



Application Notes for Configuring Axtel SIP Trunk Service with Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedures required for configuring Session Initiation Protocol (SIP) trunk service between Axtel and an Avaya SIP-enabled enterprise solution. The Avaya SIP-enabled enterprise solution consists of Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

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.

The SIP trunk service offered by Axtel provides customers with PSTN access via a SIP trunk between the enterprise and Axtel's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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.....	3
2.	General Test Approach and Test Results.....	3
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration	7
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager.....	11
5.1.	Licensing and Capacity	11
5.2.	System Features.....	12
5.3.	IP Node Names.....	14
5.4.	Codecs	15
5.5.	IP Network Regions	17
5.6.	Signaling Group	19
5.7.	Trunk Group.....	21
5.8.	Calling Party Information.....	25
5.9.	Inbound Routing.....	26
5.10.	Outbound Routing	27
6.	Configure the Avaya Session Border Controller for Enterprise	31
6.1.	System Access.....	31
6.2.	System Management	32
6.3.	Global Profiles.....	33
6.3.1.	Server Interworking Avaya-CM	33
6.3.2.	Server Interworking SP-General.....	36
6.3.3.	Routing Profiles	39
6.3.4.	Signaling Manipulation.....	43
6.3.5.	Server Configuration.....	45
6.3.6.	Topology Hiding.....	51
6.4.	Domain Policies	55
6.4.1.	Signaling Rules	55
6.4.2.	End Point Policy Groups.....	61
6.5.	Device Specific Settings.....	63
6.5.1.	Network Management.....	63
6.5.2.	Media Interface	64
6.5.3.	Signaling Interface	66
6.5.4.	End Point Flows.....	68
7.	Axtel SIP Trunk Configuration.....	72
8.	Verification and Troubleshooting	72
8.1.	General Verification Steps	72
8.2.	Avaya Aura® Communication Manager Verification.....	72
8.3.	Avaya Session Border Controller for Enterprise Verification	72
9.	Conclusion	77
10.	References.....	77
11.	Appendix A.....	78

1. Introduction

These Application Notes describe the procedures required for configuring Session Initiation Protocol (SIP) trunk service between Axtel and an Avaya SIP-enabled enterprise solution. The Avaya SIP-enabled enterprise solution consists of Avaya Aura® Communication Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints. The solution does not include Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

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

The Avaya enterprise solution can be configured to authenticate with the SIP service provider using either SIP Trunk Registration (Dynamic) or Static IP Authentication. Even though these Application Notes cover the configuration of the Avaya SBCE using SIP Trunk Registration (Dynamic) for authentication with Axtel, both authentication methods were successfully tested during the compliance tests.

The terms “Service Provider” and “Axtel” will be used interchangeable throughout these Application Notes.

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Axtel SIP Trunk service via a broadband connection to the public Internet.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- SIP Trunk Registration (Dynamic) and Static IP Authentication with the service provider.
- Incoming PSTN calls to various Deskphones types. Deskphone types included H.323, digital, and analog at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various Deskphones types. Deskphone types included H.323, digital, and analog at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the callee.
- 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.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones in the “This Computer” and “Other Phone” modes. (H.323).
- Various call types, including local, long distance national, cellular, etc.
- Proper Codec negotiation and two way speech-path. (Testing was performed with codecs: G.729A, G.711A and G.711U, Axtel’s preferred codec order).
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail, etc.), with DTMF tone transmissions passed as out-of-band RTP events (RFC 2833).
- Caller ID presentation and Caller ID restriction.
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular call redirection).
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling the SIP connection.
- Routing inbound PSTN calls to call center agent queues.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test.
- Operator services such as dialing 0 or 0 + 10 digits are not supported by Axtel.
- T.38 fax is not supported by Axtel.
- Network Call Redirection (NCR) using the REFER or 302 Moved Temporarily methods are not supported Axtel.
- International calls were restricted by Axtel, hence they were not tested.

2.2. Test Results

Interoperability testing of the Axtel SIP Trunk service with the Avaya SIP-enabled enterprise solution was completed successfully, with the observations/limitations listed below:

- **Caller ID on outbound calls:** On outbound calls, the caller ID number displayed on the PSTN user was always the main number assigned to the SIP trunk by Axtel, regardless of the specific DID number sent in the origination headers from the enterprise. This seems to be the desired configuration on the Axtel network, and it is listed here simply as an observation.
- **Outbound Calling Party Number (CPN) Block:** To support outbound privacy calls (calling party number blocking), Communication Manager sends “anonymous” as the calling number in the SIP From header, uses the P-Asserted-Identity (PAI) header to pass the actual calling party number and includes “Privacy: id” in the INVITE message. During testing Axtel’s network was configured to ignore the SIP From header for this purpose thus the Calling Party Number (CPN) was not blocked, the main number assigned to the SIP trunk by Axtel continued to be displayed on the PSTN user as described in the above observation.
- **Caller ID on incoming calls from U.S. based PSTN numbers:** Calls originating from PSTN telephones based in the U.S. to DID numbers in Mexico assigned to the SIP trunk, will display unrecognized numbers (e.g., **5511641931**, **5551470694**, etc.). During the compliance test, Axtel provided a local PSTN test number in Monterrey, Mexico. A SIP-based softphone was registered to this local PSTN number and was used to originate and terminate PSTN calls to and from the enterprise. The correct Caller ID was displayed at the enterprise extensions when calling from this local PSTN number. This behavior is not necessarily indicative of a limitation of the combined Axtel/Avaya solution, this seems to be the desired behavior for international calls, it is listed here simply as an observation.
- **Enterprise phones displays “anonymous”:** On outbound calls, the 200 OK message sent from Axtel as a response to the INVITE sent by the enterprise included a P-Asserted-Identity (PAI) header with an “anonymous;phone-context=unknown” parameter. The inclusion of this header made the display on the enterprise extensions (calling party) change from the called number to “anonymous”, once the calls was answered by the PSTN party. To avoid this issue, a Signaling Rule was created on the Avaya SBCE to remove the PAI header in the 200 OK sent by Axtel on outbound calls.
- **Fax:** At the present time Axtel only supports G.711 fax pass-through transmission, T.38 fax is not supported. G.711 fax pass-through is available with Communication Manager on a “best effort” basis, it’s not guaranteed that it will work; therefore G.711 fax pass-through is not recommended with this solution and was not tested.
- **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 the Axtel network. The following headers were removed by using Signaling Rules and a Sigma Script in the Avaya SBCE: Alert-Info, AV-Global-Session-ID, Endpoint-View, P-

AV-Message-ID, P-Charging-Vector, P-Location and Remote-Address. See **Sections 6.3.4** and **7.4.1** later in this document.

2.3. Support

For technical support on the Axtel SIP trunk service offer, visit <http://www.axtel.mx/>

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 Axtel SIP trunk service through the public internet.

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

- Avaya S8300 Server running Communication Manager.
- Avaya G450 Media Gateway.
- Dell R210 V2 Server running Avaya SBCE.
- Avaya 96x0-Series IP Telephones (H.323).
- Avaya 96x1-Series IP Telephones (H.323).
- Avaya one-X® Communicator soft phones (H.323).
- Avaya 2420 Digital telephones.
- Analog Telephones.
- Desktop PC running various administration interfaces.
- PC running a SIP-based softphone application that is registered to a local switch in Monterrey Mexico.
- U.S. based deskphones connected to the PSTN.

Located at the edge of the enterprise is the Avaya Session Border Controller for Enterprise. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP media traffic entering or leaving the enterprise flow through the Avaya Session Border Controller for Enterprise. This way, the Avaya Session Border Controller for Enterprise can protect the enterprise against any SIP-based attacks. The Avaya Session Border Controller for Enterprise provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya Session Border Controller for Enterprise and Axtel across the public IP network is SIP over UDP. The transport protocol between the Avaya Session Border Controller for Enterprise and Avaya Aura® 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 the Avaya Session Border Controller for Enterprise and Avaya Aura® Communication Manager.

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

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

For inbound calls, the calls flowed from the service provider to the Avaya Session Border Controller for Enterprise then to Avaya Aura® Communication Manager. Once the call arrived at Avaya Aura® 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 Avaya Aura® Communication Manager for outbound feature treatment such as Automatic Route Selection (ARS) and Class of Service restrictions. Once Avaya Aura® Communication Manager selected the proper SIP trunk; the call is routed to the Avaya Session Border Controller for Enterprise for egress to Axtel's network.

During the compliance test, in addition to the DID numbers assigned to the SIP trunk, Axtel provided a local test number in Monterrey, Mexico. A SIP-based softphone was registered to this local PSTN number and was used to originate and terminate PSTN calls to and from the enterprise.

