



Application Notes for Configuring Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 to support Group of Gold Line SIP Trunking – Issue 1.0

Abstract

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

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

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

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	10
5.	Configure Avaya Aura® Communication Manager	11
5.1.	Licensing and Capacity	11
5.2.	System Features.....	12
5.3.	IP Node Names.....	13
5.4.	Codecs	13
5.5.	IP Network Regions	14
5.6.	Signaling Group	15
5.7.	Trunk Group.....	17
5.8.	Calling Party Information.....	19
5.9.	Inbound Routing.....	19
5.10.	Outbound Routing	20
6.	Configure Avaya Aura® Session Manager	22
6.1.	System Manager Login and Navigation.....	23
6.2.	SIP Domain	24
6.3.	Locations	24
6.4.	Adaptations.....	26
6.5.	SIP Entities.....	27
6.6.	Entity Links	31
6.7.	Routing Policies	32
6.8.	Dial Patterns	33
7.	Configure Avaya Session Border Controller for Enterprise	36
7.1.	System Access.....	36
7.2.	System Management	37
7.3.	Network Management	38
7.4.	Media Interfaces	39
7.5.	Signaling Interfaces.....	40
7.6.	Server Interworking.....	42
7.6.1.	Server Interworking Profile – Enterprise.....	42
7.6.2.	Server Interworking Profile – Service Provider.....	45
7.7.	Signaling Manipulation	47
7.8.	Server Configuration	48
7.8.1.	Server Configuration Profile – Enterprise	48
7.8.2.	Server Configuration Profile – Service Provider	49
7.9.	Routing	51
7.9.1.	Routing Profile – Enterprise	51

7.9.2.	Routing Profile – Service Provider	52
7.10.	Topology Hiding.....	53
7.10.1.	Topology Hiding Profile – Enterprise	53
7.10.2.	Topology Hiding Profile – Service Provider.....	54
7.11.	End Point Policy Groups	55
7.11.1.	End Point Policy Group – Enterprise	55
7.11.2.	End Point Policy Group – Service Provider.....	56
7.12.	End Point Flows.....	57
7.12.1.	End Point Flow – Enterprise	57
7.12.2.	End Point Flow – Service Provider	58
8.	Group of Gold Line SIP Trunking Configuration.....	59
9.	Verification and Troubleshooting	59
9.1.	General Verification Steps	59
9.2.	Communication Manager Verification.....	59
9.3.	Session Manager Verification	60
9.4.	Avaya SBCE Verification	61
10.	Conclusion	64
11.	References.....	64
12.	Appendix A: SigMa Script.....	65

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Group of Gold Line SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 and various Avaya endpoints, as listed in **Section 4**.

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

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 Group of Gold Line SIP Trunking 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 trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk via the service provider network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using “This Computer” and “Other Phone” modes. (H.323, SIP).
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows softphones (SIP).
- Inbound and outbound PSTN calls to/from SIP remote workers using Avaya 96x1 deskphones, and the Avaya one-X® Communicator and Avaya Communicator for Windows softphones.
- Various call types, including: local, long distance and international.
- Codecs G729A, G.711MU, G.711A and proper codec negotiation.
- Inbound and outbound PSTN calls using VoIP media resources in Avaya Media Gateways and the Avaya Aura® Media Server at the enterprise network.
- DTMF tones passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail redirection and navigation.
- User features such as hold and resume, transfer and conference.
- Off-net call transferring, call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.
- Fax T.38.

The following items are not supported and were not tested:

- Network Call Redirection using REFER or 302 Move Temporarily method is not currently supported by Group of Gold Line.
- Inbound toll-free and emergency (911) calls are supported but were not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of Group of Gold Line SIP Trunking with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **Call Transfer to the PSTN:** Since Network Call Redirection (NCR) using REFER or the 302 Moved Temporarily method is not currently supported by Group of Gold Line, NCR needs to be disabled on the Trunk Group form in Avaya Communication Manager.
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that have no significance in the service provider's network. These headers were removed with the purposes of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider's network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location (**Section 6.4**). Additionally, the parameters "gsid" and "epv" were removed from outbound Contact headers using a Signaling Script in the Avaya SBCE (**Section 7.7**).

2.3. Support

For technical support on the Group of Gold Line solutions, please use the support link at <http://www.groupofgoldline.com>.

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Group of Gold Line SIP Trunking service through a public Internet WAN connection.

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

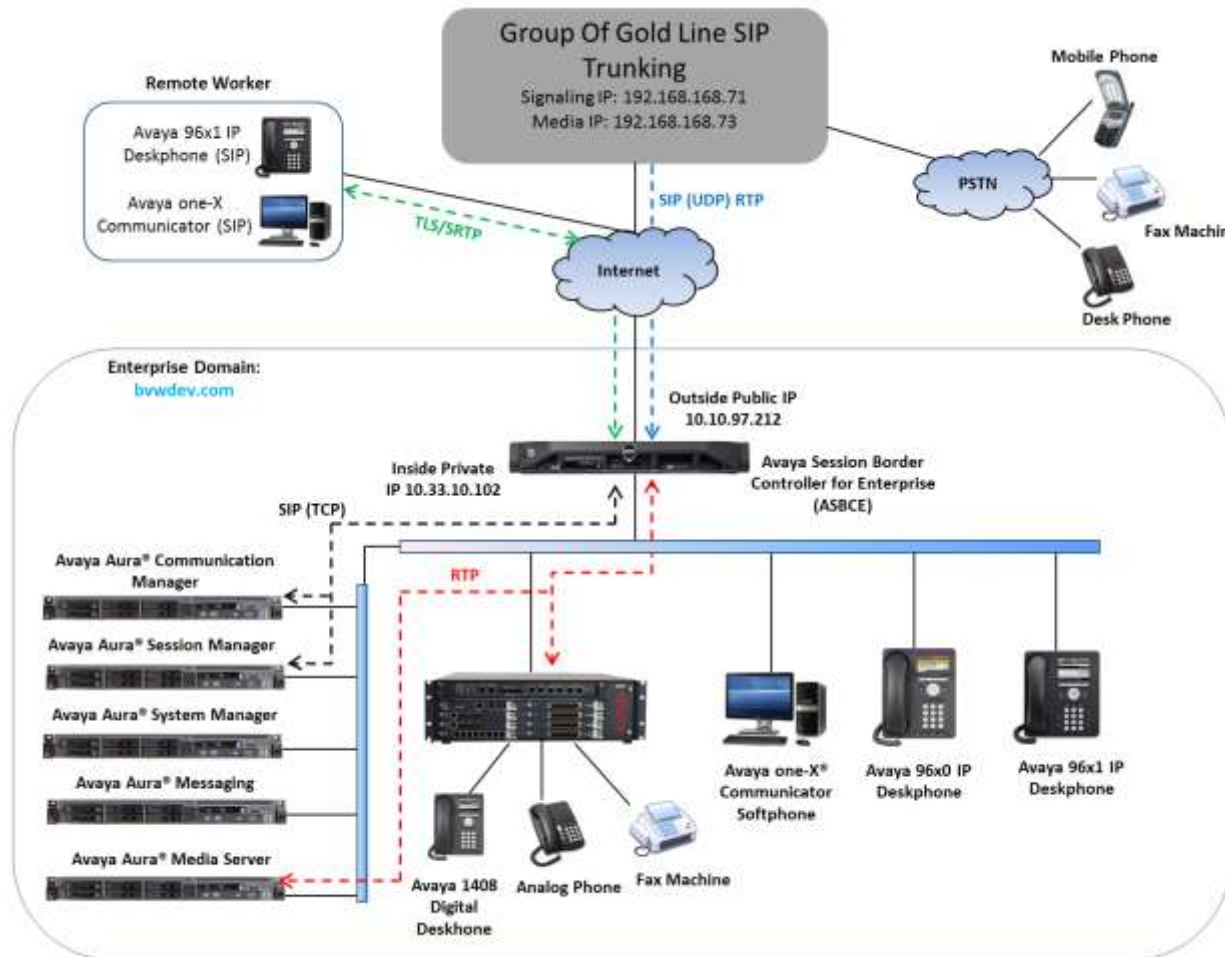


Figure 1: Avaya SIP Enterprise Solution connected to Group of Gold Line SIP Trunking.

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

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

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

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

For security reasons, TLS and SRTP are the recommended protocols to be used by all remote workers endpoints. During the tests, TCP and RTP were used with Avaya one-X® Communicator for tracing and troubleshooting purposes.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [5] in the **References** section for additional information on this topic.

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

The transport protocol between the Avaya SBCE and Group of Gold Line across the public IP network was UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network was TCP.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE, then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

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

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

As part of the Avaya Aura® version 7.0 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Server (Avaya AMS) as a media resource. The Avaya AMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the Avaya AMS and a G450 Media Gateway were utilized during the compliance test. The configuration of the Avaya AMS is not discussed in this document. For more information on the installation and administration of the Avaya AMS in Communication Manager refer to [6] and [7] in the **References** section.

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

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager in Virtualized Environment	7.0 Service Pack 1 (R017x.00.0.441.0 patch 22477)
Avaya Aura® Session Manager in Virtualized Environment	7.0 (7.0.0.0.700007)
Avaya Aura® System Manager in Virtualized Environment	7.0.0.1 (7.0.0.0.16266-7.0.9.7001011)
Avaya Session Border Controller for Enterprise in Virtualized Environment	7.0.0-21-6602
Avaya Aura® Messaging in Virtualized Environment	6.3.3
Avaya Aura® Media Server in Virtualized Environment	7.7.0.226
Avaya G450 Media Gateway	37.19.0
Avaya 96x0 Series IP Deskphones	S3.250A (H323) 2.69 (SIP)
Avaya 96x1 Series IP Deskphones	6.615 (H323) 7.0.0.39 (SIP)
Avaya one-X® Communicator (H.323, SIP)	6.2.6.03-FP7
Avaya Communicator for Windows	2.1.2.75
Avaya 1408 Digital Telephone	R45.0
Analog Telephone	N/A
Group of Gold Line	
Sonus GSX9000HD (Network Border Switch)	V09.00.04 R000

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

5. Configure Avaya Aura® Communication Manager

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

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

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 **24** 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.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES			USED
Maximum Administered H.323 Trunks:		4000	0
Maximum Concurrently Registered IP Stations:		2400	2
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	7
Maximum Administered SIP Trunks:		4000	24
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

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**.

```
display system-parameters features                               Page 1 of 19
                        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/Tone on Hold: music Type: ext
1112
                        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.

