



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3 and Avaya Session Border Controller for Enterprise Rel. 6.3.1 to support Claro SIP Trunking Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking service for an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 6.3, Avaya Aura® Session Manager Rel. 6.3, and Avaya Session Border Controller for Enterprise Rel. 6.3.1 to support Claro SIP Trunking Services.

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.

Claro SIP Trunking Service provides PSTN access via SIP trunks between the enterprise and Claro's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	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.....	16
5.6.	Signaling Group	17
5.7.	Trunk Group.....	19
5.8.	Calling Party Information.....	23
5.9.	Inbound Routing.....	24
5.10.	Outbound Routing	26
6.	Configure Avaya Aura® Session Manager	29
6.1.	System Manager Login and Navigation.....	30
6.2.	Specify SIP Domain	31
6.3.	Add Location.....	32
6.4.	SIP Entities	35
6.5.	Entity Links	39
6.6.	Routing Policies	42
6.7.	Dial Patterns	43
6.8.	Add/View Avaya Aura® Session Manager	46
7.	Configure Avaya Session Border Controller for Enterprise	48
7.1.	Log in Avaya SBCE.....	48
7.2.	Global Profiles.....	51
7.2.1.	Server Interworking Avaya-SM.....	51
7.2.2.	Server Interworking SP-General.....	54
7.2.3.	Signaling Manipulation.....	56
7.2.4.	Server Configuration.....	58
7.2.5.	Routing Profiles	63
7.2.6.	Topology Hiding.....	67
7.3.	Domain Policies	71
7.3.1.	Application Rules.....	71
7.3.2.	Media Rules	73
7.3.3.	Signaling Rules	73
7.3.4.	End Point Policy Groups.....	81

7.4.	Device Specific Settings.....	84
7.4.1.	Network Management.....	84
7.4.2.	Media Interface	86
7.4.3.	Signaling Interface	88
7.4.4.	End Point Flows.....	91
8.	Claro SIP Trunking Service Configuration.....	95
9.	Verification and Troubleshooting	96
9.1.	Troubleshooting	96
9.1.1.	Communication Manager.....	96
9.1.2.	Session Manager	96
9.1.3.	Avaya SBCE	97
10.	Conclusion	101
11.	References.....	102
12.	Appendix A: SigMa Script.....	104

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) trunk service between the service provider Claro 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 Communication Manager), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.3.1 (hereafter referred to as Avaya SBCE), and various Avaya endpoints. This solution does not extend to configurations without the Avaya Session Border Controller for Enterprise or Avaya Aura® Session Manager.

During the interoperability testing, feature test cases were executed to ensure interoperability between Claro and Communication Manager.

During the interoperability testing, a VPN connection was used to connect the simulated Avaya enterprise network to Claro's network via the public Internet. The connection could also be done without the use of VPN, by directly connecting the Avaya SBCE to a public facing SBC located in Claro's network. This is accomplished by assigning public IP addresses, capable of being reached across the public Internet, to the Avaya SBCE (interface B1) and to the Claro SBC.

Customers using an Avaya SIP-enabled enterprise solution with Claro 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" and "Claro" will be used interchangeable throughout these Application Notes

2. General Test Approach and Test Results

The general test approach was to simulate an enterprise site in the Avaya Solution & Interoperability Test Lab by connecting Communication Manager, Session Manager and the Avaya SBCE to Claro 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 trunk interoperability, the following areas were tested for compliance:

- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by Claro. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x0 Series IP Deskphones (H.323), Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator soft phone (H.323 and SIP), Avaya Communicator for Windows (SIP) soft phone, analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 deskphones (SIP), Avaya one-X® Communicator (SIP) and Avaya Communicator for Windows (SIP).
- Outgoing calls to the PSTN were routed via Claro's network to the various PSTN destinations.
- 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 parties.
- 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.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU, G.711A and G.729A (Claro's preferred codec order).
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages, 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) calls.
- 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.
- T.38 fax.

Note: Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes. For Remote Worker configuration details, see Reference [13].

Items not supported or not tested included the following:

- Inbound toll-free calls, outbound Toll-Free calls, 911 calls (emergency), “0” calls (Operator), 0+10 digits calls (Operator Assisted), and 411 calls (Local Directory Assistance) were not tested.
- The SIP REFER method for call redirection was not tested for reasons noted in **Section 2.2**.

2.2. Test Results

Interoperability testing of Claro SIP Trunk service with an Avaya SIP-enabled enterprise solution was completed successfully with the following observations/limitations.

- **SIP REFER:** Calls from the PSTN to Communication Manager that are re-directed to another PSTN endpoint by the Communication Manager user, with REFER enabled in Communication Manager (**Network Call Redirection** set to “y” under the **trunk-group**), did not work properly. Testing was done with REFER disabled in Communication Manager (**Network Call Redirection** set to “n” under the **trunk-group**), refer to **Section 5.7**.
- **Caller ID display on Call Forward to the PSTN:** For Calls from the PSTN to Communication Manager which were Forwarded back out to the PSTN, the caller ID number displayed at the PSTN was always of the first DID number assigned to the SIP Trunk, regardless of the PSTN number being used to originate the call.
- **Caller ID display on EC500 extension to cellular:** For EC500 extension to cellular calls the Caller ID display at the Mobile/cellular station was always of the first DID number assigned to the SIP Trunk, regardless of the PSTN number being used to originate the call.
- **No matching codec on outbound calls:** If an unsupported audio codec is received by Claro on the SIP Trunk (e.g., 726A-32K), Claro will respond with “500 Server Internal Error” instead of “488 Not Acceptable Here”, the user will hear re-order tones. This issue does not have any user impact, it is listed here simply as an observation.
- **SIP UPDATE:** SIP UPDATES was causing problems with call transfers to the PSTN and with other call types to the PSTN. For this solution SIP UPDATES needs to be disabled on the SIP Trunk. SIP UPDATE was disabled on the SIP Trunk by the addition of a Signaling Manipulation script (SigMa) on the Avaya SBCE, refer to **Section 7.2.3**.
- **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. Calls from Communication Manager to voice mail systems located at the PSTN, requiring the use DTMF tones to retrieve voice mail messages, failed with Media shuffling enabled in Communication Manager (**Direct IP-IP Audio Connections** set to y under the **signaling-group**): digits entered were not recognized by the voice mail system. For the compliance test, Media shuffling was disabled in Communication Manager, refer to **Section 5.6**.
- **SIP header optimization:** There are multiple SIP headers used by the Avaya solution that have no particular use to the Service Provider. These headers were removed in order to block private IP addresses and other enterprise information from being propagated outside of the enterprise boundaries, and to reduce the size of the packets entering Claro’s

network. Refer to **Sections 7.2.3** and **7.3.3** for the complete list of headers that were removed.

2.3. Support

For support on Claro systems visit the corporate Web page at:

<http://www.claro.com.do/wps/portal/do/sc/empresas>

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

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 Claro SIP Trunk service through the public Internet.

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

- Avaya S8300D 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 Deskphones (H.323).
- Avaya 96x1-Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator soft phones (H.323 and SIP).
- Avaya Communicator for Windows soft phone (SIP)
- Avaya 2420 Digital Deskphones.
- Analog Deskphones.
- Desktop PC running various administration interfaces.

Located at the edge of the enterprise is a VPN Firewall, followed by the Avaya SBCE. The Avaya SBCE has two physical interfaces: interface **B1** is used to connect to the public network, interface **A1** is used to connect to the private network. Since a VPN connection was used with this solution to connect Claro's network to the enterprise, the **A1** interface was used for access to the private enterprise network and to route calls to Claro's network across the VPN tunnel. In this solution, the **B1** interface was used for remote workers access to the enterprise. The configuration required for the **B1** interface is not discussed in this document.

When a VPN connection is not used, the **B1** interface is normally used for remote workers access to the private network and to route calls to the Service Provider across the public Internet.

All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE and through the VPN Firewall. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Claro, through the VPN Tunnel, and across the public Internet, is SIP over UDP. The transport protocol between the Avaya SBCE and Session Manager across the enterprise IP network is SIP over TCP. The transport protocol between Session Manager and Communication Manager across the enterprise IP network is SIP over TLS. Note that for ease of troubleshooting during the testing, the compliance test was conducted with the Transport Method set to TCP between Session Manager and Communication Manager.

For security reasons, any actual public IP addresses and routable DID numbers used in the reference configuration have been masked.

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 Claro to the Avaya SBCE through the VPN Tunnel, 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 was 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 Claro's network through the VPN Tunnel.

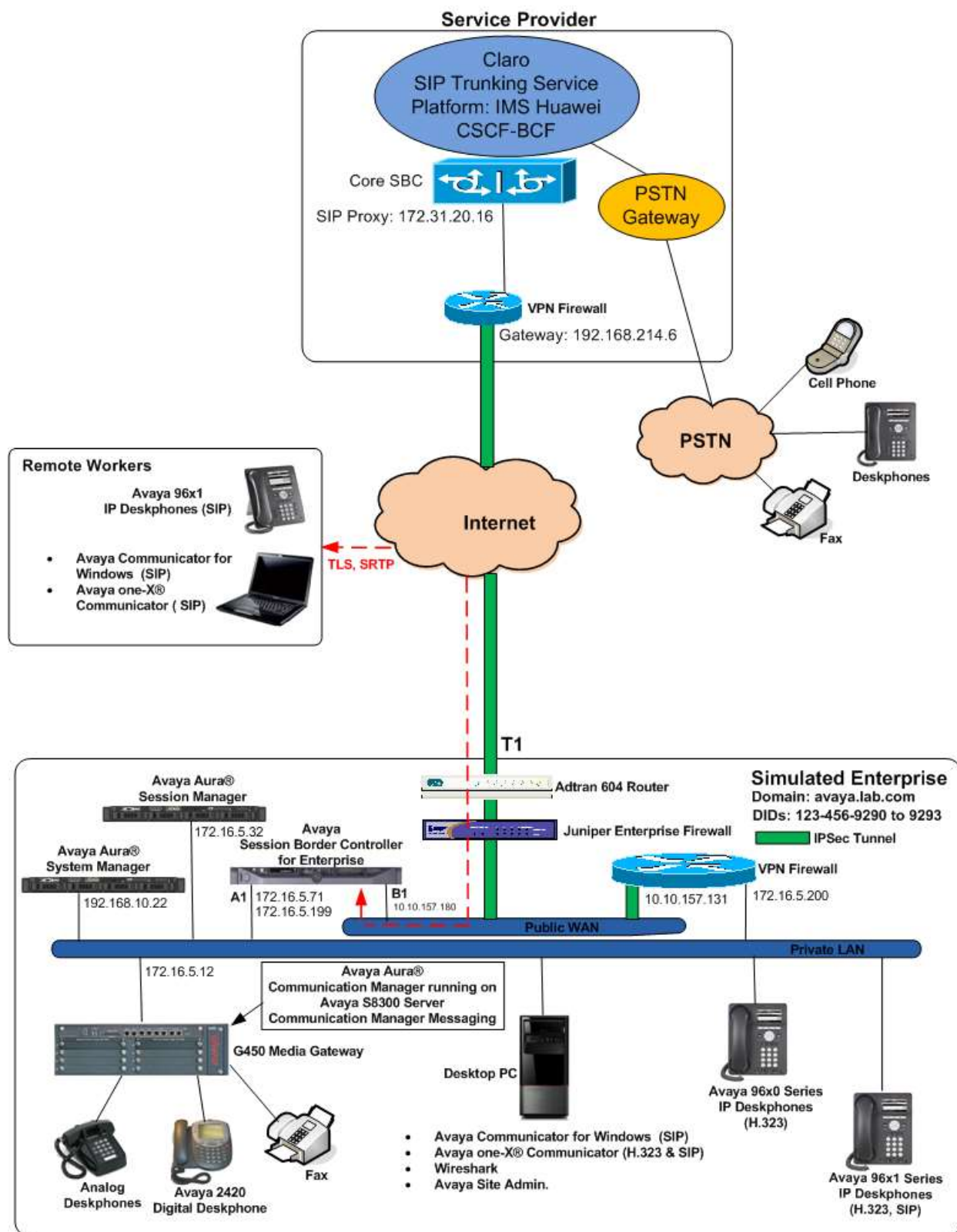


Figure 1: Avaya SIP-enabled Enterprise Solution and Claro SIP Trunking Service

4. Equipment and Software Validated

The following equipment and software were used for the compliance testing in the simulated enterprise:

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on an Avaya S8300D Server.	6.3.9.1 (Service Pack 9.1) (03.0.124.0-22098)
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.11 (Service Pack 11) (6.3.11.0.631103)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.11 (Service Pack 11) Build No. 6.3.0.8.5682-6.3.8.4711 Software Update Rev. No. 6.3.11.8.2871
G450 Gateway	36.12.0
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.3.1-22-4653
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)	6.2.5.03-SP5
Avaya Communicator for Windows (SIP)	2.1.0.69
Avaya 96x0 Series IP Deskphones (H.323)	Avaya one-X® Deskphone Edition Version S3.240A
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 6.5.0.17
Avaya 2420 Series Digital Deskphone	--
Lucent Analog Deskphone	--
Claro	
IMS Huawei CSCF-BCF	V100R010C00SPC100
SBC Huawei SessionEngine2600	V200R009ENG30SPC100

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 Claro. 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 shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements are not revealed. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise, including any 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 7
Maximum Administered SIP Trunks: 4000 22
Maximum Administered Ad-hoc Video Conferencing Ports: 4000 0
Maximum Number of DS1 Boards with Echo Cancellation: 80 0
Maximum TN2501 VAL Boards: 10 0
Maximum Media Gateway VAL Sources: 50 1
Maximum TN2602 Boards with 80 VoIP Channels: 128 0
Maximum TN2602 Boards with 320 VoIP Channels: 128 0
Maximum Number of Expanded Meet-me Conference Ports: 300 0

(NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 3**, verify that **ARS** is set to **y**.

```
display system-parameters customer-options Page 3 of 11
OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y Audible Message Waiting? y
Access Security Gateway (ASG)? n Authorization Codes? y
Analog Trunk Incoming Call ID? y CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y CAS Main? n
Answer Supervision by Call Classifier? y Change CDR by FAC? n
ARS? y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y Cvg OF Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n DCS (Basic)? y
ASAI Link Core Capabilities? n DCS Call Coverage? y
ASAI Link Plus Capabilities? n DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n DS1 MSP? y
ATM WAN Spare Processor? n DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y

(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    ::

( 7 of 7 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the Service Provider. For the compliance test, **ip-codec-set 2** was used for this purpose. Claro SIP Trunking supports G.711MU, G.711A and G.729A. Thus, these codecs were included in this set. Enter **G.711MU**, **G.711A** and **G.729A** in the **Audio Codec** column of the table; this is Claro's preferred codec order. Default values can be used for all other fields.

change ip-codec-set 2 Page 1 of 2

IP CODEC SET

Codec Set: 2

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

Media Encryption

1: none

2:

3:

On **Page 2**, set the **Fax Mode** to **t.38-standard** (T.38 fax is supported by Claro).

change ip-codec-set 2 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? ☐

	Mode	Redundancy	Packet Size(ms)
FAX	t.38-standard	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

ECM: y

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 AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS RSVP Enabled? n
H.323 Link Bounce Recovery? y
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									
dst rgn	codec set	direct WAN	BW-limits Units	Video Total Norm	Intervening Prio Shr Regions	Dyn CAC	I G A R L	M G L	t c e
1	2	u	NoLimit				n		t
2	2							all	
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									

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** and **7.2.4**. Lastly, the transport method between the Avaya SBCE and Claro is UDP. This is defined in **Section 7.2.4**.
- 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	Group Type: sip	
IMS Enabled? <input type="checkbox"/>	Transport Method: tcp	
Q-SIP? <input type="checkbox"/>		
IP Video? <input type="checkbox"/>		Enforce SIPS URI for SRTP? <input type="checkbox"/>
Peer Detection Enabled? <input checked="" type="checkbox"/>	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <input type="checkbox"/>		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <input type="checkbox"/>		
Alert Incoming SIP Crisis Calls? <input type="checkbox"/>		
Near-end Node Name: procr	Far-end Node Name: Lab-HG-SM	
Near-end Listen Port: 5070	Far-end Listen Port: 5070	
	Far-end Network Region: 2	
Far-end Domain: avaya.lab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? <input type="checkbox"/>	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? <input type="checkbox"/>	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? <input type="checkbox"/>	
Enable Layer 3 Test? <input type="checkbox"/>	IP Audio Hairpinning? <input type="checkbox"/>	
	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 **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

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

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** 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. Note that the value assigned to the **Preferred Minimum Session Refresh Interval (sec)** field is doubled and assigned to the “Min-SE” Header Field in SIP INVITE messages for calls originating from Communication Manager. Using the default setting of **600** seconds as in the example, the “Min-SE” Header Field would be populated for 1200 seconds in SIP INVITE messages originating from Communication Manager.

change trunk-group 2		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: <u>auto</u>		
		Redirect On OPTIM Failure: <u>5000</u>
SCCAN? <u>n</u>	Digital Loss Group: <u>18</u>	
	Preferred Minimum Session Refresh Interval(sec): <u>600</u>	
Disconnect Supervision - In? <u>y</u> Out? <u>y</u>		
XOIP Treatment: <u>auto</u>		Delay Call Setup When Accessed Via IGAR? <u>n</u>
Caller ID for Service Link Call to H.323 1xC: <u>station-extension</u>		

On **Page 3**, set the **Numbering Format** field to *public*. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign when passed in the SIP “From”, “Contact”, “P-Asserted Identity” and “Diversion” headers.

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: public UI Treatment: service-provider

Replace Restricted Numbers? y
Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y

Page 4 was configured using the parameters highlighted below.

- Set the **Network Call Redirection** field to *n*. This setting directs 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*. When enabled, the Diversion Header (in the outbound INVITE message) 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 Claro.
- Set the **Convert 180 to 183 for Early Media** to *y*.
- Set the **Identity for Calling Party Display** to *From*.

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

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are assigned by the 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. The DID numbers were mapped to enterprise extensions 3041, 3044, 3045 and 5016. These 11-digit numbers were used for the outbound calling party information on the Service Provider trunk when calls were originated from these extensions.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	3			4	Total Administered: 6
4	5			4	Maximum Entries: 240
4	3041	2	11234569290	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	3044	2	11234569291	11	
4	3045	2	11234569292	11	
4	5016	2	11234569293	11	
					Communication Manager automatically inserts a '+' digit in this case.

In a real customer environment, normally DID numbers are comprised of the local extension plus a prefix. If this is true, then a single public numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with 9 will send the calling party number as the **CPN 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 9 (e.g., 11234569xxx).

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	3			4	Total Administered: 6
4	5			4	Maximum Entries: 240
4	9	2	1123456	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
—	—	—	—	—	Communication Manager automatically inserts a '+' digit in this case.
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	

5.9. Inbound Routing

DID numbers received from Claro 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. Note that since Claro includes the “+” in the **Request-URI** of INVITE messages, the “+” was added to the **Incoming Number Digits**.

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	12	+11234569290	12	3041	
public-ntwrk	12	+11234569291	12	3044	
public-ntwrk	12	+11234569292	12	3045	
public-ntwrk	12	+11234569293	12	5016	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	
public-ntwrk	—	—	—	—	

25 of 106
Claro CMSMASBCE

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: 3				
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 178                                     Page 1 of 2
                                ARS DIGIT ANALYSIS TABLE
                                Location: all                    Percent Full: 3

```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req
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
1809	11	11	2	hnpa	___	n
181	11	11	deny	fnpa	___	n
182	11	11	deny	fnpa	___	n
183	11	11	deny	fnpa	___	n
184	11	11	deny	fnpa	___	n
185	11	11	deny	fnpa	___	n
186	11	11	deny	fnpa	___	n
187	11	11	deny	fnpa	___	n
188	11	11	deny	fnpa	___	n

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the Service Provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the 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.

change route-pattern 2												Page 1 of 3		
						Pattern Number: 2		Pattern Name: <u>Serv. Provider</u>						
						SCCAN? <u>n</u>		Secure SIP? <u>n</u>						
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts			DCS/ QSIG Intw	IXC			
1:	<u>2</u>	<u>0</u>	<u>1</u>	—	—	—	—			<u>n</u>	<u>user</u>			
2:	—	—	—	—	—	—	—			<u>n</u>	<u>user</u>			
3:	—	—	—	—	—	—	—			<u>n</u>	<u>user</u>			
4:	—	—	—	—	—	—	—			<u>n</u>	<u>user</u>			
5:	—	—	—	—	—	—	—			<u>n</u>	<u>user</u>			
6:	—	—	—	—	—	—	—			<u>n</u>	<u>user</u>			
BCC VALUE						TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No. Dgts	Numbering Format	LAR
0 1 2 M 4 W						Request						Subaddress		
1:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>							<u>none</u>
2:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>							<u>none</u>
3:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>							<u>none</u>
4:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>							<u>none</u>
5:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>							<u>none</u>
6:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>							<u>none</u>

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

6. Configure Avaya Aura® Session Manager

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

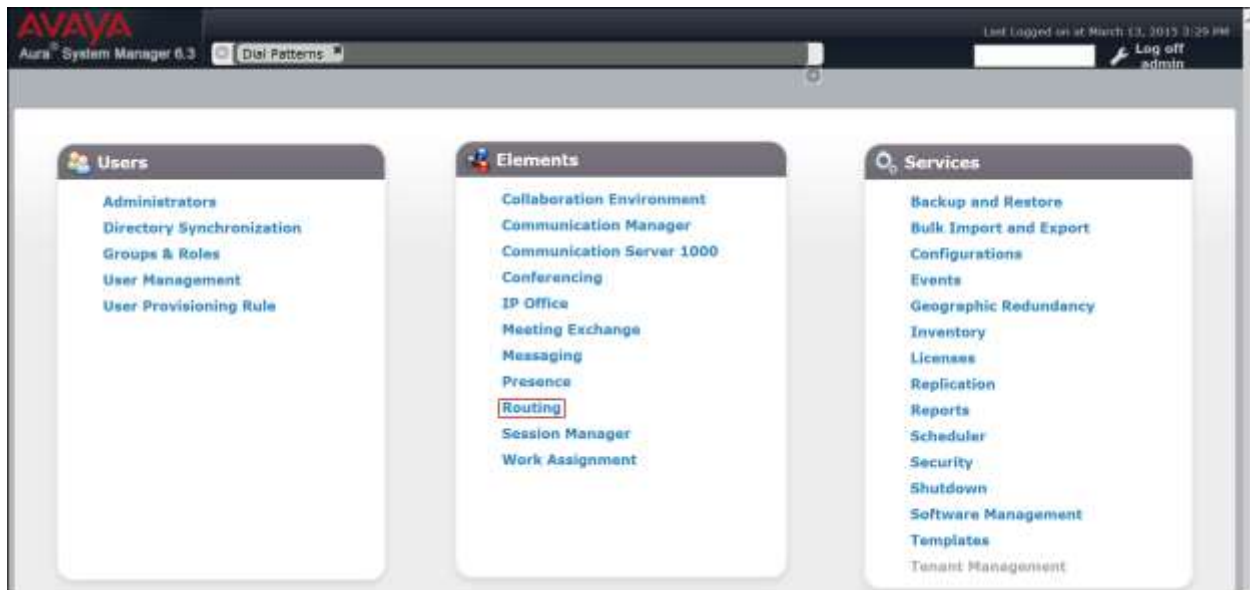
- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager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

It may not be necessary to create all the items above when configuring a connection to the Service Provider since some of these items would have already been defined as part of the initial Session Manager installation. 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.

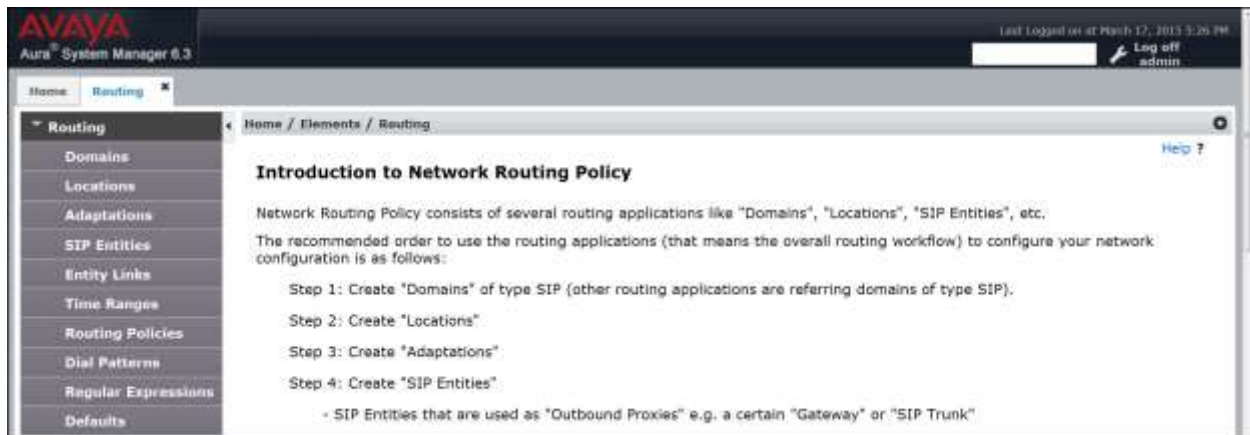
Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity
--

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials (not shown). The screen shown below is then displayed. Click on **Routing**.



