connection Type SUBID

Back Finish

The following screen capture shows the **General** tab of the newly created **Session Manager** profile.

**Session Border Controller for Enterprise**

Alarms 1 Incidents Status Logs Diagnostics Users Settings Help Log Out

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Domain DoS Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups PPM Services Domain Policies TLS Management Device Specific Settings

**Server Configuration: Session Manager**

Add

Session Manager

Service Provider

Com Manager

CS1000

IP Office

General Authentication Heartbeat Advanced

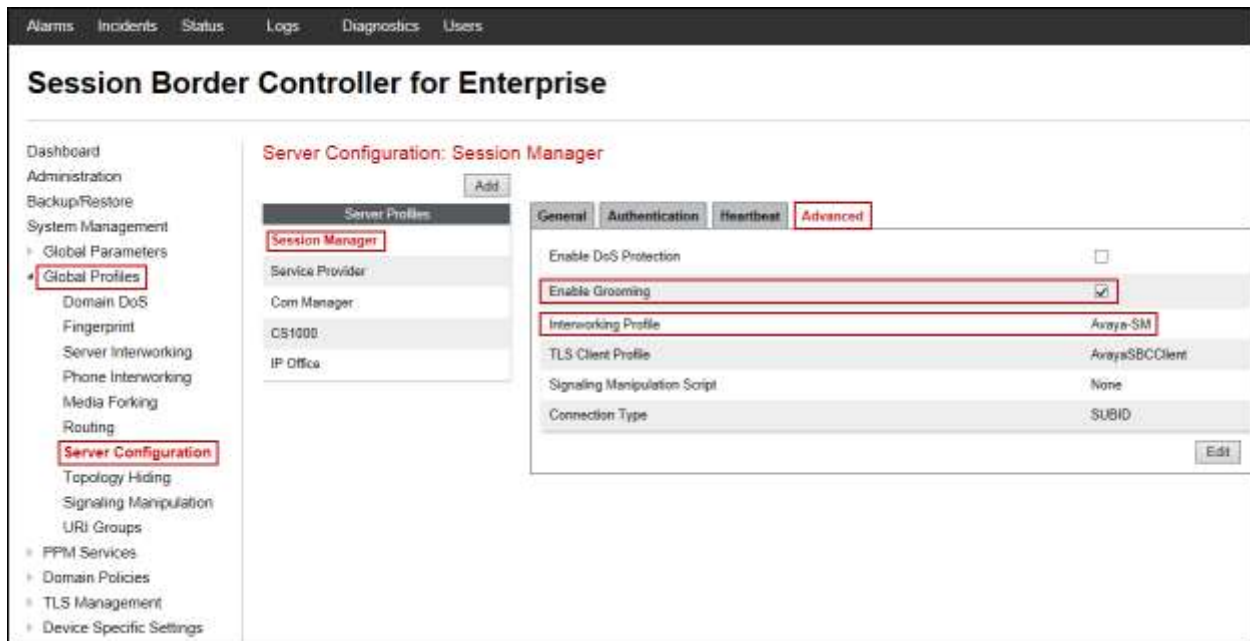
Server Type Call Server

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 172.16.6.32       | 8061 | TLS       |
| 172.16.6.32       | 8060 | TCP       |

Edit

Rename Clone Delete

The following screen capture shows the **Advanced** tab of the newly created **Session Manager** profile.





To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add** in the **Server Profiles** section and enter the profile name: *Service Provider*.

On the **Add Server Configuration Profile - General** window:

- **Server Type:** Select *Trunk Server*.
- **IP Address / FQDN:** *10.10.112.6* (IP Address of the Service Provider SIP Proxy).
- **Port:** *5060*.
- **Transports:** Select *UDP*.
- Click **Next**.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 10.10.112.6       | 5060 | UDP       |

On the **Authentication** tab:

- Check the *Enable Authentication* box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- **Realm:** *10.10.112.6* (IP Address of the Service Provider SIP Proxy).
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

|  |                                     |
|--|-------------------------------------|
| Enable Authentication                                  | <input checked="" type="checkbox"/> |
| User Name  | User123                             |
| Realm<br>(Leave blank to detect from server challenge) | 10.10.112.6                         |
| Password   | *****                               |
| Confirm Password                                       | *****                               |

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, **1800** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
  - **From URI**: Use the **User Name** entered above under the **Authentication** screen (**User123**) and the Public IP address of the Avaya SBCE (**192.168.157.189**), as shown on the screen below.
  - **To URI**: Use the **User Name** entered above under the **Authentication** screen (**User123**) and the Service Provider Proxy IP address (**10.10.112.6**), as shown on the screen below.
- Click **Next**.

The screenshot shows a configuration window titled "Add Server Configuration Profile - Heartbeat". It contains the following fields and values:

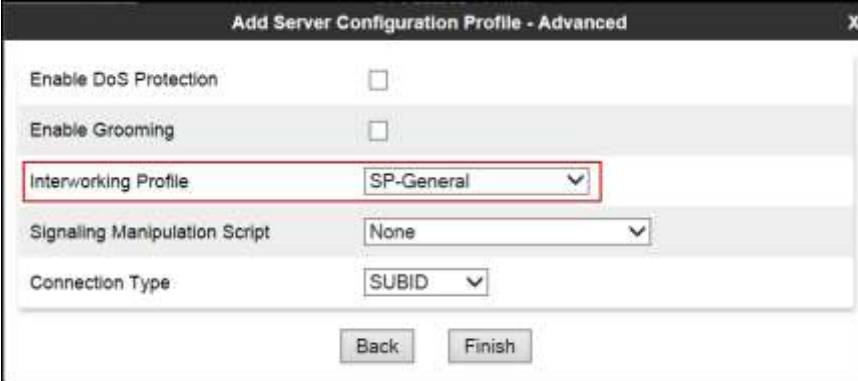
| Field            | Value                               |
|------------------|-------------------------------------|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method           | REGISTER                            |
| Frequency        | 1800 seconds                        |
| From URI         | User123@192.168.1                   |
| To URI           | User123@10.10.112.6                 |

At the bottom of the window are "Back" and "Next" buttons. A red box highlights the "Enable Heartbeat", "Method", "Frequency", "From URI", and "To URI" fields.

In the **Advanced** window:

- Select **SP-General** from the **Interworking Profile** drop down menu.
- Leave other fields with their default values for now, a **Signaling Manipulation Script** will be assigned later.
- Click **Finish**.

The following screen capture shows the **Advanced** tab of the **Service Provider** Server Configuration Profile.



The screenshot displays the 'Add Server Configuration Profile - Advanced' window. It features a list of configuration options with corresponding controls: 'Enable DoS Protection' and 'Enable Grooming' are checkboxes; 'Interworking Profile' is a dropdown menu currently set to 'SP-General'; 'Signaling Manipulation Script' is a dropdown menu currently set to 'None'; and 'Connection Type' is a dropdown menu currently set to 'SUBID'. At the bottom of the window are two buttons: 'Back' and 'Finish'. A red rectangular box highlights the 'Interworking Profile' dropdown menu.