```
display system-parameters features                               Page 9 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS
CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: Restricted
      CPN/ANI/ICLID Replacement for Unavailable Calls: Unavailable

DISPLAY TEXT
principal
                        Identity When Bridging:
                        User Guidance Display? n
      Extension only label for Team button on 96xx H.323 terminals? n
INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code:
      International Access Code:
```

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 Session Manager security module (*interopASM*). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AMS1	10.33.10.90	
TFTP	10.10.98.86	
default	0.0.0.0	
interopASM	10.33.1.12	
procr	10.33.1.6	

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 3 was used for this purpose. Group of Gold Line used codecs G.729A, G711MU and G711A on the SIP trunk, in this order of preference. Enter the corresponding codecs in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 3		Page 1 of 2
IP CODEC SET		
Codec Set: 3		
Audio Codec	Silence Suppression	Frames Per Pkt
		Packet Size (ms)
1: G.729	n	2 20
2: G.711MU	n	2 20
3: G.711A	n	2 20

On **Page 2**, set the **Fax Mode** to *t.38-standard*.

change ip-codec-set 3		Page 2 of 2
IP CODEC SET		
Allow Direct-IP Multimedia? n		
	Mode	Redundancy
FAX	t.38-standard	0 ECM: y
Modem	off	0
TDD/TTY	US	3
H.323 Clear-channel	n	0
SIP 64K Data	n	0 20

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 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwddev.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**, 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 needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

```
change ip-network-region 3                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 3
Location: 1           Authoritative Domain: bvwddev.com
Name: public         Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 3         Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION
PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled?
n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region **3** 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 **1** will be used for calls between region **3** (the service provider region) and region **1** (the rest of the enterprise).

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

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

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

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

add signaling-group 3		Page 1 of 2
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: interopASM	
Near-end Listen Port: 5080	Far-end Listen Port: 5080	
	Far-end Network Region: 3	
Far-end Domain: bvwdev.com		
		Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3		IP Audio Hairpinning? n
Enable Layer 3 Test? y		Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TCP, the well-known port value is 5060). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. For the compliance test both the **Near-end Listen Port** and **Far-end Listen Port** were set to **5080**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to **n**, then the Avaya Media Gateway or the Avaya AMS will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Avaya AMS, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields.

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

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

```
add trunk-group 3                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 3                                     Group Type: sip          CDR Reports: y
  Group Name: For-Public                           COR: 1                 TN: 1             TAC: #03
  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: 3
                                                    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. The default value of **600** seconds was used.