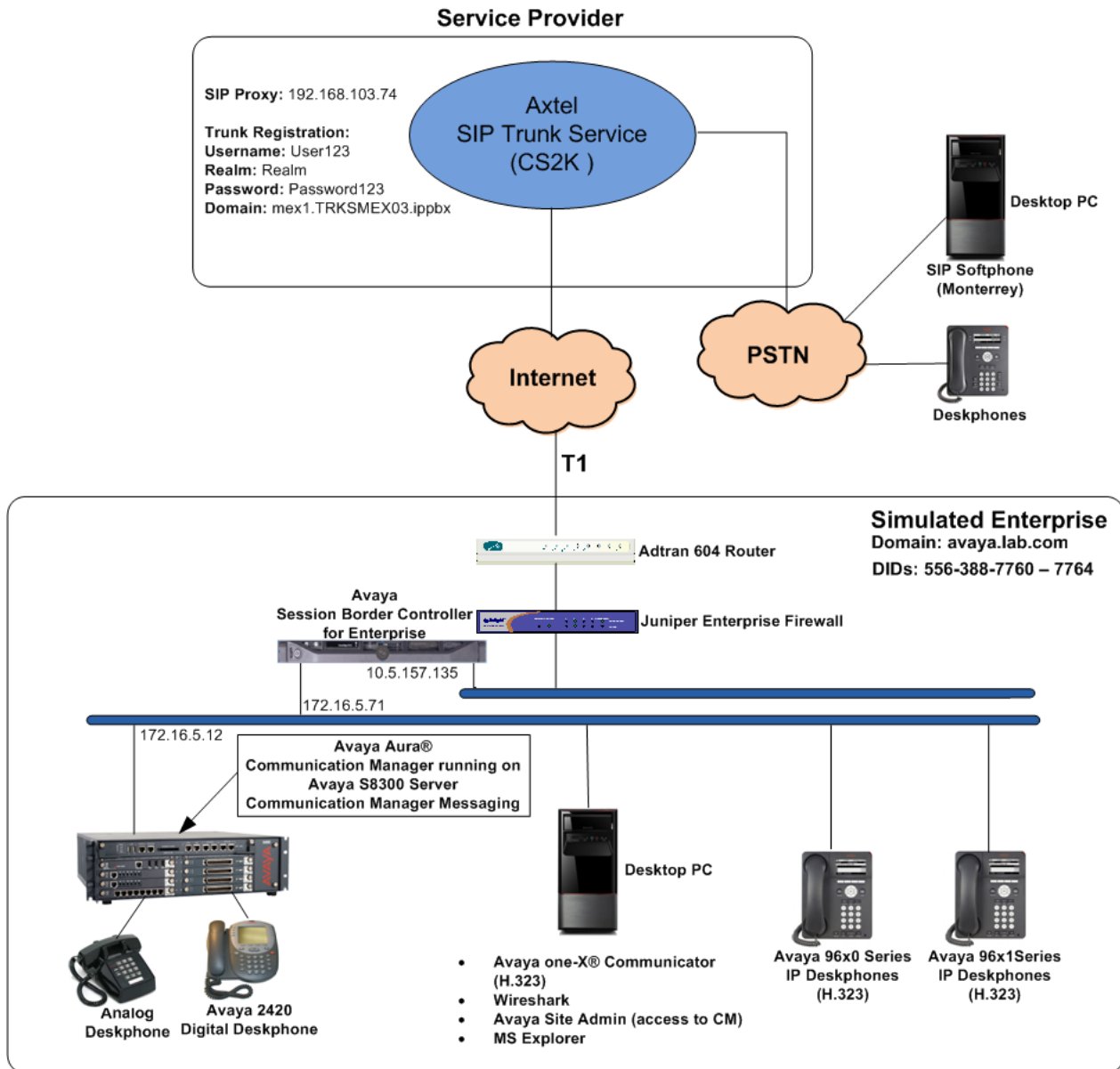


Figure 1: Avaya SIP Enterprise Solution connected to Axtel SIP Trunk Service

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager running on an Avaya S8300Server.	6.3.5 (Service Pack 5) (03.0.124.0-21460)
G450 Gateway.	35.8.0
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server.	6.2.1.Q07
Avaya Aura® Integrated Management Site Administrator.	6.0.07
Avaya Aura® Communication Manager Messaging (CMM).	CMM 6.3 (Service Pack 2) (03.0.124.0-0202)
Avaya one-X® Communicator (H.323).	6.2.2.07-SP2
Avaya 96x0 Series IP Telephones (H.323).	Avaya one-X® Deskphone Edition Version S3.212A
Avaya 96x1 Series IP Telephones (H.323).	Avaya one-X® Deskphone H.323 Version 6.3.1
Avaya 2420 Series Digital Telephone.	--
Lucent Analog Telephone.	--
Axtel	
CS2K	CVM13
Sonus SBC 5200	V03.01.02R000

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Communication Manager and Media Gateway platforms running similar software versions.

5. Configure Avaya Aura® Communication Manager

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

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **4000** licenses 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	4	
Maximum Administered SIP Trunks:			4000	22	
Maximum Administered Ad-hoc Video Conferencing Ports:			4000	0	
Maximum Number of DS1 Boards with Echo Cancellation:			80	0	
Maximum TN2501 VAL Boards:			10	0	
Maximum Media Gateway VAL Sources:			50	1	
Maximum TN2602 Boards with 80 VoIP Channels:			128	0	
Maximum TN2602 Boards with 320 VoIP Channels:			128	0	
Maximum Number of Expanded Meet-me Conference Ports:			300	0	
(NOTE: You must logoff & login to effect the permission changes.)					

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the 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:		<u>restricted</u>
CPN/ANI/ICLID Replacement for Unavailable Calls:		<u>unavailable</u>
DISPLAY TEXT		
Identity When Bridging:		<u>principal</u>
User Guidance Display?		<u>n</u>
Extension only label for Team button on 96xx H.323 terminals?		<u>n</u>
INTERNATIONAL CALL ROUTING PARAMETERS		
Local Country Code:		____
International Access Code:		____
SCCAN PARAMETERS		
Enable Enbloc Dialing without ARS FAC?		<u>n</u>
CALLER ID ON CALL WAITING PARAMETERS		
Caller ID on Call Waiting Delay Timer (msec):		<u>200</u>

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and the private interface of the Avaya SBCE (**ASBCE_A1**). These node names will be needed when configuring 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. Axtel uses codecs G.729A, G.711A and G.711MU, in this order of preference. Enter **G.729A**, **G.711A** and **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

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

Media Encryption

1: none

2:

3:

On **Page 2**, set the **Fax Mode** to *off*. As described in **Section 2.2**, T.38 fax is not currently supported by Axtel. Fax should not be used with this solution.

change ip-codec-set 2

Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy
FAX	<u>off</u>	<u>0</u>
Modem	<u>off</u>	<u>0</u>
TDD/TTY	<u>US</u>	<u>3</u>
Clear-channel	<u>n</u>	<u>0</u>

5.5. IP Network Regions

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

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

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

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

change ip-network-region 2										Page 4 of 20		
Source Region: 2		Inter Network Region Connection Management								I		M
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Intervening Prio Shr	Regions	Dyn CAC	A R	A L	G		t c e t
1	2	y	NoLimit							n		
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 the Avaya SBCE for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used 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 the Communication Manager will serve as an Evolution Server.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and the Avaya SBCE. For the compliance test, *tcp* was used.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field defaults to **Others** and cannot be changed via administration.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *ASBCE_A1*. This node name maps to the IP address of the private interface of the Avaya SBCE, as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port. The default well-known port value for SIP over TCP is 5060. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set **Enable Layer 3 Test** to *y*. This will enable Communication Manager to send SIP OPTIONS to the Avaya SBCE and subsequently to Axtel, to monitor the health of the SIP trunk.
- 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? <u>n</u>	Transport Method: <u>tcp</u>		
Q-SIP? <u>n</u>			
IP Video? <u>n</u>	Enforce SIPS URI for SRTP? <u>y</u>		
Peer Detection Enabled? <u>y</u>	Peer Server: Others		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? <u>n</u>			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? <u>y</u>			
Near-end Node Name: <u>procr</u>	Far-end Node Name: <u>ASBCE_A1</u>		
Near-end Listen Port: <u>5060</u>	Far-end Listen Port: <u>5060</u>		
	Far-end Network Region: <u>2</u>		
Far-end Domain: <u>avaya.lab.com</u>			
Incoming Dialog Loopbacks: <u>eliminate</u>	Bypass If IP Threshold Exceeded? <u>n</u>		
DTMF over IP: <u>rtp-payload</u>	RFC 3389 Comfort Noise? <u>n</u>		
Session Establishment Timer(min): <u>3</u>	Direct IP-IP Audio Connections? <u>y</u>		
Enable Layer 3 Test? <u>y</u>	IP Audio Hairpinning? <u>n</u>		
H.323 Station Outgoing Direct Media? <u>n</u>	Initial IP-IP Direct Media? <u>n</u>		
	Alternate Route Timer(sec): <u>6</u>		

5.7. Trunk Group

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

- Set the **Group Type** field to *sip*.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group added in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

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

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the default value of **600** seconds was used.

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>	

On **Page 3**, set the **Numbering Format** field to *public*. 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.

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

On **Page 4**, leave the **Network Call Redirection** field set to the default value *n*. Axtel does not support Network Call Redirection methods using REFER or 302 Temporarily Unavailable messages. Set **Send Diversion Header** to *n* and the **Support Request History** field to *n*. Set the **Telephone Event Payload Type** to *101*, and **Convert 180 to 183 for Early Media** to *y*, the values preferred by Axtel. Default values were used for all other fields.