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



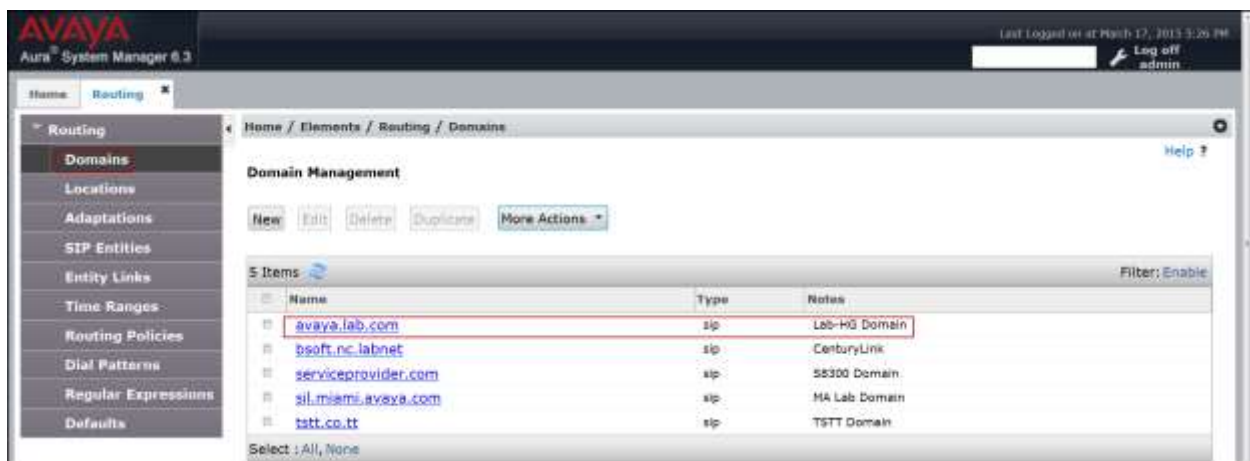
6.2. Specify SIP Domain

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

To add a domain Navigate to **Routing** → **Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select *sip* from the pull-down menu.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save (not show).

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



6.3. Add Location

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

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

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

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Locations' and shows the configuration for a location named 'HG Session Manager'. The 'General' section is active, showing the 'Name' field populated with 'HG Session Manager' and an empty 'Notes' field. Below this, the 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section includes fields for 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', and 'Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'. The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', 'Latency before Overall Alarm Trigger', and 'Latency before Multimedia Alarm Trigger'. The 'Location Pattern' section at the bottom shows a table with one entry: 'IP Address Pattern'. The interface includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

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

Avaya
Aura System Manager 6.3

Home / Elements / Routing / Locations

Location Details

General

Name: HG Communication Manager

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☐

Per-Call Bandwidth Parameters

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

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

Minimum Multimedia Bandwidth: 64 Kbit/Sec

Default Audio Bandwidth: 80 Kbit/Sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

Latency before Overall Alarm Trigger: 5 Minutes

Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

IP Address Pattern

Notes

Commit Cancel

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

The screenshot displays the Avaya Aura System Manager 6.3 interface. The top navigation bar shows 'Home / Elements / Routing / Locations'. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- Name:** HG ASBCE
- Notes:** HG Avaya SBCE
- Dial Plan Transparency in Survivable Mode:** Enabled: ☐
- Listed Directory Number:**
- Associated CM SIP Entity:**
- Overall Managed Bandwidth:**
 - Managed Bandwidth Units: Kbit/sec
 - Total Bandwidth:
 - Multimedia Bandwidth:
 - Audio Calls Can Take Multimedia Bandwidth: ☐
- Per-Call Bandwidth Parameters:**
 - Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec
 - Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec
 - Minimum Multimedia Bandwidth: 64 Kbit/Sec
 - Default Audio Bandwidth: 80 Kbit/Sec
- Alarm Threshold:**
 - Overall Alarm Threshold: 80 %
 - Multimedia Alarm Threshold: 80 %
 - Latency before Overall Alarm Trigger: 5 Minutes
 - Latency before Multimedia Alarm Trigger: 5 Minutes
- Location Pattern:**
 - Add Remove
 - 0 Items
 - IP Address Pattern
 - Filter: Enable

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

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 web interface. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following 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 form, 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 with columns for Port, Protocol, Default Domain, and Notes. The table contains the following data:

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 'Add' button and a table with 0 items. The table has columns for 'Response Code & Reason Phrase', 'Mark Entity Up/Down', and 'Notes'. The interface includes 'Commit' and 'Cancel' buttons at the bottom right.

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

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

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu with sub-items: Domains, Locations, Adaptations, **SIP Entities** (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and shows the 'General' tab for the entity 'HG CM Trunk 2'. The form includes the following fields and sections:

- Name:** HG CM Trunk 2
- FQDN or IP Address:** 172.16.5.12
- Type:** CM
- Notes:** CM SIP Trunk 2
- Adaptation:** (dropdown menu)
- Location:** HG Communication Manager
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Credential name:** (text field)
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:** (checkbox)
- Shared Bandwidth Manager:** (checkbox)
- Primary Session Manager Bandwidth Association:** (dropdown menu)
- Backup Session Manager Bandwidth Association:** (dropdown menu)
- SIP Responses to an OPTIONS Request:** (section with 'Add' and 'Remove' buttons)

At the bottom of the form, there is a table with the header 'Response Code & Reason Phrase' and columns for 'Mark Entity Up/Down' and 'Notes'. The table currently shows 0 items. The interface also includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

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

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

AVAYA
Aura System Manager 6.3

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: HG ASBCE

FQDN or IP Address: 172.16.5.71

Type: Other

Notes: HG ASBCE

Adaptation:

Location: HG ASBCE

Time Zone: America/New_York

SIP Timer S/F (in seconds): 4

Credential name:

Call Detail Recording: None

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

SIP Responses to an OPTIONS Request

Add Remove

0 Items

Filter: Enable

Response Code & Reason Phrase	Mark Entity Up/Down	Notes
-------------------------------	---------------------	-------

Commit Cancel

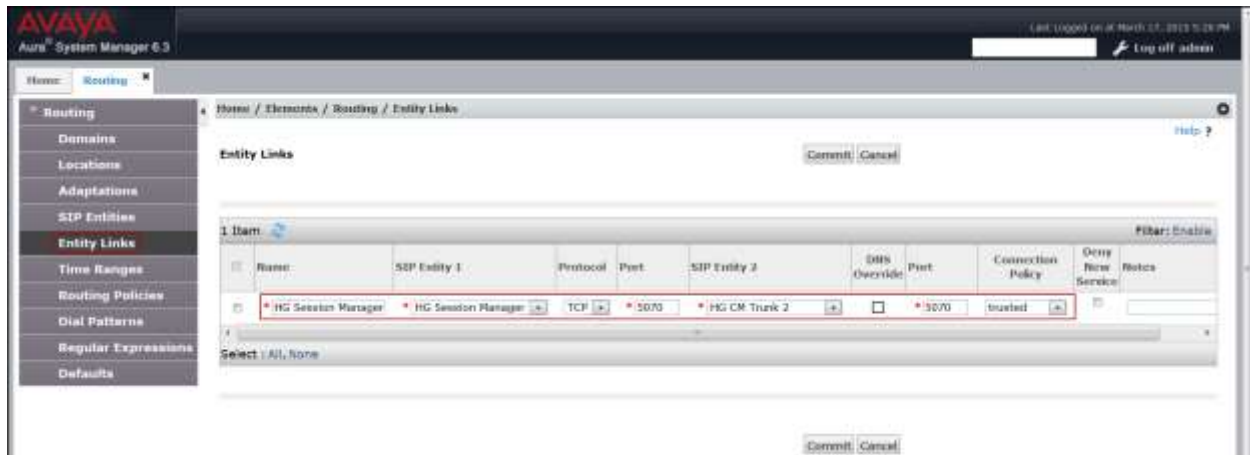
6.5. Entity Links

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:

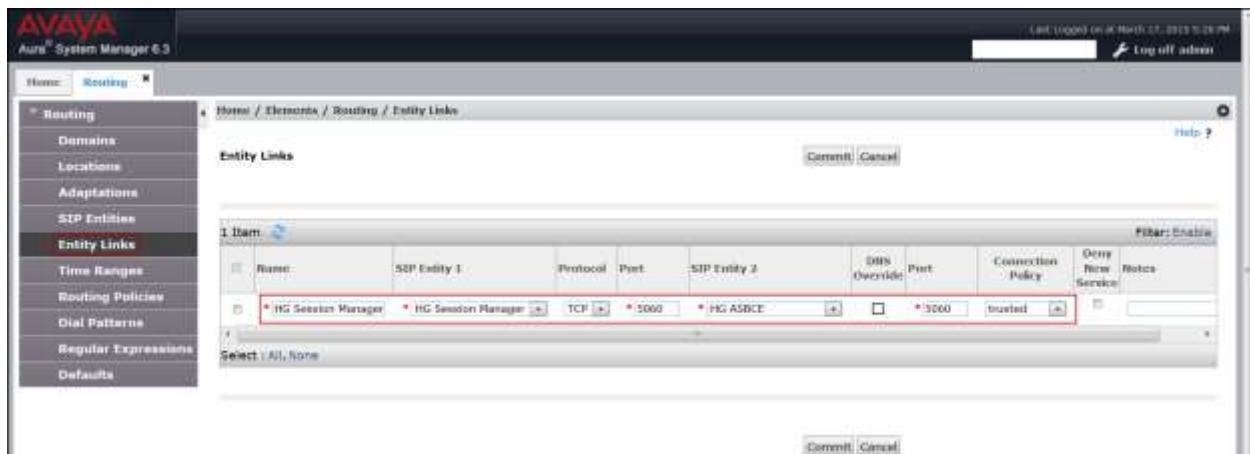
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link. For Communication Manager this was matched to the **Transport Method** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **Transport** defined on the **Server Configuration** for Session Manager (Call Server) in **Section 7.2.4**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this was matched to the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **Port** defined on the **Server Configuration** for Session Manager (Call Server) in **Section 7.2.4**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager or the Avaya SBCE select the respective 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 was matched to the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**. For the Avaya SBCE, this was matched to the **TCP Port** defined for the private **Signaling Interface** on the Avaya SBCE in **Section 7.4.3**.
- **Connection Policy:** Select *Trusted*.
- 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.

Entity Links

21 Items

Name	SDP Entity 1	Protocol	Port	SDP Entity 2	DNS Override	Port	Connection Policy	Derive 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 Acme Packet 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 EdgeMax SBC 5060_UDP	HG Session Manager	UDP	5060	EdgeMax 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 ASBC 5060_TCP	HG Session Manager	TCP	5060	HG ASBC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager_HG CM Trunk 1_5060_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:

Avaya Aura System Manager 6.3

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

Name: To HG CM Trunk 2

Disabled: ☐

Retries: 0

Notes: Inbound calls to HG CM Trunk 2

SIP Entity as Destination

Select

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

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and shows the 'General' tab. The 'Name' field is set to 'To HG ASBCE'. The 'Disabled' checkbox is unchecked. The 'Retries' field is set to '0'. The 'Notes' field contains the text 'Outbound calls via ASBCE'. Below the form, there is a section titled 'SIP Entity as Destination' with a 'Select' button. At the bottom, a table lists the routing policy details:

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 Claro 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, SIP Domain **Avaya.lab.com** could have been used instead.

AVAYA
Aura® System Manager 6.3

Home / Elements / Routing / Dial Patterns

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

Add Remove

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy (Enabled)	Routing Policy (Destination)	Routing Policy Notes
CSXk Node	CSXK7.0	To HG ASBCE	0	<input checked="" type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE
HG Communication Manager		To HG ASBCE	0	<input checked="" type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE
MA Communication Manager	HP DL360	Outbound to MA AA-SBC	0	<input checked="" type="checkbox"/>	MA_AA-SBC	
MA Communication Manager	HP DL360	Outbound to MA ASBCE	0	<input checked="" type="checkbox"/>	MA_SBCE	Outbound to MA_SBCE
SIL Lab Others		Outbound to MA ASBCE	0	<input checked="" type="checkbox"/>	MA_SBCE	Outbound to MA_SBCE

Select: All, from

The following dial pattern used for the compliance testing was for inbound calls to the enterprise. It uses dial pattern **+1123** matching the “+” and the first four digits sent by Claro on inbound calls to the enterprise. The pattern also matches the “+” and the first four digits of DID numbers assigned to Communication Manager in **Section 5.9 Inbound Routing**. 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**.