```
add trunk-group 3                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                                    Redirect On OPTIM Failure: 5000
  SCCAN? n                                           Digital Loss Group: 18
                                                    Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
```

On **Page 3**, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. When *public* format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. The addition of the “+” sign impacted interoperability with Group of Gold Line. Thus, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (see **Section 5.10**). Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call has enabled CPN block.

add trunk-group 3	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no

On **Page 4**, set the **Network Call Redirection** field to *n*. See Section 2.2 for more details on this setting. Set the **Send Diversion Header** field to *y*, this is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Support Request History** field to *n*.

Set the **Telephone Event Payload Type** to **101**, and **Convert 180 to 183 for Early Media** to *y*, the values preferred by Group of Gold Line. Default values were used for all other fields.

add trunk-group 3	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	Send Transferring Party Information? n
	Network Call Redirection? n
	Send Diversion Header? y
	Support Request History? n
	Telephone Event Payload Type: 101
	Convert 180 to 183 for Early Media? y
	Always Use re-INVITE for Display Updates? n
	Identity for Calling Party Display: P-Asserted-Identity
	Block Sending Calling Party Location in INVITE? n
	Accept Redirect to Blank User Destination? n
	Enable Q-SIP? N
	Interworking of ISDN Clearing with In-Band Tones: keep-channel-active

5.8. Calling Party Information

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

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp (s)	Prefix	Len	
4	33	1		4	Total Administered: 10
4	34	1		4	Maximum Entries: 540
4	3300	3	6474441234	10	
4	3301	3	6474441235	10	
4	3302	3	6474441236	10	
4	3404	3	6474441237	10	
4	3402	3	6474441238	10	

5.9. Inbound Routing

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

change inc-call-handling-trmt trunk-group 3					Page 1 of 3
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	10	6474441234	10	3300	
public-ntwrk	10	6474441235	10	3301	
public-ntwrk	10	6474441236	10	3402	
public-ntwrk	10	6474441237	10	3404	
public-ntwrk	10	6474441238	10	3402	

5.10. Outbound Routing

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	4	ext						
24	4	aar						
28	5	aar						
30	4	aar						
33	4	ext						
34	4	ext						
4	4	aar						
9	1	fac						
*	3	dac						
#	3	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 12		
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: *05					
Answer Back Access Code:					
Attendant Access Code:					
Auto Alternate Routing (AAR) Access Code:					
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: *10					
CDR Account Code Access Code:					
Change COR Access Code:					
Change Coverage Access Code:					
Conditional Call Extend Activation:			Deactivation:		
Contact Closure Open Code:			Close Code:		

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 3, which contains the SIP trunk group to the service provider.

change ars analysis 4							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 2
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
411	3	3	3	svcl		n	
647	10	10	3	hnpa		n	
011	10	14	3	intl		n	
1613	10	11	3	fnpa		n	
1800	11	11	3	fnpa		n	

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 3 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** Set to **unk-unk**. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

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

Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration.

6. Configure Avaya Aura® Session Manager

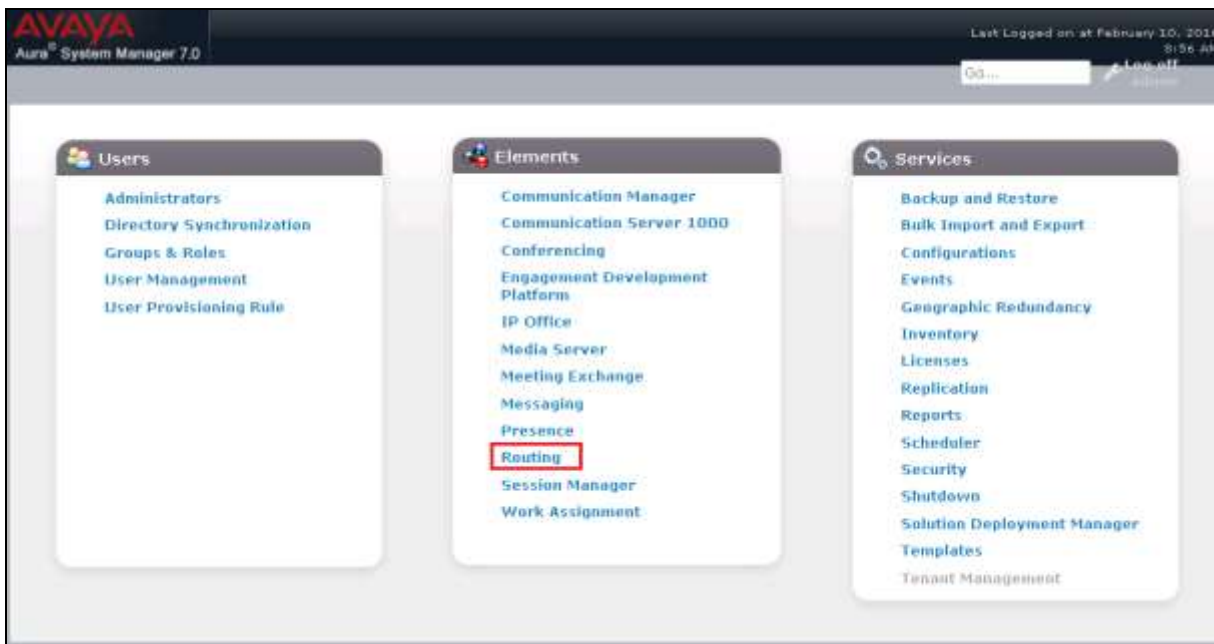
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.

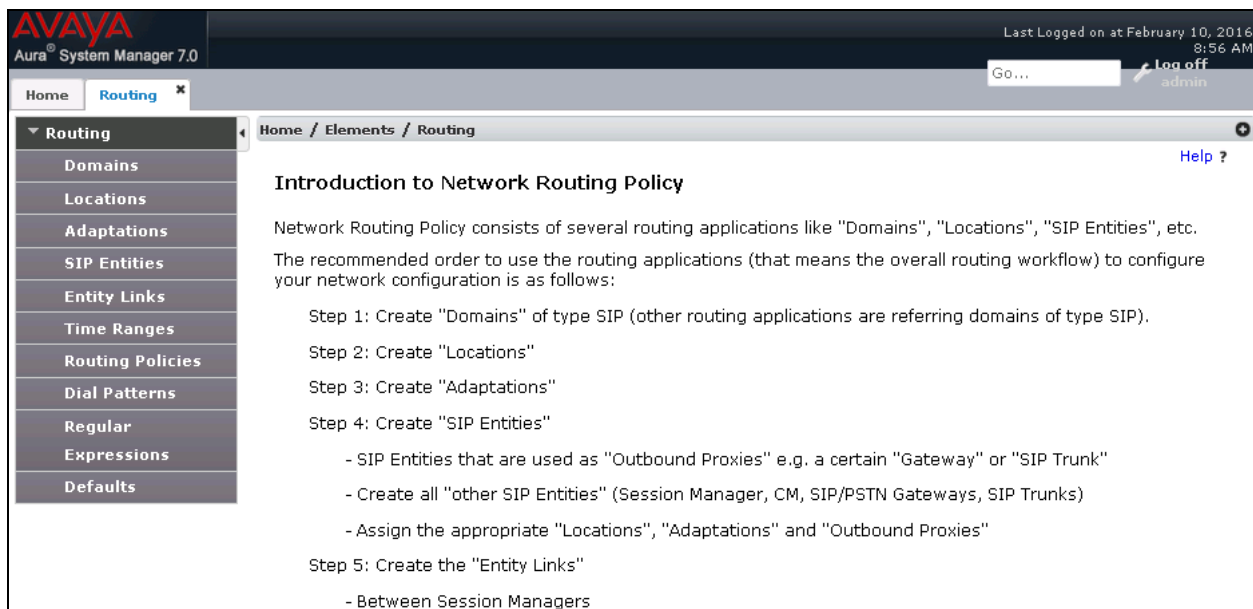
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. System Manager Login and Navigation

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



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



6.2. SIP Domain

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

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

Click **Commit**. The screen below shows the entry for the enterprise domain.

The screenshot shows the 'Domain Management' interface. On the left is a navigation pane with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the title 'Domain Management' are 'Commit' and 'Cancel' buttons. A table shows '1 Item' with a refresh icon and a 'Filter: Enable' link. The table has three columns: 'Name', 'Type', and 'Notes'. The first row contains 'bvwdev.com', 'sip', and 'SIP Domain'. At the bottom right are 'Commit' and 'Cancel' buttons.

Name	Type	Notes
* bvwdev.com	sip	SIP Domain

6.3. Locations

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

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

Defaults can be used for all other parameters.

The following screen shows the location details for the location named **BvwDevSIL**. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Default values were used for all parameters. The Location Pattern section is added with IP Address pattern of IP phones and Aura System.

The screenshot displays the 'Location Details' configuration page for a location named 'BvwDevSIL'. The page is part of a web application with a sidebar menu on the left containing options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The page is organized into several sections: 'General', 'Dial Plan Transparency in Survivable Mode', 'Overall Managed Bandwidth', 'Per-Call Bandwidth Parameters', 'Alarm Threshold', and 'Location Pattern'.

General

* Name: BvwDevSIL
Notes: Belleville DevConnect

Dial Plan Transparency in Survivable Mode

Enabled: ☐
Listed Directory Number:
Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec
* Minimum Multimedia Bandwidth: 64 Kbit/Sec
* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %
Multimedia Alarm Threshold: 80 %
* Latency before Overall Alarm Trigger: 5 Minutes
* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

2 Items Filter: Enable

	IP Address Pattern	Notes
<input checked="" type="checkbox"/>	* 10.33.1.*	Net 10.33.1.0 for Aura System
<input checked="" type="checkbox"/>	* 10.33.5.*	Net 10.33.5.0 for IP phone

6.4. Adaptations

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

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

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

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

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

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

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left with their default values.

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel

General

* **Adaptation Name:** Outbound_Header_Removal

* **Module Name:** DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	eRHdrs	Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View

Select : All, None

Egress URI Parameters:

Notes:

6.5. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes Communication Manager and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**
If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of the Session Manager SIP Entity. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

AVAYA
Aura® System Manager 7.0

Last Logged on at February 10, 2016 8:56 AM

Go... Log off admin

Home Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel Help ?

General

* Name: ASM70

* FQDN or IP Address: 10.33.1.12

Type: Session Manager

Notes:

Location: BvwDevSIL

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

To define the ports that Session Manager will use to listen for SIP requests, scroll down to the Port section of the SIP Entity Details screen. This section is only present for Session Manager SIP entities. The screen below shows the ports used by Session Manager in the shared lab environment. TCP port 5060 and 5080 and TLS port 5061 are the ones directly relevant to the SIP trunk to Group of Gold Line in the reference configuration.

Listen Ports

TCP Failover port:

TLS Failover port:

Add Remove

4 Items Filter: Enable

	Listen Ports	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	bvwdev.com	
<input type="checkbox"/>	5060	UDP	bvwdev.com	
<input type="checkbox"/>	5061	TLS	bvwdev.com	
<input type="checkbox"/>	5080	TCP	bvwdev.com	

Select : All, None

The following screen shows the addition of the SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**.

AVAYA
Aura® System Manager 7.0

Last Logged on at February 10, 2016 8:56 AM
Go... Log off admin

Home Routing * Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details

General

* Name: ACM-Trunk3-Public

* FQDN or IP Address: 10.33.1.6

Type: CM

Notes: Trunk to CM for public

Adaptation:

Location: BvwDevSIL

Time Zone: America/Toronto

* SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). On the **Adaptation** field, the adaptation module *Outbound_Header_Remove* previously defined in **Section 6.4** is selected.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.0", and a "Last Logged on at February 10, 2016 8:56 AM" timestamp. A "Go..." search bar and a "Log off admin" link are also present. The left sidebar contains a tree view with "Routing" selected, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "SIP Entity Details" and includes "Commit" and "Cancel" buttons. The breadcrumb trail reads "Home / Elements / Routing / SIP Entities". The form is divided into three sections: "General", "Loop Detection", and "SIP Link Monitoring".

SIP Entity Details

General

- * Name: Avaya SBCE70
- * FQDN or IP Address: 10.33.10.102
- Type: SIP Trunk
- Notes:
- Adaptation: Outbound_Headers_Remove
- Location: BywDevSIL
- Time Zone: America/Toronto
- * SIP Timer B/F (in seconds): 4
- Credential name:
- Securable: ☐
- Call Detail Recording: egress

Loop Detection

- Loop Detection Mode: On
- Loop Count Threshold: 5
- Loop Detection Interval (in msec): 200

SIP Link Monitoring

- SIP Link Monitoring: Use Session Manager Configuration

6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.

Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. The page title is 'Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, and SIP Entity 2. The row contains: Name: SM-CM-Trunk3-5080, SIP Entity 1: ASM70, Protocol: TCP, Port: 5080, and SIP Entity 2: ACM-Trunk3-Put. At the bottom, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2
SM-CM-Trunk3-5080	ASM70	TCP	5080	ACM-Trunk3-Put

The Entity Link to the Avaya SBCE is show below. **TCP** and port **5060** were used.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb trail is 'Home / Elements / Routing / Entity Links'. The page title is 'Entity Links'. There are 'Commit' and 'Cancel' buttons. Below the title, there is a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, and SIP Entity 2. The row contains: Name: SM-SBCE70-5060, SIP Entity 1: ASM70, Protocol: TCP, Port: 5060, and SIP Entity 2: Avaya SBCE70. At the bottom, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2
SM-SBCE70-5060	ASM70	TCP	5060	Avaya SBCE70

6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).

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

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

The screenshot shows the 'Routing Policy Details' page for a policy named 'To-CM-Trunk3'. The left navigation pane is expanded to 'Routing Policies'. The 'General' section contains the following fields: 'Name' (To-CM-Trunk3), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (empty). The 'SIP Entity as Destination' section shows a 'Select' button and a table with one entry: 'ACM-Trunk3-Public' with FQDN '10.33.1.6', Type 'CM', and Notes 'Trunk to CM for public'. The top right has 'Commit' and 'Cancel' buttons and a 'Help ?' link.

Name	FQDN or IP Address	Type	Notes
ACM-Trunk3-Public	10.33.1.6	CM	Trunk to CM for public

The screenshot shows the 'Routing Policy Details' page for a policy named 'To-ASBCE'. The left navigation pane is expanded to 'Routing Policies'. The 'General' section contains the following fields: 'Name' (To-ASBCE), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (Route to SBC A1 IP 10.33.10.102). The 'SIP Entity as Destination' section shows a 'Select' button and a table with one entry: 'Avaya SBCE70' with FQDN '10.33.10.102', Type 'SIP Trunk', and Notes (empty). The top right has 'Commit' and 'Cancel' buttons and a 'Help ?' link.

