

**Spectrum Enterprise SIP Trunking Service
Avaya Aura® Communication Manager Rel. 6.3,
Avaya Aura® Session Manager Rel. 6.3 and
Avaya Session Border Controller for Enterprise Rel. 6.2.1
IP PBX Configuration Guide**

About Spectrum Enterprise:

Spectrum Enterprise is a division of Charter Communications following a merger with Time Warner Cable and acquisition of Bright House Networks. Spectrum Enterprise is a national provider of scalable, fiber technology solutions. The Spectrum Enterprise portfolio includes networking and managed services solutions, including Internet access, Ethernet and Managed Network Services, Voice, TV and Cloud solutions. Our industry-leading team of experts works closely with clients to achieve greater business success.

About this document:

Spectrum Enterprise assures IP PBX compatibility by conducting interoperability testing to ensure any potential compatibility issues have been resolved prior to installation. Please review the IP PBX configuration instructions in this guide prior to your installation date.

Be advised that this document may contain references to Charter or Charter Business. All references to Charter should be read as Spectrum Enterprise.

Thank you,

Spectrum Enterprise



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. 6.2.1 to support Charter Communications SIP Trunking Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk 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. 6.2.1, to interoperate with Charter Communications 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.

Charter Communications SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Charter Communications 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	7
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Licensing and Capacity	12
5.2.	System Features.....	13
5.3.	IP Node Names.....	14
5.4.	Codecs	15
5.5.	IP Network Region.....	17
5.6.	Signaling Group	18
5.7.	Trunk Group.....	20
5.8.	Calling Party Information.....	23
5.9.	Inbound Routing.....	24
5.10.	Outbound Routing	25
6.	Configure Avaya Aura® Session Manager	28
6.1.	System Manager Login and Navigation.....	29
6.2.	Specify SIP Domain	30
6.3.	Add Location.....	31
6.4.	SIP Entities	34
6.5.	Entity Links	38
6.6.	Routing Policies	41
6.7.	Dial Patterns	42
6.8.	Add/View Avaya Aura® Session Manager	45
7.	Configure Avaya Session Border Controller for Enterprise (Avaya SBCE).....	47
7.1.	Log in Avaya SBCE.....	47
7.2.	Global Profiles.....	50
7.2.1.	Server Interworking - Avaya-SM	50
7.2.2.	Server Interworking - SP-General	53
7.2.3.	Routing Profiles	55
7.2.4.	Server Configuration.....	59
7.2.5.	Topology Hiding.....	69
7.2.6.	Signaling Manipulation.....	72
7.3.	Domain Policies	75
7.3.1.	Create Application Rules	75
7.3.2.	Media Rules	76
7.3.3.	Signaling Rules	77
7.3.4.	End Point Policy Groups.....	82

7.4.	Device Specific Settings.....	85
7.4.1.	Network Management.....	85
7.4.2.	Media Interface	87
7.4.3.	Signaling Interface	89
7.4.4.	End Point Flows.....	91
8.	Charter SIP Trunking Service Configuration	95
9.	Verification and Troubleshooting	96
9.1.1.	Verification Steps:	96
9.1.2.	Troubleshooting:.....	96
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) trunk service between Charter Communications 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. 6.2.1 (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 Charter Communications 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”, “Charter” or “Charter Communications” 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 Charter 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 Charter. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x0 Series IP Telephones (H.323 and SIP), Avaya 96x1 Series IP Telephones (H.323 and SIP), Avaya 2420 Digital Telephones, Avaya one-X® Communicator (H.323 and SIP), analog telephones.

- Outgoing calls to the PSTN were routed via Charter'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 Flare® Experience 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 to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711MU (Charter supported audio codec).
- No matching codecs.
- Voicemail and DTMF tone support (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 Call Transfers.
- 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 Error! Reference source not found. **Error! Reference source not found..**

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 Charter.
- Inbound toll-free calls and 911 emergency 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 (UI) was not tested.
- T.38 fax is not supported by Charter; 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 Charter SIP Trunking service with an Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **Call Display on Transferred Calls to PSTN:** Caller ID display is not updated on PSTN phones involved with call transfers from Communication Manager to the PSTN. After the call transfer is completed, the PSTN phone does not display the actual connected party but instead shows the ID of the host station that initiated the call transfer. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Charter solution. It is listed here simply as an observation.
- **No matching codec on outbound calls:** If an unsupported audio codec is received by Charter on the SIP Trunk (e.g., 722), Charter will respond with “404 Not Found” instead of “488 Not Acceptable Here”, the user will hear re-order. This issue does not have any user impact, it is listed here simply as an observation.
- **Calls from the PSTN to busy DID numbers assigned to Communication Manager stations (users):** Any time a DID number assigned to a Communication Manager station is busy (talking) with a PSTN station/user, Charter will send “INFO” instead of “INVITE” messages to Communication Manager when other PSTN stations/users attempt to call the busy DID number. Embedded within the “INFO” message body is the message: “Play tone CallwaitingTone1”. The PSTN stations/users attempting to call the busy DID number will here ring-back tone for 2+ minutes, the Communication Manager station (user) is never alerted of additional calls coming in from the PSTN (the Communication Manager phone does NOT ring). The Communication Manager stations were configured with multiple call appearances and are able to receive additional calls on any idle call appearance. Communication Manager expects to receive “INVITE” messages to complete additional calls to idle call appearances. This behavior is only seen when the Communication Manager stations are busy talking with PSTN stations/users, if the Communication Manager stations are busy talking with other Communication Manager stations (internal call within Communication Manager), this behavior does not occur. This issue was reported to Charter and is being investigated by Charter.
- **Outbound Calling Party Number (CPN) Blocking:** To support user privacy on outbound calls (calling party number blocking), when enabled by the Communication Manager user, Communication Manager sends “anonymous” as the calling number in the SIP “From” header and includes “Privacy: id” in the INVITE message. During the compliance test, Charter’s network responded with “404 Not Found” to outbound calls with privacy enabled on Communication Manager endpoints, resulting on the call failing to complete.
- **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 calls types, such as Local Directory Assistance Calls (e.g. 411 in the U.S.), 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**).

- **Release of resources after one of the PSTN users hangs-up:** Certain calls to the PSTN, such as calls from the PSTN to a Communication Manager station that are transferred back to the PSTN (blind or consultative transfers), are not disconnected/released immediately after **one** of the PSTN parties hangs-up the call (goes on-hook), while the other PSTN party remains off-hook/connected. If one of the PSTN parties hangs-up the call (goes on-hook), while the other PSTN party remains connected/off-hook, the call on the PSTN station that remains connected/off-hook and the SIP trunk resources involved in the call are not released for a period of approximately 32 seconds. SIP trunk resources are released by Communication Manager after approximately 32 seconds. The call on the PSTN station that remains connected/off-hook is also released after 32 seconds. The reason for the delay is that Charter does NOT send a BYE message to Communication Manager after one of the PSTN parties hangs-up the call (goes on-hook). If **both** PSTN parties hang-up at the **same time**, Charter sends a BYE message to Communication Manager, resulting in Communication Manager releasing the SIP trunk resources involved in the call. The call on the PSTN station that remains connected/off-hook is also released. This issue was reported to Charter and is being investigated by Charter.
- **The “diversion-inhibited” field added by Communication Manager:** The “diversion-inhibited” field added by Communication Manager to the Diversion Headers included in INVITE messages, was causing Charter to reject calls being re-directed to the PSTN with a “404 Not Found” response (e.g., call transfers to the PSTN, twinning to Mobile station (EC500), etc.). A SigMa script was created on the Avaya SBCE to remove this field from the Diversion Header included in INVITE messages before forwarding to Charter.

2.3. Support

For support on Charter Communications systems visit the corporate Web page at: <https://www.charterbusiness.com/> or call 800-314-7195.

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 Charter 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 (H.323 and SIP)
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Flare® Experience 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 Charter 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.

For security reasons, any actual public IP addresses used in the configuration have been masked. Similarly, any references to real routable PSTN numbers have also been either masked or digits have been blurred out.

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 Charter's network.