AVAYA
Aura® System Manager 6.3

Home / Routing / Dial Patterns

Dial Pattern Details

General

Pattern: +1123
 Min: 5
 Max: 12

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

Originating Locations and Routing Policies

Add Remove

1 Item

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

Select: All, None

Note: The same procedure should be followed to add other required dial patterns.

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.

AVAYA
Aura System Manager 6.3

Log off
admin

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

Return

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) | Connection Settings | Event Server |
Expand All | Collapse All

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:
*SIP Firewall Configuration: Rule Set for HG Session Man...

7. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of the Avaya SBCE to connect to Claro's SIP Trunking service.

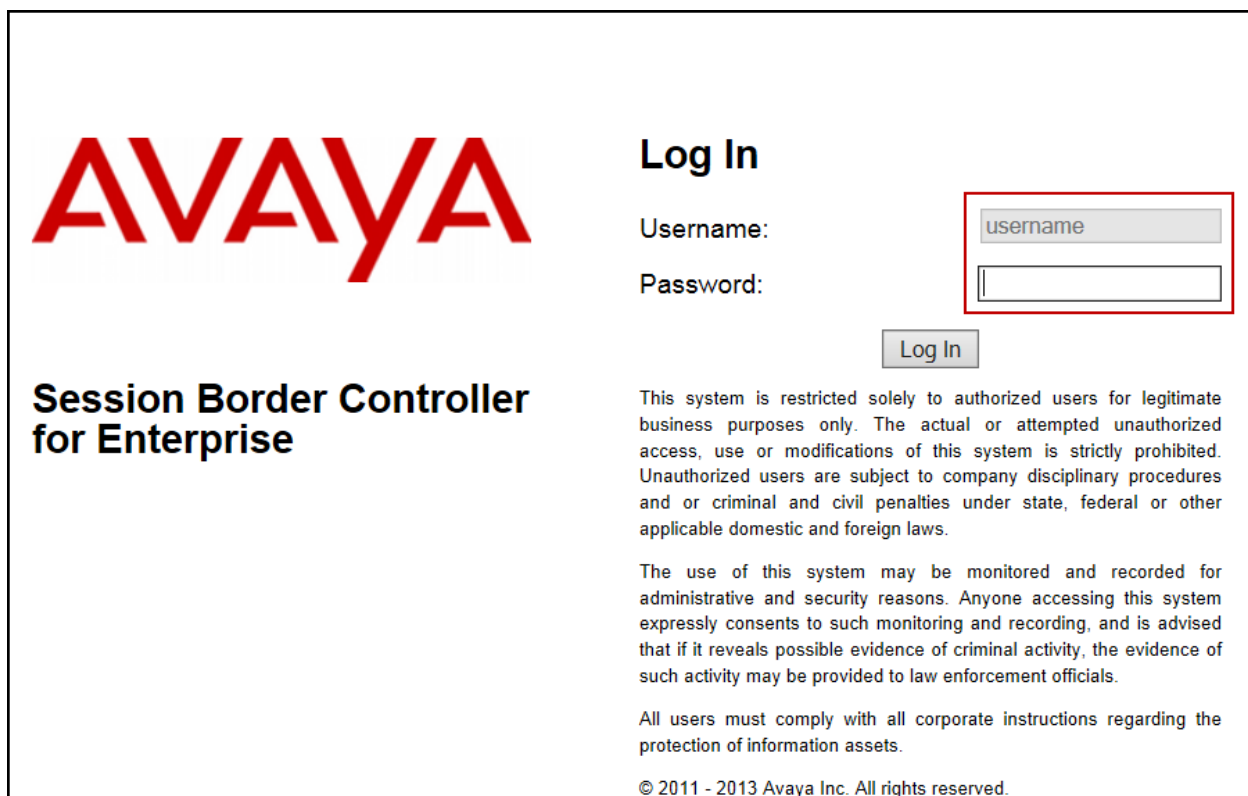
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

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

7.1. Log in Avaya SBCE

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

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



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label, a "Password:" label, and two input fields. The top input field is labeled "username" and is highlighted with a red border. Below it is an empty password field. A "Log In" button is positioned below the password field. To the right of the login fields, there is a disclaimer text block and a copyright notice at the bottom.

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.

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The left sidebar contains navigation links: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Dashboard' and is divided into three sections. The 'Information' section displays system details: System Time (01:07:20 AM GMT-06:00), Version (6.3.1-22-4853), Build Date (Fri Nov 21 17:35:09 EST 2014), License State (OK), Aggregate Licensing Overages (0), and Peak Licensing Overage Count (0). The 'Installed Devices' section shows a table with one device: EMS, Avaya SBCE. The 'Alarms (past 24 hours)' section shows 'None found'. The 'Incidents (past 24 hours)' section shows five incidents, all with the message 'Avaya SBCE: No Server Flow Matched for Incoming Message'. The 'Notes' section shows 'No notes found'.

Information	
System Time	01:07:20 AM GMT-06:00
Version	6.3.1-22-4853
Build Date	Fri Nov 21 17:35:09 EST 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices	
EMS	Avaya SBCE

Alarms (past 24 hours)	
None found.	

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

Notes	
No notes found.	

To view the system information that 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.

The screenshot shows the Avaya Session Border Controller for Enterprise System Management page. The left sidebar contains navigation links: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'System Management' and has tabs for Devices, Updates, SSL VPN, and Licensing. The 'Devices' tab is selected, showing a table with one device: Avaya SBCE, Management IP (192.168.1.100), Version (6.3.1-22-4853), and Status (Commissioned). The table also includes links for Reboot, Shutdown, Restart Application, View, Edit, and Uninstall.

Device Name	Management IP	Version	Status
Avaya SBCE	192.168.1.100	6.3.1-22-4853	Commissioned

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

The **System Information** screen shows **Network Configuration**, **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.

System Information: Avaya SBCE

General Configuration		Device Configuration		License Allocation	
Appliance Name	Avaya SBCE	HA Mode	No	Standard Sessions	2000
Box Type	SIP	Two Bypass Mode	No	Advanced Sessions	2000
Deployment Mode	Proxy			Scopia Video Sessions	500
				Encryption	

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
172.16.5.102	172.16.5.102	255.255.255.0	172.16.5.254	B1
172.16.5.103	172.16.5.103	255.255.255.0	172.16.5.254	B1
172.16.5.104	172.16.5.104	255.255.255.0	172.16.5.254	A1
172.16.5.199	172.16.5.199	255.255.255.0	172.16.5.254	A1

DNS Configuration		Management IP(s)	
Primary DNS	172.16.5.102	IP	172.16.5.71
Secondary DNS			
DNS Location	DMZ		
DNS Client IP	172.16.5.71		

On the previous screen, note that the **A1** interface corresponds to the inside interface (Private Network side) and **B1** interface corresponds to the outside interface (Public Network side) of the Avaya SBCE. Since a VPN connection was used with this solution to connect Claro's network to the enterprise network, the **A1** interface was used for access to the private enterprise network and to route calls to Claro's network across the VPN tunnel. In this solution, the **B1** interface was used for remote workers access to the enterprise. The configuration required for the **B1** interface is not discussed in this document. Refer to **Figure 1** for the IP addresses for both the A1 and B1 interfaces on the Avaya SBCE.

When a VPN connection is not used, the **B1** interface is normally used for remote workers access to the private network as well as to route calls to the Service Provider across the public Internet.

The management IP was blurred out for security reasons. The IP addresses used for the remote worker configuration was also blurred out since the remote worker configuration is beyond the scope of these Application Notes and is not discussed in these Application Notes.

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

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”, and then modified to meet specific requirements for the enterprise SIP-enabled solution.

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** (not shown).

For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the **General** tab:

- Check **T.38 Support**.
- Click **Next**.
- Leave other fields with their default values.
- Click **Finish** in the **Editing Profile** window.

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 links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration areas, with 'Global Profiles' expanded to show 'Server Interworking'. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'cs2100', 'avaya-sm', 'OCS-Edge-Server', 'cisco-cm', 'csp', 'Sipera-Hub', 'OCS-FrontEnd-Server', 'Avaya-SM' (highlighted), 'SP-General', 'Avaya-CS1000', 'Avaya-IP0', and 'Avaya-CM'. An 'Add' button is located above the list. The 'Avaya-SM' profile is selected, and its configuration is shown in the 'General' tab. The configuration table lists various settings and their values.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.30 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

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 links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo.

On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' expanded and 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left and a configuration table on the right.

The profile list on the left includes: es2100, avaya-ru, OCS-Edge-Server, cisco-cdm, cupa, Sipera-File, OCS-FrontEnd-Server, **Avaya-SM**, SP-General, Avaya-CS1000, Avaya-IPD, and Avaya-CM.

The configuration table for the 'Avaya-SM' profile is shown with the 'Advanced' tab selected. The table has columns for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Advanced' tab contains the following settings:

Setting	Value
Record Routes	Both
Topology Hiding: Change Call ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Contact 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
Lyric Extensions	No

7.2.2. Server Interworking SP-General

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

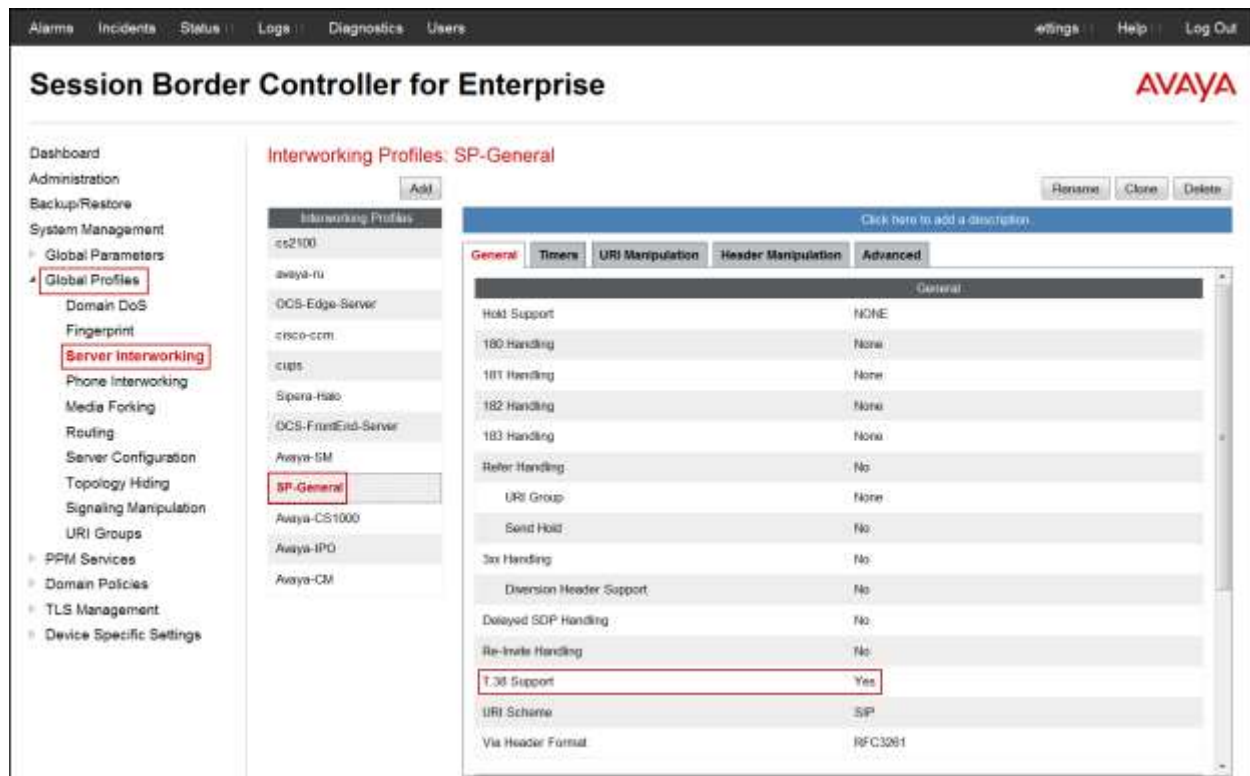
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add**.