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

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected in the trunk group to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering 1** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs) and they are used to authenticate the caller with the Service Provider. In the sample configuration, five DID numbers were assigned for testing. These DID numbers were used as 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: 7
4	5			4	Maximum Entries: 240
4	3040	2	5563887760	10	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	3041	2	5563887761	10	
4	3045	2	5563887762	10	
4	3046	2	5563887763	10	
4	3048	2	5563887764	10	
—	—	—	—	—	Communication Manager automatically inserts a '+' digit in this case.
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	
—	—	—	—	—	

5.9. Inbound Routing

DID numbers received from Axtel can be mapped to internal extensions or Vector Directory Numbers (VDNs) on the enterprise, using the incoming call handling treatment of the receiving trunk group. During the compliance test, Axtel sent 10 digit numbers to the enterprise. Use the **change inc-call-handling-trmt trunk-group 2** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 2					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	10	5563887760	10	3040			
public-ntwrk	10	5563887761	10	3041			
public-ntwrk	10	5563887762	10	3046			
public-ntwrk	10	5563887763	10	3045			
public-ntwrk	10	5563887764	10	3048			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			
public-ntwrk	—	—	—	—			

5.10. Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 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 0** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk group to the service provider.

change ars analysis 0							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 3	
Dialed String	Total		Route	Call	Node	ANI		
	Min	Max	Pattern	Type	Num	Reqd		
001	13	18	2	intl		n		
01	12	12	2	natl		n		
040	3	3	2	svcl		n		
045	13	13	2	natl		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 2** 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 for the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **2** was used.
- **FRL:** Set the Facility Restriction Level (FRL) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- Default values were used for all other fields.

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	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits			QSIG			
							Dgts			Intw			
1:	<u>2</u>	<u>0</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.	Numbering	LAR			
0	1	2	M	4	W			Dgts	Format				
												Subaddress	
1:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>		<u>-</u>	<u>next</u>		
2:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>		<u>-</u>	<u>none</u>		
3:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>		<u>-</u>	<u>none</u>		
4:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>		<u>-</u>	<u>none</u>		
5:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>		<u>-</u>	<u>none</u>		
6:	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>y</u>	<u>n</u>	<u>n</u>	<u>rest</u>		<u>-</u>	<u>none</u>		

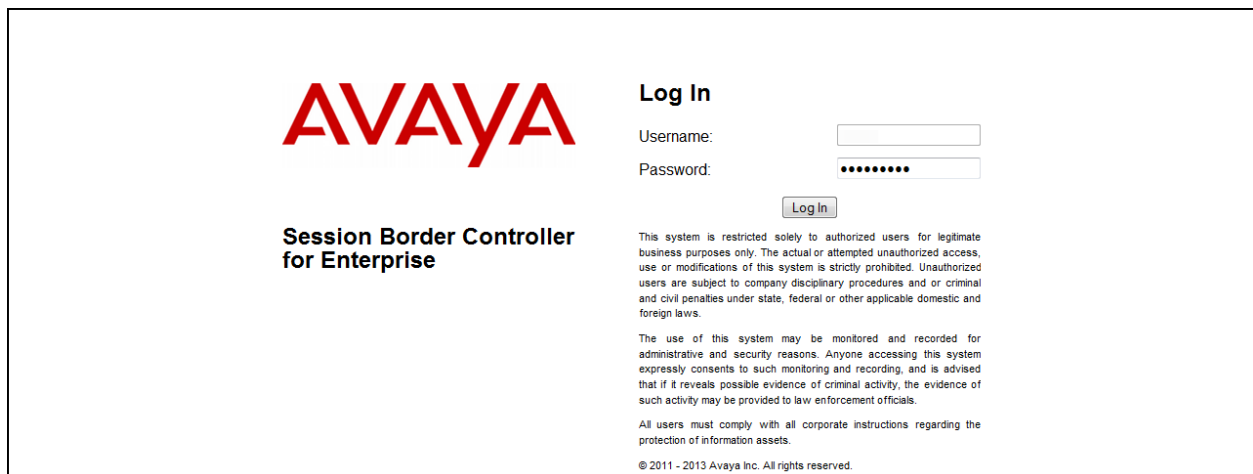
6. Configure the Avaya Session Border Controller for Enterprise

In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Axtel SIP Trunk service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the SBC installation and initial provisioning, consult the Avaya SBCE documentation listed in the **References** section.

Note: During the next pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it.

6.1. System Access

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



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, under the heading "Log In", there are input fields for "Username:" and "Password:". The password field is masked with dots. Below the password field is a "Log In" button. To the right of the login fields, there is a disclaimer: "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." Below this, another disclaimer states: "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." At the bottom, it says: "All users must comply with all corporate instructions regarding the protection of information assets." and "© 2011 - 2013 Avaya Inc. All rights reserved."

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.

6.2. System Management

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

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device and the network settings. Note that the **A1** and **B1** interfaces correspond to the inside (private) and outside (public) interfaces for the Avaya SBCE. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Axtel.

System Information: Sipera

General Configuration

Appliance Name Sipera
Box Type SIP
Deployment Mode Proxy

Device Configuration

HA Mode No
Two Bypass Mode No

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
10.5.157.135	10.5.157.135	255.255.255.192	10.5.157.129	B1
192.168.1.100	192.168.1.100	255.255.255.192	192.168.1.100	B1
192.168.1.100	192.168.1.100	255.255.255.192	192.168.1.100	B1
192.168.1.100	192.168.1.100	255.255.255.192	192.168.1.100	B1

DNS Configuration

Primary DNS 172.16.5.102
Secondary DNS
DNS Location DMZ
DNS Client IP 172.16.5.71

Management IP(s)

IP 192.168.1.100

6.3. Global Profiles

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

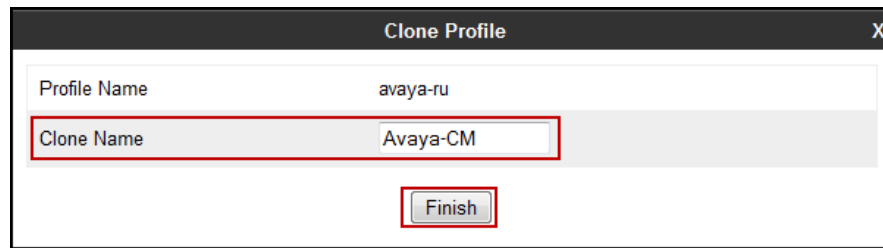
6.3.1. Server Interworking Avaya-CM

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the reference configuration, Communication Manager functions as the Call Server and the Axtel SIP Proxy as the Trunk Server.

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.

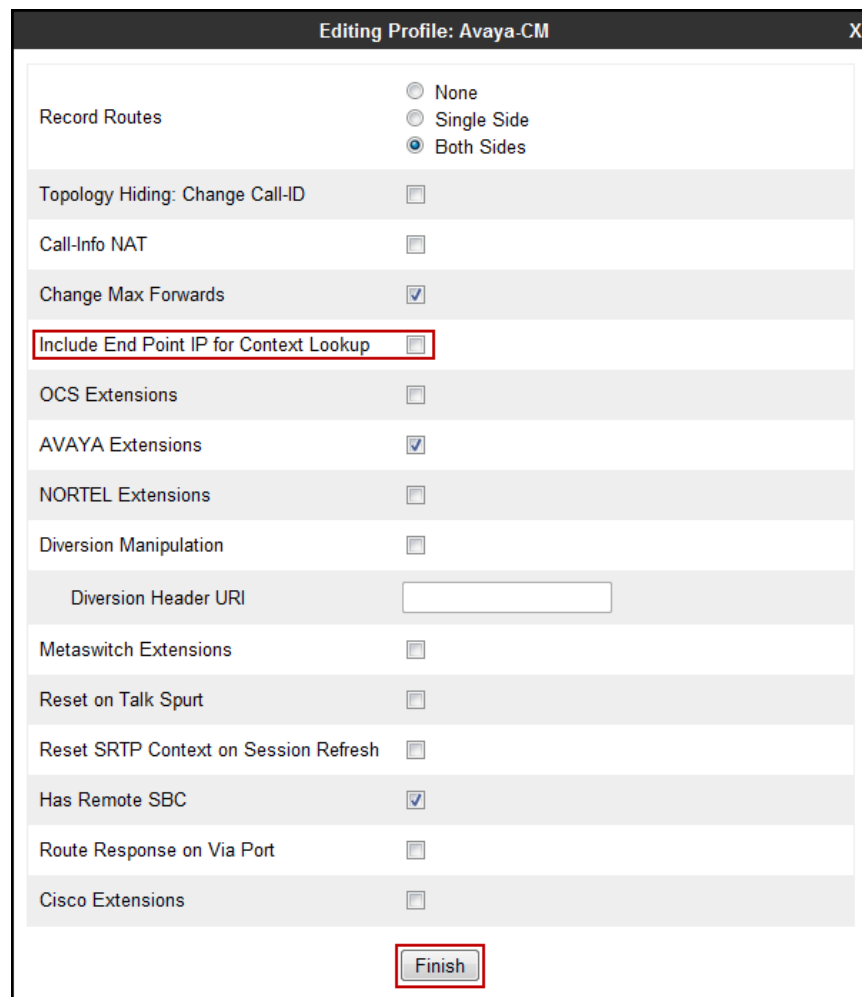
Enter the new profile name in the **Clone Name** field, the name of **Avaya-CM** was chosen in this example. Click **Finish**.



The 'Clone Profile' dialog box shows the 'Profile Name' as 'avaya-ru' and the 'Clone Name' as 'Avaya-CM'. The 'Finish' button is at the bottom right.

For the newly created **Avaya-CM** profile, select the Advanced tab; click **Edit** (not shown) at the bottom of the screen:

- Uncheck **Include End Point IP for Context Lookup**.
- Leave all other fields with their default values.
- Click **Finish**.



