



Avaya Solution & Interoperability Test Lab

Application Notes for AT&T SIP Trunking Service with Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Aura® Communication Manager Release 7.0 and Avaya Aura® Session Manager 7.0 with SIP Trunks to the Avaya Session Border Controller for Enterprise 7.0 (Avaya SBCE) when used to connect the AT&T SIP Trunking Service available from AT&T (Australia).

AT&T SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the AT&T 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 any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

AT&T is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1	Interoperability Compliance Testing.....	4
2.2	Test Results	5
2.3	Support	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager	9
5.1	System-Parameters Customer-Options	9
5.2	System-Parameters Features	10
5.3	Dial Plan	11
5.4	IP Node Names.....	12
5.5	IP Interface for Procr.....	12
5.6	IP Network Regions	13
5.7	IP Codec Parameters	15
5.8	SIP Trunks.....	16
5.8.1	Signaling Group	16
5.8.2	Trunk Group.....	17
5.9	Calling Party Information.....	20
5.10	Incoming Call Handling Treatment	20
5.11	Outbound Routing	21
5.12	Avaya G430 Media Gateway Provisioning	23
5.13	Avaya Aura® Media Server Provisioning.....	24
5.13.1	Signaling Group for Media Server.....	24
5.13.2	Adding Media Server.....	25
5.14	Save Communication Manager Translations.....	25
6.	Configure Avaya Aura® Session Manager	26
6.1	Configure SIP Domain	27
6.2	Configure Locations	27
6.3	Configure SIP Entities.....	27
6.3.1	Configure Session Manager SIP Entity	28
6.3.2	Configure Communication Manager SIP Entity	28
6.3.3	Configure Avaya SBCE SIP Entity	30
6.4	Configure Entity Links.....	30
6.4.1	Configure Entity Link to Communication Manager.....	31
6.4.2	Configure Entity Link for Avaya SBCE.....	32
6.5	Configure Routing Policies	32
6.5.1	Configure Routing Policy for Communication Manager.....	32
6.5.2	Configure Routing Policy for Avaya SBCE	33
6.6	Configure Dial Patterns	33

7.	Configure Avaya Session Border Controller for Enterprise	37
7.1	System Management – Status	38
7.2	Global Profiles.....	39
7.2.1	Uniform Resource Identifier (URI) Groups.....	39
7.2.2	Server Interworking – Session Manager	40
7.2.3	Server Interworking – AT&T	43
7.2.4	Server Configuration – Session Manager	45
7.2.5	Server Configuration – AT&T.....	47
7.2.6	Routing – To Session Manager	49
7.2.7	Routing – To AT&T	50
7.2.8	Topology Hiding – Session Manager	51
7.2.9	Topology Hiding – AT&T	51
7.2.10	Domain Policies	52
7.2.11	Application Rules.....	52
7.2.12	Border Rules	52
7.2.13	Media Rules	53
7.2.14	Signaling Rules	54
7.2.15	Endpoint Policy Groups.....	54
7.3	Device Specific Settings.....	54
7.3.1	Network Management.....	54
7.3.2	Media Interfaces.....	55
7.3.3	Signaling Interface	56
7.3.4	Endpoint Flows – For Session Manager	57
7.3.5	Endpoint Flows – For AT&T.....	58
8.	Verification Steps.....	59
8.1	Avaya Session Border Controller for Enterprise.....	59
8.2	Avaya Aura® Communication Manager	61
8.3	Avaya Aura® Session Manager Status	62
8.4	Telephony Services	63
9.	Conclusion	63
10.	Additional References.....	63

1. Introduction

These Application Notes illustrate a sample configuration Avaya Aura® Communication Manager Release 7.0 and Avaya Aura® Session Manager 7.0 with SIP Trunks to the Avaya Session Border Controller for Enterprise 7.0 (Avaya SBCE) when used to connect to the AT&T SIP Trunking Service available from AT&T (Australia).

Avaya Aura® Session Manager 7.0 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 7.0 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya SBCE 7.0 is the point of connection between Avaya Aura® Session Manager and the AT&T SIP Trunking Service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The SIP Trunking Service available from AT&T is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The AT&T SIP Trunking Service allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

2. General Test Approach and Test Results

The general test approach was to make calls through the Avaya SBCE while DoS policies are in place using various codec settings and exercising common and advanced PBX features.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising 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

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, the Avaya SBCE, and the AT&T SIP Trunking Service.