The following screen capture shows the **General** tab of the newly created **Service Provider** Server Configuration Profile.



The following screen capture shows the **Authentication** tab of the newly created **Service Provider** Server Configuration Profile.



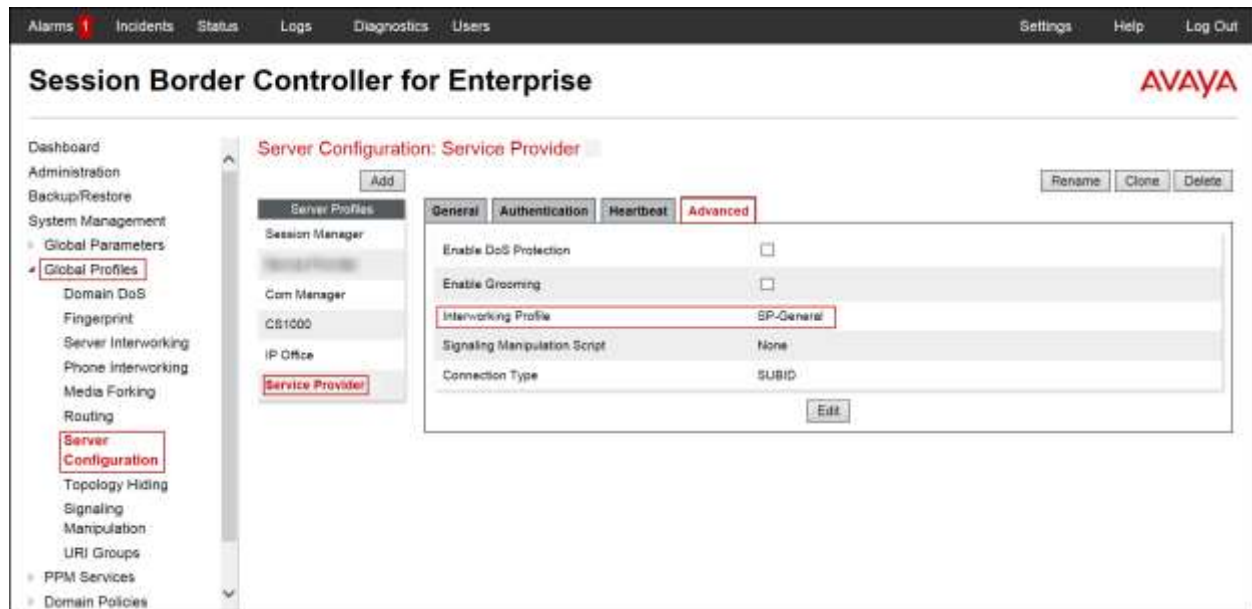
The following screen capture shows the **Heartbeat** tab of the newly created **Service Provider** Server Configuration Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu lists various system management options, with "Global Profiles" and "Server Configuration" highlighted. The main content area is titled "Server Configuration: Service Provider" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this, a tabbed interface shows "General", "Authentication", "Heartbeat", and "Advanced" tabs. The "Heartbeat" tab is active, displaying a configuration table with the following details:

|                  |                                     |
|------------------|-------------------------------------|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method           | REGISTER                            |
| Frequency        | 1800 seconds                        |
| From URI         | User123@192.168.157.188             |
| To URI           | User123@10.10.112.8                 |

An "Edit" button is located at the bottom right of the configuration table.

The following screen capture shows the **Advanced** tab of the newly created **Service Provider** Server Configuration Profile.



## 7.2.4. Routing Profiles

Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing profiles were created, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: *Route\_to\_SM*.
- Click **Next**.

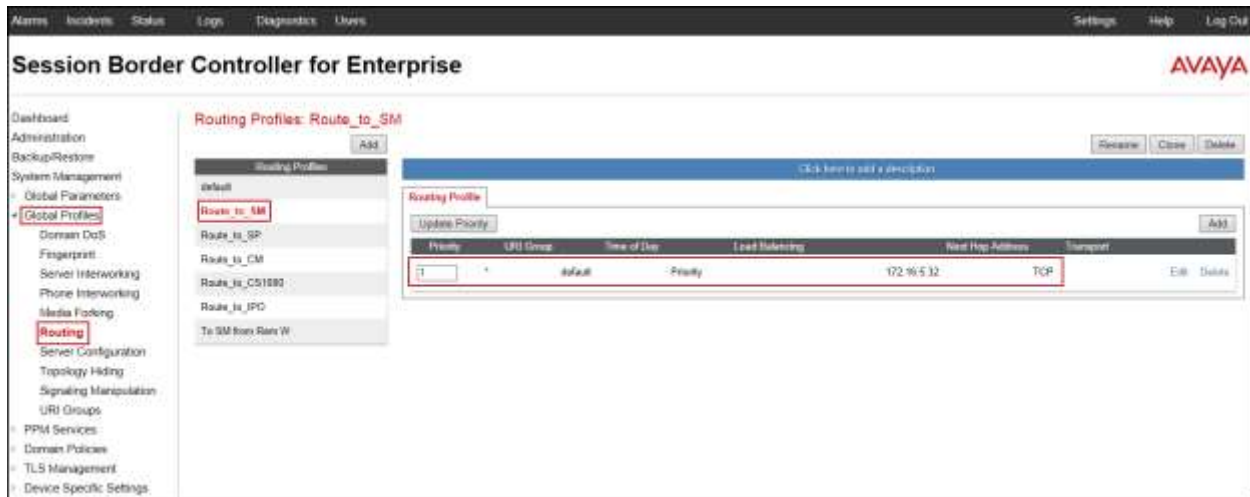
On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select *Session Manager*.
- **Next Hop Address:** Select *172.16.5.32:5060 (TCP)* (Session Manager IP address, Port and Transport).
- Click **Finish**.

| Priority / Weight | Server Configuration | Next Hop Address       | Transport |
|-------------------|----------------------|------------------------|-----------|
| 1                 | Session Manage       | 172.16.5.32:5060 (TCP) | None      |



The following screen shows the newly created **Route\_to\_SM** Profile.



Similarly, for the outbound route:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route\_to\_SP**.
- Click **Next**.

On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Service Provider**.
- **Next Hop Address:** Select **10.10.112.6:5060 (UDP)** (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration screen. The 'URI Group' is set to '\*' and 'Time of Day' is set to 'default'. The 'Load Balancing' is set to 'Priority' and 'NAPTR' is unchecked. The 'Transport' is set to 'None' and 'Next Hop Priority' is checked. The 'Next Hop In-Dialog' is unchecked and 'Ignore Route Header' is unchecked. The 'Add' button is visible. Below the configuration fields, there is a table with columns for Priority / Weight, Server Configuration, Next Hop Address, and Transport. The table contains one row with a priority of 1, Server Configuration of Service Provider, Next Hop Address of 10.10.112.6:5060 (UDP), and Transport of None. The 'Delete' button is visible next to the row. The 'Back' and 'Finish' buttons are at the bottom.