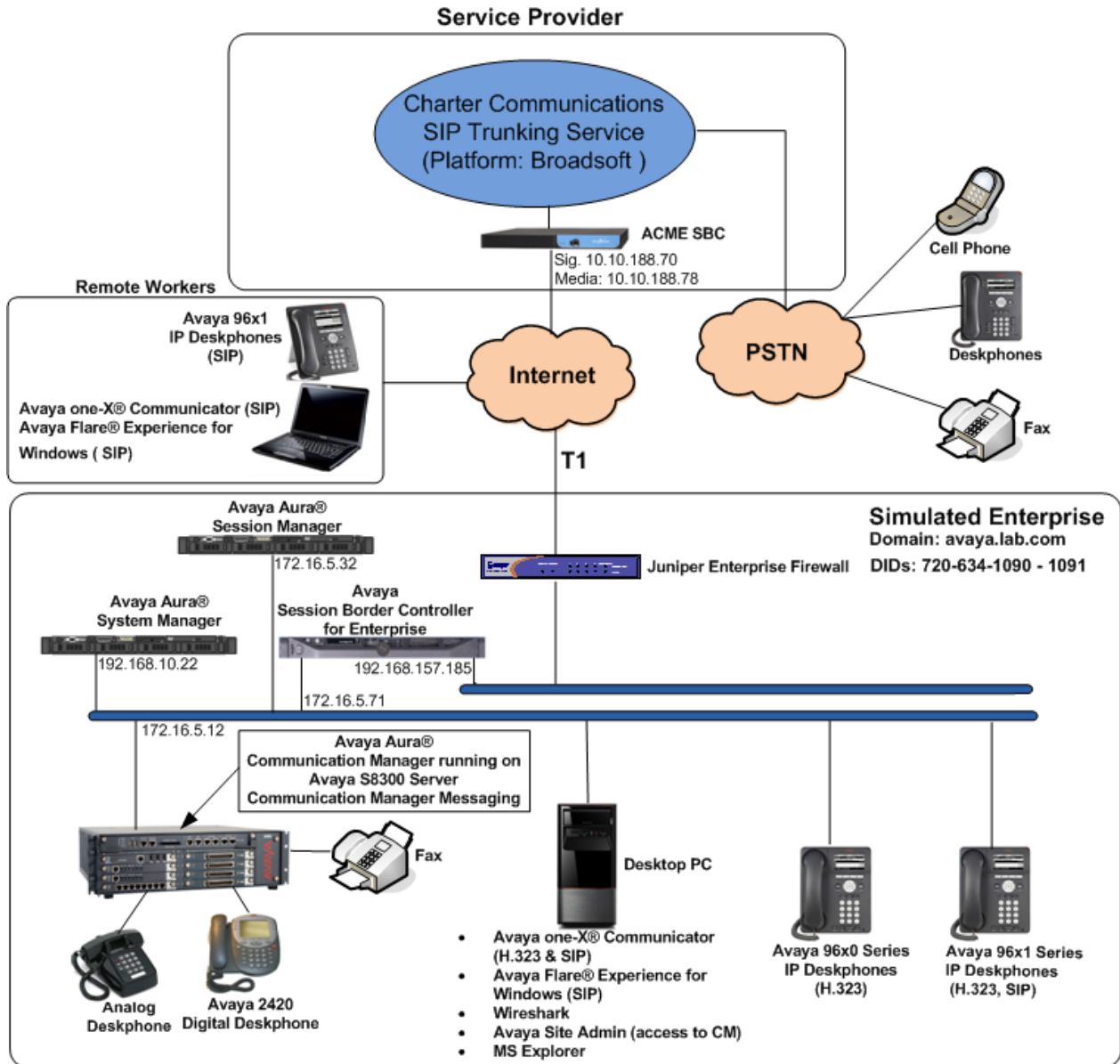


Figure 1: Avaya SIP-enabled Enterprise Solution and Charter SIP Trunking Service

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on an Avaya S8300 Server.	6.3.7.1 (Service Pack 6.3.7.1) (03.0.124.0-21895)
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.9 (Service Pack 9) (6.3.9.0.639011)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.9 (Service Pack 9) Build No. 6.3.0.8.5682-6.3.8.4414 Software Update Rev. No. 6.3.9.1.2482
G450 Gateway	35.8.0
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.1.Q18
Avaya Aura® Integrated Management Site Administrator	6.0.07
Avaya Aura® Communication Manager Messaging (CMM)	CMM 6.3 (Service Pack 4) (03.0.124.0-0402)
Avaya one-X® Communicator (SIP & H.323)	6.2.4.07-FP4
Avaya Flare® Experience for Windows (SIP)	1.1.4.23
Avaya 96x0 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition Version S3.220A
Avaya 96x1 Series IP Deskphones (H.323)	Avaya one-X® Deskphone H.323 Version 6.4014
Avaya 96x1 Series IP Deskphones (SIP)	Avaya one-X® Deskphone SIP Version 6.4.0.33
Avaya 2420 Series Digital Deskphones	--
Lucent Analog Deskphones	--
Charter Communications	
Broadworks Broadsoft Application Server	R17 SP4
ACME Packet 4500 Series SBC	nnSCX6.2.0mp

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 Charter. 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.

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 UAL Boards: 10 0
Maximum Media Gateway UAL 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
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
CPN/ANI/ICLID Replacement for Restricted Calls: restricted
CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

DISPLAY TEXT
                                                Identity When Bridging: principal
                                                User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
Local Country Code:       
International Access Code:       

SCCAN PARAMETERS
Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
Caller ID on Call Waiting Delay Timer (msec): 200

```

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
                        IP NODE NAMES

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. Charter 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      Silence      Frames      Packet
Codec      Suppression  Per Pkt    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 Charter).

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

                                IP Codec Set

                                Allow Direct-IP Multimedia? n

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


Use the **change ip-codec-set** command to define a list of codecs to use for telephones within the enterprise. For the compliance test, **ip-codec-set 1** was used for this purpose. Default values can be used for all other fields.

```

change ip-codec-set 1                                     Page 1 of 2

                                IP CODEC SET

Codec Set: 1

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

Media Encryption
1: none
2: _____
3: _____

```

On Page 2, set the Fax Mode to *off*.

```

change ip-codec-set 1                                     Page 2 of 2

                                IP Codec Set

                                Allow Direct-IP Multimedia? n

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

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 rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Video Prio	Intervening Shr	Intervening Regions	Dyn CAC	G A	A G	t c	
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 Charter 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
                                SIGNALING GROUP

Group Number: 2
IMS Enabled? n
Q-SIP? n
IP Video? n
Peer Detection Enabled? y
Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr
Near-end Listen Port: 5070
Far-end Node Name: Lab-HG-SM
Far-end Listen Port: 5070
Far-end Network Region: 2
Far-end Domain: avaya.lab.com
Incoming Dialog Loopbacks: eliminate
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
Enable Layer 3 Test? n
Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? n
IP Audio Hairpinning? n
Alternate Route Timer(sec): 6

```

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
Signalng 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 *private*. 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” and “P-Asserted Identity” headers. The addition of the + sign impacted interoperability with Charter. Thus, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. Default values were used for all other fields.

```
change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                    Maintenance Tests? y

  Numbering Format: private
                                                    UUI Treatment: service-provider
                                                    Replace Restricted Numbers? y
                                                    Replace Unavailable Numbers? y

  Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

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 Charter. Set **Convert 180 to 183 for Early Media** to *y*.

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

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. 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 3042 and 5015. These 10-digit numbers were used for the outbound calling party information on the service provider trunk when calls were originated from these extensions. Note that the DID number to enterprise extension mapping shown below is not complete, Charter only provided two DID numbers for the testing.

change private-numbering 1					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len		
4	3			4	Total Administered: 4 Maximum Entries: 540	
4	5			4		
4	3042	2	7206341090	10		
4	5015	2	7206341091	10		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		
—				—		

In a real customer environment, normally DID numbers are comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with 1 will send the calling party number as the **Private Prefix** plus the extension number. The example shown in the screenshot below is assuming that the local extensions in the DID numbers begin with a 1 (e.g., 7206341xxx).

```
change private-numbering 1 Page 1 of 2
NUMBERING - PRIVATE FORMAT
```

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	3			4	Total Administered: 4 Maximum Entries: 540
4	5			4	
4	1	2	720634	10	

5.9. Inbound Routing

DID numbers received from Charter 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/Feature	Number Len	Number Digits	Del	Insert
public-ntwrk	10	7206341090	10	3042
public-ntwrk	10	7206341091	10	5015
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/Feature	Number Len	Number Digits	Del	Insert
public-ntwrk	10	720634	6	
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 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 HNPA 10 digit numbers are left unchanged.
- **Numbering Format:** *unk-unk* Calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR:** *none*.

change route-pattern 2															Page 1 of 3	
										Pattern Number: 2		Pattern Name: <u>Serv. Provider</u>				
										SCCAN? n		Secure SIP? n				
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts				DCS/ QSIG	IXC				
1:	<u>2</u>	<u>0</u>	<u>1</u>								n	user				
2:											n	user				
3:											n	user				
4:											n	user				
5:											n	user				
6:											n	user				

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

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:

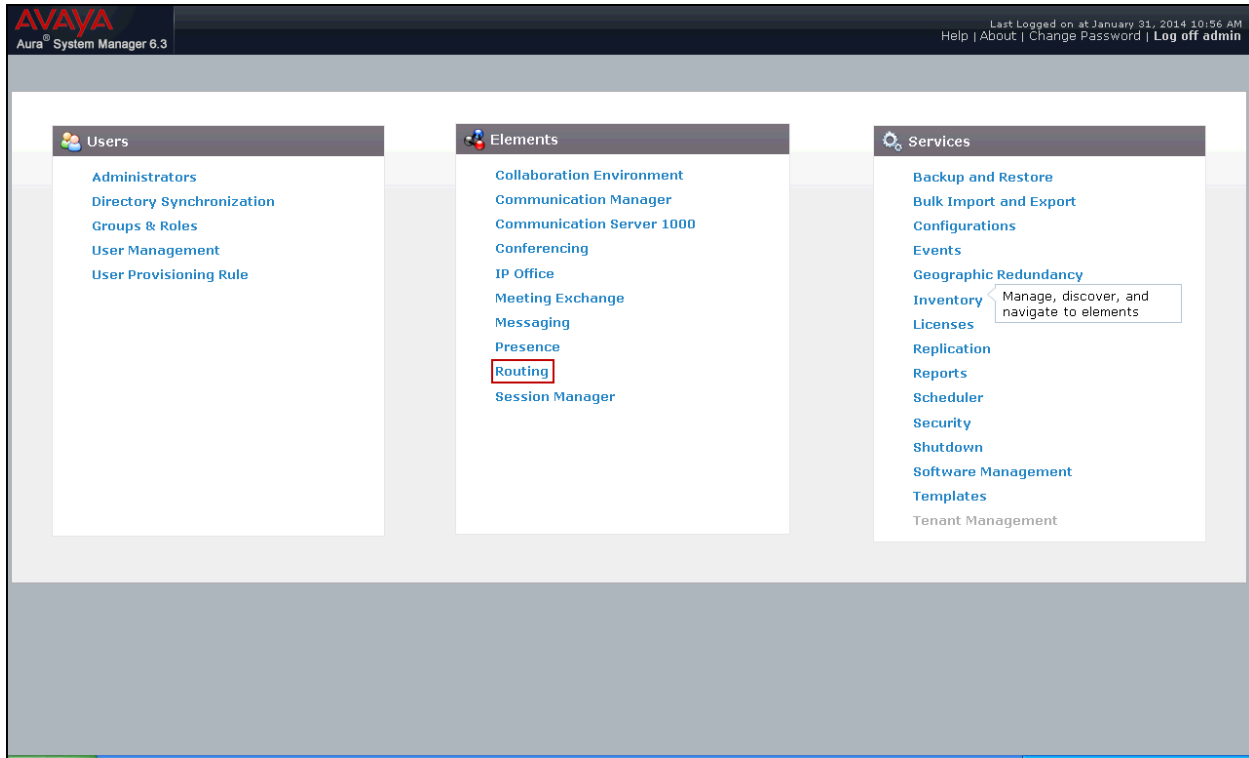
- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager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

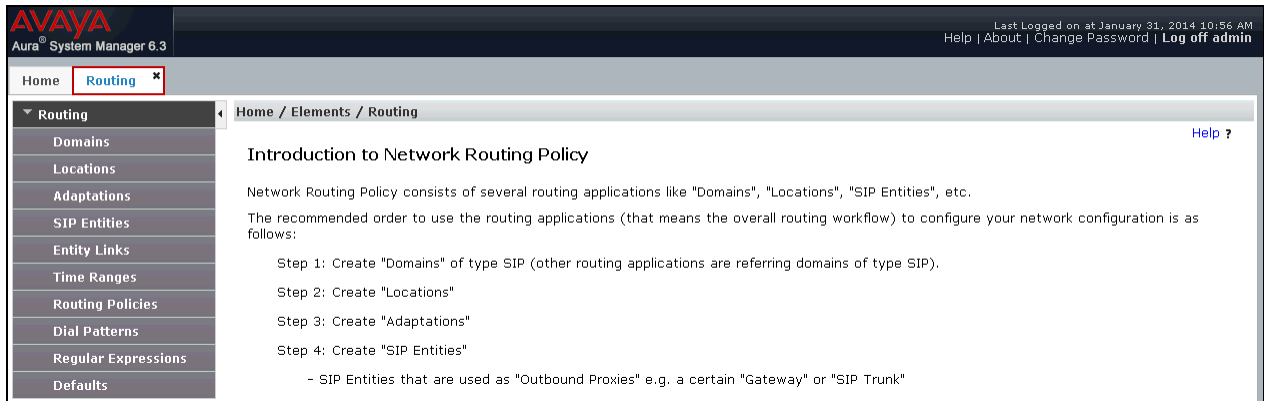
<p>Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity</p>

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.