The 'Editing Profile: Avaya-CM' dialog box shows various settings. The 'Record Routes' section has radio buttons for 'None', 'Single Side', and 'Both Sides' (selected). The 'Include End Point IP for Context Lookup' checkbox is unchecked and highlighted with a red box. The 'Finish' button is at the bottom right.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management and configuration options, with 'Global Profiles' expanded to show 'Server Interworking' and 'Avaya-CM' highlighted. The main content area is titled 'Interworking Profiles: Avaya-CM' and features an 'Add' button and action buttons (Rename, Clone, Delete). A list of interworking profiles is shown on the left, with 'Avaya-CM' selected. The 'General' tab is active, displaying a table of configuration parameters 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
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

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

DTMF	
DTMF Support	None

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, 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 navigation pane lists various configuration areas, with "Global Profiles" expanded and "Server Interworking" selected. The main content area is titled "Interworking Profiles: Avaya-CM" and features a list of profiles on the left, including "cs2100", "avaya-ru", "OCS-Edge-Server", "cisco-ccm", "cups", "Sipera-Halo", "OCS-FrontEnd-Server", "Avaya-SM", "SP-General", "Avaya-CS1000", "Avaya-IPO", "Avaya-CM" (highlighted), and "Test". An "Add" button is present above the list. The right pane shows the configuration for the "Avaya-CM" profile, with tabs for General, Timers, URI Manipulation, Header Manipulation, and Advanced (selected). The Advanced tab contains a table of settings:

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

Buttons for "Rename", "Clone", "Delete", and "Edit" are visible at the top and bottom of the configuration pane.

6.3.2. 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** (not shown).

Enter the new profile name, the name of **SP-General** was chosen in this example. Accept the default values for all fields by clicking **Next** multiple times and then Click **Finish** (not shown).

The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "SP-General". Below the input field is a button labeled "Next".

The following screen capture shows the **General** tab of the newly created **SP-General** profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, 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' and 'SP-General' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this is a list of interworking profiles, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (selected), 'Avaya-CS1000', 'Avaya-IPO', 'Avaya-CM', and 'Test'. The 'General' tab is active, showing a table of configuration parameters. The table is divided into three sections: General, Privacy, and DTMF. The General section includes parameters like Hold Support, 180 Handling, 181 Handling, 182 Handling, 183 Handling, Refer Handling, URI Group, 3xx Handling, Diversion Header Support, Delayed SDP Handling, Re-Invite Handling, T.38 Support, URI Scheme, and Via Header Format. The Privacy section includes Privacy Enabled, User Name, P-Asserted-Identity, P-Preferred-Identity, and Privacy Header. The DTMF section includes DTMF Support. The values for these parameters are mostly 'None' or 'No'.

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

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

DTMF	
DTMF Support	None

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management and configuration options, with 'Global Profiles' and 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and features a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (selected), 'Avaya-CS1000', 'Avaya-IPO', 'Avaya-CM', and 'Test'. An 'Add' button is located above this list. To the right, the 'Advanced' tab is active, showing a table of configuration parameters. Above the table are buttons for 'Rename', 'Clone', and 'Delete', and a link to 'Click here to add a description.' The table lists various SIP-related settings and their values.

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

6.3.3. Routing Profiles

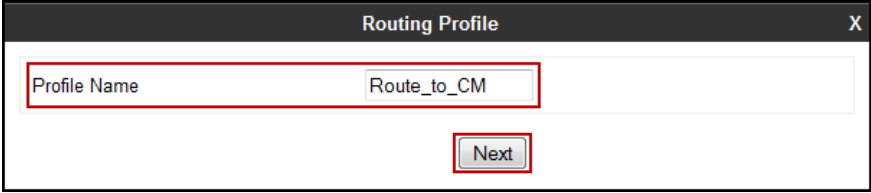
Routing profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

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

On the left navigation pane, select **Global Profiles → Routing**. From the **Routing profiles** list, select **Add** (not shown).

Enter the new profile name, the name of *Route_to_CM* was chosen in this example.

- Click **Next**.



The screenshot shows a 'Routing Profile' dialog box with a dark header bar containing the title 'Routing Profile' and a close button 'X'. Below the header is a light gray area with a 'Profile Name' label and a text input field containing 'Route_to_CM'. A red rectangular box highlights the input field. Below the input field is a 'Next' button, also highlighted with a red rectangular box.

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.12** (Communication Manager IP address).
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport:** select **TCP**.
- Click **Finish**.

The screenshot shows a 'Routing Profile' configuration window. At the top, a blue banner states: 'Each URI group may only be used once per Routing Profile.' Below this is a section titled 'Next Hop Routing'. It contains a 'URI Group' dropdown menu. Underneath, there are two 'Next Hop Server' entries. The first entry, 'Next Hop Server 1', has the IP address '172.16.5.12' entered in its text field. The second entry, 'Next Hop Server 2', is empty. Below the servers, there are several checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (unchecked), 'Ignore Route Header for Messages Outside Dialog' (unchecked), 'NAPTR' (unchecked), and 'SRV' (unchecked). At the bottom, the 'Outgoing Transport' section has three radio buttons: 'TLS' (unchecked), 'TCP' (checked), and 'UDP' (unchecked). At the very bottom are 'Back' and 'Finish' buttons.

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	172.16.5.12
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	<input checked="" type="checkbox"/>
Use Next Hop for In Dialog Messages	<input type="checkbox"/>
Ignore Route Header for Messages Outside Dialog	<input type="checkbox"/>
NAPTR	<input type="checkbox"/>
SRV	<input type="checkbox"/>
Outgoing Transport	<input type="radio"/> TLS <input checked="" type="radio"/> TCP <input type="radio"/> UDP

Back Finish

The following screen shows the newly created **Route_to_CM** Profile.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a navigation pane lists various configuration areas, with "Global Profiles" expanded and "Routing" selected. The main content area is titled "Routing Profiles: Route_to_CM" and features an "Add" button. Below this, a list of routing profiles is shown, including "default", "Route_to_SM", "Route_to_SP", "Route_to_CM" (highlighted), "Route_to_CS1000", "Route_to_IP0", and "To SM from Rem W". To the right of the list, a "Routing Profile" configuration form is visible, showing a table with columns for Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The table contains one entry with Priority 1, URI Group *, and Next Hop Server 1 172.16.5.12. The "Add" button is also present in the top right corner of the configuration form.

Similarly add a Routing Profile for outbound calls, which are sent to the Service Provider SIP trunk.

On the left navigation pane, select **Global Profiles → Routing**. From the **Routing profiles** list, select **Add** (not shown).

Enter the new profile name, the name of **Route_to_SP** was chosen in this example.

- Click **Next**.

The screenshot shows a "Routing Profile" configuration dialog box. It has a title bar with "Routing Profile" and a close button (X). Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route_to_SP". Below the input field, there is a "Next" button.

On the next screen, complete the following:

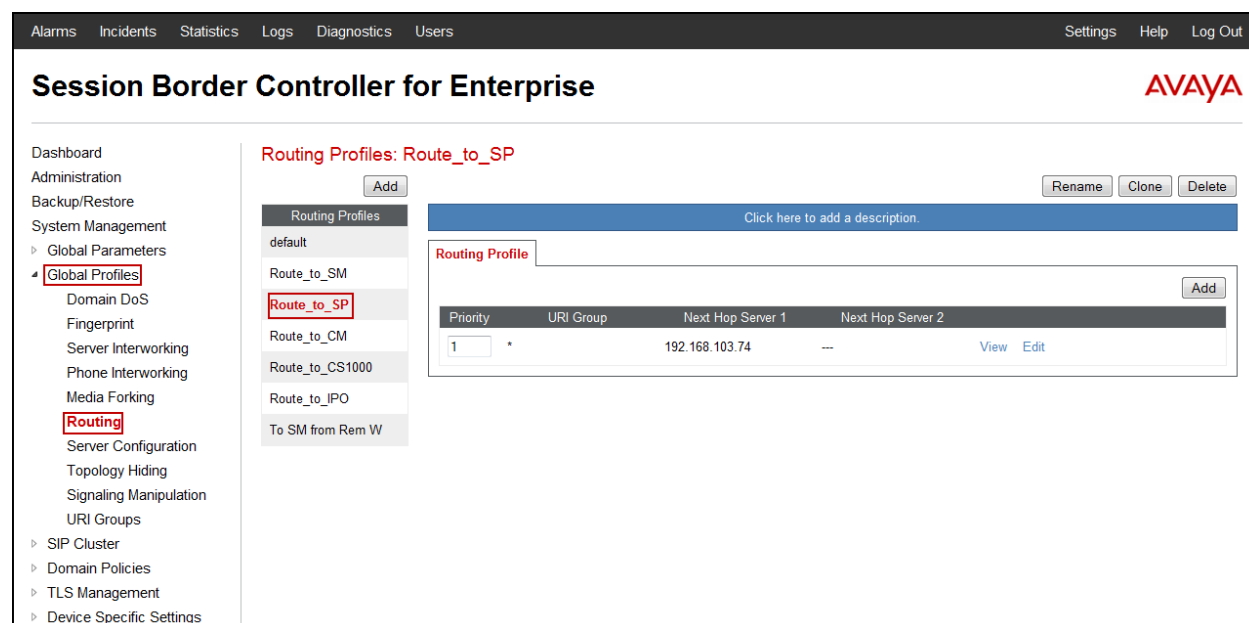
- **Next Hop Server 1: 192.168.103.74** (Service Provider SIP Proxy IP address).
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport:** select **UDP**.
- Click **Finish**.