The following screen capture shows the newly created **Route\_to\_SP** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management and configuration options, with 'Global Profiles' and 'Routing' highlighted. The main content area is titled 'Routing Profiles: Route\_to\_SP' and features an 'Add' button. Below this, a list of routing profiles is shown, with 'Route\_to\_SP' selected. The 'Routing Profile' configuration table is visible, showing a single entry with a priority of 1, a URI Group of '\*', a Time of Day of 'default', a Load Balancing of 'Priority', a Next Hop Address of '10.10.112.6', and a Transport of 'UDP'. The table has columns for Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport, with 'Edit' and 'Delete' buttons for each row.

| Priority | URI Group | Time of Day | Load Balancing | Next Hop Address | Transport |
|----------|-----------|-------------|----------------|------------------|-----------|
| 1        | *         | default     | Priority       | 10.10.112.6      | UDP       |

### 7.2.5. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, 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.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: *Session\_Manager***.
- Click **Finish**.

The following screen capture shows the newly added **Session\_Manager** Profile. Note that for Session Manager no values were overwritten (default).

The screenshot displays the Avaya Session Border Controller for Enterprise configuration page. The left sidebar shows the navigation menu with 'Topology Hiding' selected under 'Configuration'. The main content area is titled 'Topology Hiding Profiles: Session\_Manager'. It features a list of profiles on the left, including 'default', 'cisco\_th\_profile', 'Session\_Manager' (highlighted), 'Service\_Provider', 'Com Manager', 'CS1000', and 'IP Office'. An 'Add' button is present above the list. To the right, the 'Session\_Manager' profile is detailed, showing a table of topology hiding rules. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The rules listed are: To (IP/Domain, Auto, ---), Refer-To (IP/Domain, Auto, ---), Record-Route (IP/Domain, Auto, ---), From (IP/Domain, Auto, ---), Request-Line (IP/Domain, Auto, ---), Referred-By (IP/Domain, Auto, ---), Via (IP/Domain, Auto, ---), and SDP (IP/Domain, Auto, ---). An 'Edit' button is located at the bottom of the table.

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

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: Service\_Provider**.
- Click **Finish**.

The following screen capture shows the newly added **Service\_Provider** Profile. Note that for the Service Provider no values were overwritten (default).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu shows the 'Global Profiles' section expanded, with 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: Service\_Provider'. It features a list of profiles on the left, including 'default', 'osco\_th\_profile', 'Session\_Manager', 'Service\_Provider' (highlighted), 'Com Manager', 'CS1000', and 'IP Office'. The 'Service\_Provider' profile is selected, and its configuration is shown in a table. The table has columns for 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table lists several headers: 'To', 'Refer-To', 'Record-Route', 'From', 'Request-Line', 'Referred-By', 'Via', and 'SDP'. Each header has a corresponding 'Criteria' of 'IPDomain' and a 'Replace Action' of 'Auto'. The 'Overwrite Value' column shows a default value of '---' for each header. An 'Add' button is located at the top right of the table, and an 'Edit' button is at the bottom right.

| Header       | Criteria | Replace Action | Overwrite Value |
|--------------|----------|----------------|-----------------|
| To           | IPDomain | Auto           | ---             |
| Refer-To     | IPDomain | Auto           | ---             |
| Record-Route | IPDomain | Auto           | ---             |
| From         | IPDomain | Auto           | ---             |
| Request-Line | IPDomain | Auto           | ---             |
| Referred-By  | IPDomain | Auto           | ---             |
| Via          | IPDomain | Auto           | ---             |
| SDP          | IPDomain | Auto           | ---             |

## 7.2.6. Signaling Manipulation

The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described below.

The Signaling Manipulation Script shown below is needed to remove unwanted headers to prevent them from being sent to the Service provider.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen.

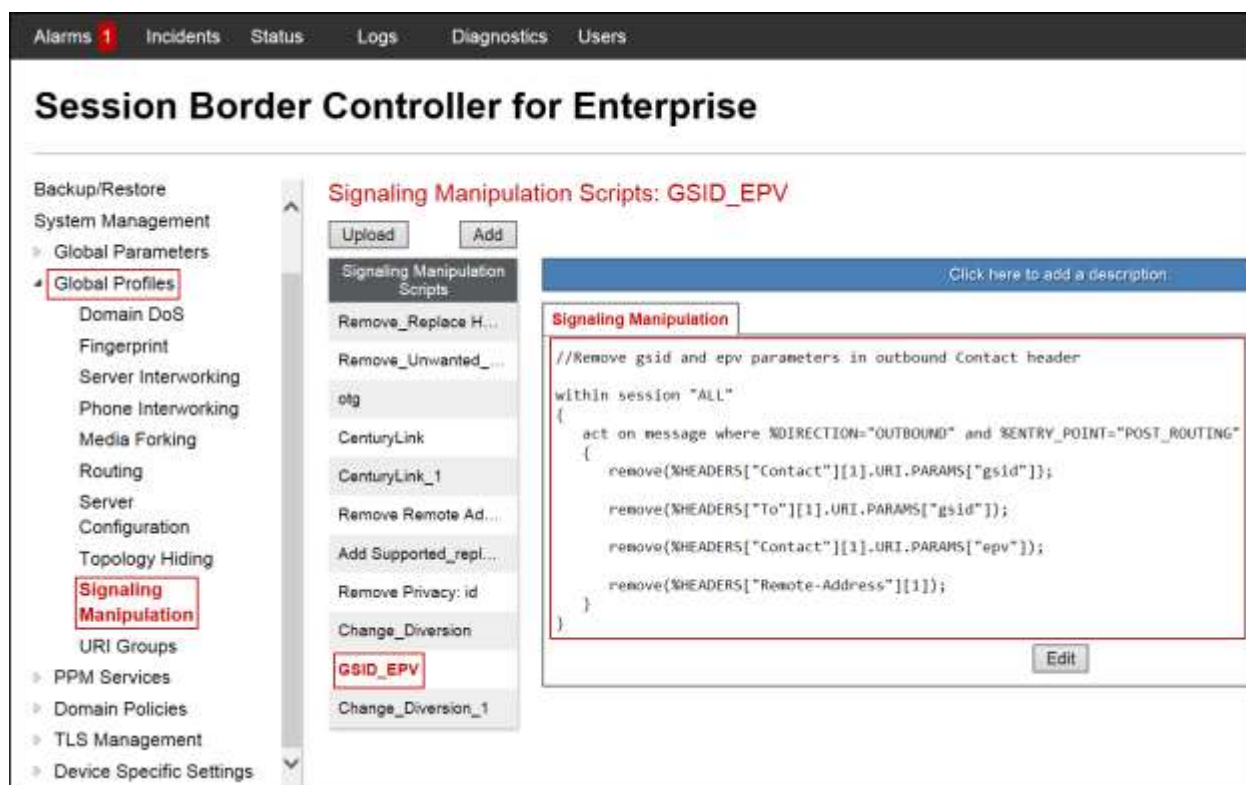
- For **Title** enter a name, the name of *GSID\_EPV* was chosen in this example.
- Enter the script as shown on the screen below (**Note**: The script can be copied from **Appendix A**).
- Click **Save**.