The compliance testing was based on the standard Avaya GSSCP test plan. The testing covered functionality required for compliance as a solution supported on the AT&T SIP Trunk network. Calls were made to and from the PSTN across the AT&T network. The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including H.323, SIP and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) and Avaya Communicator for Windows soft phones. Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested.
- Dialing plans including local, long distance, international, outbound toll-free, calls etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A, G.711MU and G.729A.
- Media and Early Media transmissions.
- Incoming and outgoing fax using T.38-standard.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.
- Network Call Redirection.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

2.2 Test Results

Interoperability testing of AT&T SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Inbound call** – It was observed that in the inbound call from PSTN phones to Avaya SIP IP phones, Avaya Aura® Session Manager responded back with SIP 500 “Server Internal Error” to the SIP INVITE message sent from AT&T Sip Trunk. This was found to be caused by low value of Max-forwards header value (i.e. 10) in the SIP INVITE message to Avaya SBCE. Resolution of the issue was done by AT&T Engineer by increasing the value of Max-forwards header of SIP message at AT&T’s Session Border Controller to 50.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.
- **AT&T Australia:** Customers should contact their AT&T Business representative or follow the support links available on <http://www.corp.att.com/ap/about/where/australia/>.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya Aura® Communication Manager running on VMware ESXi 5.5.
- Avaya Aura® Session Manager running on VMware ESXi 5.5.
- Avaya Aura® System Manager running on VMware ESXi 5.5.
- Avaya Aura® Messaging running on VMware ESXi 5.5.
- Avaya G430 Media Gateway.
- Avaya Aura® Media Server running on VMware ESXi 5.5. The Media Server can act as a media gateway Gxxx series in providing tones, announcements or music on hold.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running H.323/SIP software.
- Avaya one-X® Communicator 6.2.
- Avaya Communicator for Windows 2.1.
- The Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the AT&T SIP Trunking Service and the enterprise internal network.

All IP addresses shown in the diagram are private IP addresses.