The screenshot shows a 'Routing Profile' configuration window. At the top, a blue banner states: 'Each URI group may only be used once per Routing Profile.' Below this is a section titled 'Next Hop Routing'. It contains several fields and checkboxes:

- 'URI Group' is a dropdown menu with a '*' icon.
- 'Next Hop Server 1' is a text field containing '192.168.103.74'.
- 'Next Hop Server 2' is an empty text field.
- 'Routing Priority based on Next Hop Server' is a checked checkbox.
- 'Use Next Hop for In Dialog Messages' is an unchecked checkbox.
- 'Ignore Route Header for Messages Outside Dialog' is an unchecked checkbox.
- 'NAPTR' is an unchecked checkbox.
- 'SRV' is an unchecked checkbox.
- 'Outgoing Transport' is a radio button group with three options: 'TLS', 'TCP', and 'UDP'. 'UDP' is selected.

At the bottom of the window are two buttons: 'Back' and 'Finish'.

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



6.3.4. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform a granular header manipulation 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 [4] on the **References** section for more information on this topic.

A Sigma script was created during the compliance test to remove the “Remote-Address” header, used by the Avaya SBCE, from all outbound messages. This header contains private IP addresses that should not be propagated outside the enterprise limits.

Note: Additional Avaya SBCE header manipulation will be performed by implementing Signaling Rules, in **Section 6.4.1** later in this document.

On the left navigation pane, select **Global Profiles** → **Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add** (not shown).

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

The screenshot shows the 'Signaling Manipulation Editor' window. At the top left, the title 'Remove Remote Address' is entered in a text box. To the right of this text box is a 'Save' button. Below the title box is a large text area containing a script. The script is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"] [1]);
  }
}
```

The following screen capture shows the newly created **Signaling Manipulation Script**.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation pane with a tree structure. The 'Global Profiles' folder is expanded, and 'Signaling Manipulation' is selected. In the center, a list of 'Signaling Manipulation Scripts' is shown. The script 'Remove Remote A...' is highlighted. To the right of this list is a large text area displaying the script content. The script is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"] [1]);
  }
}
```

Below the script text area is an 'Edit' button. At the top right of the script area are buttons for 'Download', 'Clone', and 'Delete'. Above the script area is a blue bar with the text 'Click here to add a description.'

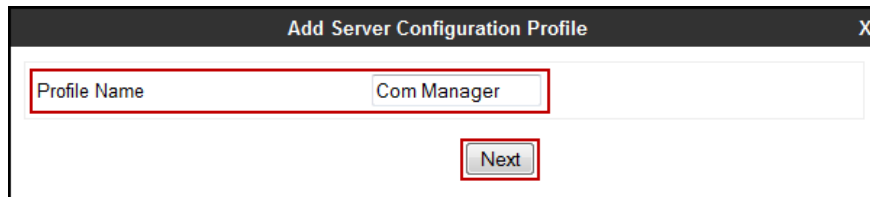
6.3.5. Server Configuration

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

To add the Server Profile for the Call Server, on the left navigation pane, select **Global Profiles** → **Server Configuration**. From the **Server Profiles** list, select **Add** (not shown).

Enter the new Server name, the name of *Com Manager* was chosen in this example.

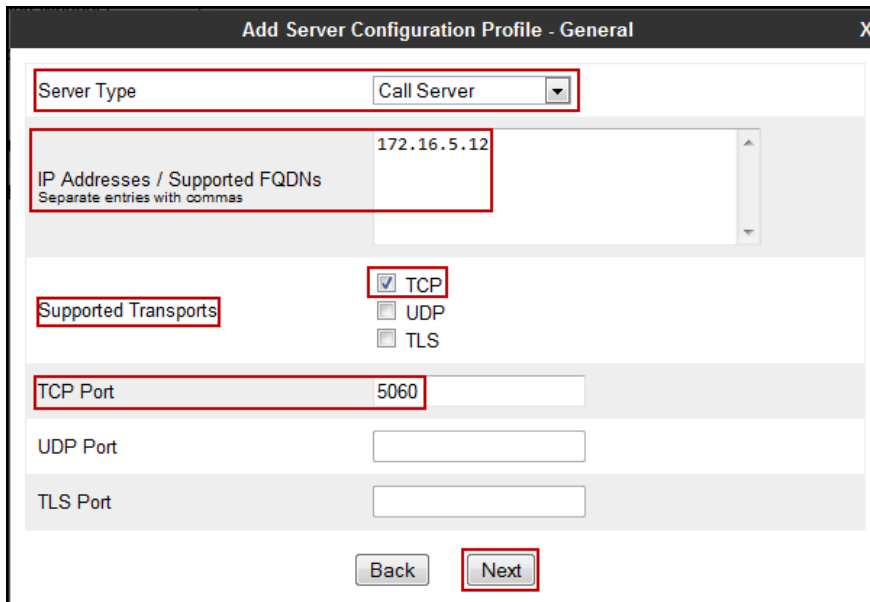
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Com Manager". Below this field, there is a "Next" button.

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

- **Server Type:** select *Call Server*.
- **IP Address:** *172.16.5.12* (IP Address of Communication Manager).
- **Supported Transports:** check *TCP*.
- **TCP Port:** enter *5060*.
- Click **Next**.



The screenshot shows a window titled "Add Server Configuration Profile - General". It has a close button (X) in the top right corner. The "Server Type" dropdown is set to "Call Server". Below it, the "IP Addresses / Supported FQDNs" text area contains "172.16.5.12". Under the "Supported Transports" section, the "TCP" checkbox is checked, while "UDP" and "TLS" are unchecked. The "TCP Port" text field contains "5060". There are empty text fields for "UDP Port" and "TLS Port". At the bottom, there are "Back" and "Next" buttons.

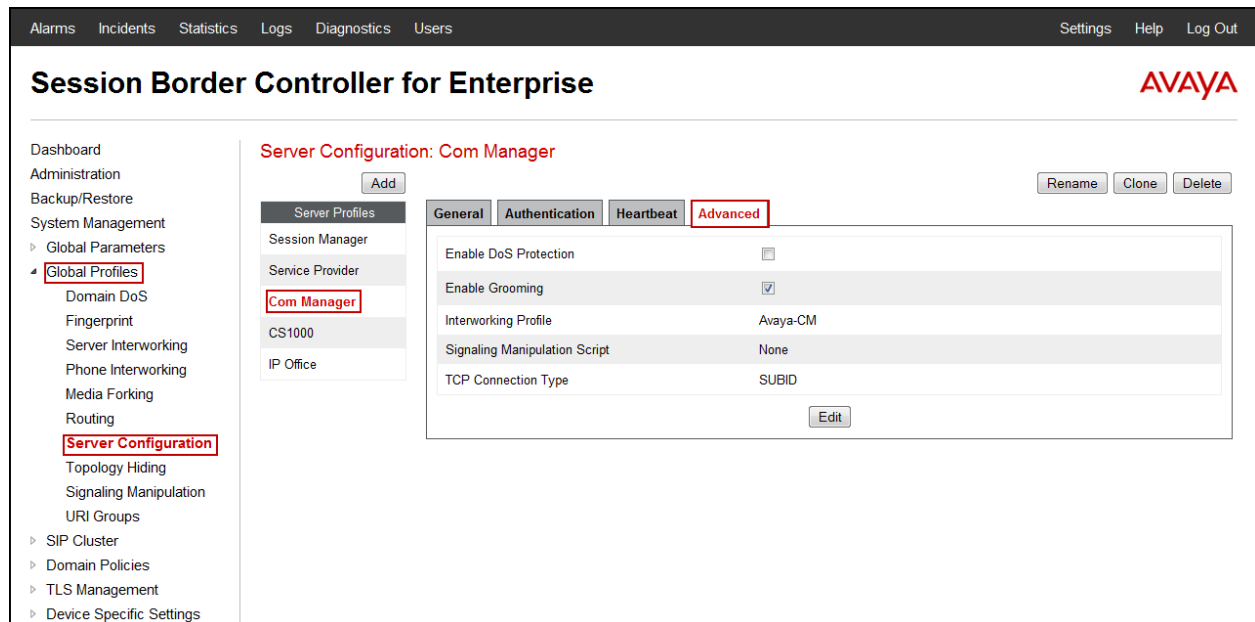
- Click **Next** in the **Authentication** window (not shown).
- Click **Next** in the **Heartbeat** window (not shown).

On the **Advanced** window:

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

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

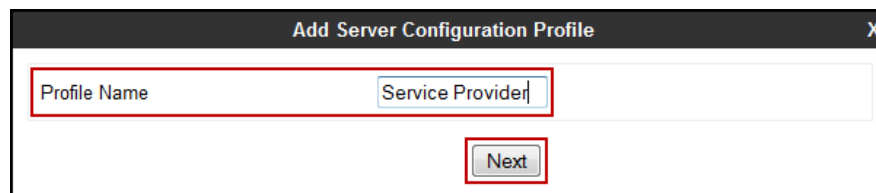
The following screen capture shows the **Advanced** tab of the newly created **Com Manager** Server Profile.



To add the Server Profile for the Trunk Server, on the left navigation pane, select **Global Profiles** → **Server Configuration**. From the **Server Profiles** list, select **Add** (not shown).

Enter the new Server name, the name of *Service Provider* was chosen in this example.

- Click **Next**.