## Signaling Manipulation Editor

Title

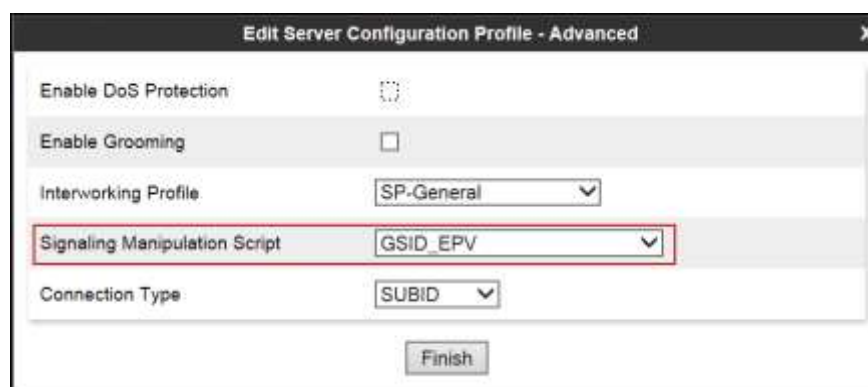
```
1 //Remove gsid and epv parameters in outbound Contact header
2
3 within session "ALL"
4 {
5     act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
6     {
7         remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
8         remove(%HEADERS["To"][1].URI.PARAMS["gsid"]);
9         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
10        remove(%HEADERS["Remote-Address"][1]);
11    }
12 }
13
14
15 }
```

The following screen capture shows the newly added **GSID\_EPV** Signaling Manipulation Script.

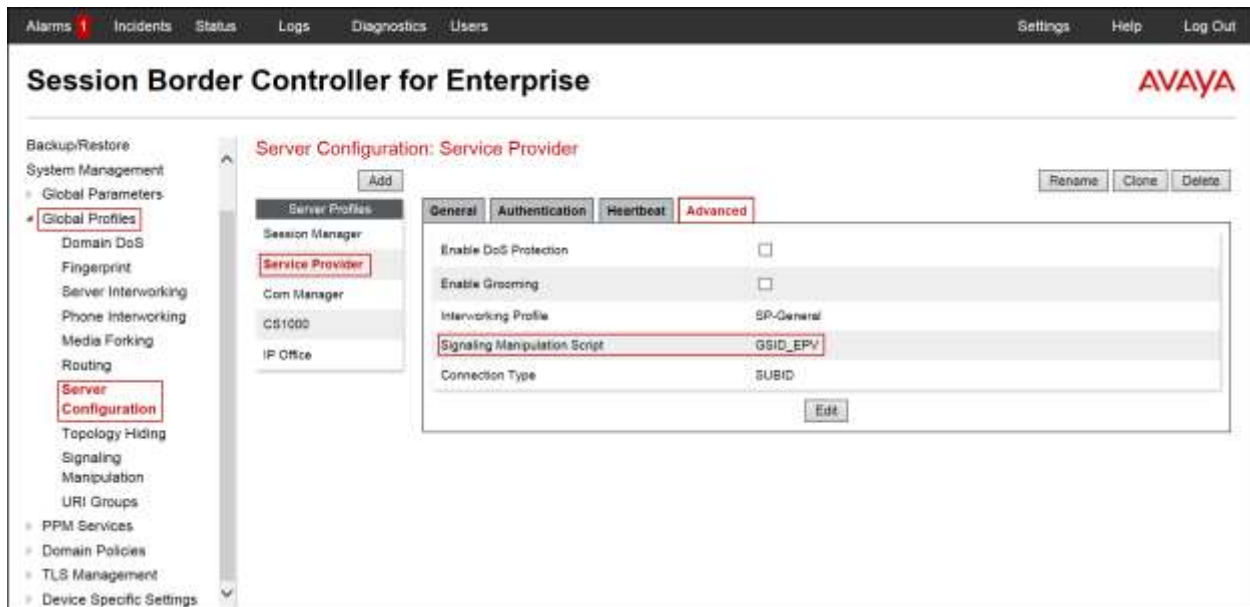


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 7.2.3**.

Go to **Global Profiles** → **Server Configuration** → **Service Provider** → **Advanced** tab → **Edit**. Select **GSID\_EPV** from the drop down menu on the **Signaling Manipulation Script** field. Click **Finish** to save and exit.



The following screen capture shows the **Advanced** tab of the previously added **Service Provider** Server Configuration Profile with the **Signaling Manipulation Script** assigned.





## 7.3. Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

### 7.3.1. Application Rules

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

From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Click on the **Add** button to add a new rule.
- **Rule Name:** enter the name of the profile, e.g., **2000 Sessions**.
- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** was used in the sample configuration.
- Click **Finish**.

| Application Type | In                                  | Out                                 | Maximum Concurrent Sessions | Maximum Sessions Per Endpoint |
|------------------|-------------------------------------|-------------------------------------|-----------------------------|-------------------------------|
| Audio            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2000                        | 2000                          |
| Video            | <input type="checkbox"/>            | <input type="checkbox"/>            |                             |                               |
| IM               | <input type="checkbox"/>            | <input type="checkbox"/>            |                             |                               |

**Miscellaneous**

CDR Support

☒ None  
☐ CDR w/ RTP  
☐ CDR w/o RTP

RTCP Keep-Alive

☐

Back

Finish

The following screen capture shows the newly created **2000 Sessions** Application Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' > 'Application Rules' selected. The main content area is titled 'Application Rules: 2000 Sessions'. It features a list of application rules on the left, with '2000 Sessions' highlighted. The right pane shows the configuration for this rule. It includes a table for 'Application Rule' with columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The 'Audio' row is checked for both In and Out, with values of 2000 for both. The 'Video' and 'IM' rows are unchecked. Below the table is a 'Miscellaneous' section with 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is at the bottom right of the configuration pane.

| Application Type | In                                  | Out                                 | Maximum Concurrent Sessions | Maximum Sessions Per Endpoint |
|------------------|-------------------------------------|-------------------------------------|-----------------------------|-------------------------------|
| Audio            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2000                        | 2000                          |
| Video            | <input type="checkbox"/>            | <input type="checkbox"/>            |                             |                               |
| IM               | <input type="checkbox"/>            | <input type="checkbox"/>            |                             |                               |

| Miscellaneous   |      |
|-----------------|------|
| CDR Support     | None |
| RTCP Keep-Alive | No   |

### 7.3.2. Media Rules

For the compliance test, the existing **default-low-med** Media Rule was used.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' > 'Media Rules' selected. The main content area is titled 'Media Rules: default-low-med'. It features a list of media rules on the left, with 'default-low-med' highlighted. The right pane shows the configuration for this rule. It includes a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below the warning is a tabbed interface with tabs for 'Media NAT', 'Media Encryption', 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FECC'. The 'Media NAT' tab is active, showing a 'Learn Media IP dynamically' checkbox and an 'Edit' button.

### 7.3.3. Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

Headers such as Alert-Info, P-Location, P-Charging-Vector and others are sent in SIP messages from Session Manager to the Avaya SBCE for egress to the Service Provider's network. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both requests and responses for both inbound and outbound calls.