Enter the new profile name (not shown), the name of **SP-General** was chosen in this example. Click **Next**:

On the **General** tab:

- Check **T.38 Support**.
- Leave other fields with their default values.
- Click **Next** until the Advanced tab is reached, then click **Finish** on the Advanced tab.

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



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 links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo.

On the left, a sidebar menu lists various configuration areas, with **Global Profiles** expanded to show **Server Interworking** as the selected option.

The main content area is titled **Interworking Profiles: SP-General**. It features a list of profiles on the left, including **SP-General**, which is highlighted. To the right of this list, there are tabs for **General**, **Timers**, **URI Manipulation**, **Header Manipulation**, and **Advanced**, with the **Advanced** tab currently selected.

The **Advanced** tab displays a table of configuration settings:

Setting	Value
Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
QCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SIP Content on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No
Lync Extensions	No

7.2.3. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [5] in the **References** section for more information on this topic.

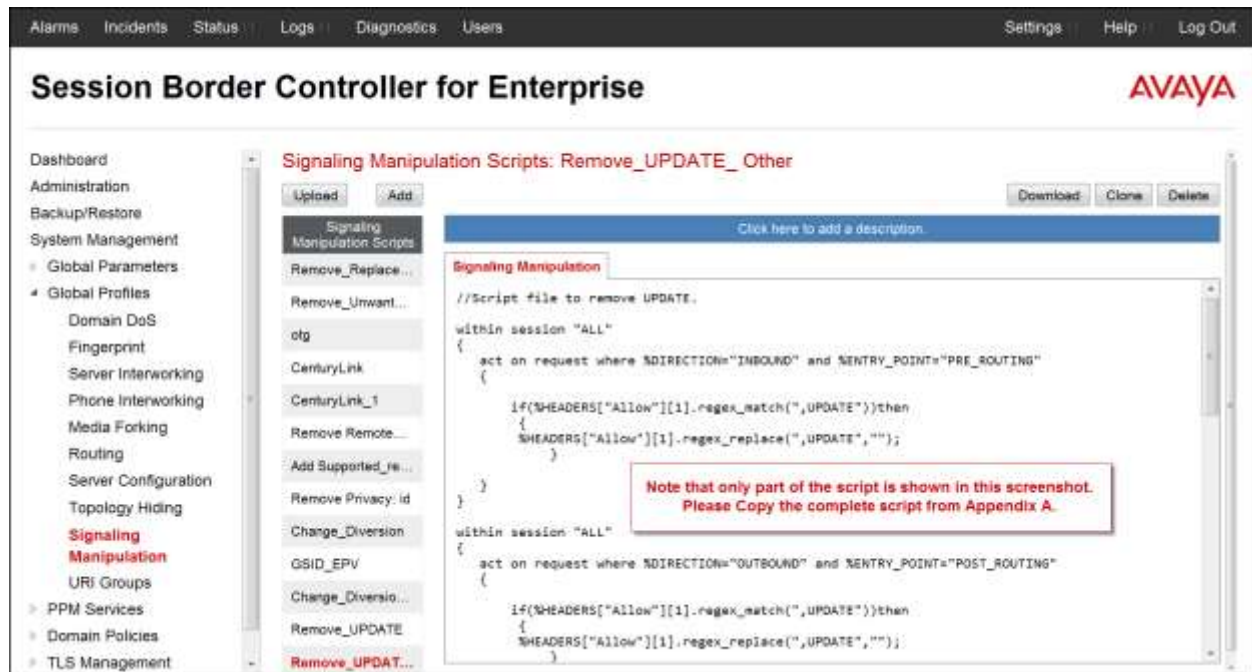
A Sigma script was created during the compliance test to disable/remove SIP UPDATES on the SIP trunk (refer to **Section 2.2**), to remove headers that should not be exposed outside of the enterprise and to remove headers that have no value to the service provider.

Note: Additional Avaya SBCE header manipulation will be performed by implementing Signaling Rules, in **Section 7.3.3** later in this document.

On the left navigation pane, select **Global Profiles → Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name ***Remove_UPDATE_Other*** was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

The following screen capture shows the **Remove_UPDATE_Other** SigMa script after it was added.



Note: Only part of the script is shown on the above screenshot, the **complete** script should be copied from **Appendix A**.

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** window:

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

IP Address / FQDN	Port	Transport
172.16.5.32	5060	TCP

- Click **Next** in the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** in the **Add Server Configuration Profile - Heartbeat** window (not shown).

In the **Add Server Configuration Profile - 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**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya-SM

Signaling Manipulation Script None

TCP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Back Finish

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

Session Border Controller for Enterprise

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

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

Server Configuration: Session Manager

Add

Session Manager

Service Provider

Com Manager

CS1000

IP Office

General Authentication Heartbeat Advanced

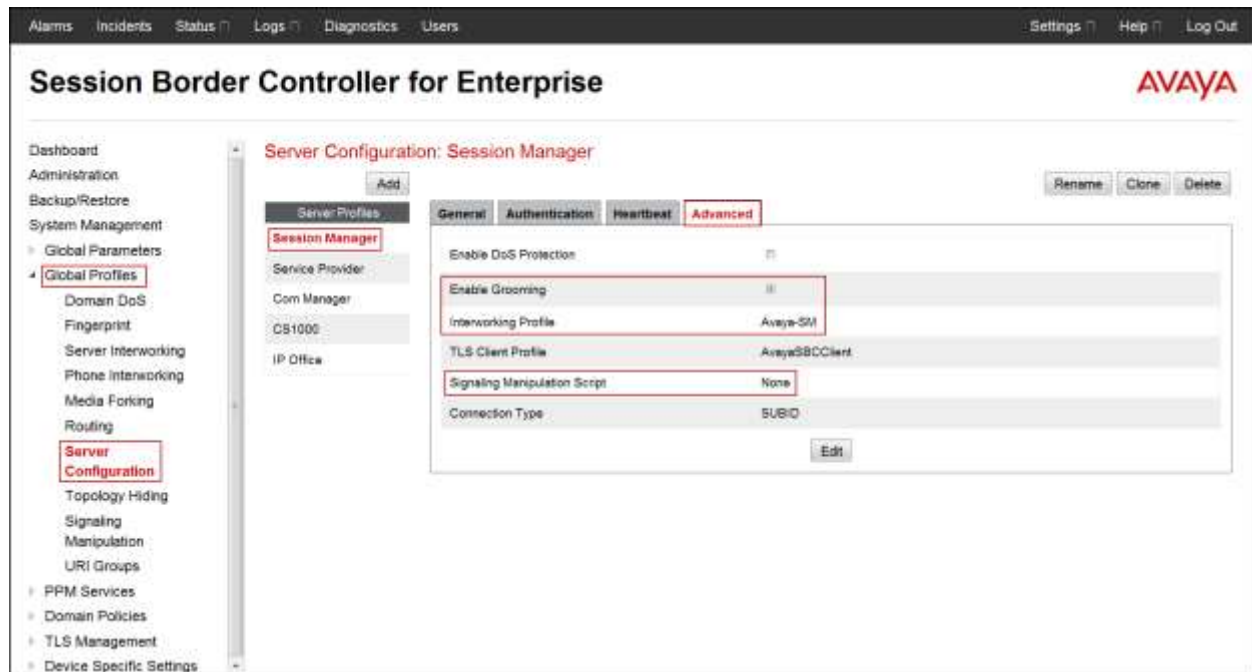
Server Type Cell Server

IP Address / FQDN	Port	Transport
172.16.5.32	5060	TCP

Edit

Rename Clone Delete

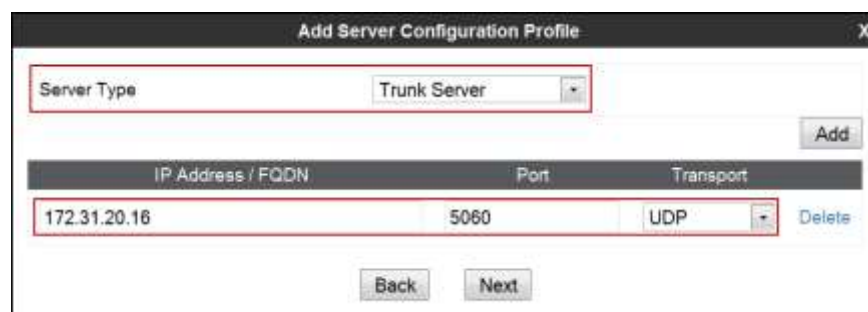
The following screen capture shows the **Advanced** tab of the newly created **Session Manager** Server Profile.



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

In the **Add Server Configuration Profile** window

- **Server Type:** select *Trunk Server*.
- **IP Address/FQDN:** *172.31.20.16* (Service Provider's SIP Proxy IP address).
- **Port:** *5060*.
- **Transports:** Select *UDP*.
- Click **Next**.



- Click **Next** in the **Add Server Configuration Profile - Authentication** window (not shown).
- Click **Next** in the **Add Server Configuration Profile - Heartbeat** window (not shown).

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

- Select **SP-General** from the **Interworking Profile**.
- Select **Remove_UPDATE_Other** from the **Signaling Manipulation Script**, script created in **Section 7.2.3**.
- Click **Finish**.

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

Signaling Manipulation Script Remove_UPDATE_Other

Connection Type SUBID

Back Finish

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

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

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

Server Configuration: Service Provider

Add Rename Clone Delete

Server Profile General Authentication Heartbeat Advanced

Session Manager

Service Provider

Com Manager

CS1000

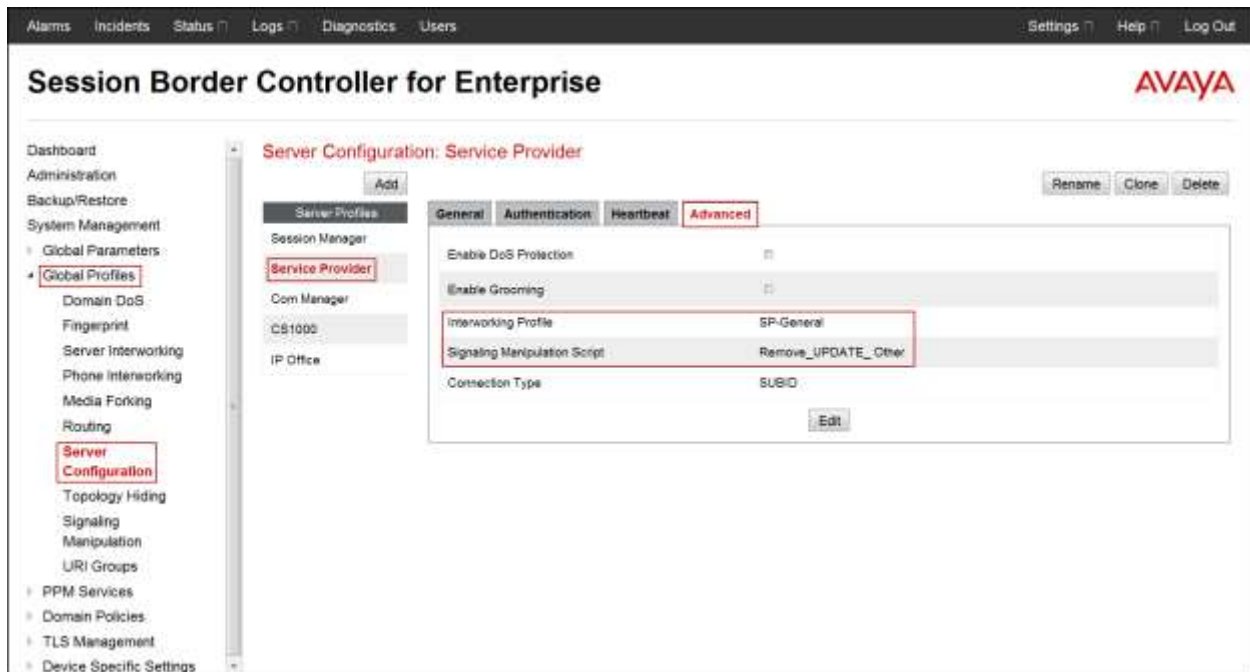
IP Office

Server Type Trunk Server

IP Address / FQDN	Port	Transport
172.31.20.15	5060	UDP

Edit

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



7.2.5. 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.

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

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SM**.
- Click **Next**.

On the **Routing Profile** screen complete the following:

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

The screenshot shows the 'Routing Profile' configuration window. It includes fields for 'URI Group' and 'Time of Day' (set to 'default'). Below these are sections for 'Load Balancing' (set to 'Priority'), 'NAPTR' (unchecked), 'Transport' (set to 'None'), and 'Next Hop Priority' (checked). There is also an 'Ignore Route Header' checkbox (unchecked) and an 'Add' button. A table at the bottom lists the configured next-hop addresses:

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

Buttons for 'Back' and 'Finish' are located at the bottom of the window.