Name	FQDN or IP Address	Type	Notes
Avaya SBCE70	10.33.10.102	SIP Trunk	

6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, or select “**ALL**” to route incoming calls to all SIP domains.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with **647**, which was the DID range of numbers assigned by Group of Gold Line to the SIP trunk, arriving from location **Avaya SBCE**, used route policy **To-CM-Trunk 3** to Communication Manager.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details

Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-CM-Trunk3	0	<input type="checkbox"/>	ACM-Trunk3-Public	

Select : [All](#), [None](#)

Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows that 11 digit dialed numbers for outbound calls, beginning with a number such as **1613** used for test purposes during the compliance test, arriving from the **Communication Manager** location, will use route policy **To-ASBCE**, which sends the call out to the PSTN via Avaya SBCE and the Group of Gold Line SIP Trunk.

Dial Pattern Details Commit Cancel Help ?

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove 1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-ASBCE	0	<input type="checkbox"/>	Avaya SBCE70	Route to SBC A1 IP 10.33.10.102

Select : All, None

Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider's network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

7.1. System Access

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



The login page features the Avaya logo on the left. To the right, under the heading "Log In", are input fields for "Username" and "Password", followed by a "Log In" button. Below the login fields, there is a block of legal disclaimer text regarding unauthorized access and system monitoring. At the bottom left of the page, it says "Session Border Controller for Enterprise".

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



The dashboard interface includes a top navigation bar with links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is divided into several sections:

- Left Navigation Pane:** Contains links for Dashboard, Administration, Backup/Restore, System Management (with sub-links for Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings), and other system management options.
- Dashboard Information Table:**

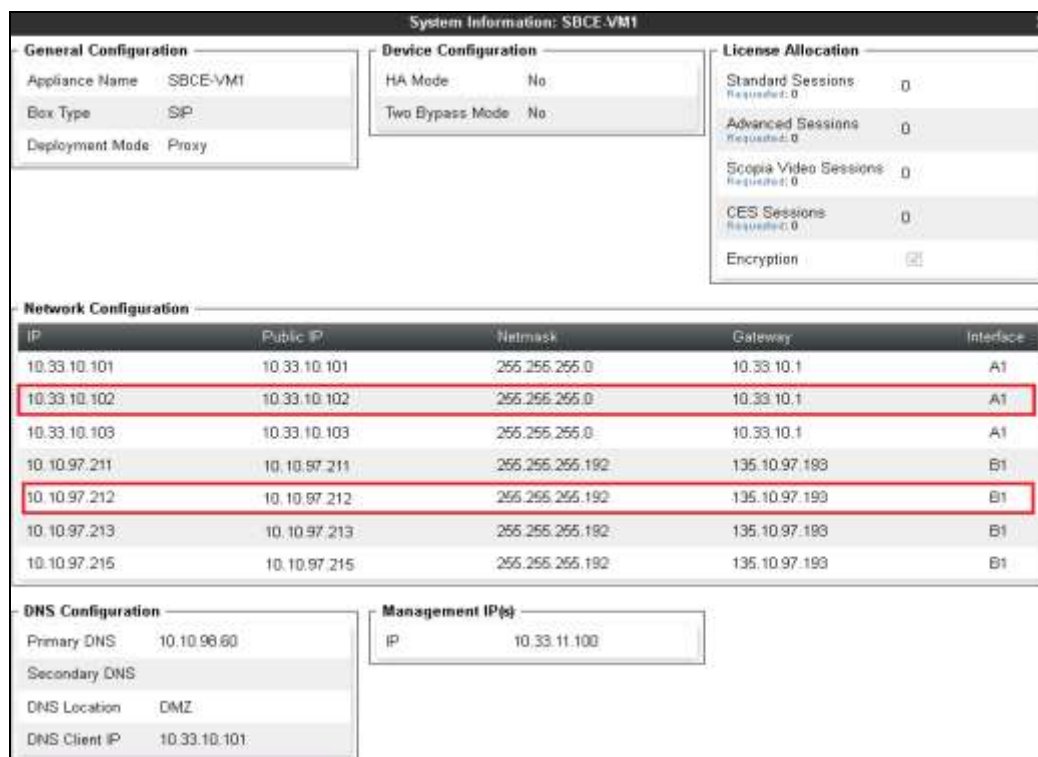
Information	
System Time	02:21:08 PM EST Refresh
Version	7.0.0-21-6602
Build Date	Sun Aug 9 21:08:40 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	-
Failed Login Attempts	3
- Installed Devices:** A list showing "EMS" and "SBCE-VM1".
- Alarms (past 24 hours):** A section indicating "None found".
- Incidents (past 24 hours):** A section indicating "None found".

7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **SBCE-VM1** 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. 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 configuration and network settings.



The **A1** and **B1** interfaces correspond to the private and public interfaces of the Avaya SBCE. Note that the highlighted **A1** and **B1** IP addresses are the ones used for the SIP trunk to the service provider, and the ones relevant to these Application Notes. Other IP addresses assigned to these interfaces are used to support remote workers and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

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

7.3. Network Management

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

Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, **SBCE-VM1** in the sample configuration. On the **Networks** tab, verify or enter the network information as needed. Note that the **A1** and **B1** interfaces correspond to the private and public interfaces for the Avaya SBCE.

In the configuration used during the compliance test, IP address **10.33.10.102** was assigned to interface **A1**, and IP address **10.10.97.212** was assigned to interface **B1**.



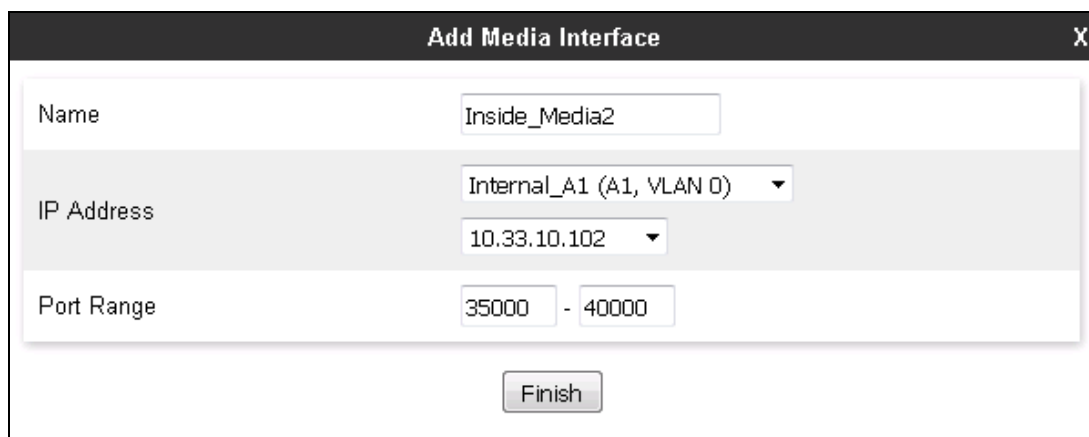
On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary to enable the interfaces.



7.4. Media Interfaces

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

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Under **IP Address**, select from the drop-down menus the network and IP address associated with the private interface of the Avaya SBCE (A1). The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.



Add Media Interface X

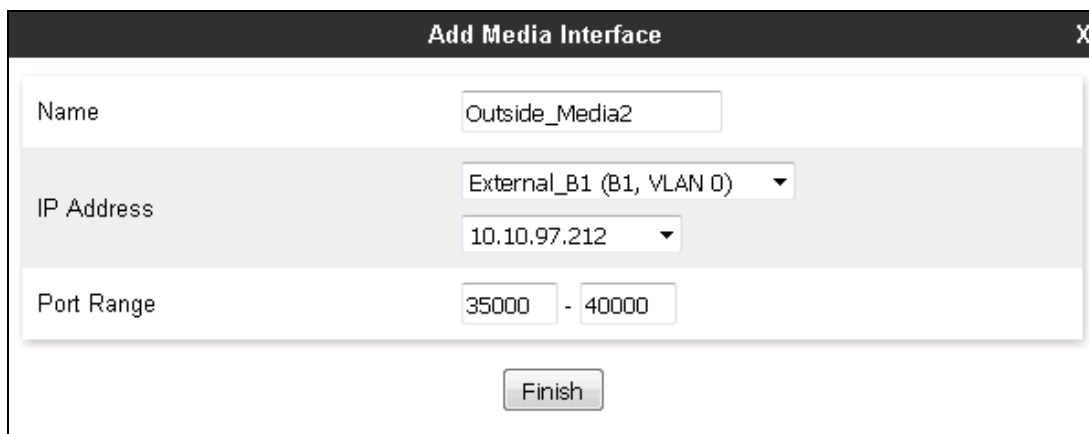
Name: Inside_Media2

IP Address: Internal_A1 (A1, VLAN 0) ▼
10.33.10.102 ▼

Port Range: 35000 - 40000

Finish

A Media Interface facing the public network side was similarly created with the name **Outside_Media2**, as shown below. Under **IP Address**, the network and IP address associated with the public interface of the SBCE (B1) were selected from the drop-down menus. The **Port Range** was left at the default values. Click **Finish**.



Add Media Interface X

Name: Outside_Media2

IP Address: External_B1 (B1, VLAN 0) ▼
10.10.97.212 ▼

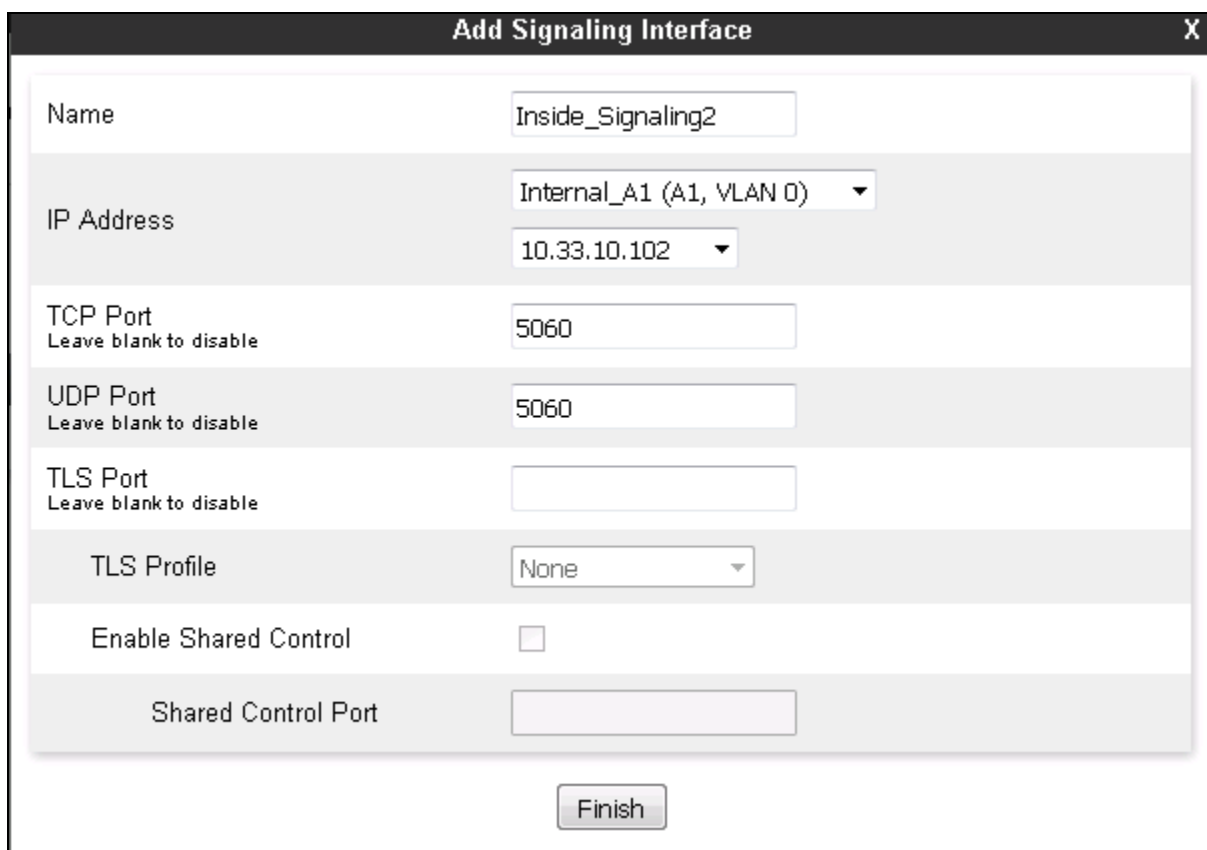
Port Range: 35000 - 40000

Finish

7.5. Signaling Interfaces

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

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Under **IP Address**, select from the drop-down menus the network and IP address associated with the private interface of the SBCE (A1). Enter **5060** for **TCP** and **UDP Port**, since TCP port 5060 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**. Click **Finish**.



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

Field Label	Value
Name	Inside_Signaling2
IP Address	Internal_A1 (A1, VLAN 0) (Network) 10.33.10.102 (IP)
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

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

A second Signaling Interface with the name **Outside_Signaling2** was similarly created in the service provider's direction. Under **IP Address**, the network and IP address associated with the public interface of the SBCE (B1) were selected from the drop-down menus. Enter **5060** for **UDP Port**, since this is the protocol and port that was used by the Avaya SBCE to listen to the service provider's SIP traffic. Click **Finish**.