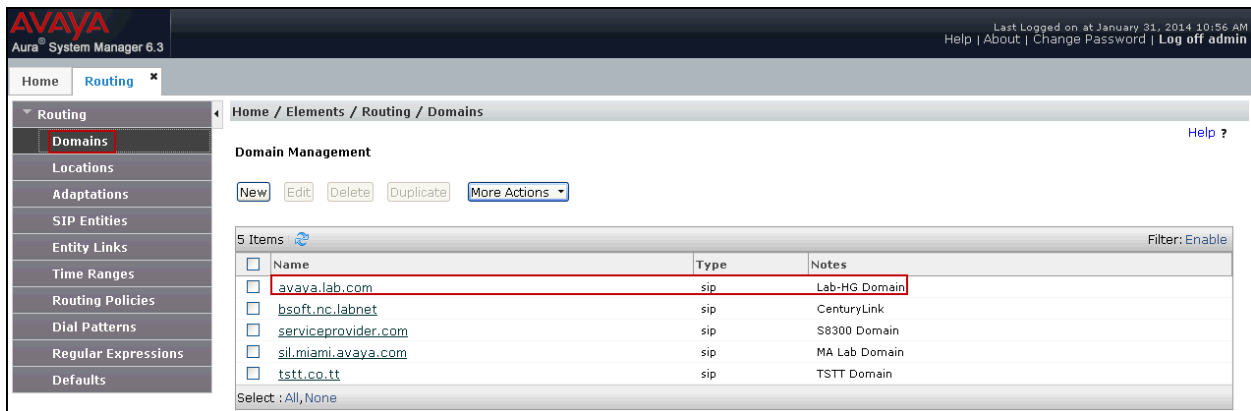
6.2. Specify SIP Domain

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 interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains the following sections:

- Location Details:** Includes 'Commit' and 'Cancel' buttons.
- General:** The 'Name' field is set to 'HG Session Manager' and is highlighted with a red box. The 'Notes' field is empty.
- Dial Plan Transparency in Survivable Mode:** The 'Enabled' checkbox is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty.
- Overall Managed Bandwidth:** The 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec'. The 'Total Bandwidth' and 'Multimedia Bandwidth' fields are empty. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked.
- Per-Call Bandwidth Parameters:** The 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)' fields are set to '1000 Kbit/Sec'. The 'Minimum Multimedia Bandwidth' field is set to '64 Kbit/Sec'. The 'Default Audio Bandwidth' dropdown is set to '80 Kbit/sec'.
- Alarm Threshold:** The 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' dropdowns are both set to '80 %'. The 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' fields are both set to '5 Minutes'.
- Location Pattern:** Includes 'Add' and 'Remove' buttons. Below, there is a table with 0 items, a search icon, and a 'Filter: Enable' button. One item is listed: 'IP Address Pattern' with a 'Notes' column.

At the bottom of the form, there are 'Commit' and 'Cancel' buttons.

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 top navigation bar includes the Avaya logo, the text 'Aura System Manager 6.3', and a user status area indicating 'Last Logged on at January 31, 2014 10:56 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The main interface is titled 'Home / Elements / Routing / Locations' and features a left-hand navigation menu with options like 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'Locations' menu item is highlighted.

The main content area is titled 'Location Details' and contains several sections for configuration:

- General:** Includes a 'Name' field set to 'HG Communication Manager' (highlighted with a red box), a 'Notes' field, and 'Commit' and 'Cancel' buttons.
- Dial Plan Transparency in Survivable Mode:** Features an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' dropdown menu.
- Overall Managed Bandwidth:** Includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.
- Per-Call Bandwidth Parameters:** Contains fields for 'Maximum Multimedia Bandwidth (Intra-Location)' (1000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (1000 Kbit/Sec), '* Minimum Multimedia Bandwidth' (64 Kbit/Sec), and '* Default Audio Bandwidth' (80 Kbit/Sec).
- Alarm Threshold:** Includes 'Overall Alarm Threshold' (80 %), 'Multimedia Alarm Threshold' (80 %), '* Latency before Overall Alarm Trigger' (5 Minutes), and '* Latency before Multimedia Alarm Trigger' (5 Minutes).
- Location Pattern:** Features 'Add' and 'Remove' buttons, a table with 'IP Address Pattern' and 'Notes' columns, and 'Filter: Enable' text.

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

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

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 6.3', and a user status area indicating 'Last Logged on at January 31, 2014 10:56 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The main interface has a left-hand menu with 'Routing' selected, and a sub-menu where 'Locations' is highlighted. The main content area is titled 'Home / Elements / Routing / Locations' and contains the following sections:

- Location Details:** Includes 'General' information with a red box around the '* Name: HG ASBCE' field and a 'Notes: HG Avaya SBCE' field. There are 'Commit' and 'Cancel' buttons at the top right of this section.
- Dial Plan Transparency in Survivable Mode:** Features an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' text box, and an 'Associated CM SIP Entity' dropdown menu.
- Overall Managed Bandwidth:** Includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' text boxes, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.
- Per-Call Bandwidth Parameters:** Contains four fields: 'Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec', 'Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec', '* Minimum Multimedia Bandwidth: 64 Kbit/Sec', and '* Default Audio Bandwidth: 80 Kbit/sec'.
- Alarm Threshold:** Includes 'Overall Alarm Threshold: 80 %', 'Multimedia Alarm Threshold: 80 %', '* Latency before Overall Alarm Trigger: 5 Minutes', and '* Latency before Multimedia Alarm Trigger: 5 Minutes'.
- Location Pattern:** Features 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' option. The table has columns for 'IP Address Pattern' and 'Notes'. 'Commit' and 'Cancel' buttons are at the bottom right.

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 6.3 interface. The breadcrumb navigation shows 'Home / Elements / Routing / SIP Entities'. The left sidebar has 'SIP Entities' selected. The main area is titled 'SIP Entity Details' and contains the following configuration fields:

- 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 main configuration, there is a 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. A 'Port' section includes input fields for 'TCP Failover port' and 'TLS Failover port', with 'Add' and 'Remove' buttons.

A table lists 9 items for SIP Link Monitoring:

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	
5080	TCP	avaya.lab.com	
5081	TCP	avaya.lab.com	
5085	UDP	avaya.lab.com	
5086	TCP	avaya.lab.com	

At the bottom, there is a 'SIP Responses to an OPTIONS Request' section with an empty table (0 items) and 'Add'/'Remove' buttons. The table has columns for 'Response Code & Reason Phrase', 'Mark Entity Up/Down', and 'Notes'. 'Commit' and 'Cancel' buttons are located at the bottom right of the interface.

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 interface. The top navigation bar includes 'Home' and 'Routing'. The left sidebar shows a tree view with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains the following configuration fields:

- Name:** HG CM Trunk 2
- FQDN or IP Address:** 172.16.5.12
- Type:** CM
- Notes:** CM SIP Trunk 2
- Adaptation:** (empty dropdown)
- Location:** HG Communication Manager
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration

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.

The screenshot displays the Avaya Aura System Manager 6.3 interface for configuring a SIP Entity. The left sidebar shows a navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'General' section with the following fields:

- Name:** HG ASBCE
- FQDN or IP Address:** 172.16.5.71
- Type:** Other
- Notes:** HG ASBCE
- Adaptation:** (empty dropdown)
- Location:** HG ASBCE
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty dropdown)
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration

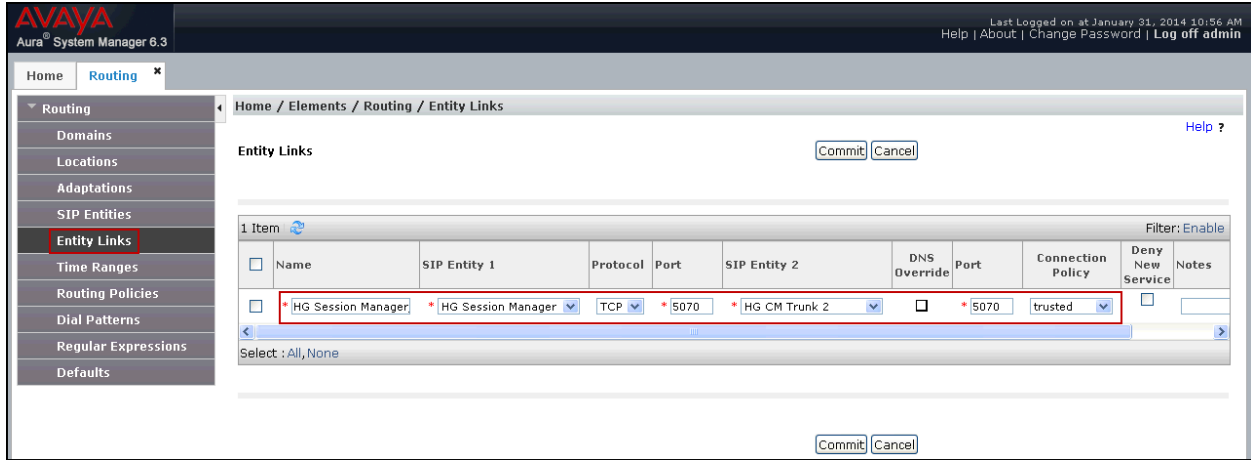
6.5. Entity Links

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:

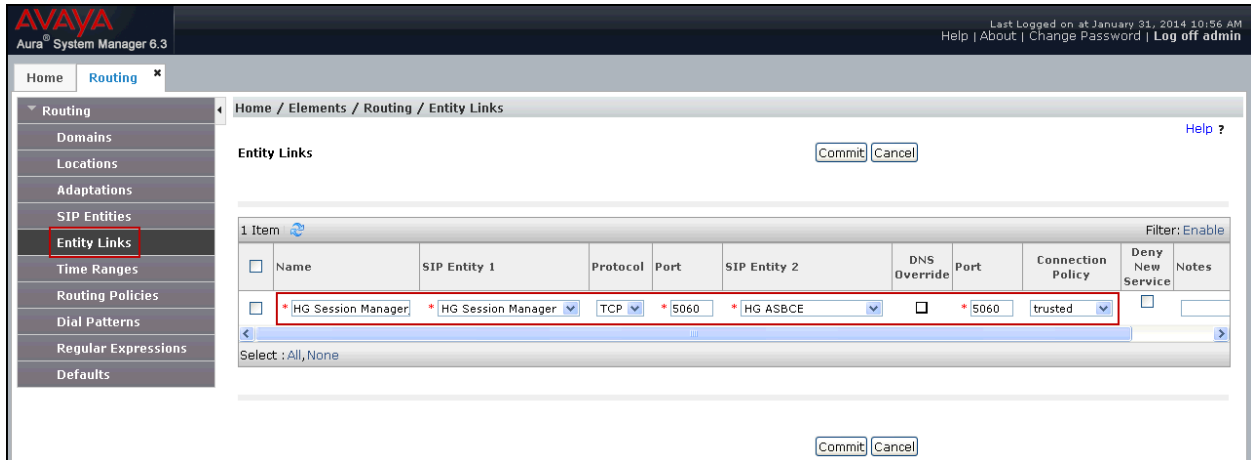
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end 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 following screen shows the entity link to the Avaya SBCE:



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.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with 'Entity Links' highlighted. The main content area shows the 'Entity Links' configuration page with a table of 21 items. The table has the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The following rows are highlighted with red boxes:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
HG Session Manager AAC_5060_TCP	HG Session Manager	TCP	5060	AAC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	AAC Entity Link
HG Session Manager sip1_5060_TCP	HG Session Manager	TCP	5060	Acme Packet sip1	<input type="checkbox"/>	5060	trusted	<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"/>	
HG Session Manager SBC_5060_UDP	HG Session Manager	UDP	5060	EdgeMarc SBC	<input type="checkbox"/>	5060	trusted	<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"/>	
HG Session Manager_HG ASBCE_5060_TCP	HG Session Manager	TCP	5060	HG ASBCE	<input type="checkbox"/>	5060	trusted	<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"/>	
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:

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and user information: 'Last Logged on at January 31, 2014 4:45 PM', 'Help | About | Change Password | Log off admin'. The left sidebar shows a navigation menu with 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (To HG CM Trunk 2), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (Inbound calls to HG CM Trunk 2). The 'SIP Entity as Destination' section has a 'Select' button. Below this is a table with the following data:

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 shows the Avaya Aura System Manager 6.3 interface. The left-hand navigation pane is expanded to 'Routing Policies'. The main content area displays the 'Routing Policy Details' for a policy named 'HG ASBCE'. The 'General' section includes the following fields:

- Name:** To HG ASBCE
- Disabled:**
- Retries:** 0
- Notes:** Outbound calls via ASBCE

Below the 'General' section is the 'SIP Entity as Destination' section with 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 Charter 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.