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

On the left, a sidebar menu lists various configuration areas: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing (highlighted), Server Configuration, Topology Hiding, Signaling, Manipulation, URI Groups, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

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 (highlighted), Route_to_SP, Route_to_CM, Route_to_CS1000, Route_to_IPC, and To SM from Rem W. The 'Route_to_SM' profile is selected, showing its configuration details.

The 'Route_to_SM' profile configuration includes a description field with the placeholder 'Click here to add a description.' Below this is a table with the following columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table contains one entry:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	172.16.5.32	TCP

Buttons for 'Update Priority', 'Add', 'Edit', and 'Delete' are visible next to the table entry.

Similarly, for the outbound route:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SP**.
- Click **Next**.

On the **Routing Profile** screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select *Service Provider*.
- **Next Hop Address:** Select **172.31.20.16:5060 (UDP)** (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.

The screenshot shows the 'Routing Profile' configuration window. It includes fields for 'URI Group', 'Time of Day', 'Load Balancing', 'Transport', 'Next Hop In-Dialog', and 'Ignore Route Header'. An 'Add' button is located below these fields. Below the 'Add' button is a table with the following columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The first row of the table is highlighted with a red box and contains the values: '1', 'Service Provider', '172.31.20.16:5060 (UDP)', and 'None'. A 'Delete' button is located to the right of the 'None' value. At the bottom of the window are 'Back' and 'Finish' buttons.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	172.31.20.16:5060 (UDP)	None

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

On the left, a sidebar menu lists various configuration areas: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing (highlighted), Server Configuration, Topology Hiding, Signaling, Manipulation, URI Groups, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled 'Routing Profiles: Route_to_SP'. It features a list of routing profiles on the left: default, Route_to_SM, Route_to_SP (highlighted), Route_to_CM, Route_to_CS1000, Route_to_IPO, and To SM from Rem W. The 'Route_to_SP' profile is selected, and its configuration is shown on the right.

The 'Route_to_SP' profile configuration includes a table with the following columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table contains one entry:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	172.31.20.16	UDP

Buttons for 'Add', 'Update Priority', 'Rename', 'Clone', and 'Delete' are visible. The 'Add' button is located at the top right of the profile configuration area, and the 'Update Priority' button is located above the table.

7.2.6. 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.
- For **Request-Line** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Enterprise (***avaya.lab.com***) under **Overwrite Value**.
- For **From** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the enterprise (***avaya.lab.com***) under **Overwrite Value**.
- For **To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (***avaya.lab.com***) under **Overwrite Value**.

The screenshot shows a window titled "Edit Topology Hiding Profile" with a table of SIP headers and their configuration. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The rows are: Record-Route, SDP, Referred-By, Request-Line, From, Via, To, and Refer-To. The Request-Line, From, and To rows are highlighted with a red box, indicating they are the focus of the configuration. The Replace Action for these rows is set to "Overwrite" and the Overwrite Value is set to "avaya.lab.com".

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

Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' expanded and 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: Session_Manager' and features an 'Add' button and action buttons (Rename, Clone, Delete). Below this is a table for configuring topology hiding rules. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. Several rows are visible, with 'Request-Line', 'From', 'To', and 'Refer-To' highlighted by red boxes. The 'Request-Line' and 'From' rows show an 'Overwrite' action with the value 'avaya.lab.com'. The 'To' row also shows an 'Overwrite' action with the value 'avaya.lab.com'. The 'Refer-To' row shows an 'Auto' action. An 'Edit' button is located at the bottom of the table.

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.lab.com
From	IP/Domain	Overwrite	avaya.lab.com
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.lab.com
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 added **Service_Provider** Topology Hiding profile.
- For **Request-Line** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the service provider (***ims.claro.com.do***) under **Overwrite Value**.
- For **From** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***ims.claro.com.do***) under **Overwrite Value**.
- For **To** under **Header**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the service provider (***ims.claro.com.do***) under **Overwrite Value**.

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

Finish

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

Session Border Controller for Enterprise AVAYA

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Topology Hiding Profiles: Service_Provider

[Add](#) [Rename](#) [Clone](#) [Delete](#)

Click here to add a description.

Topology Hiding

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

[Edit](#)

7.3. Domain Policies

Domain Policies allow the configuration of 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. Domain Policies include rules for Application, Media, Signaling, Security, etc.

Note: The **default-trunk** Application Rule could have been used instead of creating a new one, but a new Application Rule was created to allow changes in the future.

7.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

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

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

Miscellaneous
CDR Support: ☒ None, ☐ CDR w/ RTP, ☐ CDR w/o RTP
RTCP Keep-Alive: ☐

Back Finish

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

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

On the left, a sidebar menu lists various configuration areas, with 'Domain Policies' and 'Application Rules' highlighted. The 'Application Rules' section is expanded, showing a list of rules including 'default', 'default-trunk', 'default-subscriber-low', 'default-subscriber-h...', 'default-server-low', 'default-server-high', '2000 Sessions', '500 Sessions', 'Remote-Workers', and 'test'. The '2000 Sessions' rule is selected.

The main content area shows the configuration for the '2000 Sessions' rule. It includes a title 'Application Rules: 2000 Sessions' and buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below the title, there is a blue bar with the text 'Click here to add a description.'.

The 'Application Rule' section contains a table with the following data:

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

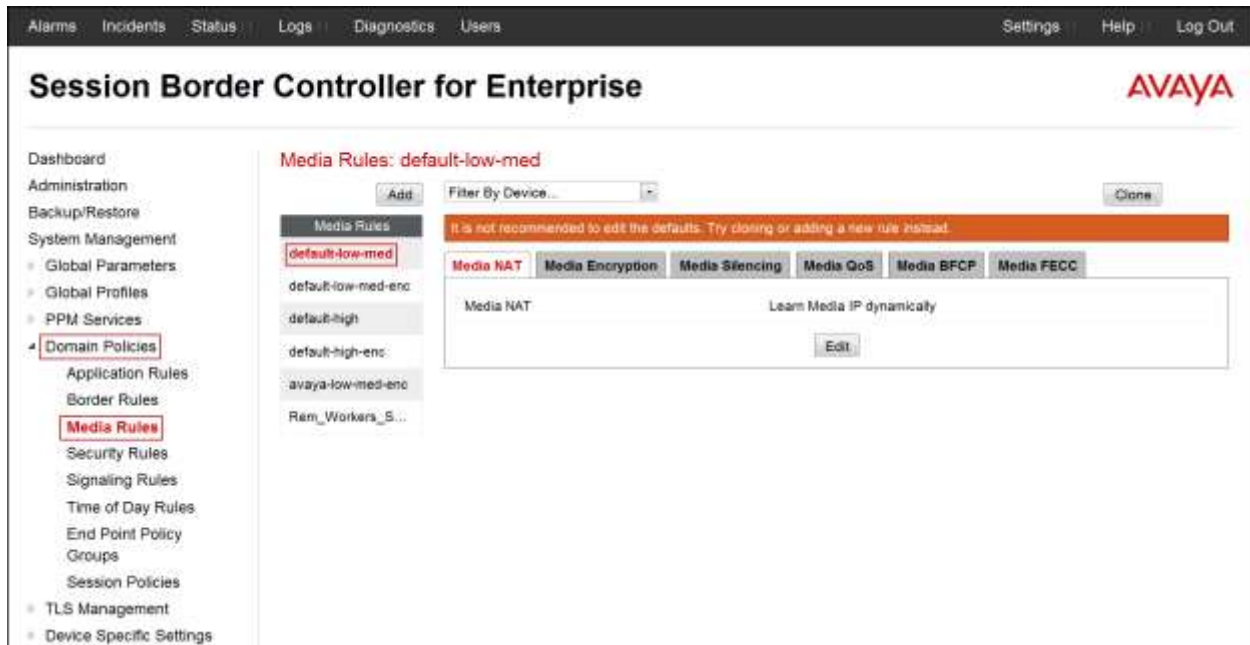
Below the table, there is a 'Miscellaneous' section with the following data:

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

An 'Edit' button is located at the bottom right of the 'Miscellaneous' section.

7.3.2. Media Rules

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



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 Rule was created, to later be applied in the direction of the enterprise to block unwanted headers coming from Session Manager from being propagated to Claro's network. To add this header, 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_CM_SigRule*. Click **Finish**.

Select the **Request Headers** tab of the newly created *SessMgr_CM_SigRule* Signaling Rule.

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

- Select **Add in Header Control**.

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

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

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

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

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

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

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

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

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

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

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

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

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

The following screen capture shows the **Request Headers** tab of the **SessMgr_CM_SigRule** Signaling Rule.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows a navigation menu with 'Domain Policies' expanded and 'Signaling Rules' selected. The main content area is titled 'Signaling Rules: SessMgr_CM_SigRule'. It features a table with columns: Row, Header Name, Method Name, Header Criteria, Action, Proprietary, and Direction. The table lists seven headers, with the last two, 'P-Charging-Vector' and 'P-Location', highlighted with a red border. The 'Request Headers' tab is active, and the 'Add In Header Control' button is visible.

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

Next, select the **Response Headers** tab of the newly created **SessMgr_CM_SigRule** 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*.
- **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 **AV-Global-Session-ID** header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *AV-Global-Session-ID*.
- **Response Code:** *4XX*.
- **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:** *5XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

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

- Select **Add in Header Control**.
- **Header Name:** *Alert-Info*.

- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

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

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

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

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

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

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

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

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-AV-Message-ID*.

- **Response Code:** *200*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

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

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

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

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Conference*.
- **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**.

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

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name:** *P-Location*.
- **Response Code:** *4XX*.
- **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:** *5XX*.
- **Method Name:** *ALL*.
- **Header Criteria:** *Forbidden*.
- **Presence Action:** *Remove Header*.
- Click **Finish**.

The following screen capture shows the **Response Headers** tab of the **SessMgr_CM_SigRule** signaling rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'Signaling Rules' selected. The main content area shows the configuration for the 'SessMgr_CM_SigRule' signaling rule. The 'Response Headers' tab is active, displaying a table of response headers.

Line	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Describe
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
3	AV-Global-Session-ID	4XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
4	AV-Global-Session-ID	5XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
5	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	0:00 Delete
6	Endpoint-Name	1XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
7	Endpoint-Name	2XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
8	P-AM-Message-ID	1XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
9	P-AM-Message-ID	2XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
10	P-Changing-Vector	2XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
11	P-Confidence	2XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
12	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
13	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
14	P-Location	4XX	ALL	Forbidden	Remove Header	Yes	0:00 Delete
15	P-Location	5XX	ALL	Forbidden	Remove Header	Yes	0:00 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 Group**, under **Group Name** enter *Enterprise*.

- **Application Rule:** *2000 Sessions*.
- **Border Rule:** *default*.
- **Media Rule:** *default-low-med*.
- **Security Rule:** *default-low*.
- **Signaling Rule:** *SessMgr_CM_SigRule*.
- Click **Finish**.

Policy Group

Application Rule: 2000 Sessions

Border Rule: default

Media Rule: default-low-med

Security Rule: default-low

Signaling Rule: SessMgr_CM_SigRule

Back Finish

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

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles PPM Services **Domain Policies** Application Rules Border Rules Media Rules Security Rules Signaling Rules Time of Day Rules **End Point Policy Groups** Session Policies TLS Management Device Specific Settings

Policy Groups: Enterprise

Add Filter By Device: [v] Rename Clone Delete

Click here to add a description.

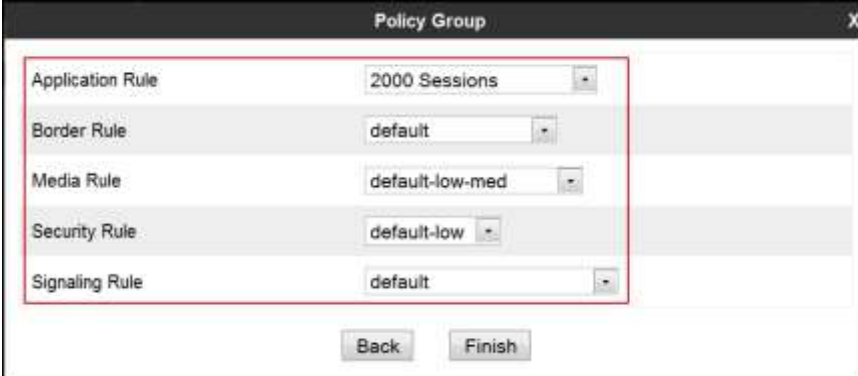
Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	Summary
1	2000 Sessions	default	default-low-med	default-low	SessMgr_CM_SigRule	Edit

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**, under **Group Name** enter *Service Provider*.