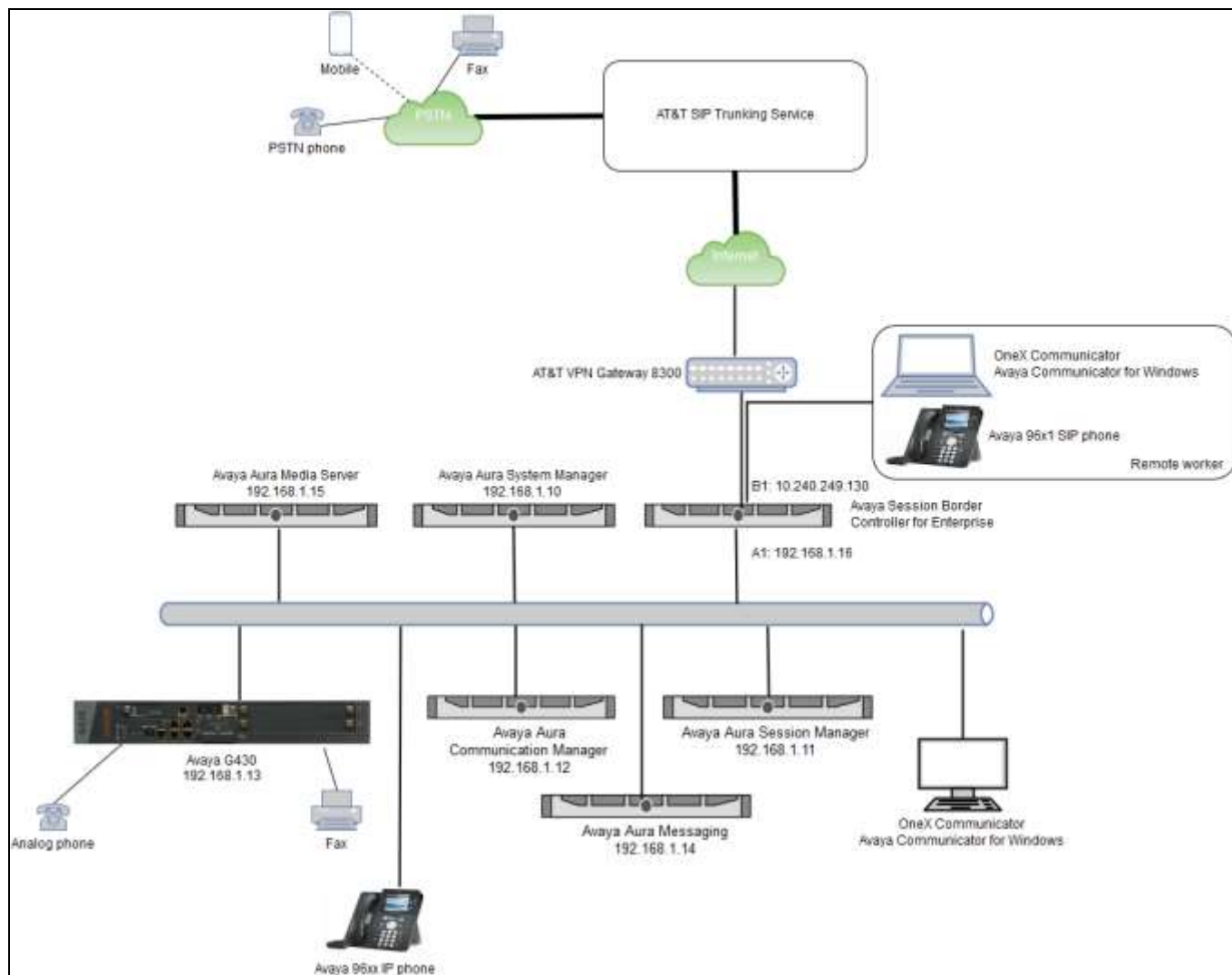


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura Communication Manager 7.0	7.0.0.3.1.441.22947
Avaya Aura Session Manager 7.0 SP2	7.0.0.2.700201
Avaya Aura System Manager 7.0 SP2	Build No. - 7.0.0.0.16266- 7.0.9.7002010 Software Update Revision No: 7.0.0.2.4416
Avaya Aura Messaging 6.3.3	6.3.3.0.11348
Avaya Session Border Controller for Enterprise 7.0	7.0.0-21-6602
Avaya Media Gateway G430	g430_sw_37_21_0
Avaya Aura Media Server 7.7	7.7.0.281
Avaya One-X Communicator 6.2	6.2.11.03
Avaya Communicator for Windows 2.1	2.1.3.80
Avaya One-X Agent H323 2.5.8	2.5.58020.0
Avaya 96x1 series – SIP phone	7.0.1.0.46
Avaya 96xx series – H.323 phone	6.6115
Service Provider	
AT&T SIP Trunking Service	Genband

5. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these Application Notes. Other parameter values may or may not match based on local configurations.

5.1 System-Parameters Customer-Options

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

NOTE - For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.

Follow the steps shown below:

1. Enter the **display system-parameters customer-options** command. On **Page 2** of the form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		0	0
Max Concur Registered Unauthenticated H.323 Stations:		0	0
Maximum Video Capable Stations:		41000	1
Maximum Video Capable IP Softphones:		1000	2
Maximum Administered SIP Trunks:		24000	70
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0

2. On **Page 6** of the form, verify that the **Private Networking** and **Processor Ethernet** fields are set to **y**.

display system-parameters customer-options	Page 6 of 12
OPTIONAL FEATURES	
Multinational Locations? n	Station and Trunk MSP? y
Multiple Level Precedence & Preemption? y	Station as Virtual Extension? y
Multiple Locations? n	
Personal Station Access (PSA)? y	System Management Data Transfer? n
PNC Duplication? n	Tenant Partitioning? y
Port Network Support? y	Terminal Trans. Init. (TTI)? y
Posted Messages? y	Time of Day Routing? y
	TN2501 VAL Maximum Capacity? y
Private Networking? y	Uniform Dialing Plan? y
Processor and System MSP? y	Usage Allocation Enhancements? y
Processor Ethernet? y	
	Wideband Switching? y
Remote Office? y	Wireless? n
Restrict Call Forward Off Net? y	
Secondary Data Module? y	

5.2 System-Parameters Features

Follow the steps shown below:

1. Enter the **display system-parameters features** command. On **Page 1** of the form, verify that the **Trunk-to-Trunk Transfer** is set to **all**.