Dial Pattern Details

General

* Pattern: 1
 * Min: 1
 * Max: 11

Emergency Call:
 Emergency Priority: 1
 Emergency Type:
 SIP Domain: -ALL-
 Notes:

Originating Locations and Routing Policies

6 Items

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	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 EdgeMarc	0	<input checked="" type="checkbox"/>	EdgeMarc 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

The following dial pattern used for the compliance testing was for inbound calls to the enterprise. It uses dial pattern **720** matching the NPA of the DID numbers assigned to the enterprise by Charter. This dial pattern was configured with the destination SIP Domain of **avaya.lab.com**, Originating Location Name **HG ASBCE**, and Routing Policy name **To HG CM Trunk 2**.

The screenshot shows the 'Dial Pattern Details' configuration page in Avaya Aura System Manager 6.3. The 'General' section includes the following fields:

- Pattern:** 720
- Min:** 3
- Max:** 10
- Emergency Call:**
- Emergency Priority:** 1
- Emergency Type:** [Empty]
- SIP Domain:** avaya.lab.com
- Notes:** [Empty]

The 'Originating Locations and Routing Policies' section shows a table with one item:

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

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 side of the header, it indicates "Last Logged on at January 31, 2014 4:45 PM" and provides links for "Help", "About", "Change Password", and "Log off admin".

The main navigation menu on the left includes "Home", "Session Manager", "Dashboard", "Session Manager Administration", "Communication Profile Editor", "Network Configuration", "Device and Location Configuration", "Application Configuration", "System Status", "System Tools", and "Performance".

The current page is titled "View Session Manager" and is located under the path "Home / Elements / Session Manager / Session Manager Administration". A "Return" button is visible in the top right corner of the page content.

The configuration is organized into two sections:

- General:**
 - SIP Entity Name: HG Session Manager
 - Description: Lab-HG SM
 - Management Access Point Host Name/IP: 172.16.5.31
 - Direct Routing to Endpoints: Enable
 - VMware Virtual Machine:
- Security Module:**
 - SIP Entity IP Address: 172.16.5.32
 - Network Mask: 255.255.255.0
 - Default Gateway: 172.16.5.254
 - Call Control PHB: 46
 - QOS Priority: 6
 - Speed & Duplex: Auto
 - VLAN ID: (field is empty)

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

This section describes the required configuration of the Avaya SBCE to connect to Charter's 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: During the next pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it.

7.1. Log in to 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 management IP address of the Avaya SBCE.

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



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

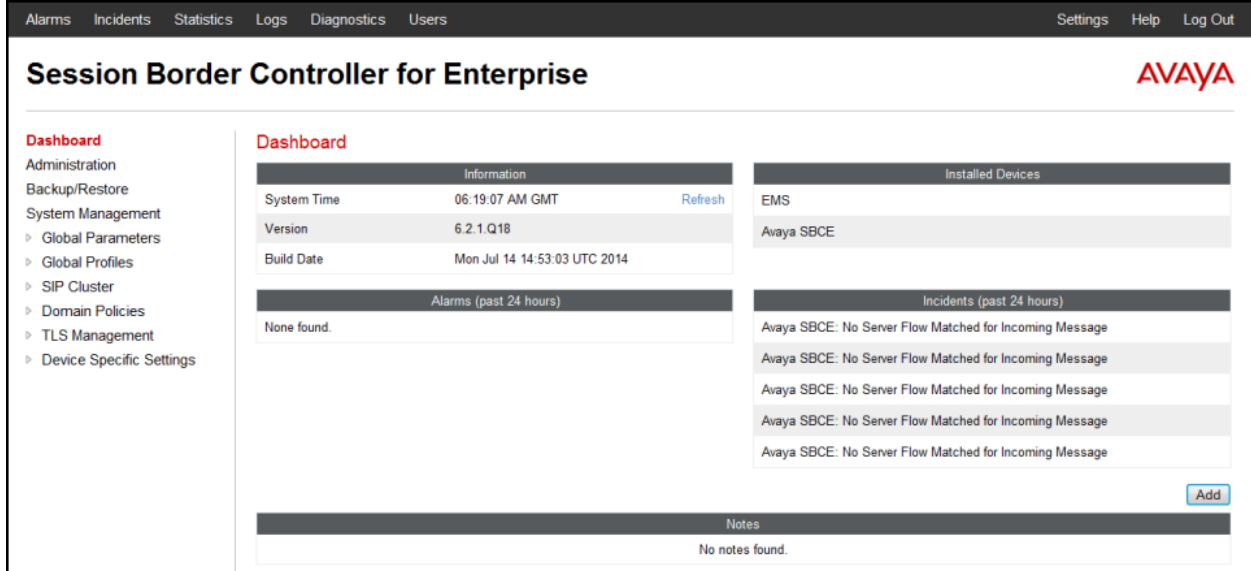
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under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

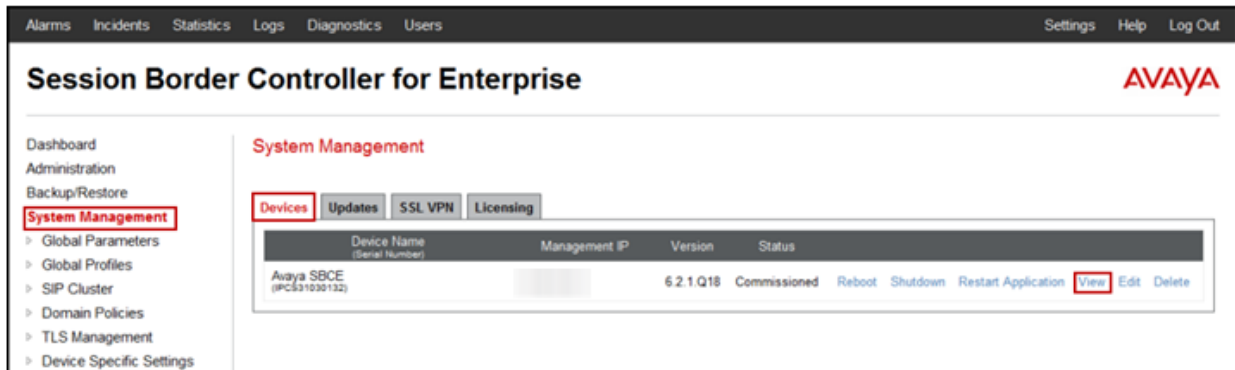
All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

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



To view the system information that has been 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 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 **Network Settings**, **DNS Configuration** and **Management IP** 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.

IMPORTANT! – During the Avaya SBCE installation, the Management interface, (labeled “M1”), of the Avaya SBCE must be provisioned on a different IP subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.

The screenshot shows the 'System Information: Avaya SBCE' window with the following configuration details:

General Configuration		Device Configuration	
Appliance Name	Avaya SBCE	HA Mode	No
Box Type	SIP	Two Bypass Mode	No
Deployment Mode	Proxy		

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
192.168.157.185	192.168.157.185	255.255.255.192	192.168.157.129	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 Charter. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document. These IP addresses, including the management IP address, have been blurred out for security reasons.

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 Charter, 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.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', '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 is a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', and 'Global Profiles'. The 'Global Profiles' section is expanded, and 'Server Interworking' is highlighted.

The main content area is titled 'Interworking Profiles: Avaya-SM'. It features an 'Add' button and a list of profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, **Avaya-SM**, SP-General, Avaya-CS1000, Avaya-IPO, and Avaya-CM.

The configuration for the 'Avaya-SM' profile is shown in the 'General' tab. It includes a description field and several settings:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', '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 is a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', and 'Global Profiles'. The 'Global Profiles' section is expanded, and 'Server Interworking' is highlighted with a red box.

The main content area is titled 'Interworking Profiles: Avaya-SM'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A list of interworking profiles is shown on the left, with 'Avaya-SM' selected and highlighted with a red box. The 'Advanced' tab is active, showing a table of configuration parameters:

Parameter	Value
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

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

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 Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the AVAYA logo. The left navigation pane is expanded to "Global Profiles" > "Server Interworking", with "SP-General" selected in the "Interworking Profiles" list. The main content area shows the configuration for "Interworking Profiles: SP-General". The "General" tab is active, displaying various settings:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
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

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

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

The left sidebar contains a navigation menu with categories like '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', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. 'Server Interworking' is highlighted with a red box.

The main content area is titled 'Interworking Profiles: SP-General' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A list of interworking profiles is shown on the left, with 'SP-General' highlighted in red. The 'Advanced' tab is selected, displaying a table of configuration options:

General	Timers	URI Manipulation	Header Manipulation	Advanced
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 Spurt			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 table.

7.2.3. 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 next screen, complete the following:

- **Next Hop Server 1: 172.16.5.32** (Session Manager signaling interface IP address).
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport:** select **TCP**.
- Click **Finish**.

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group *

Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port 172.16.5.32

Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port

Routing Priority based on Next Hop Server

Use Next Hop for In Dialog Messages

Ignore Route Header for Messages Outside Dialog

NAPTR

SRV

Outgoing Transport TLS TCP UDP

Finish

The following screen capture shows the newly created **Route_to_SM** Routing Profile.

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

The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'Routing', and 'SIP Cluster'. The 'Global Profiles' and 'Routing' items are highlighted with red boxes.

The main content area is titled 'Routing Profiles: Route_to_SM'. It features an 'Add' button and a list of routing profiles: 'default', 'Route_to_SM', 'Route_to_SP', 'Route_to_CM', 'Route_to_CS1000', 'Route_to_IPO', and 'To SM from Rem W'. The 'Route_to_SM' profile is selected and highlighted with a red box.

Below the list, there is a table for the selected profile. The table has columns for 'Priority', 'URI Group', 'Next Hop Server 1', and 'Next Hop Server 2'. The data row shows a priority of '1', an asterisk '*' for the URI Group, and '172.16.5.32' for the Next Hop Server 1. There are 'View' and 'Edit' links for this entry.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	172.16.5.32	--

Similarly, for the outbound route:

- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SP**.
- Click **Next**.
- **Next Hop Server 1: 10.10.188.70** (Service Provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport:** select **UDP**.
- Click **Finish**.