Add Signaling InterfaceX

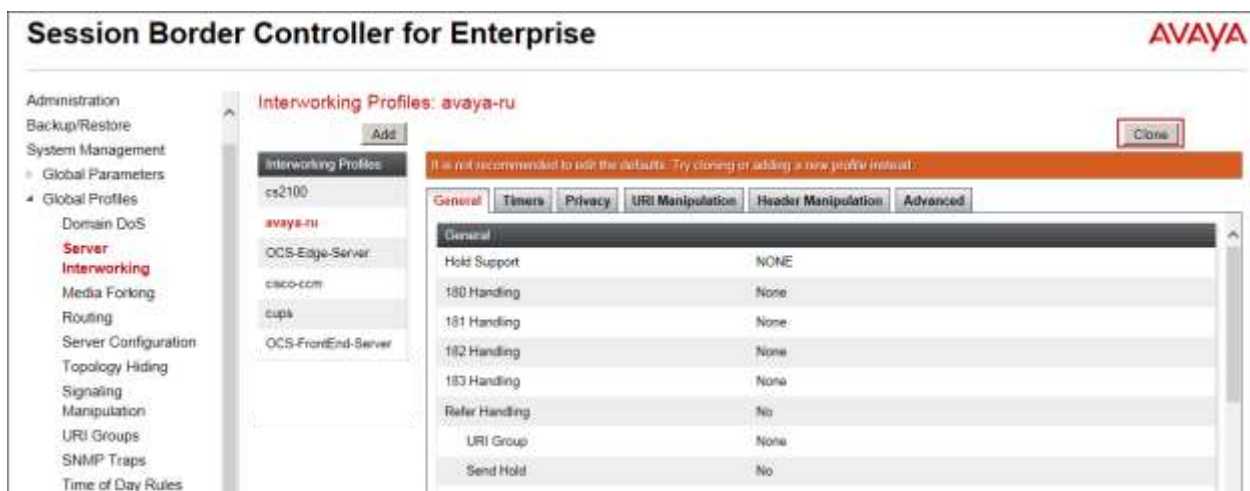
Name	Outside_Signaling2
IP Address	External_B1 (B1, VLAN 0) 10.10.97.212
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	
Finish	

7.6. Server Interworking

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

7.6.1. Server Interworking Profile – Enterprise

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



Enter a descriptive name for the cloned profile. Click **Finish**.

Clone Profile X

Profile Name

avaya-ru

Clone Name

Session Manager

Finish

On the newly cloned **Session Manager** interworking profile, on the **General** tab, scroll down to the bottom of the page and click **Edit** (not shown). Check the **T.38 Support** box. All other parameters retain their default values. Click **Finish**.

Editing Profile: Session Manager

General

Hold Support ☒ None
☐ RFC2543 - c=0.0.0.0
☐ RFC3264 - a=sendonly

180 Handling ☒ None ☐ SDP ☐ No SDP

181 Handling ☒ None ☐ SDP ☐ No SDP

182 Handling ☒ None ☐ SDP ☐ No SDP

183 Handling ☒ None ☐ SDP ☐ No SDP

Refer Handling ☐

URI Group

Send Hold ☐

Delayed Offer ☐

3xx Handling ☐

Diversion Header Support ☐

Delayed SDP Handling ☐

Re-Invite Handling ☐

Prack Handling ☐

Allow 18X SDP ☐

T.38 Support ☒

URI Scheme ☒ SIP ☐ TEL ☐ ANY

Via Header Format ☒ RFC3261
☐ RFC2543


Finish

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries or keep their default values. The **Advanced** tab settings are shown on the screen below:

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes		Both Sides			
Include End Point IP for Context Lookup		Yes			
Extensions		Avaya			
Diversion Manipulation		No			
Has Remote SBC		Yes			
Route Response on Via Port		No			
DTMF					
DTMF Support		None			
<div>Edit</div>					

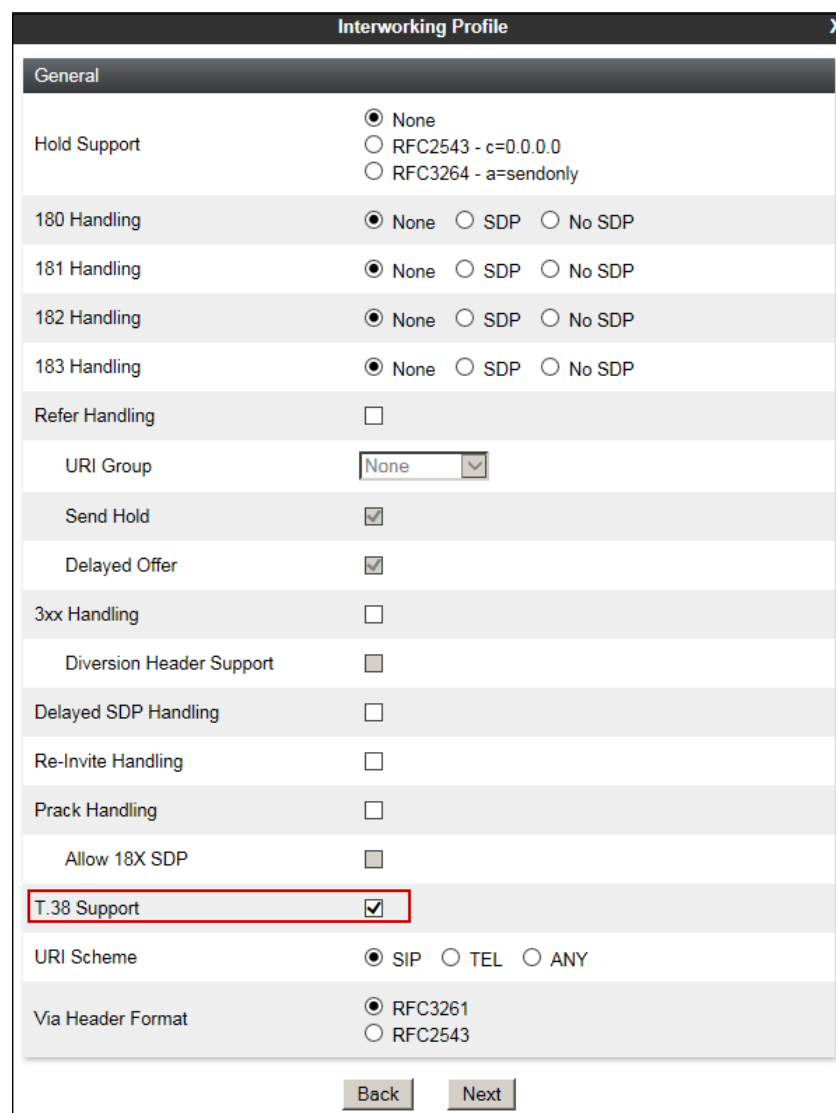
7.6.2. Server Interworking Profile – Service Provider

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



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 "Service Provider". Below the input field is a "Next" button.

On the **General** screen, check the **T.38 Support** box. All other parameters retain their default values. Click **Next**.



The screenshot shows the "Interworking Profile" dialog box with the "General" tab selected. The "T.38 Support" checkbox is checked and highlighted with a red rectangle. Other settings include: Hold Support (None), 180 Handling (None), 181 Handling (None), 182 Handling (None), 183 Handling (None), Refer Handling (unchecked), URI Group (None), Send Hold (checked), Delayed Offer (checked), 3xx Handling (unchecked), Diversion Header Support (unchecked), Delayed SDP Handling (unchecked), Re-Invite Handling (unchecked), Prack Handling (unchecked), Allow 18X SDP (unchecked), URI Scheme (SIP), and Via Header Format (RFC3261). The "Back" and "Next" buttons are at the bottom.

Parameter	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input checked="" type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Click **Next** on the **SIP Timers** and **Privacy** tabs (not shown). On the **Advanced/DTMF** tab, select **Both Sides** under **Record Routes**. Accept the defaults settings for all other fields. Click **Finish**.

Interworking Profile

X

Record Routes

☐ None

☐ Single Side

☒ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☐

Extensions

None

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

Back

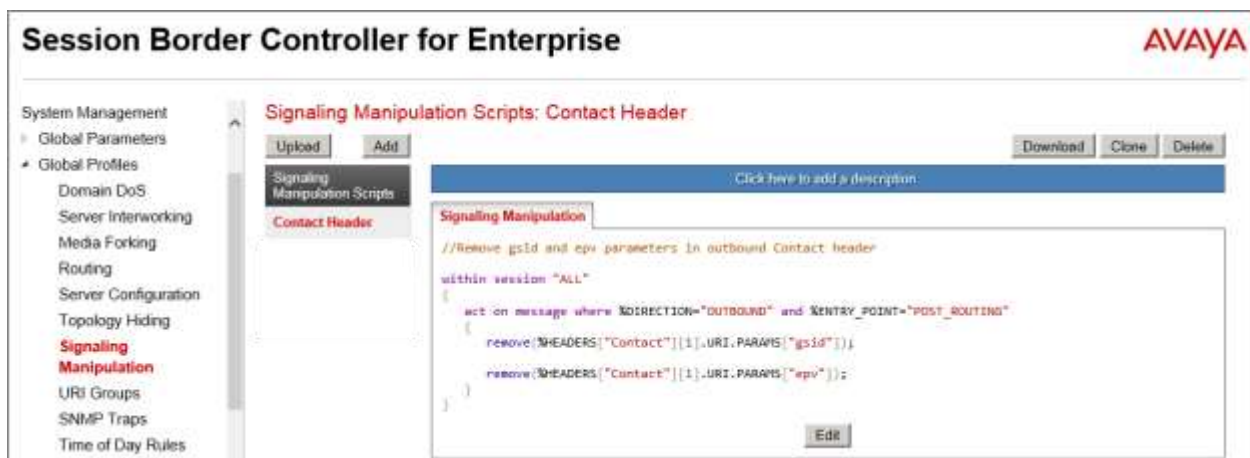
Finish

7.7. Signaling Manipulation

The screen below shows the finished Signaling Manipulation script named *Contact Header* created during the compliance test. This script was used to remove the “gsid” and “epv” parameters from outbound “Contact” headers. These parameters have no significance to the service provider and add unnecessary size to the outbound messages.

The script will later be applied to the Server Configuration profile corresponding to the service provider, later in **Section 7.8.2**.

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



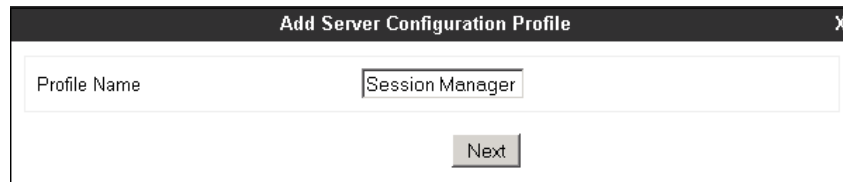
The details of the script used can be found in **Appendix A** in this document.

7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and the SIP Proxy at the service provider network (Trunk Server).

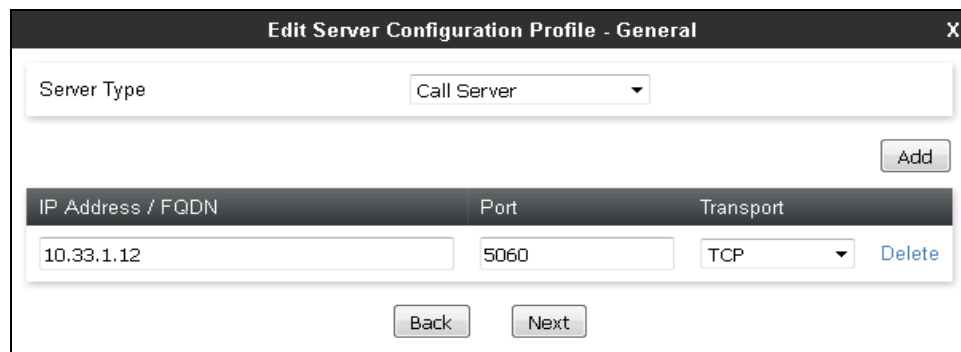
7.8.1. Server Configuration Profile – Enterprise

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



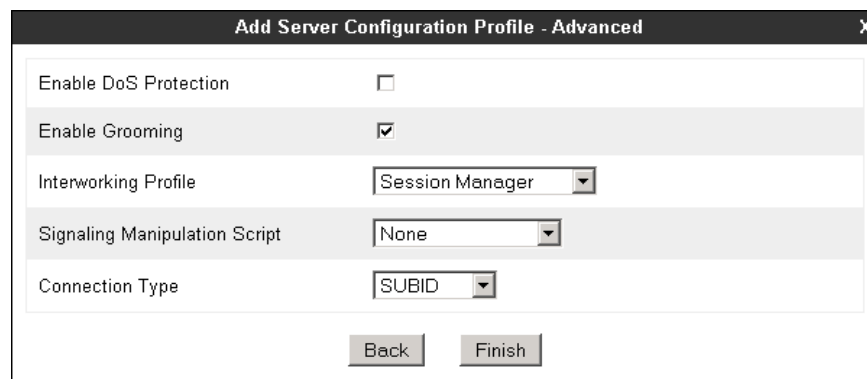
The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Session Manager". Below this field is a "Next" button.

On the **Server Configuration Profile General** Tab select **Call Server** from the drop down menu under the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.4**). Enter **5060** under **Port** and select **TCP** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously in **Section 6.5**. Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. Inside the dialog, there is a "Server Type" dropdown menu set to "Call Server". Below this is an "Add" button. Underneath is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "10.33.1.12", "5060", and "TCP". There is a "Delete" button next to the first row. At the bottom of the dialog are "Back" and "Next" buttons.

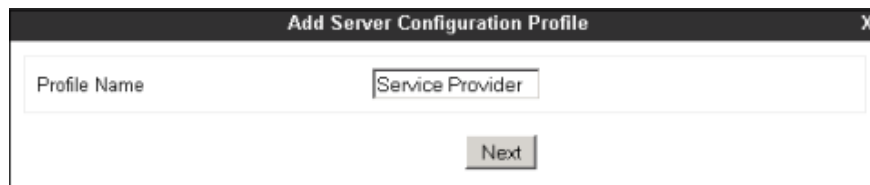
Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select **Session Manager** from the **Interworking Profile** drop down menu. Click **Finish**.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It has a close button (X) in the top right corner. Inside the dialog, there are several settings: "Enable DoS Protection" (unchecked), "Enable Grooming" (checked), "Interworking Profile" (dropdown set to "Session Manager"), "Signaling Manipulation Script" (dropdown set to "None"), and "Connection Type" (dropdown set to "SUBID"). At the bottom are "Back" and "Finish" buttons.

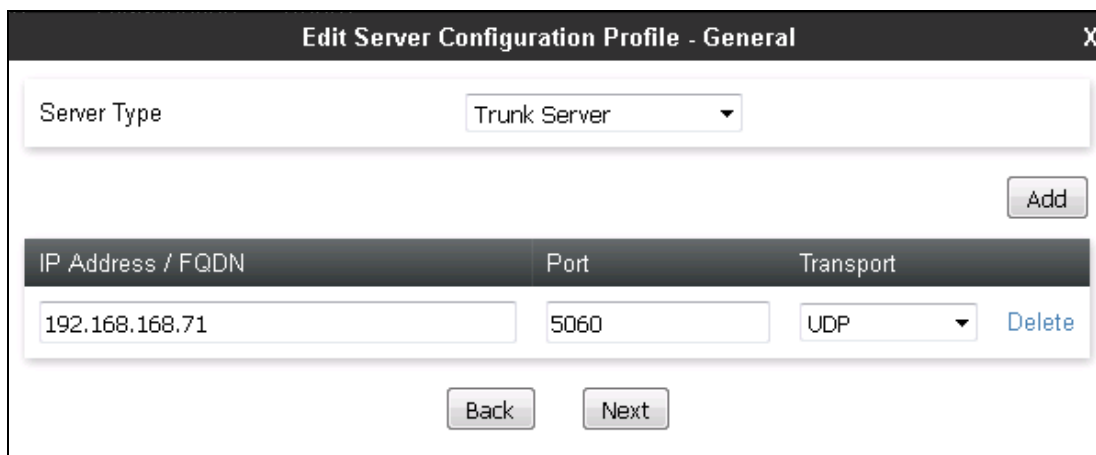
7.8.2. Server Configuration Profile – Service Provider

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



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" which contains the text "Service Provider". Below this field is a "Next" button.