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): 1	
Off-Premises Tone Detect Timeout Interval (seconds): 20	
AAR/ARS Dial Tone Required? y	
Music (or Silence) on Transferred Trunk Calls? no	
DID/Tie/ISDN/SIP Intercept Treatment: attendant	
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred	
Automatic Circuit Assurance (ACA) Enabled? n	
Abbreviated Dial Programming by Assigned Lists? n	
Auto Abbreviated/Delayed Transition Interval (rings): 2	
Protocol for Caller ID Analog Terminals: Bellcore	
Display Calling Number for Room to Room Caller ID Calls? n	

2. On **Page 9** verify that a text string has been defined to replace the **Calling Party Number (CPN)** for restricted or unavailable calls. 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
                                Identity When Bridging: principal
                                User Guidance Display? n
  Extension only label for Team button on 96xx H.323 terminals? n

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

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

5.3 Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

Follow the steps shown below:

- Enter the **change dialplan analysis** command to provision the following dial plan.
 - 4-digit extensions with a **Call Type** of **ext** beginning with **847** (which is a subset of DID numbers (028059847x) assigned by AT&T).
 - 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code * for SIP Trunk Access Codes (TAC).

display dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
6	1	fac						
847	4	ext						
9	1	fac						
*	3	dac						
#	4	fac						

5.4 IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used. Note that the Communication Manager procr name and IP address are entered during installation. The procr IP address was used to define the Communication Manager SIP Entities in **Section 6.3.2**.

Follow the steps shown below:

- Enter the **change node-names ip** command, and add node names and IP addresses for the following:
 - Session Manager SIP signaling interface (e.g., **ve3-sm** and **192.168.1.11**).
 - Media Server (e.g., **ve4-ams** and **192.168.1.15**).

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
ve3-sm	192.168.1.11	
ve4-ams	192.168.1.15	
default	0.0.0.0	
procr	192.168.1.12	
procr6	::	

5.5 IP Interface for Procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters defined during installation.

- Verify that **Enable Interface?** , **Allow H.323 Endpoints?** , and **Allow H248 Gateways?** fields are set to **y**.
- In the reference configuration the procr is assigned to **Network Region: 1**.
- The default values are used for the remaining parameters.

display ip-interface pro		Page 1 of 2
		IP INTERFACES
Type: PROCR		Target socket load: 19660
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
		IPV4 PARAMETERS
Node Name: procr	IP Address: 192.168.1.12	

5.6 IP Network Regions

For the compliance testing, ip-network-region 1 was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is **sipinterop.net**. This domain name appears in the “From” header of SIP message originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to **yes**. Shuffling can be further restricted at the trunk level under the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.7**.
- Default values can be used for all other fields.

```
display ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1              Authoritative Domain: sipinterop.net
Name: 123ER              Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
Codec Set: 1                Inter-region IP-IP Direct Audio: yes
UDP Port Min: 16384                IP Audio Hairpinning? n
UDP Port Max: 53999
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 34
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS                AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y                RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
Subnet Mask: /24
```

On **Page 4**, define the IP codec set to be used for traffic in region 1. In the compliance testing, Communication Manager, the Avaya G430 Media Gateway, IP/SIP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields.

display ip-network-region 1										Page	4 of	20
Source Region: 1 Inter Network Region Connection Management										I	A	M
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c	G	A	t
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e		
1	1								all			
2								n				t
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												

Non-IP telephones (e.g., analog, digital) derive their network region from the IP interface of the Avaya G430 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

display ip-interface procr										Page	1 of	2
IP INTERFACES												
Type: PROCR										Target socket load: 19660		
Enable Interface? y										Allow H.323 Endpoints? y		
Network Region: 1										Allow H.248 Gateways? y		
										Gatekeeper Priority: 5		
										IPV4 PARAMETERS		
Node Name: procr										IP Address: 192.168.1.12		
Subnet Mask: /24												

To define network region 1 for the Avaya G430 Media Gateway, use **change media-gateway** command as shown in the following screen.

change media-gateway 1		Page	1 of	2
MEDIA GATEWAY 1				
Type:	g430			
Name:	g430			
Serial No:	10IS2xxxxxxx			
Link Encryption Type:	any-ptls/tls	Enable CF?	n	
Network Region:	1	Location:	1	
		Site Data:	1	
Recovery Rule:	none			
Registered?	y			
FW Version/HW Vintage:	37 .21 .0 /1			
MGP IPV4 Address:	192.168.1.13			
MGP IPV6 Address:				
Controller IP Address:	192.168.1.12			
MAC Address:	00:1b:4f:3f:14:48			
Mutual Authentication?	optional			

5.7 IP Codec Parameters

Follow the steps shown below:

1. Enter the **change ip-codec-set x** command, where **x** is the number of the IP codec set specified in **Section 5.6**. On **Page 1** of the **ip-codec-set** form, ensure that **G.711A**, **G.711MU** and **G.729A** are included in the codec list. Note that the packet interval size will default to 20ms.