A Signaling Rules were created, to later be applied in the direction of the Enterprise or the Service Provider. To create a rule to block these headers coming from Session Manager from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** in the **Signaling Rules** list.
- Click on **Clone** on top right of the screen.
- Enter a name: *SessMgr\_SigRule*. Click **Finish**.

Select the **Request Headers** tab of the newly created Signaling rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Alert-Info** header:

- Select **Add in Header Control**.
- **Header Name:** *Alert-Info*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Endpoint-View** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *Endpoint-View*.
- **Method Name:** *ALL*.

- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **History-Info** header:

- Select **Add in Header Control**.
- **Header Name:** *History-Info*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-Id*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Charging-Vector** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Charging-Vector*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

The following screen capture shows the **Request Headers** tab of the **SessMgr\_SigRule** Signaling Rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), Time of Day Rules, End Point Policy Groups, Session Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Signaling Rules: SessMgr\_SigRule' and includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a tabbed interface with tabs for 'General', 'Requests', 'Responses', 'Request Headers' (selected), 'Response Headers', 'Signaling QoS', and 'UCID'. The 'Request Headers' tab displays a table with columns: Row, Header Name, Method Name, Header Criteria, Action, Proprietary, and Direction. The table contains 7 rows of data, all with 'Remove Header' as the action and 'Forbidden' as the criteria.

| Row | Header Name          | Method Name | Header Criteria | Action        | Proprietary | Direction |
|-----|----------------------|-------------|-----------------|---------------|-------------|-----------|
| 1   | AV-Global-Session-ID | ALL         | Forbidden       | Remove Header | Yes         | IN        |
| 2   | Alert-Info           | ALL         | Forbidden       | Remove Header | No          | IN        |
| 3   | Endpoint-View        | ALL         | Forbidden       | Remove Header | Yes         | IN        |
| 4   | History-Info         | ALL         | Forbidden       | Remove Header | No          | IN        |
| 5   | P-AV-Message-ID      | ALL         | Forbidden       | Remove Header | Yes         | IN        |
| 6   | P-Charging-Vector    | ALL         | Forbidden       | Remove Header | Yes         | IN        |
| 7   | P-Location           | ALL         | Forbidden       | Remove Header | Yes         | IN        |

Select the **Response Headers** tab.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name: AV-Global-Session-ID**.
- **Response Code: 1XX**.
- **Method Name: ALL**.
- **Header Criteria: Forbidden**.
- **Presence Action: Remove Header**.
- Click **Finish**.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name: AV-Global-Session-ID**.
- **Response Code: 200**.
- **Method Name: ALL**.
- **Header Criteria: Forbidden**.
- **Presence Action: Remove Header**.
- Click **Finish**.

To add the **Alert-Info** header:

- Select **Add in Header Control**.
- **Header Name:** *Alert-Info*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Endpoint-View** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *Endpoint-View*.
- **Response Code:** *1XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **Endpoint-View** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *Endpoint-View*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-ID*.
- **Response Code:** *1XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-AV-Message-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-ID*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Charging-Vector** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Charging-Vector*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *1XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

To add the **P-Location** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

The following screen capture shows the **Response Headers** tab of the **SessMgr\_SigRule** Signaling Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Domain Policies' and 'Signaling Rules' highlighted. The main content area is titled 'Signaling Rules: SessMgr\_SigRule' and features a list of rules on the left and a detailed configuration table on the right. The 'Response Headers' tab is selected in the configuration table.

**Signaling Rules: SessMgr\_SigRule**

Filter By Device:  Rename Clone Delete

Click here to add a description:

**General Requests Responses Request Headers Response Headers Signaling QoS UCID**

Add In Header Control Add Out Header Control

| Row | Header Name          | Response Code | Method Name | Header Criteria | Action        | Proprietary | Direction |                      |                        |
|-----|----------------------|---------------|-------------|-----------------|---------------|-------------|-----------|----------------------|------------------------|
| 1   | AV-Global-Session-ID | 1XX           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 2   | AV-Global-Session-ID | 200           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 3   | Alert-Info           | 200           | ALL         | Forbidden       | Remove Header | No          | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 4   | Endpoint-View        | 1XX           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 5   | Endpoint-View        | 200           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 6   | P-AV-Message-ID      | 1XX           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 7   | P-AV-Message-ID      | 200           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 8   | P-Charging-Vector    | 200           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 9   | P-Location           | 1XX           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |
| 10  | P-Location           | 200           | ALL         | Forbidden       | Remove Header | Yes         | IN        | <a href="#">Edit</a> | <a href="#">Delete</a> |



### 7.3.4. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add** in the **Policy Groups** section.

- **Group Name:** *Enterprise*.
- **Application Rule:** *2000 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *default-low-med*.
- **Security Rule:** *default-low*.
- **Signaling Rule:** *SessMgr\_SigRule*.
- Click **Finish**.

| Policy Group     |                 |
|------------------|-----------------|
| Application Rule | 2000 Sessions   |
| Border Rule      | default         |
| Media Rule       | default-low-med |
| Security Rule    | default-low     |
| Signaling Rule   | SessMgr_SigRule |

Back Finish

The following screen capture shows the newly created **Enterprise** End Point Policy Group.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo.

On the left, a sidebar menu lists various configuration areas, with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Enterprise' and features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'CCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-sub...', 'avaya-def-high-server', 'Enterprise', and 'Service Provider'. The 'Enterprise' group is selected.

The right pane shows the configuration for the 'Enterprise' policy group. It includes a 'Filter By Device...' dropdown, 'Rename', 'Clone', and 'Delete' buttons, and a 'Click here to add a description...' link. Below this is a table with columns for Order, Application, Border, Media, Security, and Signaling. The table contains one entry with Order 1, Application '2000 Sessions', Border 'default', Media 'default-low-med', Security 'default-low', and Signaling 'SessMgt\_SigRule'. An 'Edit' button is next to the entry.

| Order | Application   | Border  | Media           | Security    | Signaling       |
|-------|---------------|---------|-----------------|-------------|-----------------|
| 1     | 2000 Sessions | default | default-low-med | default-low | SessMgt_SigRule |

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add** in the **Policy Groups** section.

- **Group Name:** *Service Provider.*
- **Application Rule:** *2000 Sessions.*
- **Border Rule:** *default.*
- **Media Rule:** *default-low-med.*
- **Security Rule:** *default-low.*
- **Signaling Rule:** *default.*
- Click **Finish**.

The following screen capture shows the newly created **Service Provider** End Point Policy Group.

| Order | Application   | Border  | Media           | Security    | Signaling |
|-------|---------------|---------|-----------------|-------------|-----------|
| 1     | 2000 Sessions | default | default-low-med | default-low | default   |

## 7.4. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

### 7.4.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.



The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under 'Device Specific Settings', 'Network Management' is highlighted. The main content area is titled 'Network Management: Avaya SBCE' and features two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active, showing a table with the following data:

| Name       | Gateway         | Subnet Mask   | Interface | IP Address      | Edit | Delete |
|------------|-----------------|---------------|-----------|-----------------|------|--------|
| Network_A1 | 172.16.5.254    | 255.255.255.0 | A1        | 172.16.5.71     |      |        |
| Network_B1 | 192.168.157.129 | 255.255.255.0 | B1        | 192.168.157.189 |      |        |

In the event that changes need to be made to the network configuration information, they can be entered here.