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

- **Server Type:** select *Trunk Server*.
- **IP Address:** *192.168.103.74* (Service Provider SIP Proxy IP address).
- **Supported Transports:** check *UDP*.
- **TCP Port:** enter *5060*.
- Click **Next**

The screenshot shows the 'Add Server Configuration Profile - General' window. The following fields are highlighted with red boxes:

- Server Type:** A dropdown menu set to 'Trunk Server'.
- IP Addresses / Supported FQDNs:** A text area containing '192.168.103.74'.
- Supported Transports:** A section with three checkboxes: 'TCP' (unchecked), 'UDP' (checked), and 'TLS' (unchecked).
- UDP Port:** A text field containing '5060'.
- Next:** A button at the bottom right of the window.

On the **Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential information supplied by the service provider for the authentication of the SIP trunk.
- Enter the **Realm** information supplied by the service provider for the authentication of the SIP trunk. (Must be entered, currently cannot be detected automatically from the challenge)
- Enter **Password** credential information supplied by the service provider for the authentication of the SIP trunk.
- Click **Next**.

The screenshot shows a web-based configuration window titled "Add Server Configuration Profile - Authentication". The window contains several input fields and a checkbox. A red rectangle highlights the "Enable Authentication" checkbox (which is checked), the "User Name" field (containing "User123"), the "Realm" field (containing "Realm"), the "Password" field (masked with dots), and the "Confirm Password" field (masked with dots). Below these fields are two buttons: "Back" and "Next". The "Next" button is also highlighted with a red rectangle.

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider. **60** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: use the **User Name** entered above in the **Authentication** screen and the external (public) IP addresses of the Avaya SBCE, as shown on the screen below.
 - **To URI**: Use the **User Name** entered above in the **Authentication** screen and the Service Provider Proxy Server IP address, as shown on the screen below.
- Click **Next**.

Add Server Configuration Profile - Heartbeat

Enable Heartbeat ☒

Method REGISTER

Frequency 60 seconds

From URI User123@10.5.157.135

To URI User123@192.168.103.74

Back Next

On the **Advanced** tab:

- Select **SP-General** from the **Interworking Profile** drop down menu.
- Under **Signaling Manipulation Script**, select the **Remove Remote Address** script created in Section 6.3.4.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

Signaling Manipulation Script Remove Remote Address

UDP Connection Type SUBID PORTID MAPPING

Back Finish

6.3.6. Topology Hiding

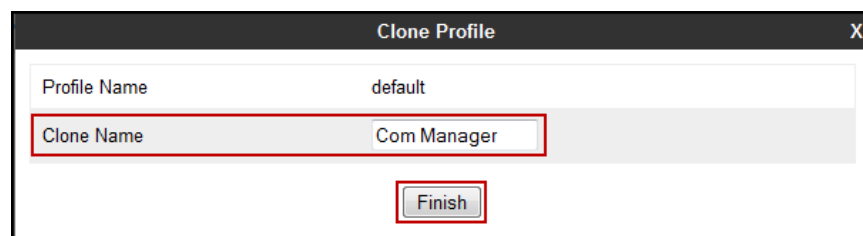
Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Communication 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 **Global Profiles** → **Topology Hiding** (not shown).

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen (not shown).
- Enter the **Profile Name: Com Manager**.
- Click **Finish**.



- Click **Edit** on the newly added **Com Manager** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the enterprise (*avaya.lab.com*) under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Enterprise (*avaya.lab.com*) under **Overwrite Value**.
- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Enterprise (*avaya.lab.com*) under **Overwrite Value**.

Edit Topology Hiding Profile X

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

Finish

The following screen capture shows the newly created **Com Manager** Topology Hiding profile.

Alarms Incidents Statistics Logs Diagnostics Users
Settings Help Log Out

Session Border Controller for Enterprise

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

Topology Hiding Profiles: Com Manager
Add Rename Clone Delete

Topology Hiding Profiles

default

cisco_th_profile

Session_Manager

Service_Provider

Com Manager

CS1000

IP Office

Click here to add a description.

Topology Hiding

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

Edit

HG; Reviewed:
SPOC 8/24/2014

Solution & Interoperability Test Lab Application Notes
©2014 Avaya Inc. All Rights Reserved.

52 of 79
Axtel_CMSBCE

Similarly, to add the Topology Hiding profile in the Service Provider direction, select **Global Profiles → Topology Hiding** (not shown).

- Select the **default** profile in the **Topology Hiding Profiles** list, then click **Clone** on top right of the screen (not shown).
- Enter the **Profile Name: Service_Provider**.
- Click **Finish**.

Clone Profile

Profile Name: default

Clone Name: Service_Provider

Finish

- Click **Edit** on the newly added **Service_Provider** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (*mex1.TRKSMEX03.ippbx*) under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (*mex1.TRKSMEX03.ippbx*) under **Overwrite Value**.
- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Service Provider (*mex1.TRKSMEX03.ippbx*) under **Overwrite Value**.

Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	mex1.TRKSMEX03.ip	Delete
Request-Line	IP/Domain	Overwrite	mex1.TRKSMEX03.ip	Delete
Record-Route	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	mex1.TRKSMEX03.ip	Delete

Finish

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, 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 'Global Profiles' expanded and 'Topology Hiding' highlighted. The main content area is titled 'Topology Hiding Profiles: Service_Provider' and features an 'Add' button. Below this, a list of profiles includes 'default', 'cisco_th_profile', 'Session_Manager', 'Service_Provider' (highlighted), 'Com Manager', 'CS1000', and 'IP Office'.

The 'Service_Provider' profile is selected, showing a table of topology hiding rules. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The rules are as follows:

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	mex1.TRKSMEX03.ippbx
Request-Line	IP/Domain	Overwrite	mex1.TRKSMEX03.ippbx
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	mex1.TRKSMEX03.ippbx

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

6.4. 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.

In the reference configuration, two new Signaling Rules were defined. All other rules under the Domain Policies menu, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

6.4.1. Signaling Rules

A Signaling Rule was created in the sample configuration to remove (block) the outbound headers shown below. This rule will later be applied to the End Point Policy Group corresponding to the enterprise:

- AV-Global-Session-ID
- Alert-Info
- Endpoint-View
- P-AV-Message-ID
- P-Location
- P-Charging-Vector

The above headers are sent in SIP messages from the Communication Manager to the Avaya SBCE. These headers have no significance to the service provider, they contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries.

To add the Signaling Rule, select **Domain Policies → Signaling Rules**, click **Add** (not shown).

- Enter an appropriate name, the name *Remove_headers* was chosen in this example.
- Click **Next**.

A screenshot of a web-based configuration interface for a 'Signaling Rule'. The window has a dark title bar with the text 'Signaling Rule' and a close button 'X'. Inside the window, there is a text input field labeled 'Rule Name' containing the text 'Remove_headers'. Below the input field, there is a 'Next' button. Both the input field and the button are highlighted with red rectangular boxes.

- Click **Next** on the next four tabs (not shown), leaving all fields in sections **Inbound Outbound**, **Content-Type Policies**, **QoS** and **UCDI** with their default values.
- Click **Finish** (not shown).

On the newly created **Remove_headers** Signaling Rule, select the **Request Headers** tab to create the manipulations performed on request messages. Select **Add In Header Control**.

The screenshot shows the 'Signaling Rules' configuration page. On the left, a list of rules includes 'Remove_headers', which is highlighted. The main area shows the 'Request Headers' tab selected. A button 'Add In Header Control' is visible. Below it, a table with columns 'Row', 'Header Name', 'Method Name', 'Header Criteria', 'Action', 'Proprietary', and 'Direction' is shown, with a message 'No request header controls exist.'

In the **Add Header Control** screen select the following:

- **Header Name:** *Alert-Info*
- **Method Name:** *INVITE*
- **Header Criteria:** *Forbidden*
- **Presence Action:** *Remove Header*
- Click **Finish**

The screenshot shows the 'Add Header Control' dialog box. It contains the following fields and values:

- Proprietary Request Header:** ☐
- Header Name:** Alert-Info
- Method Name:** INVITE
- Header Criteria:** ☒ Forbidden, ☐ Mandatory, ☐ Optional
- Presence Action:** Remove header
- Presence Action details:** 486, Busy Here
- Finish button:** Visible at the bottom.

Select **Add In Header Control** as needed to configure the remaining header control rules. For these headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Request Headers** tab should look like the following screen.

The screenshot displays the Avaya 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: Remove_headers'. It features a table with columns: Row, Header Name, Method Name, Header Criteria, Action, Proprietary, Direction, Edit, and Delete. The table contains six rows of header control rules. The 'Request Headers' tab is active, and the 'Add In Header Control' button is highlighted.

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

Select the **Response Headers** tab to similarly create the manipulations performed on response messages.

Select **Add In Header Control** as needed to configure the remaining header control rules. For these headers, make sure to check the **Proprietary Request Header** box in the **Add Header Control** tab. This will allow typing the name of the specific header on the **Header Name** box. Once completed, the **Response Headers** tab should look like the following screen.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, 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 'Domain Policies' and 'Signaling Rules' highlighted. The main content area is titled 'Signaling Rules: Remove_headers' and features a list of rules on the left and a detailed configuration table on the right. The table is currently set to the 'Response Headers' tab. The table columns are Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, Direction, and Edit/Delete links. The table contains 9 rows of rules, all with 'Forbidden' criteria and 'Remove Header' actions. The 'Proprietary' column is checked for all rules, and the 'Direction' is set to 'IN'.