On the **Add Server Configuration Profile** Tab select **Trunk Server** from the drop down menu for the **Server Type**. On the **IP Addresses / FQDN** field, enter the IP address of the service provider SIP proxy server. Enter **5060** under **Port**, and select **UDP** for **Transport**. Click **Next**.

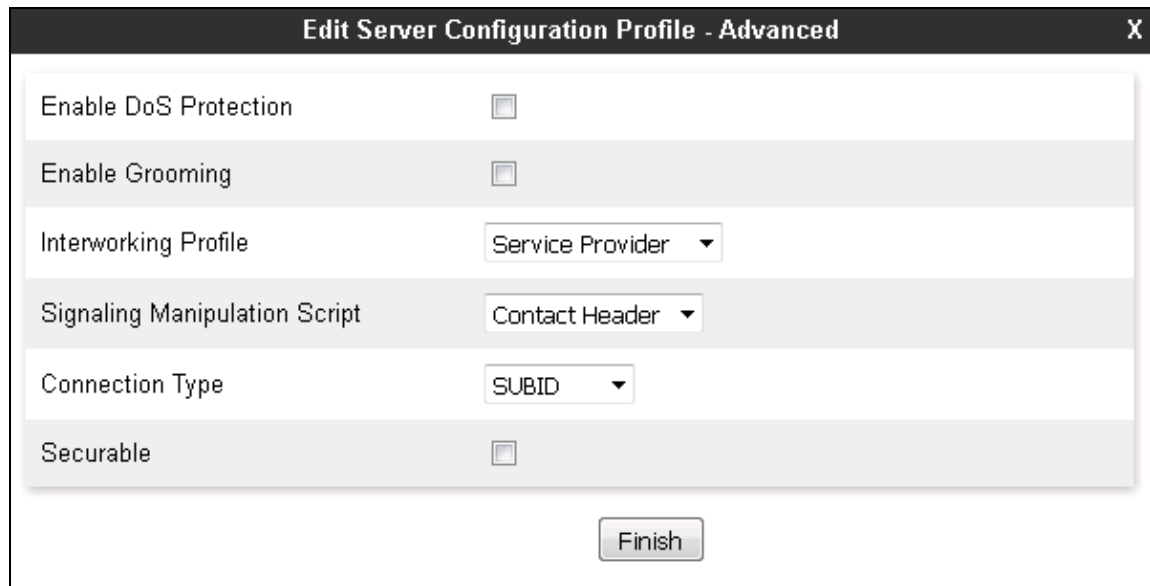


The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. Inside the dialog, there is a "Server Type" dropdown menu set to "Trunk Server". To the right of this is an "Add" button. Below this is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "192.168.168.71", "5060", and "UDP". To the right of the table is a "Delete" link. At the bottom of the dialog are "Back" and "Next" buttons.

IP Address / FQDN	Port	Transport
192.168.168.71	5060	UDP

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). The **Heartbeat** tab is kept at default so that the OPTIONS message sent from Session Manager to Avaya SBCE will be forwarded to Group of Gold Line to check the integrity of the SIP trunk.

On the **Advanced** tab, select *Service Provider* from the **Interworking Profile** drop down menu. Under **Signaling Manipulation Script**, select the *Contact Header* script created in **Section 7.7**. Click **Finish**.



Edit Server Configuration Profile - Advanced X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Service Provider ▼
Signaling Manipulation Script	Contact Header ▼
Connection Type	SUBID ▼
Securable	<input type="checkbox"/>

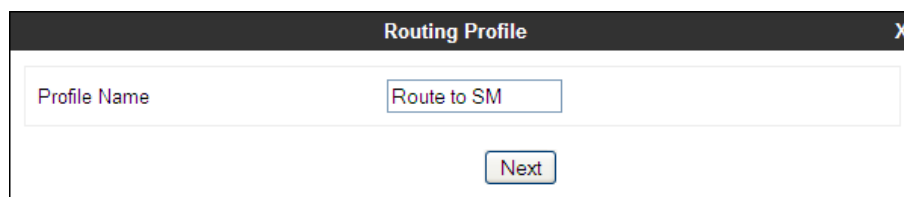
Finish

7.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the Group of Gold Line SIP trunk.

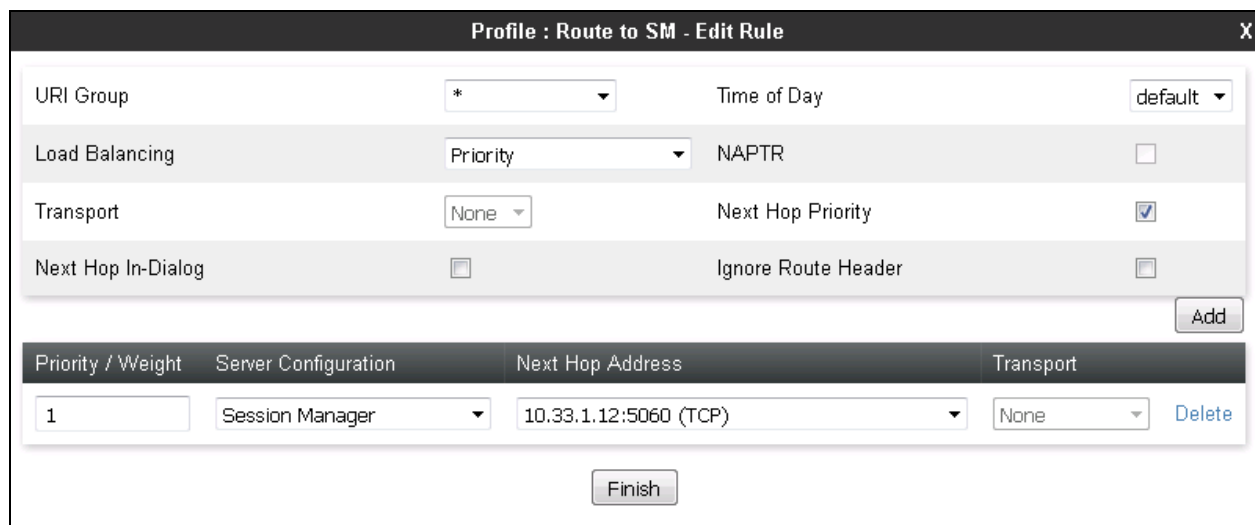
7.9.1. Routing Profile – Enterprise

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



The image shows a dialog box titled "Routing 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 "Route to SM". Below the input field is a "Next" button.

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



The image shows a dialog box titled "Profile : Route to SM - Edit Rule" with a close button (X) in the top right corner. The dialog contains several configuration fields:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐

Below these fields is an "Add" button. Underneath is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, and Transport.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manager	10.33.1.12:5060 (TCP)	None

At the bottom of the table is a "Delete" link. Below the table is a "Finish" button.

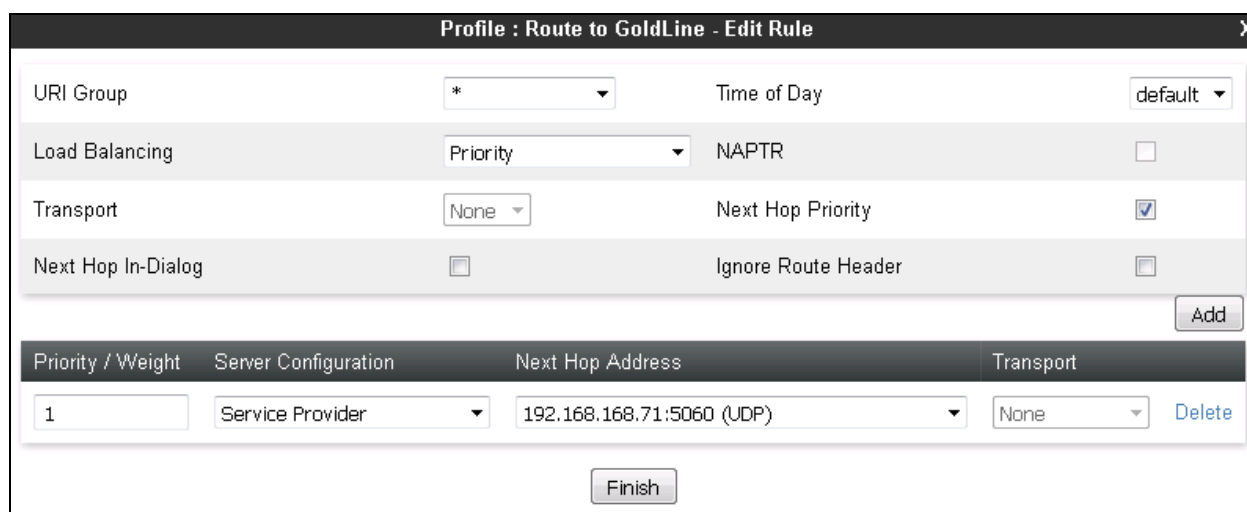
7.9.2. Routing Profile – Service Provider

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



The image shows a dialog box titled "Routing 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 "Route to GoldLine". Below this field is a button labeled "Next".

On the **Routing Profile** tab, click the **Add** button to enter the next-hop address. Enter **1** under **Priority/Weight**. Under **Server Configuration**, select **Service Provider**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Service Provider Server Configuration Profile in **Section 7.8.2**. Defaults were used for all other parameters. Click **Finish**.



The image shows a dialog box titled "Profile : Route to GoldLine - Edit Rule" with a close button (X) in the top right corner. The dialog contains several configuration fields and a table.

Configuration fields:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR: ☐
- Transport: None
- Next Hop Priority: ☒
- Next Hop In-Dialog: ☐
- Ignore Route Header: ☐

Buttons: Add, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Service Provider	192.168.168.71:5060 (UDP)	None	Delete

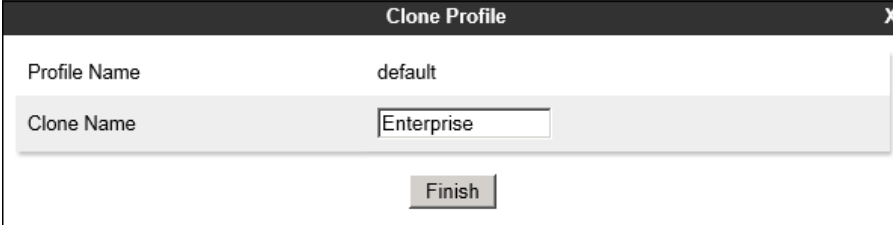
7.10. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

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

7.10.1. Topology Hiding Profile – Enterprise

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



Clone Profile	
Profile Name	default
Clone Name	Enterprise
<div>Finish</div>	

On the newly cloned *Enterprise* profile screen, click the **Edit** button (not shown).

For the **To**, **From** and the **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **bvwddev.com**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**. Default values were used for all other fields. Click **Finish**.

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

Finish

7.10.2. Topology Hiding Profile – Service Provider

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

Topology Hiding Profiles: Service Provider

Add Rename Clone Delete

Click here to add a description

Topology Hiding

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

Edit

7.11. End Point Policy Groups

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

7.11.1. End Point Policy Group – Enterprise

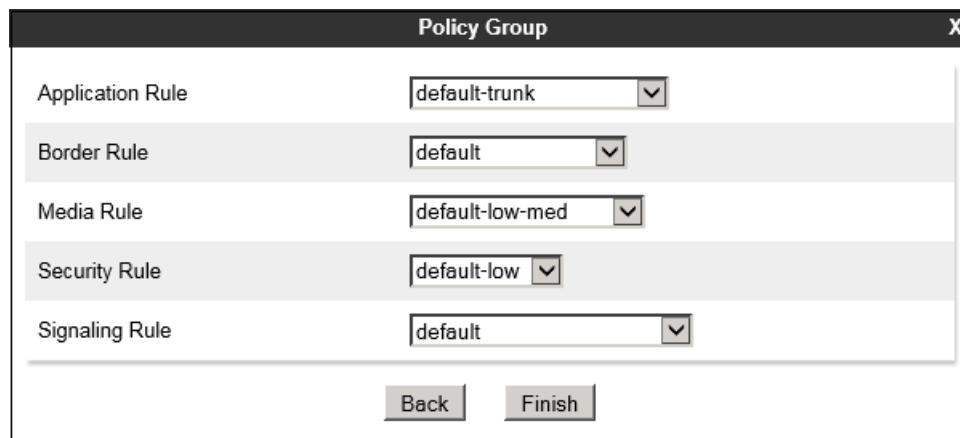
To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

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



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a label "Group Name" followed by a text input field containing the word "Enterprise". Below the input field is a "Next" button.

In the Policy Group tab, all fields used one of the default sets of rules already pre-defined in the configuration. Click **Finish**.



The screenshot shows the "Policy Group" dialog box with several dropdown menus. The "Application Rule" is set to "default-trunk", "Border Rule" is set to "default", "Media Rule" is set to "default-low-med", "Security Rule" is set to "default-low", and "Signaling Rule" is set to "default". At the bottom of the dialog are "Back" and "Finish" buttons.

7.11.2. End Point Policy Group – Service Provider

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

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

Policy Groups: Service Provider

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

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

Summary

7.12. End Point Flows

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

7.12.1. End Point Flow – Enterprise

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

Edit Flow: Session Manager Flow	
Flow Name	Session Manager Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Outside_Signaling2
Signaling Interface	Inside_Signaling2