On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled**, so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The "Device Specific Settings" category is expanded, and "Network Management" is selected. The main content area is titled "Network Management: Avaya SBCE" and features three tabs: "Devices", "Interfaces", and "Networks". The "Interfaces" tab is active, showing a table with the following data:

| Interface Name | VLAN Tag | Status   |
|----------------|----------|----------|
| A1             |          | Enabled  |
| A2             |          | Disabled |
| B1             |          | Enabled  |
| B2             |          | Disabled |

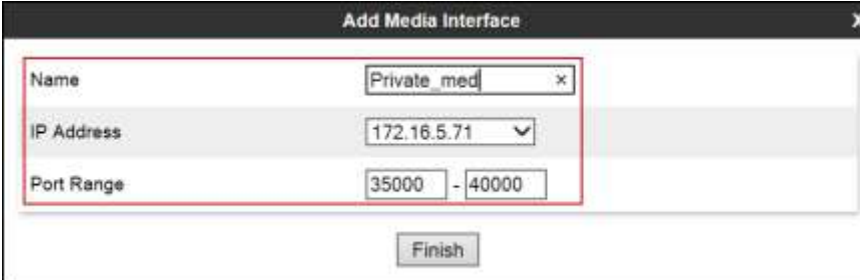
An "Add VLAN" button is located in the top right corner of the interface table.

### 7.4.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range 35000 to 40000 was used.

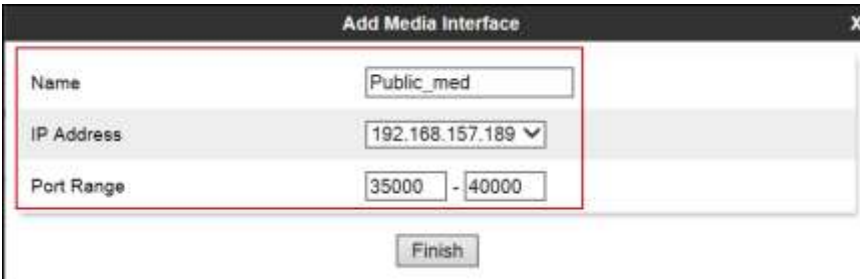
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**.

- Select **Add** in the **Media Interface** area.
- **Name:** *Private\_med*.
- Select **IP Address:** *172.16.5.71* (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Private\_med", "IP Address" with the value "172.16.5.71", and "Port Range" with the value "35000 - 40000". A red rectangular box highlights these three fields. At the bottom center of the dialog is a "Finish" button.

- Select **Add** in the **Media Interface** area.
- **Name:** *Public\_med*.
- Select **IP Address:** *192.168.157.189* (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Public\_med", "IP Address" with the value "192.168.157.189", and "Port Range" with the value "35000 - 40000". A red rectangular box highlights these three fields. At the bottom center of the dialog is a "Finish" button.

The following screen capture shows the newly created Media Interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Device Specific Settings" and "Media Interface" highlighted. The main content area is titled "Media Interface: Avaya SBCE" and contains a sub-menu with "Devices" and "Avaya SBCE". A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is a table of media interfaces with columns for Name, Media IP, Port Range, and actions (Edit, Delete). The table lists two interfaces: "Private\_med" and "Public\_med", both with Media IP 192.168.157.189 and Port Range 35000 - 40000. There are also two disabled interfaces listed below.

| Name         | Media IP        | Port Range    | Edit | Delete |
|--------------|-----------------|---------------|------|--------|
| Private_med  | 192.168.157.189 | 35000 - 40000 | Edit | Delete |
| Public_med   | 192.168.157.189 | 35000 - 40000 | Edit | Delete |
| Disabled_med | 192.168.157.189 | 35000 - 40000 | Edit | Delete |
| Disabled_med | 192.168.157.189 | 35000 - 40000 | Edit | Delete |

### 7.4.3. Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific** menu on the left hand side, select **Signaling Interface**.

- Select **Add** in the **Signaling Interface** area.
- **Name:** *Private\_sig*.
- Select **IP Address:** *172.16.5.71* (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port:** *5060*.
- Click **Finish**.

The screenshot shows a dialog box titled "Add Signaling Interface". It contains the following fields and controls:

- Name:** Text input field containing "Private\_sig".
- IP Address:** Dropdown menu showing "172.16.5.71".
- TCP Port:** Text input field containing "5060". Below it is the hint "Leave blank to disable".
- UDP Port:** Text input field. Below it is the hint "Leave blank to disable".
- TLS Port:** Text input field. Below it is the hint "Leave blank to disable".
- TLS Profile:** Dropdown menu showing "None".
- Enable Shared Control:** Checkable box, currently unchecked.
- Shared Control Port:** Text input field.
- Finish:** Button at the bottom right.

A red rectangular box highlights the "Name", "IP Address", and "TCP Port" fields.



- Select **Add** in the **Signaling Interface** area.
- **Name:** *Public\_sig*.
- Select **IP Address:** *192.168.157.189* (outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** *5060*.
- Click **Finish**.

**Add Signaling Interface**

Name:

IP Address:

TCP Port:

UDP Port:

TLS Port:

TLS Profile:

Enable Shared Control: ☐

Shared Control Port:

**Finish**

The following screen capture shows the newly created Signaling Interfaces.

**Session Border Controller for Enterprise**

Signaling Interface: Avaya SBCE

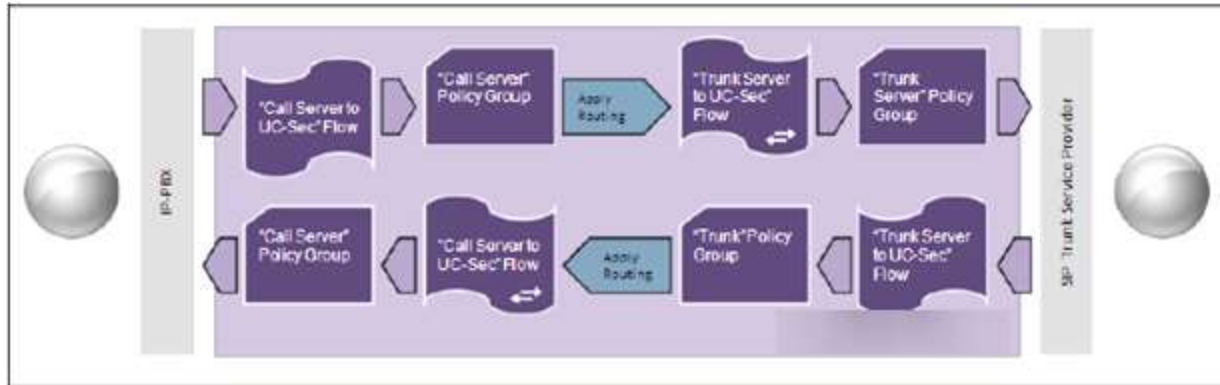
**Signaling Interface**

Modifying or deleting an existing signaling interface will require an application restart before being effect. Application restarts can be issued from [System Management](#)

| Name            | Signaling IP    | TCP Port | UDP Port | TLS Port | TLS Profile |             |
|-----------------|-----------------|----------|----------|----------|-------------|-------------|
| Private_sig     | 172.16.6.71     | 5060     | ---      | ---      | None        | Edit Delete |
| Public_sig      | 192.168.157.189 | ---      | 5060     | ---      | None        | Edit Delete |
| 192.168.157.189 | 192.168.157.189 | ---      | ---      | 5060     | None        | Edit Delete |
| 192.168.157.189 | 192.168.157.189 | ---      | ---      | 5060     | None        | Edit Delete |