The screenshot shows the 'Edit Routing Rule' dialog box with the following configuration:

- Next Hop Routing** section:
- URI Group: (dropdown menu)
- Next Hop Server 1: 10.10.188.70 (IP, IP Port, Domain, or Domain Port)
- Next Hop Server 2: (empty text box)
- Routing Priority based on Next Hop Server:
- Use Next Hop for In Dialog Messages:
- Ignore Route Header for Messages Outside Dialog:
- NAPTR:
- SRV:
- Outgoing Transport: TLS TCP UDP
- Finish button

The following screen capture shows the newly created **Route_to_SP** Routing Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management 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 is a list of routing profiles: 'default', 'Route_to_SM', 'Route_to_SP' (highlighted), 'Route_to_CM', 'Route_to_CS1000', 'Route_to_IPO', and 'To SM from Rem W'. To the right of the list is a detailed configuration form for the selected profile, including a description field and a table of routing entries.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	10.10.188.70	--	View Edit

7.2.4. Server Configuration

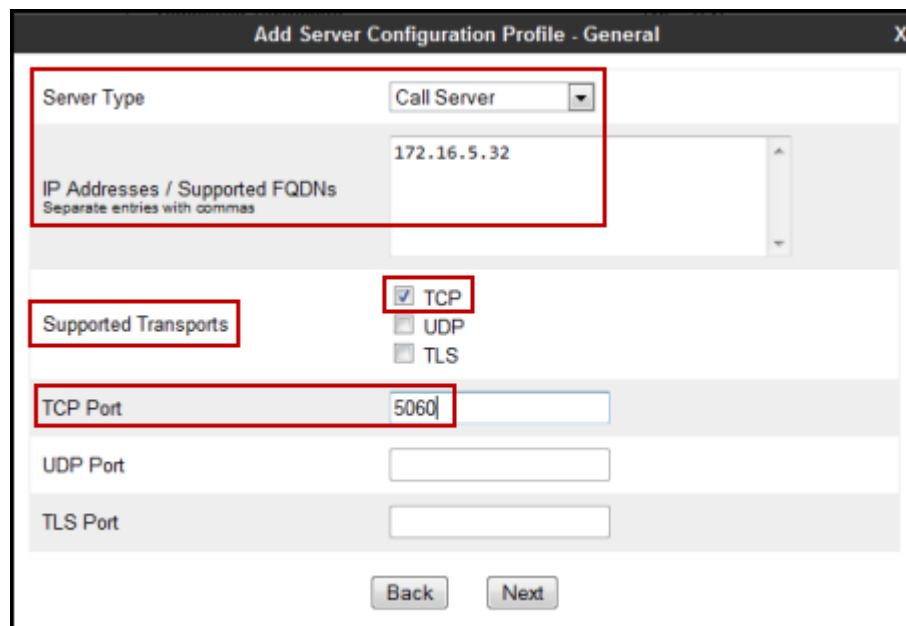
Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server which is the SIP Proxy at the service provider's network.

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

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

- **Server Type:** select *Call Server*.
- **IP Address:** *172.16.5.32* (IP Address of Session Manager).
- **Supported Transports:** check *TCP*.
- **TCP Port:** enter *5060*.
- Click **Next**.
- Click **Next** in the **Authentication** window.
- Click **Next** in the **Heartbeat** window.

The following screen capture shows the **General** tab of the **Session Manager** Server Configuration Profile.

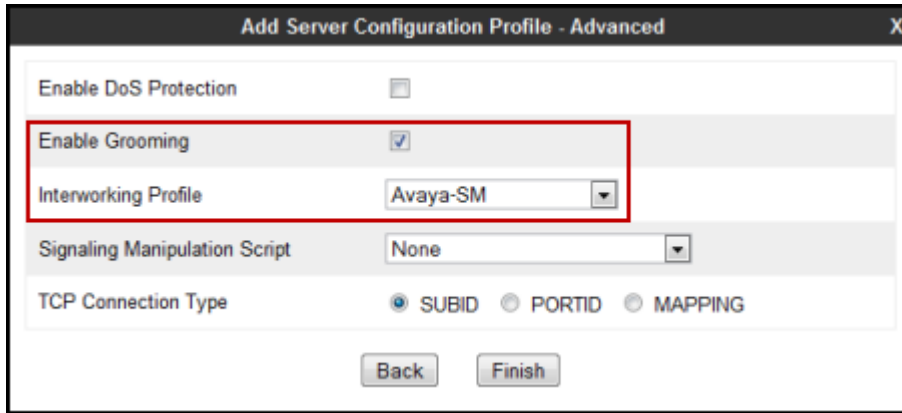


The screenshot displays the 'Add Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Call Server'. The 'IP Addresses / Supported FQDNs' field contains '172.16.5.32'. Under 'Supported Transports', the 'TCP' checkbox is checked, while 'UDP' and 'TLS' are unchecked. The 'TCP Port' field is set to '5060'. The 'UDP Port' and 'TLS Port' fields are empty. 'Back' and 'Next' buttons are visible at the bottom.

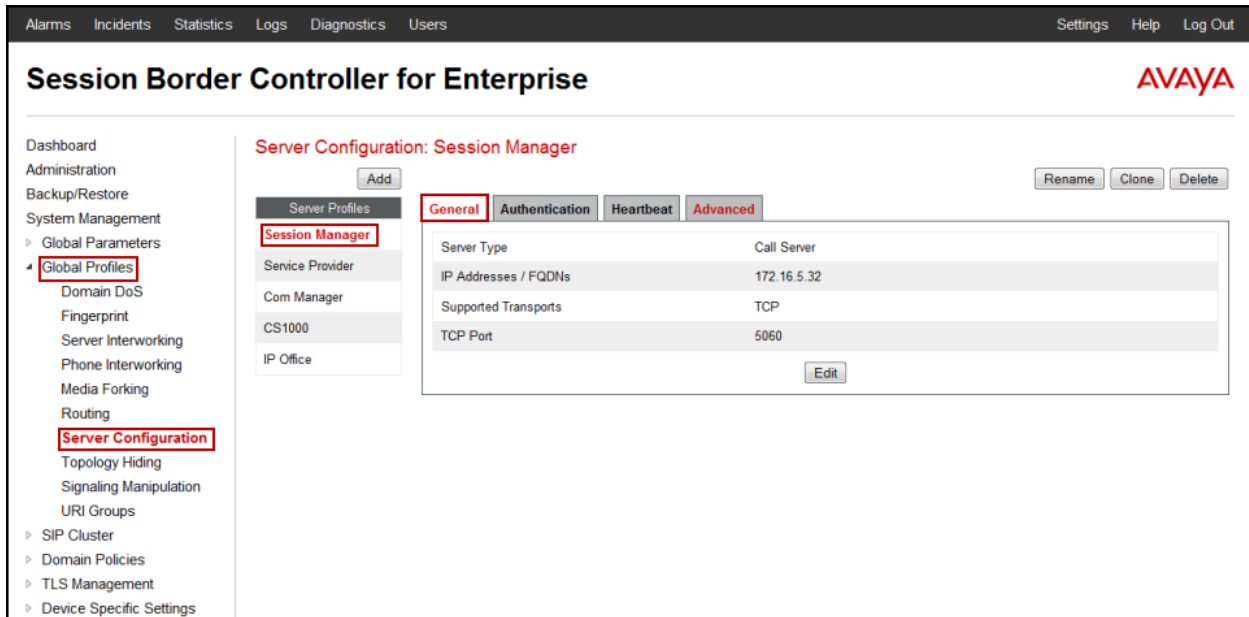
In the **Advanced** window

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

The following screen capture shows the **Advanced** tab of the **Session Manager** Server Configuration Profile.



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



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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: Session Manager' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced', with the 'Advanced' tab selected. The 'Advanced' tab contains a table of configuration options:

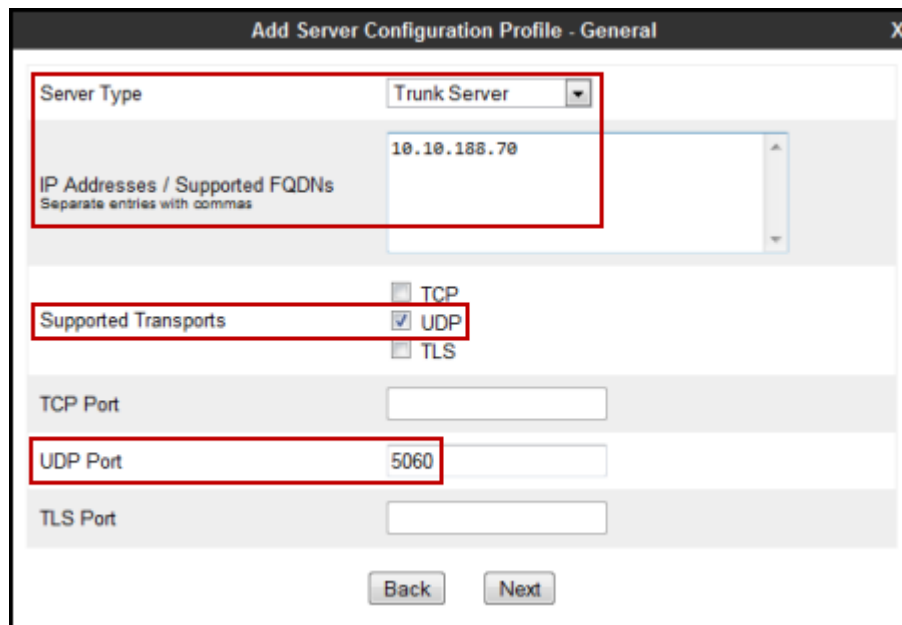
Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
TLS Client Profile	None
Signaling Manipulation Script	None
TCP Connection Type	SUBID
TLS Connection Type	SUBID

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

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*.

In the **Add Server Configuration Profile - General** window

- **Server Type:** select *Trunk Server*.
- **IP Address:** *10.10.188.70* (service provider's SIP Proxy IP address).
- **Supported Transports:** check *UDP*.
- **UDP Port:** enter *5060*.
- Click **Next**.



The screenshot displays the 'Add Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Trunk Server'. The 'IP Addresses / Supported FQDNs' field contains '10.10.188.70'. Under 'Supported Transports', the 'UDP' checkbox is checked, while 'TCP' and 'TLS' are unchecked. The 'UDP Port' field is set to '5060'. The 'TCP Port' and 'TLS Port' fields are empty. 'Back' and 'Next' buttons are visible at the bottom.

On the **Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Leave **Realm** blank.
- Enter **Password** credential provided by the service provider for SIP trunk registration.
- Click **Next**.

Add Server Configuration Profile - Authentication X

Enable Authentication

User Name

Realm
(Leave blank to detect from server challenge)

Password

Confirm Password

Back Next

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, **60** 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 Service Provider's domain name (**charterlabs.net**), as shown on the screen below.
Note: The **User Name** and **domain name** should be provided by the service provider.
 - **To URI**: Use the **User Name** entered above under the **Authentication** screen (**User123**) and the Service Provider Proxy Provider's domain name (**charterlabs.net**), as shown on the screen below.
Note: The **User Name** and **domain name** should be provided by the service provider.
- Click **Next**.

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER
Frequency	60 seconds
From URI	User123@charterlabs.r
To URI	User123@charterlabs.r
Back Next	

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 shows a configuration window titled "Add Server Configuration Profile - Advanced". It contains the following fields and options:

- Enable DoS Protection:
- Enable Grooming:
- Interworking Profile: (highlighted with a red box)
- Signaling Manipulation Script:
- UDP Connection Type: SUBID PORTID MAPPING

Buttons: Back, Finish

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. At the top, there is a navigation bar with links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. Below this, the main title 'Session Border Controller for Enterprise' is shown. On the left side, there is a sidebar menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Server Configuration: Service Provider' and features an 'Add' button. Below the title, there is a list of server profiles: Session Manager, Service Provider (highlighted), Com Manager, CS1000, and IP Office. To the right of this list, there are four tabs: General (selected), Authentication, Heartbeat, and Advanced. The General tab displays a configuration table with the following data:

Server Type	Trunk Server
IP Addresses / FQDNs	10.10.188.70
Supported Transports	UDP
UDP Port	5060

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

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. At the top, there is a navigation bar with links for 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. Below this, the main title 'Session Border Controller for Enterprise' is shown. On the left side, there is a sidebar menu with categories like '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', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Server Configuration' menu item is highlighted. The main content area is titled 'Server Configuration: Service Provider 1' and features an 'Add' button. Below the title, there is a list of server profiles: 'Session Manager', 'Com Manager', 'CS1000', 'IP Office', and 'Service Provider'. The 'Service Provider' profile is selected and highlighted. To the right of the profile list, there are four tabs: 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'Authentication' tab is active, showing a form with the following fields: 'Enable Authentication' (checked), 'User Name' (user123), and 'Realm' (---). An 'Edit' button is located at the bottom right of the form.