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



The screenshot shows a 'Policy Group' configuration window. It contains five rows, each with a label and a dropdown menu. The 'Application Rule' dropdown is set to '2000 Sessions'. The 'Border Rule' dropdown is set to 'default'. The 'Media Rule' dropdown is set to 'default-low-med'. The 'Security Rule' dropdown is set to 'default-low'. The 'Signaling Rule' dropdown is set to 'default'. At the bottom of the window are two buttons: 'Back' and 'Finish'. A red rectangular box highlights the five rows containing the rule dropdowns.

Rule Type	Selected Value
Application Rule	2000 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default

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

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

On the left, a sidebar menu lists various configuration areas, with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area shows a list of policy groups on the left and a detailed view of the 'Service Provider' group on the right.

The 'Service Provider' group details include a table with the following data:

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

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.

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

Use **Figure 1** as reference for IP address assignments.

Note: Only the highlighted entity items were created for the compliance test, and are the ones relevant to these Application Notes. Blurred out items are part of the Remote Worker configuration, which is not discussed in this Application Notes.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Network Management: Avaya SBCE

Devices Interfaces **Networks**

Avaya SBCE

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	172.16.5.254	255.255.255.0	A1	172.16.5.71	Edit Delete
Network_B1	172.16.5.254	255.255.255.0	A1	172.16.5.100	Edit Delete

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar lists various management sections, with "Device Specific Settings" expanded to show "Network Management". The main content area is titled "Network Management: Avaya SBCE" and features tabs for "Devices", "Interfaces", and "Networks". The "Interfaces" tab is active, showing a table of interfaces. The table has columns for "Interface Name", "VLAN Tag", and "Status".

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

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, port range 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside, private Media Interface of the Avaya SBCE.

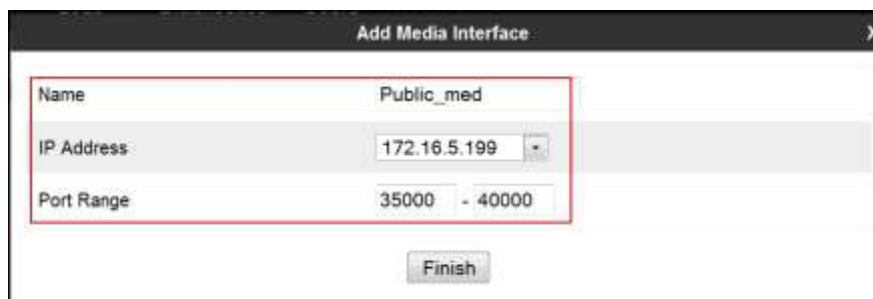
- Select **Add** in the **Media Interface** area.
- **Name:** *Private_med*.
- **IP Address:** *172.16.5.71* (Inside or A1 IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Private_med", "IP Address" with the value "172.16.5.71" and a dropdown arrow, and "Port Range" with the value "35000 - 40000". 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.

Below is the configuration of the outside, public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name:** *Public_med*.
- **IP Address:** *172.16.5.199* (IP Address of the Avaya SBCE toward the Service Provider via the VPN Tunnel).
- **Port Range:** *35000-40000*.
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Public_med", "IP Address" with the value "172.16.5.199" and a dropdown arrow, and "Port Range" with the value "35000 - 40000". 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 Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left-hand navigation menu lists various system management options, with "Device Specific Settings" and "Media Interface" highlighted. The main content area is titled "Media Interface: Avaya SBCE" and contains 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 with columns for Name, Media IP, Port Range, and actions (Edit, Delete). The table lists three media interfaces: Private_med, Public_med, and two others with partially obscured names. The first two are highlighted with red boxes.

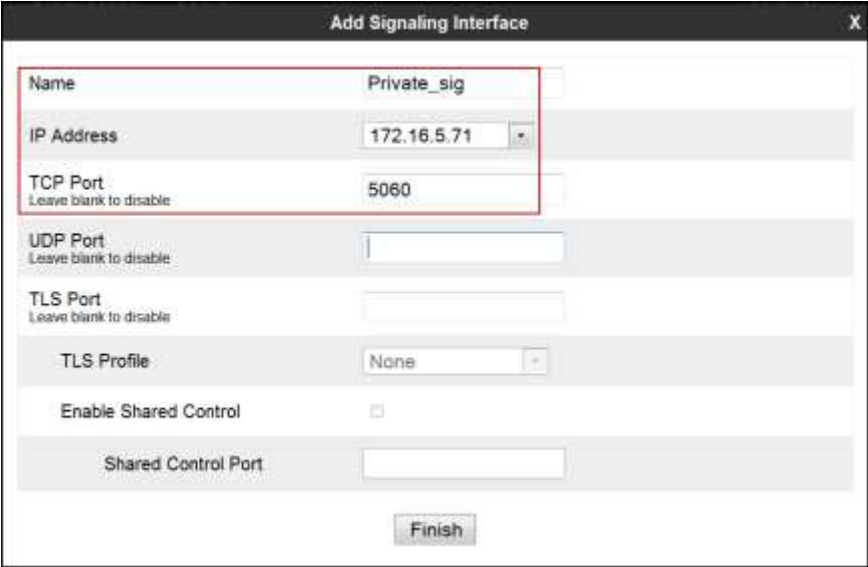
Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.71	35000 - 40000	Edit	Delete
Public_med	172.16.5.199	35000 - 40000	Edit	Delete
...	Edit	Delete
...	Edit	Delete

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**.

Below is the configuration of the inside private Signaling Interface of the Avaya SBCE.

- 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* (It should be noted that in a customer environment TLS would normally be used. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic is not encrypted).
- Click **Finish**.



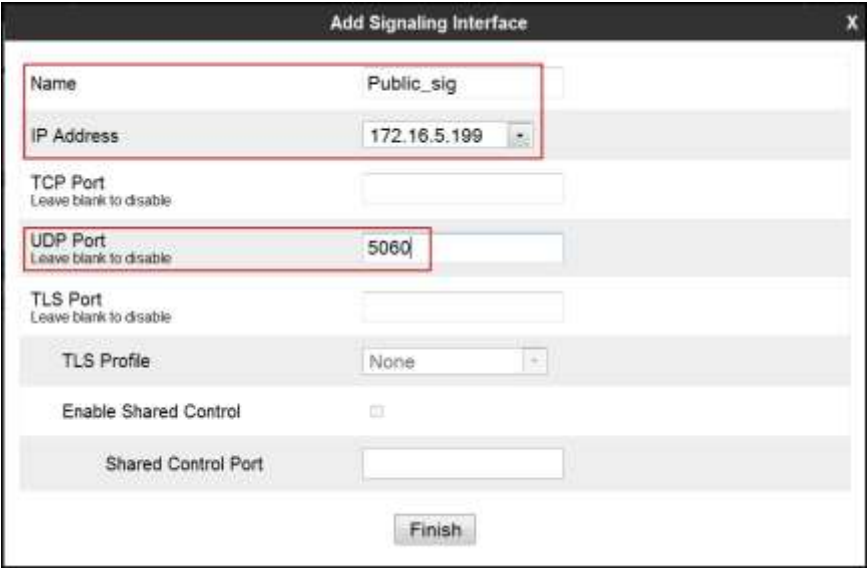
The screenshot shows a web-based configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. A red rectangular box highlights the first three fields: "Name" (containing "Private_sig"), "IP Address" (containing "172.16.5.71"), and "TCP Port" (containing "5060"). Below these are "UDP Port" (empty), "TLS Port" (empty), "TLS Profile" (containing "None"), "Enable Shared Control" (checkbox), and "Shared Control Port" (empty). The "Finish" button is located at the bottom center of the window.

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>	
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Below is the configuration of the outside, public signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area.
- **Name:** *Public_sig*.
- **IP Address:** *172.16.5.199* (IP Address of the Avaya SBCE toward the Service Provider via the VPN Tunnel).
- **UDP Port:** *5060*.
- Click **Finish**.



The screenshot shows a configuration window titled "Add Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are as follows:

Field	Value
Name	Public_sig
IP Address	172.16.5.199
TCP Port	
UDP Port	5060
TLS Port	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

The "Finish" button is located at the bottom center of the window.

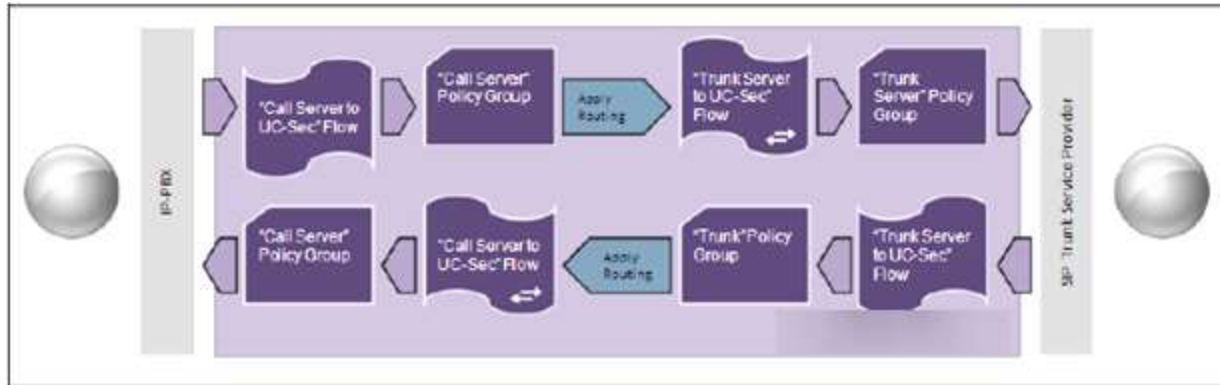
The following screen capture shows the newly created **Signaling Interfaces**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration options, with "Signaling Interface" highlighted under "Device Specific Settings". The main content area is titled "Signaling Interface: Avaya SBCE" and features a tabbed interface with "Devices" and "Signaling Interface" tabs. A warning message states: "Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this, a table lists the configured signaling interfaces:

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Private_sig	172.16.5.71	5060	---	---	None	Edit	Delete
Public_sig	172.16.5.159	---	5060	---	None	Edit	Delete
192.168.1.1	192.168.1.1	---	---	---	DefaultProfile	Edit	Delete
192.168.1.1	192.168.1.1	---	---	---	DefaultProfile	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** defines 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**, and then the **Server Flows** tab. Click **Add** (not shown).

- **Flow Name:** *SIP_Trunk_Flow*.
- **Server Configuration:** *Service Provider*.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** *Private_sig*.
- **Signaling Interface:** *Public_sig*.
- **Media Interface:** *Public_med*.
- **End Point Policy Group:** *Service Provider*.
- **Routing Profile:** *Route_to_SM* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Service_Provider*.
- **File Transfer Profile:** *None*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.



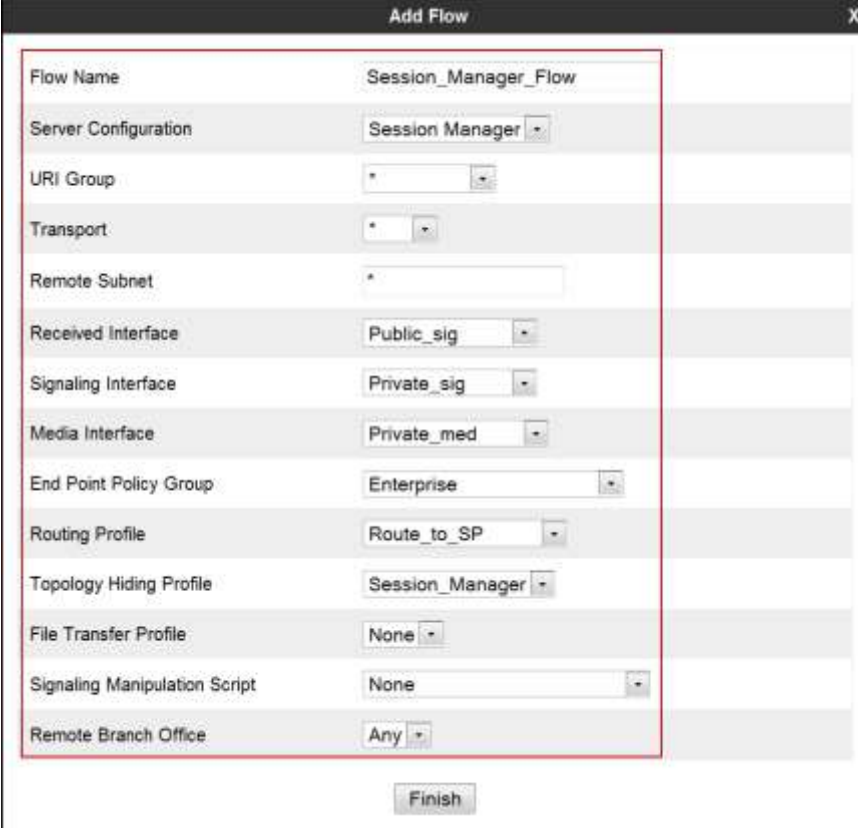
The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. Inside the window is a form with 15 fields, each with a label and a value or dropdown menu. A red rectangular box highlights the first 13 fields. The fields and their values are:

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

At the bottom of the form is a "Finish" button.