#### 7.4.4. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, then the **Server Flows** tab. Click **Add**.

- **Name:** *SIP\_Trunk\_Flow*.
- **Server Configuration:** *Service Provider*.
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** *Private\_sig*.
- **Signaling Interface:** *Public\_sig*.
- **Media Interface:** *Public\_med*.
- **End Point Policy Group:** *Service Provider*.
- **Routing Profile:** *Route\_to\_SM* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Service\_Provider*.
- **File Transfer Profile:** *None*.
- Click **Finish**.

| Field                         | Value            |
|-------------------------------|------------------|
| Flow Name                     | SIP_Trunk_Flow   |
| Server Configuration          | Service Provider |
| URI Group                     | *                |
| Transport                     | *                |
| Remote Subnet                 | *                |
| Received Interface            | Private_sig      |
| Signaling Interface           | Public_sig       |
| Media Interface               | Public_med       |
| End Point Policy Group        | Service Provider |
| Routing Profile               | Route_to_SM      |
| Topology Hiding Profile       | Service_Provider |
| File Transfer Profile         | None             |
| Signaling Manipulation Script | None             |

Finish

To create the call flow toward Session Manager, click **Add**.

- **Name:** *Session\_Manager\_Flow*.
- **Server Configuration:** *Session Manager*.
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** *Public\_sig*.
- **Signaling Interface:** *Private\_sig*.
- **Media Interface:** *Private\_med*.
- **End Point Policy Group:** *Enterprise*.
- **Routing Profile:** *Route\_to\_SP* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Session\_Manager*.
- **File Transfer Profile:** *None*.
- Click **Finish**.

The screenshot shows a window titled "Edit Flow: Session\_Manager\_Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a value or dropdown menu. A red rectangular box highlights the entire configuration area. The fields and their values are:

| Field                         | Value                |
|-------------------------------|----------------------|
| Flow Name                     | Session_Manager_Flow |
| Server Configuration          | Session Manager      |
| URI Group                     | *                    |
| Transport                     | *                    |
| Remote Subnet                 | *                    |
| Received Interface            | Public_sig           |
| Signaling Interface           | Private_sig          |
| Media Interface               | Private_med          |
| End Point Policy Group        | Enterprise           |
| Routing Profile               | Route to SP          |
| Topology Hiding Profile       | Session_Manager      |
| File Transfer Profile         | None                 |
| Signaling Manipulation Script | None                 |

At the bottom center of the window is a button labeled "Finish".

The following screen capture shows the newly created **End Point Flows**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right.

On the left sidebar, the "Device Specific Settings" menu is expanded, showing options like Network Management, Media Interface, Signaling Interface, **End Point Flows** (highlighted), Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, and Troubleshooting.

The main content area is titled "End Point Flows: Avaya SBCE". It features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of configurations. Above the table is a link to "Click here to add a new description" and an "Add" button.

The table is divided into two sections: "Server Configuration: Service Provider" and "Server Configuration: Session Manager".

**Server Configuration: Service Provider**

| Priority | Flow Name      | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |                        |
|----------|----------------|-----------|--------------------|---------------------|------------------------|-----------------|------------------------|
| 1        | SIP_Trunk_Flow | *         | Private_sig        | Public_sig          | Service Provider       | Route_to_SM     | View Clone Edit Delete |

**Server Configuration: Session Manager**

Update

| Priority | Flow Name            | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile |                        |
|----------|----------------------|-----------|--------------------|---------------------|------------------------|-----------------|------------------------|
| 2        | Session_Manager_Flow | *         | Public_sig         | Private_sig         | Enterprise             | Route_to_SP     | View Clone Edit Delete |

## 8. Time Warner Cable Business Class SIP Trunking Service Configuration

To use Time Warner Cable Business Class SIP Trunking service offering, a customer must request the service from Time Warner Cable using the established sales processes. The process can be started by contacting Time Warner Cable via the corporate web site at: <http://business.timewarnercable.com/support/overview.html> or call 866-892-4249.

Time Warner Cable is responsible for the configuration of the SIP Trunk Service. The customer will need to provide the IP address used to reach the Avaya Session Border Controller for Enterprise at the customer's enterprise site. Time Warner Cable will provide the customer the necessary information to configure the SIP trunk connection, including:

- IP address of Time Warner Cable's SIP Proxy server.
- SIP Trunk registration credentials.
- Supported codec's and order of preference.
- DID numbers.
- Etc.

## 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 useful troubleshooting commands that can be used to troubleshoot the solution.

### 9.1.1. 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 with two-way audio 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.

### 9.1.2. Troubleshooting:

#### 9.1.2.1 Communication Manager:

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

#### 9.1.2.2 Session Manager:

- **traceSM -x** – Session Manager command line tool for traffic analysis. Log in to the Session Manager 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, navigate to **Home → Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

### 9.1.2.3 Avaya SBCE:

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:** Provides information about the health of the Avaya SBCE.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) Dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is divided into several sections:

- Information:** A table showing system details.

| Information                  |                              |                         |
|------------------------------|------------------------------|-------------------------|
| System Time                  | 03:40:39 AM CST              | <a href="#">Refresh</a> |
| Version                      | 6.3.000-19-4338              |                         |
| Build Date                   | Fri Sep 26 09:14:23 EDT 2014 |                         |
| License State                | OK                           |                         |
| Aggregate Licensing Overages | 0                            |                         |
| Peak Licensing Overage Count | 0                            |                         |
- Installed Devices:** A table listing connected devices.

| Installed Devices |                                    |
|-------------------|------------------------------------|
| EMS               |                                    |
| Avaya SBCE        | <span style="color: red;">1</span> |
- Alarms (past 24 hours):** A section indicating no alarms were found.
- Incidents (past 24 hours):** A section showing an incident: "Avaya SBCE: Heartbeat Failed, Server is Down".
- Notes:** A section indicating no notes were found.

A left-hand navigation menu lists various configuration options such as Administration, Backup/Restore, System Management, and Device Specific Settings.