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

As mentioned in **Section 2.2**, Axtel included a P-Asserted-Identity (PAI) header with an “anonymous;phone-context=unknown” parameter in the 200 OK message sent from the network as a response to the INVITE sent from the enterprise for outbound calls. This parameter made the display on the enterprise extensions (calling party) change to “anonymous” once the calls was answered by the PSTN party. To avoid this, a second Signaling Rule was created to remove the PAI header from the 200 OK messages arriving from Axtel. This rule will later be applied to the End Point Policy Group corresponding to the service provider.

To add the Signaling Rule, select **Domain Policies → Signaling Rules**, click **Add** (not shown).

- Enter an appropriate name, the name **Remove PAI** was chosen in this example.
- Click **Next**.

The screenshot shows a 'Signaling Rule' configuration window. It has a title bar with 'Signaling Rule' and a close button 'X'. Inside, there is a text input field labeled 'Rule Name' containing the text 'Remove PAI'. Below this field is a 'Next' button.

- Click **Next** on the next four tabs (not shown), leaving all fields in sections **Inbound Outbound**, **Content-Type Policies**, **QoS** and **UCDI** with their default values.
- Click **Finish** (not shown).

On the newly created **Remove PAI** Signaling Rule, select the **Response Headers** tab to create the manipulations performed on response messages. Select **Add In Header Control**.

The screenshot shows 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 area shows the configuration for the 'Remove PAI' signaling rule. The 'Response Headers' tab is active, displaying a table with columns: Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, and Direction. The 'Add In Header Control' button is highlighted in the 'Response Headers' section.

In the **Add Header Control** screen select the following:

- **Header Name:** *P-Asserted-Identity*
- **Response Code:** *2XX*
- **Method Name:** *INVITE*
- **Header Criteria:** *Forbidden*
- **Presence Action:** *Remove Header*
- Click **Finish**

The screenshot shows the 'Add Header Control' dialog box with the following configuration:

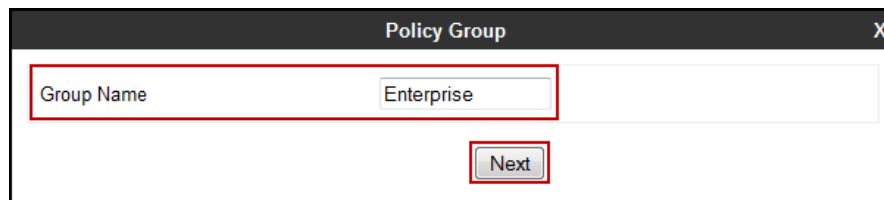
- Proprietary Response Header:** ☐
- Header Name:** P-Asserted-Identity
- Response Code:** 2XX
- Method Name:** INVITE
- Header Criteria:** ☒ Forbidden, ☐ Mandatory, ☐ Optional
- Presence Action:** Remove header
- 486:** Busy Here
- Finish:** (button)

6.4.2. End Point Policy Groups

End Point Policy Groups associate the 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, select **Domain Policies** → **End Point Policy Groups**. Click **Add** (not shown).

- Enter an appropriate name, the name *Enterprise* was chosen in this example.
- Click **Next**.



The screenshot shows a 'Policy Group' dialog box with a title bar containing 'Policy Group' and a close button 'X'. Inside the dialog, there is a text input field labeled 'Group Name' containing the text 'Enterprise'. Below this field is a button labeled 'Next'.

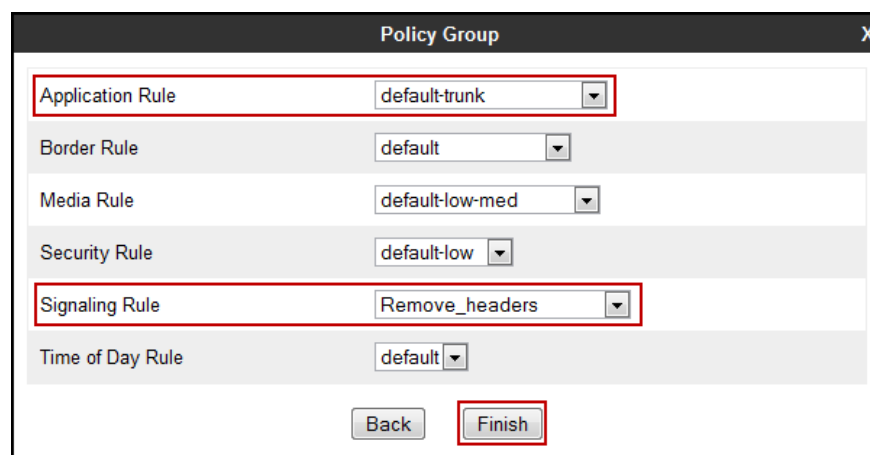
In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the *Remove_headers* rule created in **Section 6.4.1** was selected.

In the **Policy Group** screen select the following:

- **Application Rule:** *default-trunk*.
- **Signaling Rule:** *Remove_headers*.

All other fields will default to the values shown below.

- Click **Finish**.



The screenshot shows a 'Policy Group' dialog box with a title bar containing 'Policy Group' and a close button 'X'. Inside the dialog, there are several dropdown menus for selecting rules: 'Application Rule' (default-trunk), 'Border Rule' (default), 'Media Rule' (default-low-med), 'Security Rule' (default-low), 'Signaling Rule' (Remove_headers), and 'Time of Day Rule' (default). At the bottom, there are two buttons: 'Back' and 'Finish'.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'End Point Policy Groups' selected. The main content area is titled 'Policy Groups: Enterprise'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-sub...', 'avaya-def-high-server', 'Enterprise', and 'Service Provider'. The 'Enterprise' group is highlighted. The right pane shows the configuration for the 'Enterprise' group, including a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: Order 1, Application default-trunk, Border default, Media default-low-med, Security default-low, Signaling Remove_headers, and Time of Day default. The Signaling rule 'Remove_headers' is highlighted in blue.

A second End Point Policy Group was created for the service provider, repeating the steps described above. Defaults were used for all fields with the exception of the **Signaling Rule**, where the **Remove PAI** Signaling Rule created in **Section 6.4.1** was selected. The name **Service Provider** was chosen in this example. The screen below shows the newly created **Service Provider** End Point Policy Group.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'End Point Policy Groups' selected. The main content area is titled 'Policy Groups: Service Provider'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-sub...', 'avaya-def-high-server', 'Enterprise', and 'Service Provider'. The 'Service Provider' group is highlighted. The right pane shows the configuration for the 'Service Provider' group, including a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: Order 1, Application default-trunk, Border default, Media default-low-med, Security default-low, Signaling Remove PAI, and Time of Day default. The Signaling rule 'Remove PAI' is highlighted in blue.

6.5. Device Specific Settings

The **Device Specific Settings** determine server specific parameters that determine how the device will work when deployed on the network. Among the parameters defined here are IP addresses, media and signaling interfaces, call flows, etc.

6.5.1. Network Management

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

To view the Device Specific Settings, select **Device Specific Settings → Network Management**.

Under **Devices** in the center pane, select the device being managed, **Sipera** in the sample configuration. On the **Network Configuration** tab, verify or enter the network information as needed. Note that the **A1** interface is used for the internal or private side and **B1** is used for the external or public side of the Avaya SBCE.

Only the IP addresses highlighted in a red bracket are relevant to the SIP Trunk configuration settings covered under these Application Notes.

The screenshot shows the Avaya SBCE web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar lists various management sections, with "Device Specific Settings" expanded and "Network Management" highlighted. The main content area is titled "Network Management: Sipera" and has two tabs: "Network Configuration" (active) and "Interface Configuration". A warning message states: "Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management." Below this, there are input fields for A1 Netmask (255.255.255.0), A2 Netmask, B1 Netmask (255.255.255.192), and B2 Netmask, with "Add", "Save", and "Clear" buttons. A table lists IP addresses, Public IPs, Gateways, and Interfaces (A1, B1) with "Delete" links. The first two rows are highlighted with a red bracket.

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
10.5.157.135		10.5.157.129	B1	Delete
10.5.157.180		10.5.157.129	B1	Delete
10.5.157.181		10.5.157.129	B1	Delete
172.16.5.72		172.16.5.254	A1	Delete

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.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

Network Management: Sipera

Devices
Sipera

Network Configuration **Interface Configuration**

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

Note: some customer deployments may use a router, firewall or some other kind of network device between the Avaya SBCE and the service provider's network. These customers may decide to assign IP addresses to the public and private sides of the Avaya SBCE that are both in the same private subnet of the enterprise. In these particular cases, the same physical interface (A1, for example) can be assigned to both the private and public sides of the Avaya SBCE. The rest of the configuration process, like the creation of separate Media Interfaces, Signaling Interfaces, etc. as specified in the next sections of this document still remains the same.

6.5.2. Media Interface

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or Trunk Server.

To add the Media Interface in the enterprise direction, select **Device Specific Settings → Media Interface**. Click **Add** (not shown).

- Enter an appropriate name, the name **Private_med** was chosen in this example.
- Select **172.16.5.71** from the **IP Address** drop-down menu, this is the inside or private IP Address of the Avaya SBCE.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

Add Media Interface

Name: Private_med

IP Address: 172.16.5.71

Port Range: 35000 - 40000

Finish

A second Media Interface facing the public network side was similarly created with the name **Public_med**, as shown below. Under **IP Address**, select **10.5.157.135**, this is the outside or public IP Address of the Avaya SBCE. The **Port Range** was left at the default values.

Add Media Interface

Name: Public_med

IP Address: 10.5.157.135

Port Range: 35000 - 40000

Finish

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

Only the Media Interfaces highlighted in a red bracket are relevant to the SIP Trunk configuration settings covered under these Application Notes.