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

- **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* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Session_Manager*.
- **File Transfer Profile:** *None*.
- **Signaling Manipulation Script:** *None*.
- **Remote Branch Office:** *Any*.
- Click **Finish**.



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

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

At the bottom of the window, there is a "Finish" button.

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

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

On the left, a sidebar menu lists various configuration categories. Under "Device Specific Settings", the "End Point Flows" option is highlighted with a red box.

The main content area is titled "End Point Flows: Avaya SBCE". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab. Below the tabs, there is a section for "Server Configuration: Service Provider" and another for "Server Configuration: Session Manager".

The "Server Configuration: Service Provider" section contains a table with the following data:

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 Close Edit Delete

The "Server Configuration: Session Manager" section contains a table with the following data:

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

8. Claro SIP Trunking Service Configuration

To use Claro's SIP Trunking Service, a customer must request the service from Claro using the established sales processes. The process can be started by contacting Claro via the corporate web site at: <http://www.claro.com.do/wps/portal/do/sc/empresas> and requesting information.

During the signup process, Claro and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Claro's network. Claro will provide IP addresses, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc.. This information is used to complete the Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

During the interoperability testing, a VPN connection was used to connect the simulated enterprise site to Claro's network via the public Internet. The connection could also be done without the use of a VPN connection, by directly connecting the Avaya SBCE via the public Internet to a public facing SBC located in Claro's network. This is accomplished by assigning public IP addresses, capable of being reached across the public Internet, to the Avaya SBCE (interface **B1**) and to the Claro's SBC.

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.

Verification Steps:

1. 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.
2. 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.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.1. Troubleshooting

9.1.1. 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. Session Manager

- **traceSM -x** – Session Manager command line tool for traffic analysis. Login to the Session Manager management CLI 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.

9.1.3. Avaya SBCE

There are several links and menus located on the taskbar at the top of the screen of the web interface that can be used for diagnostic and troubleshooting.

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

Session Border Controller for Enterprise

Dashboard

Information

System Time	11:51:08 PM GMT-06:00	Refresh
Version	6.3.1-22-4653	
Build Date	Fri Nov 21 17:35:09 EST 2014	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message

Notes

No notes found.

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

Alarm Viewer

Devices

EMS
Avaya SBCE

Alarms

#	ID	Details	State	Time	Device
No alarms found for this device.					

Clear Selected **Clear All**

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

Session Border Controller for Enterprise AVAYA

Dashboard

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - PPM Services
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Information

System Time	11:51:08 PM GMT-08:00	Refresh
Version	6.3.1-22-4853	
Build Date	Fri Nov 21 17:35:09 EST 2014	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	

Installed Devices

EMS
Avaya SBCE

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message

[Add](#)

Notes

No notes found.

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

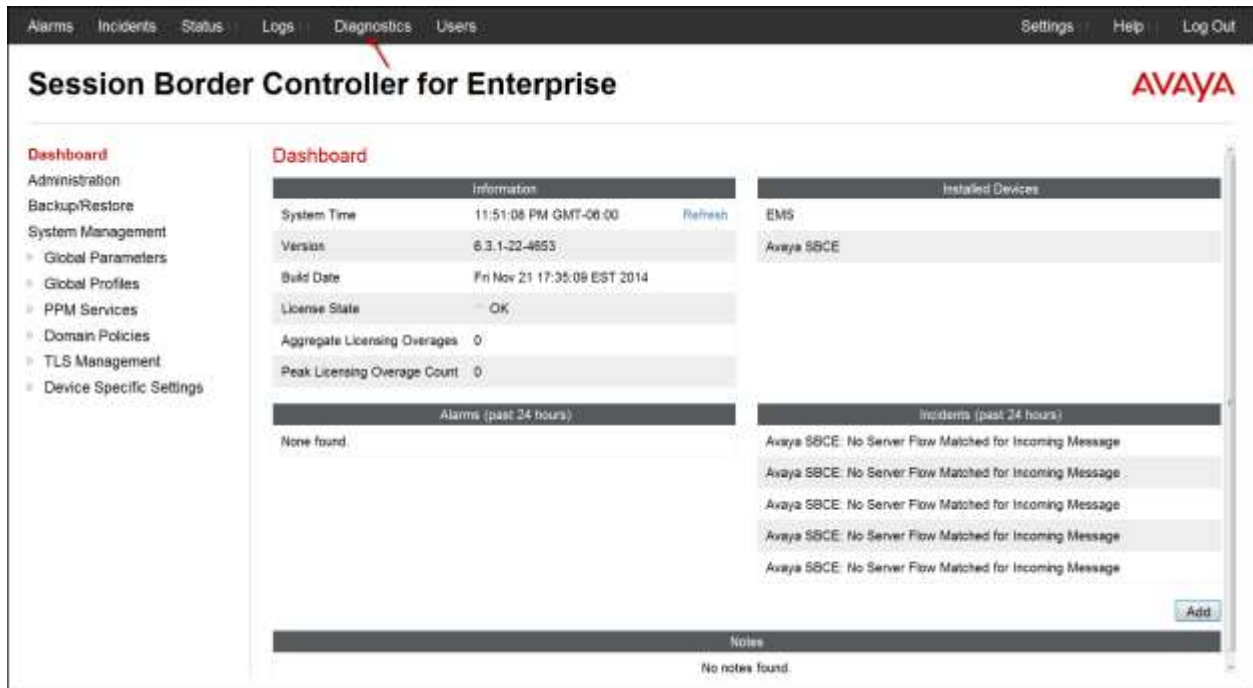
Device: Avaya SBCE Category: Protocol Discrepancy [Clear Filters](#) [Refresh](#) [Generate Report](#)

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

1

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



The following screen shows the Diagnostics page with the results of a ping test. Note that IP addresses have been blurred out for security reasons.

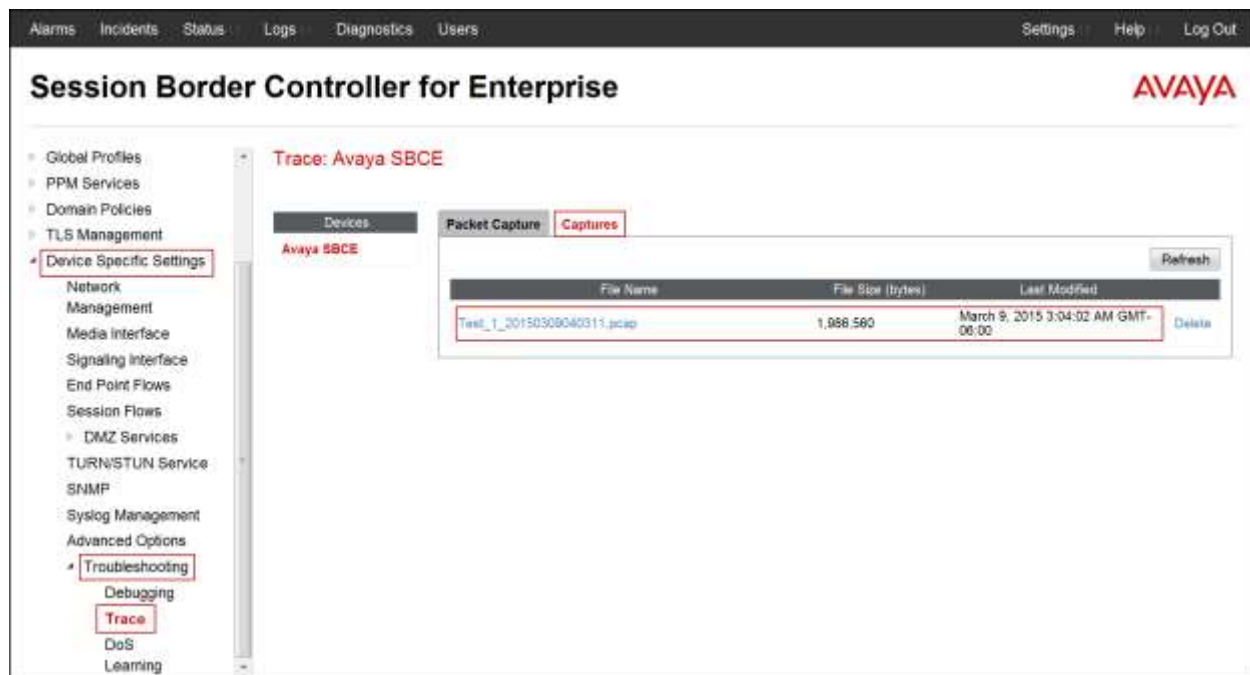


Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as pcap files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web management interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand sidebar contains a tree menu with categories like Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under "Device Specific Settings", the "Troubleshooting" sub-menu is expanded, and the "Trace" option is selected. The main content area is titled "Trace: Avaya SBCE" and features three tabs: "Devices", "Packet Capture", and "Captures". The "Packet Capture" tab is active, showing a "Packet Capture Configuration" form. This form includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (a text input field), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Test_1.pcap). Below the form are "Start Capture" and "Clear" buttons.

Packet Capture Configuration	
Status	Ready
Interface	Any
Local Address <small>[IP v4]</small>	All
Remote Address <small>* IP v4, IP v6</small>	
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	Test_1.pcap

Once the capture is stopped, click on the **Captures** tab and select the proper pcap file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.



10. Conclusion

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Aura® Communication Manager Release 6.3, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.3 to support Claro SIP Trunking Service, 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 6.3.10*, Release 6.3, Issue 6, February 2015.

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

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

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

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

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

- [7] *Administering Avaya one-X® Communicator*, Release 6.2 FP4, October 2014.
- [8] *Avaya one-X® Communicator Overview and Planning*, Release 6.2 FP4, October 2014.
- [9] *Implementing Avaya one-X® Communicator*, Release 6.2 FP4, October 2014.
- [10] *Using Avaya one-X® Communicator*, Release 6.2 FP4, October 2014.
- [11] *Using Avaya Communicator for Windows*, Release 2.1, Document Number: 18-604158, Issue 3, December 2014.
- [12] *Administering Avaya Communicator for Android, iPad, iPhone, and Windows*, Release 2.1, Issue 2, March 2015.

- [13] 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

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

<https://downloads.avaya.com/css/P8/documents/100183254>

Other resources:

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

12. Appendix A: SigMa Script

Following is the Signaling Manipulation script that was used in the configuration of the Avaya SBCE, **Section 7.2.3**. When adding this script as instructed in **Section 7.2.3** enter a name for the script in the Title (e.g., **Remove_UPDATE_Other**) and copy/paste the entire script, starting on the line **//Script to disable SIP UPDATES on the Trunk**, shown below.

Title: Remove_UPDATE_Other

//Script to disable SIP UPDATES on the Trunk.

```
within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and
  %ENTRY_POINT="PRE_ROUTING"
  {
    if(%HEADERS["Allow"][1].regex_match(",UPDATE"))then
    {
      %HEADERS["Allow"][1].regex_replace(",UPDATE","");
    }
  }
}

within session "ALL"
{
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    if(%HEADERS["Allow"][1].regex_match(",UPDATE"))then
    {
      %HEADERS["Allow"][1].regex_replace(",UPDATE","");
    }
  }
}

within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and
  %ENTRY_POINT="PRE_ROUTING"
  {
    if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
```



```

    {
    %HEADERS["Allow"][1].regex_replace(", UPDATE","");
    }

}

}

within session "ALL"
{
  act on request where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {

    if(%HEADERS["Allow"][1].regex_match(", UPDATE"))then
    {
      %HEADERS["Allow"][1].regex_replace(", UPDATE","");
    }

  }
}

```

//Script to remove gsid and epv parameters in outbound Contact header.

```

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

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

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

```

//Script to remove Remote-Address.

```

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

```

©2015 Avaya Inc. All Rights Reserved.

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

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