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

The screenshot displays the Avaya Alarm Viewer page. The top navigation bar includes the Avaya logo. The main content area is divided into two sections:

- Devices:** A list of devices on the left, including EMS and Avaya SBCE.
- Alarms:** A table showing alarms for the selected device (Avaya SBCE).

| <input checked="" type="checkbox"/> | ID | Details | State | Time | Device |
|-------------------------------------|----|---------|-------|------|--------|
| No alarms found for this device.    |    |         |       |      |        |

Buttons for "Clear Selected" and "Clear All" are located at the bottom of the Alarms section.



**Incidents** : Provides detailed reports of anomalies, errors, policies violations, etc.

**Session Border Controller for Enterprise**

**Dashboard**

**Information**

|                              |                              |                         |
|------------------------------|------------------------------|-------------------------|
| System Time                  | 03:40:39 AM CST              | <a href="#">Refresh</a> |
| Version                      | 6.3.000-19-4338              |                         |
| Build Date                   | Fri Sep 26 09:14:23 EDT 2014 |                         |
| License State                | OK                           |                         |
| Aggregate Licensing Overages | 0                            |                         |
| Peak Licensing Overage Count | 0                            |                         |

**Installed Devices**

|            |   |
|------------|---|
| EMS        |   |
| Avaya SBCE | 1 |

**Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

Avaya SBCE: Heartbeat Failed, Server is Down

[Add](#)

**Notes**

No notes found.

The following screen shows the Incident Viewer page.

**Incident Viewer**

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

Displaying results 0 to 0 out of 0.

| Type                | ID | Date | Time | Category | Device | Cause |
|---------------------|----|------|------|----------|--------|-------|
| No incidents found. |    |      |      |          |        |       |

<< < 1 > >>

**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

**Session Border Controller for Enterprise** AVAYA

**Dashboard**

Administration  
Backup/Restore  
System Management  
Global Parameters  
Global Profiles  
PPM Services  
Domain Policies  
TLS Management  
Device Specific Settings  
Network Management  
Media Interface  
Signaling Interface  
End Point Flows  
Session Flows  
DMZ Services  
TURN/STUN Service  
SNMP  
Syslog Management  
Advanced Options  
Troubleshooting

**Dashboard**

**Information**

|                              |                              |         |
|------------------------------|------------------------------|---------|
| System Time                  | 03:40:39 AM CST              | Refresh |
| Version                      | 6.3.000-19-4338              |         |
| Build Date                   | Fri Sep 26 09:14:23 EDT 2014 |         |
| License State                | OK                           |         |
| Aggregate Licensing Overages | 0                            |         |
| Peak Licensing Overage Count | 0                            |         |

**Installed Devices**

|            |
|------------|
| EMS        |
| Avaya SBCE |

**Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

Avaya SBCE: Heartbeat Failed, Server is Down

**Notes**

No notes found.

Add

The following screen shows the Diagnostics page.

**Diagnostics** AVAYA

**Devices**

Avaya SBCE

**Full Diagnostic** **Ping Test** Application Protocol

Source Device / IP: int| 192.168.157.189

Destination IP:

Ping

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**.

The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand sidebar lists various configuration categories, with "Device Specific Settings" expanded to show "Troubleshooting" and "Trace" selected. The main content area is titled "Trace: Avaya SBCE" and features three tabs: "Call Trace", "Packet Capture" (which is active), and "Captures". Below the tabs is a "Packet Capture Configuration" form with the following fields: "Status" (Ready), "Interface" (Any), "Local Address" (All), "Remote Address" (\*), "Protocol" (All), "Maximum Number of Packets to Capture" (10000), and "Capture Filename" (Test\_1.pcap). "Start Capture" and "Clear" buttons are located at the bottom right of the form.

| Packet Capture Configuration  |             |
|---|-------------|
| Status  | Ready       |
| Interface   | Any         |
| Local Address<br>(IP Port)  | All         |
| Remote Address<br>(IP Port, IP Port)  | *           |
| Protocol  | All         |
| Maximum Number of Packets to Capture  | 10000       |
| Capture Filename<br><small>Using the name of an existing capture will overwrite it.</small> | Test_1.pcap |

Once the capture is stopped, click on 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.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with "Device Specific Settings" and "Troubleshooting" expanded. Under "Troubleshooting", the "Trace" option is selected. The main content area is titled "Trace: Avaya SBCE" and features three tabs: "Call Trace", "Packet Capture", and "Captures". The "Captures" tab is active, showing a table of captured files. The table has columns for "File Name", "File Size (bytes)", and "Last Modified". A single entry is listed: "Test\_1\_20160114034138.pcap" with a size of 450,560 bytes and a timestamp of January 14, 2015 3:42:09 AM CST. A "Refresh" button is located to the right of the table. A "Delete" link is visible at the end of the row.

| File Name                  | File Size (bytes) | Last Modified                   |
|----------------------------|-------------------|---------------------------------|
| Test_1_20160114034138.pcap | 450,560           | January 14, 2015 3:42:09 AM CST |

## 10.Conclusion

These Application Notes describe the procedures necessary for configuring Time Warner Cable Business Class SIP Trunking service with Avaya Aura® Communication Manager Release 6.3, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

## 11.References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya Aura® Communication Manager, including the following, is available at: <http://support.avaya.com/>

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3.4, Issue 2, July 2014.
- [2] *Administering Avaya Aura® Communication Manager*, Release 6.3 03-300509, Issue 10, June 2014.

Product documentation for Avaya Aura® System Manager, including the following, is available at: <http://support.avaya.com/>

- [3] *Administering Avaya Aura® System Manager for Release 6.3.9*, Release 6.3, Issue 5, October 2014.

Product documentation for Avaya Aura® Session Manager, including the following, is available at: <http://support.avaya.com/>

- [4] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014.

Product documentation for the Avaya Session Border Controller for Enterprise, including the following, is available at: <http://support.avaya.com/>

- [5] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [6] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.

Product documentation for Avaya one-X® Communicator and Avaya Communicator for Windows, including the following, is available at: <http://support.avaya.com/>

- [7] *Administering Avaya one-X® Communicator*, Release 6.2 FP4, October 2014.
- [8] *Avaya one-X® Communicator Overview and Planning*, Release 6.2 FP4, October 2014
- [9] *Using Avaya Communicator for Windows*, Release 2.1, Document Number: 18-604158, Issue 3, December 2014.
- [10] *Administering Avaya Communicator for Android, iPad, iPhone, and Windows*, Release 2.1, Issue 1, December 2014.

Product documentation for Remote Worker configuration is available at the following link:

- [11] *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 1.0*  
<https://downloads.avaya.com/css/P8/documents/100183254>

Other resources:

- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*,  
<http://www.ietf.org/>

## 12. Appendix A: SigMa Script

The following Signaling Manipulation script was used in the configuration of the Avaya SBCE, **Section 7.2.6:**

**Title: GSID\_EPV**

```
//Remove gsid and epv parameters in outbound Contact header
```

```
within session "ALL"
```

```
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);

    remove(%HEADERS["To"][1].URI.PARAMS["gsid"]);

    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

    remove(%HEADERS["Remote-Address"][1]);
  }
}
```



**©2015 Avaya Inc. All Rights Reserved.**

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

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