Media Interface	Inside_Media2
End Point Policy Group	Enterprise
Routing Profile	Route to GoldLine
Topology Hiding Profile	Enterprise
Signaling Manipulation Script	None
Remote Branch Office	Any
Finish	

7.12.2. End Point Flow – Service Provider

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

Edit Flow: Service Provider FlowX

Flow Name	Service Provider Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Inside_Signaling2
Signaling Interface	Outside_Signaling2
Media Interface	Outside_Media2
End Point Policy Group	Service Provider
Routing Profile	Route to SM
Topology Hiding Profile	Service Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

8. Group of Gold Line SIP Trunking Configuration

Group of Gold Line is responsible for the configuration of the Group of Gold Line SIP Trunking service. The customer will need to provide the IP address used to reach the Avaya SBCE at the enterprise. Group of Gold Line will provide the customer the necessary information to configure the SIP trunk connection from the enterprise site to the network, including:

- IP address of the Group of Gold Line SIP Proxy server.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

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

9. Verification and Troubleshooting

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

9.1. General Verification Steps

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

9.2. Communication Manager Verification

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

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

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (*Session Manager* in the example below).

The screenshot shows the 'SIP Entity Link Monitoring Status Summary' page. The left sidebar contains a navigation menu with 'Session Manager' selected. The main content area has a breadcrumb trail: 'Home / Elements / Session Manager / System Status / SIP Entity Monitoring'. Below the title, there is a description: 'This page provides a summary of Session Manager SIP entity link monitoring status.' A 'Run Monitor' button is present. The main table, titled 'SIP Entities Status for All Monitoring Session Manager Instances', shows 1 item. The table has columns for 'Session Manager', 'Type', and 'Monitored Entities' (which includes 'Down', 'Partially Up', 'Up', 'Not Monitored', 'Deny', and 'Total'). The single row shows 'ASM70' as the Session Manager, 'Core' as the Type, and counts of 3 Down, 0 Partially Up, 9 Up, 0 Not Monitored, 0 Deny, and a Total of 12. A 'Filter: Enable' button is in the top right of the table area. At the bottom, there is a 'Select: All, None' option.

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

The screenshot shows the 'Session Manager Entity Link Connection Status' page. The left sidebar is the same as the previous screenshot. The main content area has a breadcrumb trail: 'Home / Elements / Session Manager / System Status / SIP Entity Monitoring'. Below the title, there is a description: 'This page displays detailed connection status for all entity links from a Session Manager.' A 'Summary View' button is present. The main table, titled 'All Entity Links for Session Manager: ASM70', shows 12 items. The table has columns for 'SIP Entity Name', 'SIP Entity Resolved IP', 'Port', 'Proto.', 'Deny', 'Conn. Status', 'Reason Code', and 'Link Status'. The table lists several entities, including 'IPQYM', 'ACM-Trunk3-Public', 'DevCM63', 'Interop-AAM63', 'ACM-Trunk1-Private', 'SBCE70', and 'Avaya SBCE70'. The 'Conn. Status' and 'Link Status' columns for all listed entities are 'UP'. A 'Filter: Enable' button is in the top right of the table area. At the bottom, there is a pagination control showing 'Page 1 of 2'.

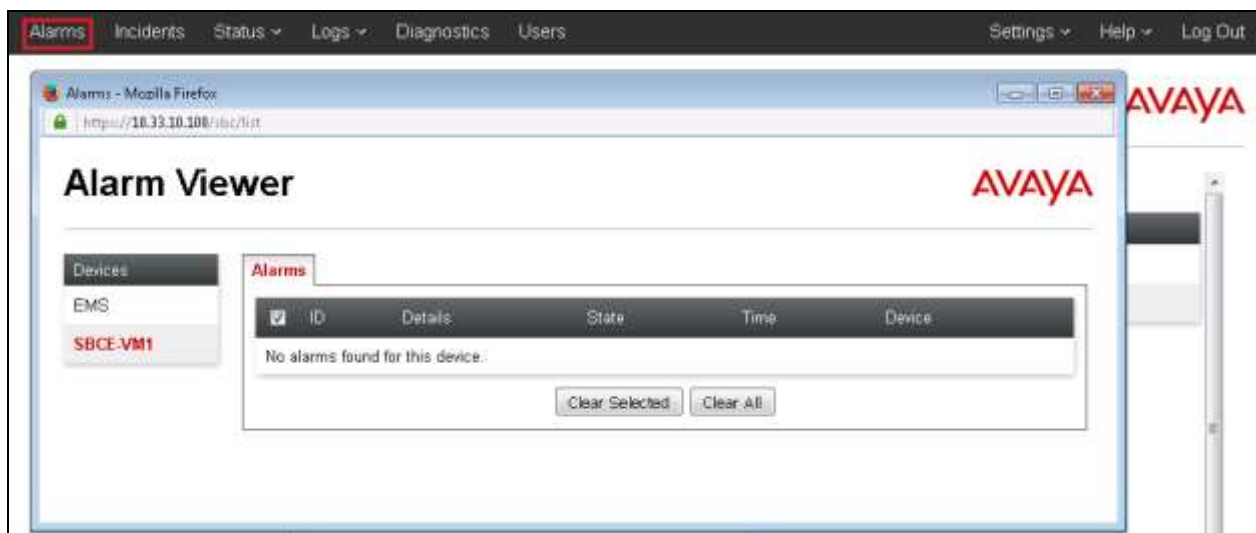
Other Session Manager useful verification and troubleshooting tools include:

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

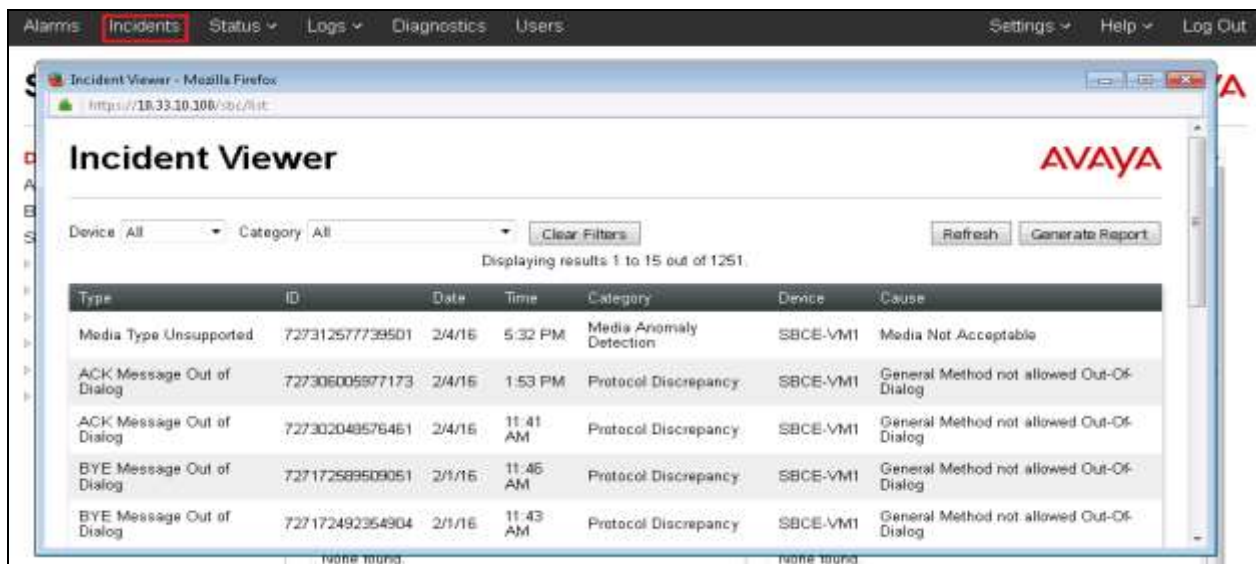
9.4. Avaya SBCE Verification

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

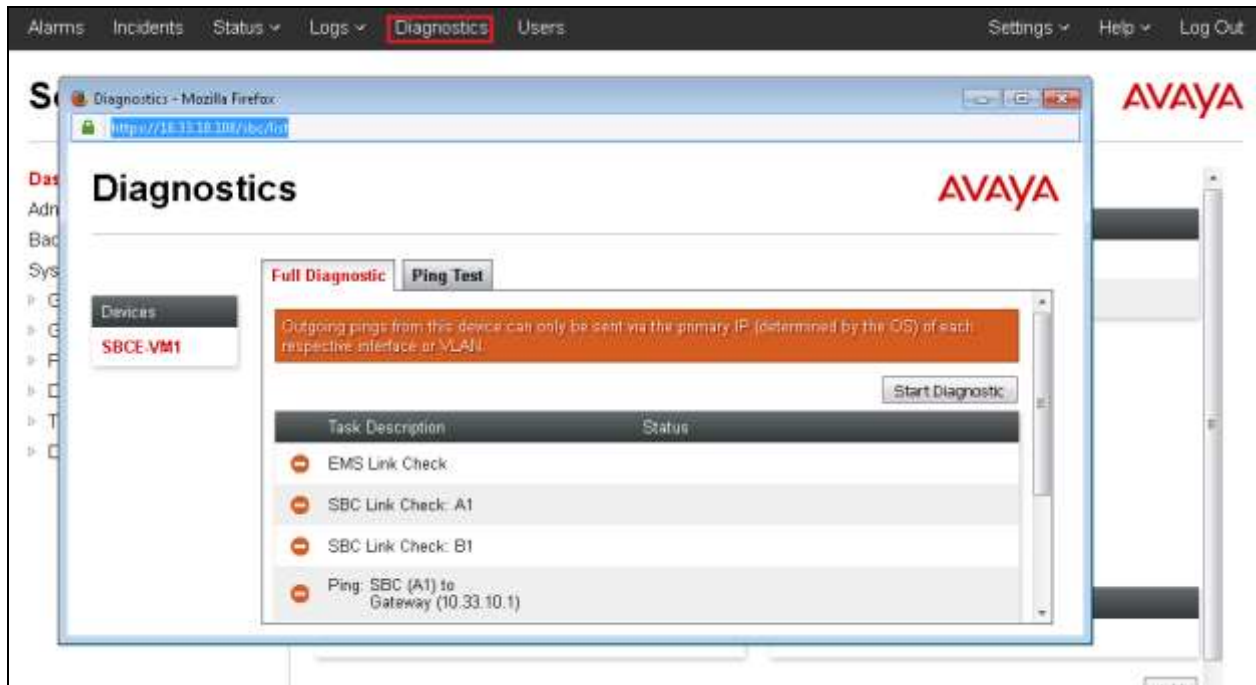
Alarms: This screen provides information about the health of the SBC.



Incidents : This screen provides detailed reports of anomalies, errors, policies violations, etc.



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



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

The screenshot shows the Avaya SBCE web interface. The left sidebar contains a navigation menu with categories like Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, the Troubleshooting section is expanded, and the Trace option is selected. The main content area is titled 'Trace: VM_SBCE' and has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section includes fields for Status (Ready), Interface (Any), Local Address (All), Remote Address (IP Port), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). There are 'Start Capture' and 'Clear' buttons at the bottom.

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.

Packet Capture		
Captures		
Last Modified	Descending	Sort Reset Refresh
File Name	File Size (bytes)	Last Modified
test_20150925183130.pcap	233,472	September 25, 2015 6:31:54 PM EDT Delete

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0, to connect to Group of Gold Line SIP Trunk Services, as shown in **Figure 1**.

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

11. References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 7.0, August 2015, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, August 2015, Document Number 555-245-205.
- [3] *Administering Avaya Aura® Session Manager*, Release 7.0, August 2015.
- [4] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [5] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015.
- [6] *Implementing and Administering Avaya Aura® Media Server*. Release 7.7. August 2015.
- [7] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*. White Paper. August 2015.
- [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/>

12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE, on **Section 7.7**.

```
//Remove gsid and epv parameters in outbound Contact header
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

©2016 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.