Session Border Controller for Enterprise

Media Interface: Sipera

Media Interface

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

Name	Media IP	Port Range	
Private_med	172.16.5.71	35000 - 40000	Edit Delete
Public_med	10.5.157.135	35000 - 40000	Edit Delete
RW_Private_med	172.16.5.72	35000 - 40000	Edit Delete
RW_Public_med	10.5.157.180	35000 - 40000	Edit Delete

6.5.3. Signaling Interface

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

To add the Signaling Interface in the enterprise direction, select **Device Specific Settings** → **Signaling Interface**. Click **Add** (not shown).

- Enter an appropriate name, the name *Private_sig* was chosen in this example.
- Select *172.16.5.71* from the **IP Address** drop-down menu, this is the inside or private IP Address of the Avaya SBCE.
- Enter *5060* for **TCP Port**.
- Click **Finish**.

The screenshot shows a web-based configuration window titled "Add Signaling Interface". The window contains the following fields and controls:

- Name:** Text input field containing "Private_sig".
- IP Address:** Dropdown menu showing "172.16.5.71".
- TCP Port:** Text input field containing "5060". Below the field is the text "Leave blank to disable".
- UDP Port:** Text input field. Below the field is the text "Leave blank to disable".
- Enable Stun:** A checkbox that is currently unchecked.
- TLS Port:** Text input field. Below the field is the text "Leave blank to disable".
- TLS Profile:** Dropdown menu showing "AvayaSBCServer".
- Enable Shared Control:** A checkbox that is currently unchecked.
- Shared Control Port:** Text input field.
- Finish:** A button at the bottom right of the form.

Red rectangles are drawn around the "Name", "IP Address", and "TCP Port" fields, and around the "Finish" button, indicating the steps to follow.

A second Signaling Interface with the name **Public_sig** facing the public network side was similarly created. Under **IP Address**, select **10.5.157.135**, this is the outside or public IP Address of the Avaya SBCE. Under **UDP Port**, enter **5060** since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.

Add Signaling Interface

Name: Public_sig

IP Address: 10.5.157.135

TCP Port: Leave blank to disable

UDP Port: 5060 Leave blank to disable

Enable Stun: ☐

TLS Port: Leave blank to disable

TLS Profile: AvayaSBCServer

Enable Shared Control: ☐

Shared Control Port:

Finish

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

Only the Signaling Interfaces highlighted in a red bracket are relevant to the SIP Trunk configuration settings covered under these Application Notes.

Session Border Controller for Enterprise

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

Signaling Interface: Sipera

Devices: Sipera

Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.71	5060	---	---	None	Edit Delete
Public_sig	10.5.157.135	---	5060	---	None	Edit Delete
RW_Private_sig	172.16.5.72	---	---	5061	AvayaSBCServer	Edit Delete
RW_Public_sig	10.5.157.180	---	---	5061	AvayaSBCServer	Edit Delete

6.5.4. End Point Flows

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

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

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** → **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown).

- **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_CM* (Note that this is the reverse route of the flow).
- **Topology Hiding Profile:** *Service_Provider*.
- **File Transfer Profile:** *None*.
- Click **Finish**.

Add FlowX

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_CM
Topology Hiding Profile	Service_Provider
File Transfer Profile	None

Finish

To create the call flow toward Communication Manager, from the **Device Specific Settings** → **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown)

- **Name:** *Comm_Manager_Flow*.
- **Server Configuration:** *Com 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:** *Com Manager*.
- **File Transfer Profile:** *None*.
- Click **Finish**.

The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a form with the following fields and values:

Field	Value
Flow Name	Comm_Manager_Flow
Server Configuration	Com 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	Com Manager
File Transfer Profile	None

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

The following screen capture shows the newly created **Server Flows**.

Only the Server Flows highlighted in a red bracket are relevant to the SIP Trunk configuration settings covered under these Application Notes.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, 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 'Device Specific Settings' and 'End Point Flows' highlighted in red. The main content area is titled 'End Point Flows: Sipera' and contains a tabbed interface with 'Subscriber Flows' and 'Server Flows' (the latter is highlighted in red). Below the tabs, there is an 'Add' button and a link to 'Click here to add a row description.' Three configuration sections are visible: 'Server Configuration: Com Manager', 'Server Configuration: Service Provider', and 'Server Configuration: Session Manager'. Each section contains a table of flows. The 'Server Configuration: Service Provider' table has one flow, 'SIP_Trunk_Flow', which is highlighted with a red bracket. The 'Server Configuration: Session Manager' table has one flow, 'SM from Rem Workers', which is also highlighted with a red bracket.

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

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_CM	View Clone Edit Delete

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM from Rem Workers	*	RW_Public_sig	RW_Private_sig	Rem Workers RTP	default	View Clone Edit Delete

7. Axtel SIP Trunk Configuration

To use Axtel's SIP Trunk service, a customer must request the service from Axtel using the established sales processes. The process can be started by contacting Axtel via the corporate web site at: <http://www.axtel.mx/> and requesting information.

During the signup process, Axtel will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. Axtel will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, SIP Trunk Registration (Dynamic) information, etc. This information is used to complete the Communication Manager and the Avaya SBCE configuration discussed in the previous sections.

8. Verification and Troubleshooting

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

8.1. General Verification Steps

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

8.2. Avaya Aura® Communication Manager Verification

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

- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group number>
Displays trunk group service state.
- **status station** <extension number>
Displays signaling and media information for an active call on a specific station.

8.3. Avaya Session Border Controller for Enterprise Verification

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

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

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Alarm Viewer

AVAYA

Devices

EMS

Sipera

Alarms

<input checked="" type="checkbox"/>	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.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Incident Viewer

AVAYA

Device All Category All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2006.


Type	ID	Date	Time	Category	Device	Cause
Message Dropped	701451499384946	6/16/14	7:16 AM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	701451491386902	6/16/14	7:16 AM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	701451487387891	6/16/14	7:16 AM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	701451371416220	6/16/14	7:12 AM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	701451367417207	6/16/14	7:12 AM	Policy	Sipera	No Server Flow Matched for Incoming Message

<< < 1 2 3 4 5 > >>

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

[Alarms](#) [Incidents](#) [Statistics](#) [Logs](#) **[Diagnostics](#)** [Users](#) [Settings](#) [Help](#) [Log Out](#)

Diagnostics



Devices

Sipera

Full Diagnostic

Ping Test

Application

Protocol

Start Diagnostic

Task Description	Status
➔ EMS Link Check	
➔ SBC Link Check: A1	
➔ SBC Link Check: B1	
➔ Ping: SBC (172.16.5.71) to Ping: Gateway (172.16.5.254)	
➔ Ping: SBC (172.16.5.71) to Ping: Primary DNS (172.16.5.102)	
➔ Ping: SBC (10.5.157.135) to Ping: Gateway (10.5.157.129)	
➔ Ping: SBC (10.5.157.135) to Ping: Primary DNS (172.16.5.102)	
➔ Ping: SBC (10.5.157.180) to Ping: Gateway (10.5.157.129)	
➔ Ping: SBC (10.5.157.180) to Ping: Primary DNS (172.16.5.102)	
➔ Ping: SBC (10.5.157.181) to Ping: Gateway (10.5.157.129)	
➔ Ping: SBC (10.5.157.181) to Ping: Primary DNS (172.16.5.102)	
➔ Ping: SBC (172.16.5.72) to Ping: Gateway (172.16.5.254)	
➔ Ping: SBC (172.16.5.72) to Ping: Primary DNS (172.16.5.102)	

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

The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand sidebar lists various management categories, with "Device Specific Settings" and "Troubleshooting" highlighted. The "Trace" option under Troubleshooting is also highlighted. The main content area is titled "Trace: Sipera" and contains 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 (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (Inc_to_CM.pcap). "Start Capture" and "Clear" buttons are at the bottom of the form.

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management and troubleshooting options, with 'Device Specific Settings' and 'Troubleshooting' highlighted. The main content area is titled 'Trace: Sipera' and contains three tabs: 'Call Trace', 'Packet Capture', and 'Captures'. The 'Captures' tab is active, showing a table with one entry: 'Inc_to_CM_20140606063339.pcap', which is 188,416 bytes and was last modified on June 6, 2014, at 6:34:06 AM GMT. A 'Delete' link is provided for this entry. A 'Refresh' button is located at the top right of the table.

File Name	File Size (bytes)	Last Modified	
Inc_to_CM_20140606063339.pcap	188,416	June 6, 2014 6:34:06 AM GMT	Delete

9. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2, to connect to the Axtel SIP Trunk service, as shown in **Figure 1**.

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

10. References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.3, June 2014, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3, June 2014, Document Number 555-245-205.
- [3] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, January 2014
- [5] *Avaya Session Border Controller for Enterprise Release Notes*. Release 6.2. FP1, December 2013
- [6] *Administering Avaya one-X® Communicator*, Release 6.2, December 2013.
- [7] *Using Avaya one-X® Communicator*, Release 6.2, December 2013.
- [8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>.
- [9] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

11. Appendix A

Signaling Manipulation script created in **Section 6.3.4** of the Avaya SBCE configuration, and included on the Trunk Server profile configuration, **Section 6.3.5**:

```
//Remove Remote-address header in outbound INVITE and 200 OK

within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
  remove(%HEADERS["Remote-Address"][1]);
}
}
```

©2014 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.