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The main title is "Session Border Controller for Enterprise".

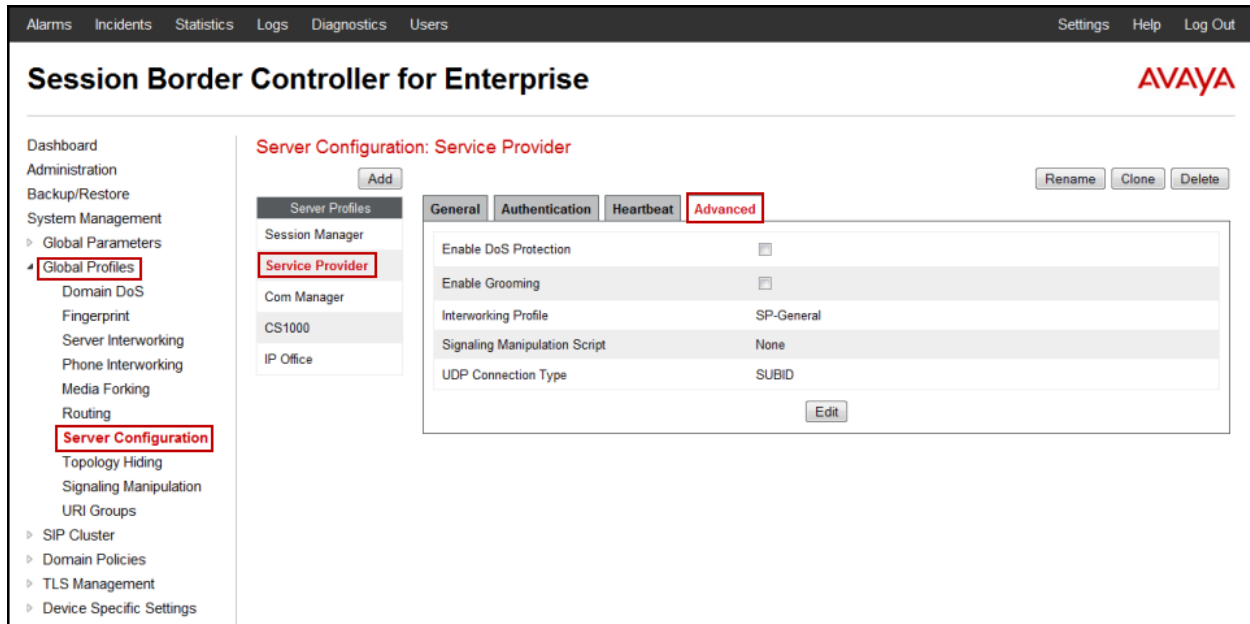
The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Server Configuration: Service Provider 1" and features an "Add" button. Below this is a "Server Profiles" list with items: Session Manager, Com Manager, CS1000, IP Office, and Service Provider (highlighted). The "Service Provider" profile is selected, and its configuration is shown in a table with tabs for General, Authentication, Heartbeat (selected), and Advanced.

General	Authentication	Heartbeat	Advanced
Enable Heartbeat			<input checked="" type="checkbox"/>
Method		REGISTER	
Frequency		60 seconds	
From URI		User123@charterlabs.net	
To URI		User123@charterlabs.net	

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.



7.2.5. 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 untrusted 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:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name: *Session_Manager***.
- Click **Finish**.
- Click **Edit** on the newly added **Session_Manager** Topology Hiding Profile.
- In the **From** header, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the enterprise (***avaya.lab.com***) under **Overwrite Value**.

- In the **To** header, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (**avaya.lab.com**) under **Overwrite Value**.
- In the **Request-Line** header, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Enterprise (**avaya.lab.com**) under **Overwrite Value**.
- Click **Finish**.

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

The following screen capture shows the newly created **Session_Manager** Topology Hiding Profile.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics 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
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings

Topology Hiding Profiles: Session_Manager

Topology Hiding Profiles: default, cisco_th_profile, **Session_Manager**, Service_Provider, Com Manager, CS1000, IP Office

Click here to add a description.

Topology Hiding

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

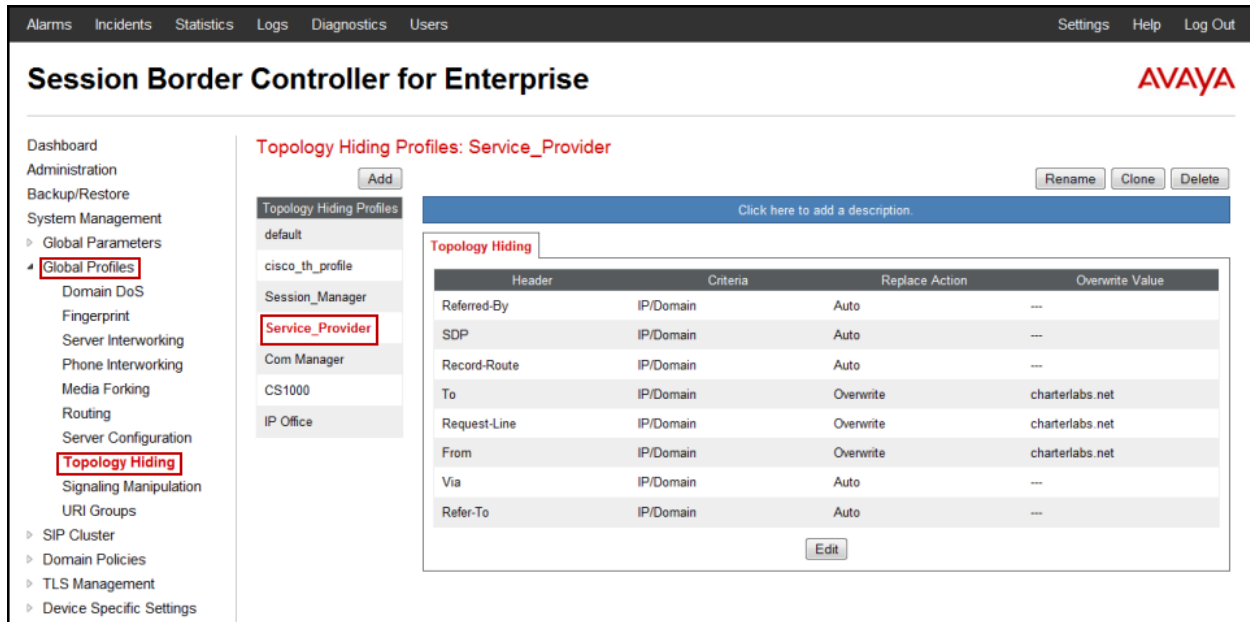
To add the Topology Hiding profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen.
- Enter the **Profile Name: *Service_Provider***.
- Click **Finish**.
- Click **Edit** on the newly created **Service_Provider** Topology Hiding profile.
- On the **To** header, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**charterlabs.net**) under **Overwrite Value**.
- On the **From** header, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**charterlabs.net**) under **Overwrite Value**.
- On the **Request-Line** header, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Service Provider (**charterlabs.net**) under **Overwrite Value**.
- Click **Finish**.

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

Finish

The following screen capture shows the newly created **Service_Provider** Topology Hiding Profile.



7.2.6. Signaling Manipulation

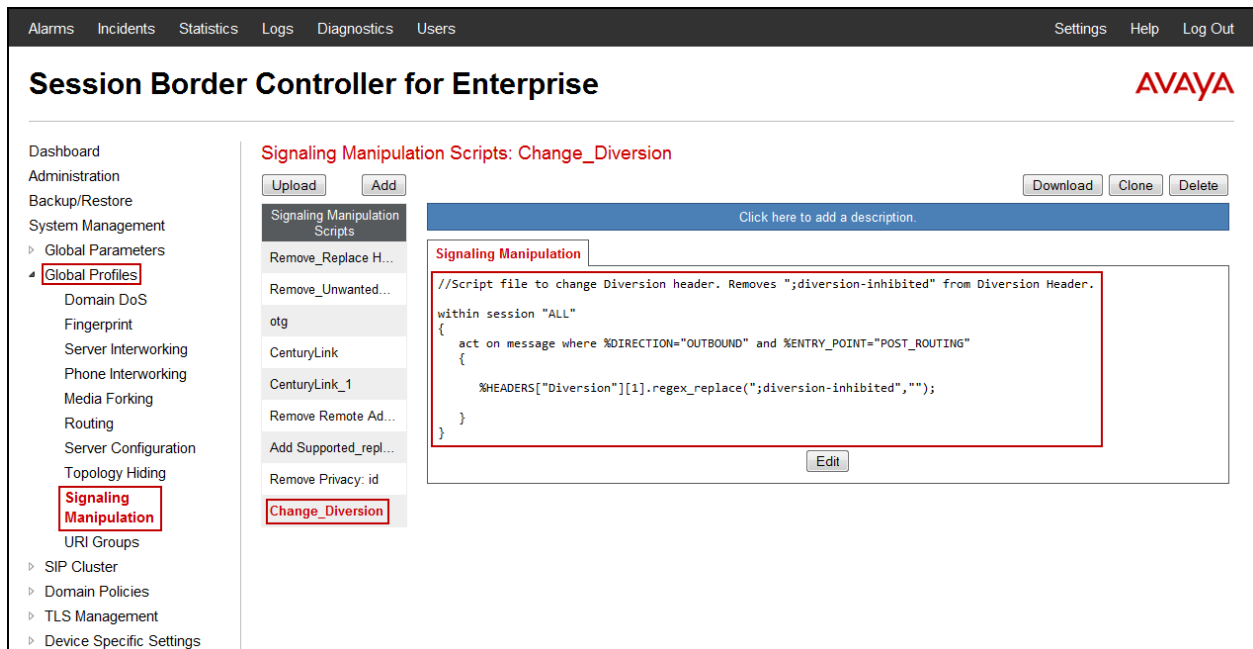
The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For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

The **diversion-inhibited** field added to the INVITE message by Communication Manager, as part of the in Diversion Header, was causing call re-directions to the PSTN to fail (e.g., call transfers to the PSTN, twinning to Mobile station (EC500), etc.). The SigMa script shown below was created to remove the **diversion-inhibited** field from Diversion Headers added by Communication Manager to INVITE messages before forwarding to Charter.

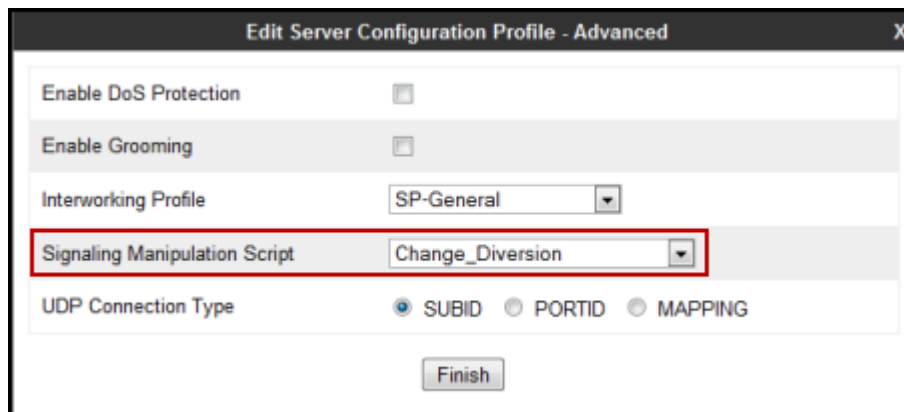
From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen.

- For **Title** enter a name, the name of *Change_Diversion* 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**.



After the Signaling Manipulation Script is created, it should be applied to the **Service Provider Server Profile** previously created in **Section 7.2.4**.

Go to **Global Profiles** → **Server Configuration** → **Service Provider** → **Advanced** tab → **Edit**. Select **Change_Diversion** 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.

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main title is 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left sidebar lists various configuration categories, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: Service Provider' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A 'Server Profiles' list on the left includes 'Session Manager', 'Service Provider', 'Com Manager', 'CS1000', and 'IP Office'. The 'Advanced' tab is active, showing a table of configuration options:

General	Authentication	Heartbeat	Advanced
Enable DoS Protection		<input type="checkbox"/>	
Enable Grooming		<input type="checkbox"/>	
Interworking Profile		SP-General	
Signaling Manipulation Script		Change_Diversion	
UDP Connection Type		SUBID	

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

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

- Select **default** in the **Application Rules** list.
- Click the **Clone** button on top right of the screen.
- **Name:** enter the name of the profile, e.g., *2000 Sessions*.
- Click **Finish**.
- Click **Edit**.
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** per license values specific to the enterprise, the value of **2000** for **Audio** and **100** for Video 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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support: None, CDR w/ RTP, CDR w/o RTP

RTCP Keep-Alive:

Buttons: Back, Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise interface. The left sidebar shows the navigation menu with 'Application Rules' highlighted under 'Domain Policies'. The main content area is titled 'Application Rules: 2000 Sessions'. It features a list of application rules on the left, with '2000 Sessions' selected. The main configuration area shows a table for 'Application Rule' with columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The table contains three rows: Audio (In: checked, Out: checked, Max Concurrent: 2000, Max Sessions: 2000), Video (In: checked, Out: checked, Max Concurrent: 100, Max Sessions: 100), and IM (In: unchecked, Out: unchecked, Max Concurrent: 0, Max Sessions: 0). Below the table is a 'Miscellaneous' section with 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is located at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100
IM	<input type="checkbox"/>	<input type="checkbox"/>	0	0

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 interface. The left sidebar shows the navigation menu with 'Media Rules' highlighted under 'Domain Policies'. 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' selected. The main configuration area shows a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below the warning is a 'Media NAT' section with a sub-section for 'Media NAT' containing the text 'Learn Media IP dynamically'. An 'Edit' button is located at the bottom right of the configuration area.

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 **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 'Signaling Rules' highlighted. The main content area displays the configuration for the 'SessMgr_SigRule' signaling rule. The 'Request Headers' tab is selected, showing a table of headers. The table has columns for Row, Header Name, Method Name, Header Criteria, Action, Proprietary, and Direction. The headers listed are AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector, and P-Location. The 'Add In Header Control' button is highlighted in red.

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	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN
5	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN
6	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 **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 main content area shows the configuration for the **Signaling Rules: SessMgr_SigRule**. The **Response Headers** tab is selected, showing a table of configured headers. The table has columns for Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, and Direction. There are also buttons for 'Add In Header Control' and 'Add Out Header Control'.

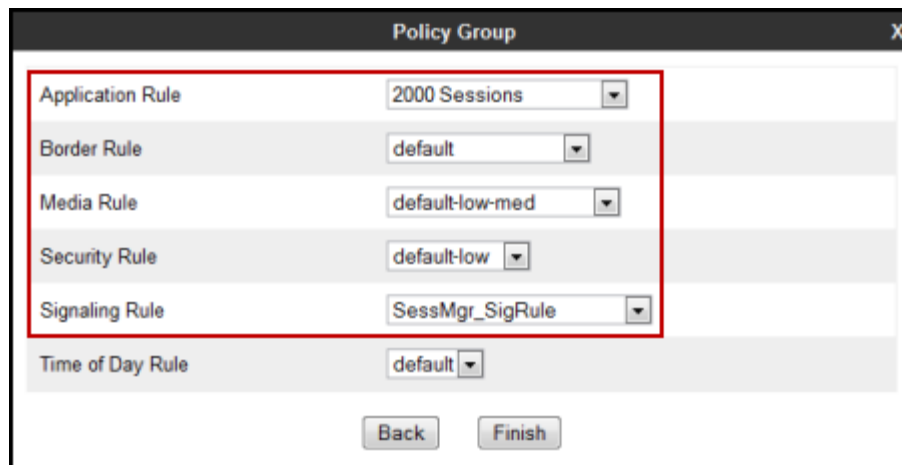
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
4	P-AV-Message-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

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**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. The dialog contains several rows of configuration options, each with a label and a dropdown menu. A red rectangular box highlights the first five rows: Application Rule, Border Rule, Media Rule, Security Rule, and Signaling Rule. The values in these dropdowns are: "2000 Sessions", "default", "default-low-med", "default-low", and "SessMgr_SigRule" respectively. Below these rows is a "Time of Day Rule" dropdown set to "default". At the bottom of the dialog are two buttons: "Back" and "Finish".

Rule Type	Selected Value
Application Rule	2000 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	SessMgr_SigRule
Time of Day Rule	default

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 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Domain Policies', and 'End Point Policy Groups'. The 'End Point Policy Groups' category is highlighted with a red box.

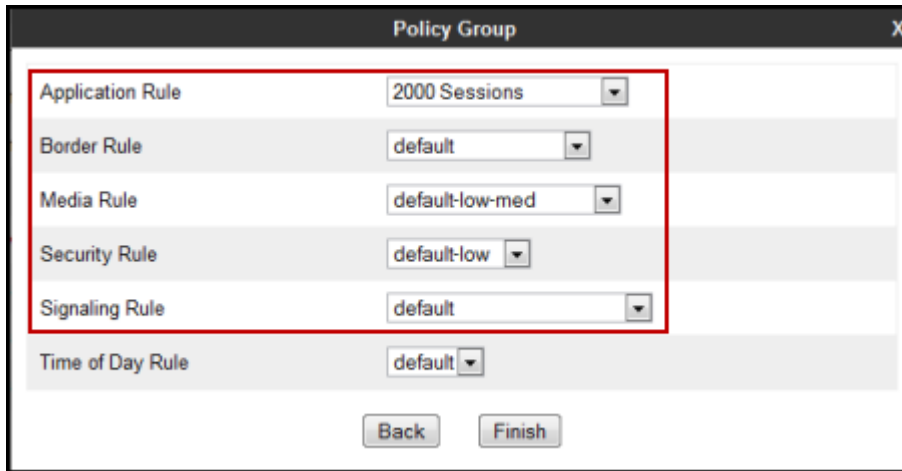
The main content area is titled 'Policy Groups: Enterprise'. It features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are two blue bars with the text 'Click here to add a description.' and 'Click here to add a row description.'

The 'Policy Group' configuration section includes a 'Summary' and 'Add' button. Below this is a table with the following data:

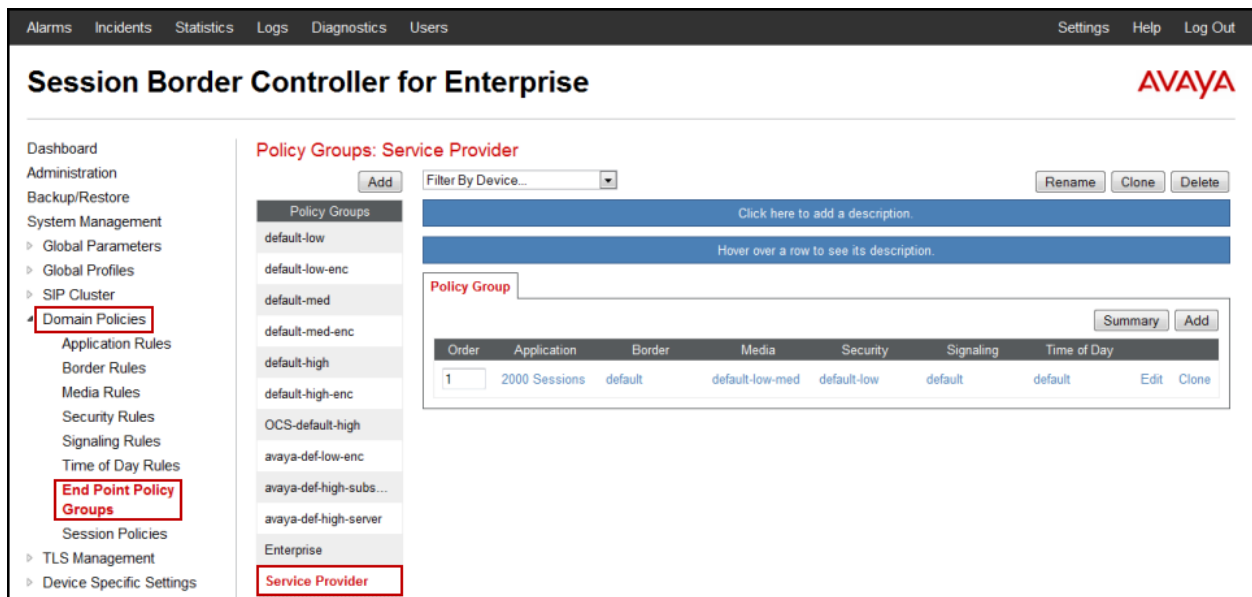
Order	Application	Border	Media	Security	Signaling	Time of Day	
1	2000 Sessions	default	default-low-med	default-low	SessMgr_SigRule	default	Edit Clone

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.



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.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

- Dashboard
- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - TLS Management
- Device Specific Settings**
 - Network Management**
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - End Point Flows
 - Session Flows
 - Relay Services
 - SNMP
 - Syslog Management
 - Advanced Options
 - Troubleshooting

Network Management: Avaya SBCE

Devices Avaya SBCE

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.192 B2 Netmask:

Add Save Clear

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
192.168.157.185		192.168.157.129	B1	Delete
				Delete
				Delete
				Delete

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 shows the Avaya SBCE web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar contains a menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. Under "Device Specific Settings", "Network Management" is highlighted. The main content area is titled "Network Management: Avaya SBCE" and has two tabs: "Network Configuration" and "Interface Configuration". The "Interface Configuration" tab is active and displays a table with the following data:

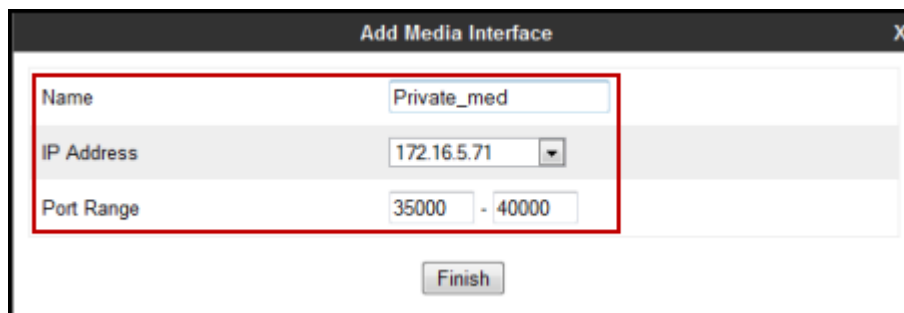
Name	Administrative Status	Toggle
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

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.

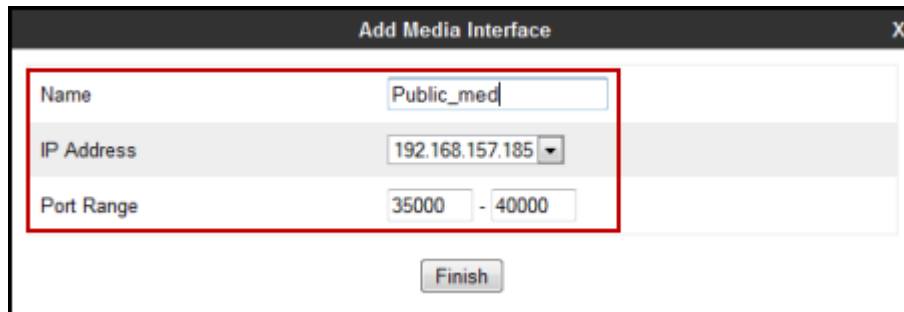
From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**.

- 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 a dropdown menu showing "172.16.5.71", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the dialog. A red rectangular box highlights the Name, IP Address, and Port Range fields.

- Select **Add** in the **Media Interface** area.
- **Name:** *Public_med*.
- Select **IP Address:** *192.168.157.185* (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 a dropdown menu showing "192.168.157.185", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the dialog. A red rectangular box highlights the Name, IP Address, and Port Range fields.

The following screen capture shows the newly created Media Interfaces.

The screenshot displays the Avaya SBCE web interface. At the top, there is a navigation bar with links for Alarms, Incidents, Statistics, 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 includes categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The "Media Interface" option under "Device Specific Settings" is highlighted with a red box. The main content area is titled "Media Interface: Avaya SBCE" and features a sub-tab "Media Interface". 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, and Port Range. Two interfaces are listed: "Private_med" and "Public_med".

Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.71	35000 - 40000	Edit	Delete
Public_med	192.168.157.185	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**.

Name	Private_sig
IP Address	172.16.5.71
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	
Enable Stun	<input type="checkbox"/>
TLS Port <small>Leave blank to disable</small>	
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

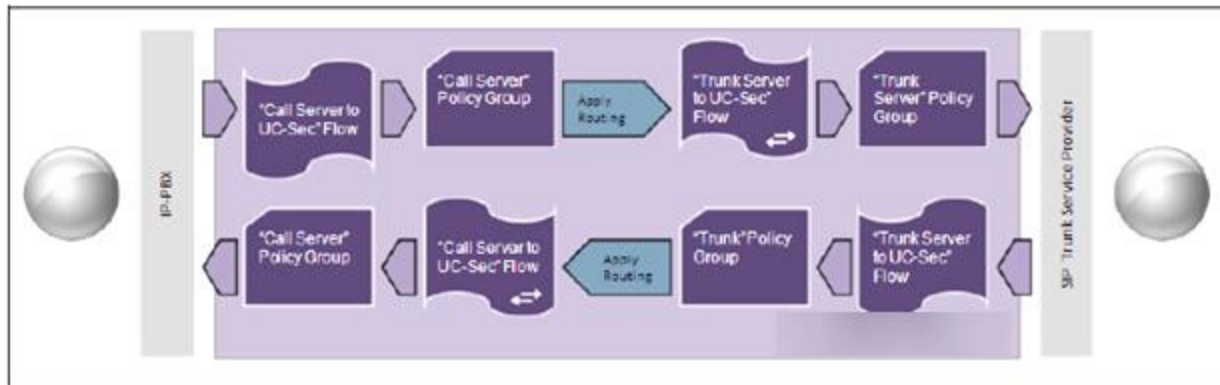
- Select **Add** in the **Signaling Interface** area.
- **Name:** *Public_sig*.
- Select **IP Address:** *192.168.157.185* (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port:** *5060*.
- Click **Finish**.

The following screen capture shows the newly created Signaling Interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.71	5060		---	None	Edit Delete
Public_sig	192.168.157.185	---	5060	---	None	Edit Delete
192.168.157.185	192.168.157.185	---	---	5060	AvayaSBCServer	Edit Delete
192.168.157.185	192.168.157.185	---	---	5060	AvayaSBCServer	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**.

Edit Flow: SIP_Trunk_Flow X

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

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 dialog box titled "Edit Flow: Session_Manager_Flow". It contains the following configuration fields:

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

A "Finish" button is located at the bottom center of the dialog.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various settings, with 'End Point Flows' highlighted under 'Device Specific Settings'. The main content area is titled 'End Point Flows: Sipera' and features two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, showing two configuration sections: 'Server Configuration: Service Provider' and 'Server Configuration: Session Manager'. Each section contains a table of flows with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The 'SIP_Trunk_Flow' and 'Session_Manager_Flow' entries are highlighted with red boxes.

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

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

8. Charter SIP Trunking Service Configuration

To use Charter Communications SIP Trunking service offering, a customer must request the service from Charter using the established sales processes. The process can be started by contacting Charter via the corporate web site at: <https://www.charterbusiness.com/> or by calling 800-314-7195.

Charter 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. Charter Communications will provide the customer the necessary information to configure the SIP trunk connection, including:

- IP address of Charter'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. Login 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 shows the Avaya SBCE Dashboard. At the top, there is a navigation bar with links for Alarms, Incidents, Statistics, 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 management options, with "Alarms" highlighted. The dashboard content is divided into several sections: "Information" (System Time: 02:23:30 PM GMT, Version: 6.2.1 Q18, Build Date: Mon Jul 14 14:53:03 UTC 2014), "Installed Devices" (listing EMS and Avaya SBCE), "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (listing four "No Server Flow Matched for Incoming Message" incidents), and "Notes" (No notes found).

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

The screenshot shows the Avaya Alarm Viewer page. The header includes "Alarm Viewer" and the AVAYA logo. On the left, a "Devices" sidebar lists "EMS" and "Avaya SBCE" (which is selected). The main area is titled "Alarms" and contains a table with columns for "ID", "Details", "State", "Time", and "Device". The table is currently empty, displaying the message "No alarms found for this device." Below the table are "Clear Selected" and "Clear All" buttons.

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

The screenshot shows the Avaya Session Border Controller for Enterprise dashboard. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. The 'Incidents' menu item is highlighted with a red arrow. The dashboard is titled 'Session Border Controller for Enterprise' and features the Avaya logo. A left sidebar contains a navigation menu with categories like 'Administration', 'System Management', and 'Device Specific Settings'. The main content area is titled 'Dashboard' and is divided into several sections: 'Information' (System Time: 02:23:30 PM GMT, Version: 6.2.1.Q18, Build Date: Mon Jul 14 14:53:03 UTC 2014), 'Installed Devices' (listing EMS and Avaya SBCE), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (listing five incidents of 'No Server Flow Matched for Incoming Message'), and 'Notes' (No notes found).

The following screen shows the Incident Viewer page.

The screenshot shows the Avaya Incident Viewer page. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. The page is titled 'Incident Viewer' and features the Avaya logo. Below the title, there are filter options: 'Device' set to 'All' and 'Category' set to 'Authentication'. There is a 'Clear Filters' button and 'Refresh' and 'Generate Report' buttons. Below the filters, it says 'Displaying results 0 to 0 out of 0.' A table with columns 'Type', 'ID', 'Date', 'Time', 'Category', 'Device', and 'Cause' is shown, with the text 'No incidents found.' in the center. At the bottom, there are navigation buttons: '<<', '<', '1', '>', and '>>'.

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

The screenshot shows the Avaya Session Border Controller for Enterprise dashboard. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics' (highlighted with a red arrow), and 'Users'. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo. A left sidebar lists various management categories like Administration, System Management, and Device Specific Settings. The main content area is titled 'Dashboard' and contains several panels: 'Information' (System Time: 02:23:30 PM GMT, Version: 6.2.1 Q18, Build Date: Mon Jul 14 14:53:03 UTC 2014), 'Installed Devices' (listing EMS and Avaya SBCE), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (multiple entries for 'No Server Flow Matched for Incoming Message'), and 'Notes' (No notes found).

The following screen shows the Diagnostics page.

The screenshot shows the Avaya Diagnostics page. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics' (highlighted with a red arrow), and 'Users'. The main header reads 'Diagnostics' with the Avaya logo. A left sidebar lists various management categories like Administration, System Management, and Device Specific Settings. The main content area is titled 'Diagnostics' and contains several panels: 'Devices' (listing Avaya SBCE), 'Full Diagnostic', 'Ping Test' (active), 'Application', and 'Protocol'. The 'Ping Test' panel shows a 'Source Device / IP' dropdown menu set to '[mgmt] 172.16.5.70' and a 'Destination IP' input field. A 'Ping' button is located below the input fields.

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 shows the Avaya SBCE web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', '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 'Device Specific Settings' and its sub-menu 'Troubleshooting' → 'Trace' highlighted. The main content area is titled 'Trace: Avaya SBCE' and contains three tabs: 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, displaying a 'Packet Capture Configuration' form. The form includes fields for 'Status' (Ready), 'Interface' (Any), 'Local Address [IP, Port]' (All), 'Remote Address' (*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Inc_to_IP0.pcap). 'Start Capture' and 'Clear' buttons are at the bottom of the form.

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.

This screenshot shows the same Avaya SBCE web interface, but with the 'Captures' tab selected. The 'Packet Capture' configuration form is no longer visible. Instead, a table lists the captured files. The table has columns for 'File Name', 'File Size (bytes)', and 'Last Modified'. A single entry is shown: 'No_180_20140721045220.pcap' with a size of 622,592 bytes and a timestamp of July 21, 2014 4:52:38 AM GMT. A 'Delete' link is provided for this entry. A 'Refresh' button is located at the top right of the table area. The navigation menu on the left remains the same, with 'Captures' highlighted in the main content area.

10. Conclusion

These Application Notes describe the procedures necessary for configuring Charter 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 6.2 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 6.2, Issue 2, January 2014.
- [6] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2013.
- [7] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, July 2013.

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

- [8] *Administering Avaya one-X® Communicator*, October 2014.
- [9] *Administering Avaya Flare® Experience for Windows*, Release 1.1, Document Number: 18-604156, Issue 4, September 2013.
- [10] *Implementing Avaya Flare® Experience for Windows*, Release 1.1, Documents Number: 18-604153, Issue 2, February 2013.
- [11] *Using Avaya one-X® Communicator*, Release 6.1, October 2011.

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

- [12] *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:

[13] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.

[14] *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: Change_Diversion

//Script file to change Diversion header. Removes ";diversion-inhibited" field from Diversion Header.

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["Diversion"][1].regex_replace(";diversion-inhibited","");
  }
}
```

©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.