change ip-codec-set 1		Page	1 of	2
IP CODEC SET				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711A	n	2	20	
2: G.711MU	n	2	20	
3: G.729A	n	2	20	
4:				
5:				
6:				
7:				
Media Encryption		Encrypted SRTCP: enforce-unenc-srtcp		
1: none				
2:				
3:				
4:				
5:				

- On **Page 2** of the ip-codec-set form, set **FAX Mode** to **t.38-standard**.

change ip-codec-set 1		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia: 15360:Kbits			
Maximum Call Rate for Priority Direct-IP Multimedia: 15360:Kbits			
	Mode	Redundancy	Packet Size (ms)
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

5.8 SIP Trunks

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group.

5.8.1 Signaling Group

This section describes the steps for administering the SIP trunk to Session Manager. This trunk corresponds to the **ve3-cm** SIP Entity defined in **Section 6.3.2**.

Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **3**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **IP Video?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **ve3-sm**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6**.
- **Far-end Domain** – Enter **sipinterop.net**. This is the domain provisioned for Session Manager in **Section 6.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).

- **Initial IP-IP Direct Media** – Set to y.
- **Enable Layer 3 Test** – Set to y. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- Default values may be used for all other fields.

display signaling-group 3		Page 1 of 3
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: ve3-sm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: sipinterop.net		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? y	
	Alternate Route Timer(sec): 30	

5.8.2 Trunk Group

Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 3). On **Page 1** of the **trunk-group** form, provision the following:

- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***03**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **5.8.1** (e.g., 3).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

display trunk-group 3		Page 1 of 22
TRUNK GROUP		
Group Number: 3	Group Type: sip	CDR Reports: y
Group Name: TO-SM	COR: 1	TN: 1
Direction: two-way	TAC: *03	
Dial Access? n	Outgoing Display? y	Night Service:
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 3	
	Number of Members: 10	

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

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.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
display trunk-group 3                                     Page      3 of   22
TRUNK FEATURES
    ACA Assignment? n                                   Measured: none
                                                    Maintenance Tests? y

Suppress # Outpulsing? n  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 5**, the **Network Call Redirection** field may be set to **n** or **y**, both approaches are supported in this solution. Setting the **Network Call Redirection** flag to **y** enables the use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These header modifications are needed to support the call display for call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Setting **n** for **Network Call Redirection**:

add trunk-group 3	Page 5 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
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? y	
Enable Q-SIP? n	

Setting **y** for **Network Call Redirection**:

add trunk-group 3	Page 5 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
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? y	
Enable Q-SIP? n	

5.9 Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, the 028059847x DID numbers provided for testing were assigned to the extensions 847x. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

display public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
4	847	3	028059	Len	
				10	Total Administered: 1
					Maximum Entries: 9999
Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.					
Communication Manager automatically inserts a '+' digit in this case.					

Repeat the same in private-numbering table:

display private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	847	3	028059	10	Total Administered: 1
					Maximum Entries: 540

5.10 Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by AT&T can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 3					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	10	028059	6		
public-ntwrk					

5.11 Outbound Routing

In these Application Notes, the **Automatic Route Selection (ARS)** feature is used to route an outbound call via the SIP trunk to the service provider. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown below.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
6	1	fac						
847	4	ext						
9	1	fac						
*	3	dac						
#	4	fac						

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

display feature-access-codes				Page 1 of 11	
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:			
Answer Back		Access Code:			
Attendant		Access Code:			
Auto Alternate Routing (AAR)		Access Code:			
Auto Route Selection (ARS) - Access Code 1: 9				Access Code 2: 6	
Automatic Callback Activation:		#002		Deactivation: #003	
Call Forwarding Activation Busy/DA:		#004 All: #005		Deactivation: #006	
Call Forwarding Enhanced Status:		#007 Act: #008		Deactivation: #009	
Call Park		Access Code: #010			
Call Pickup		Access Code: #011			
CAS Remote Hold/Answer Hold-Unhold		Access Code: #012			
CDR Account Code		Access Code: #013			
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 testing. All dialed strings are mapped to route pattern **3** for an outbound call which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
02		10	10	3	pubu		n
04		10	10	3	pubu		n
0011		12	20	3	pubu		n
000		3	3	3	emer		n

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for **route pattern 3** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **3** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** **unk-unk**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.9**.

```

change route-pattern 3
Pattern Number: 1      Pattern Name: sip
  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
2:
3:
4:
5:
6:

                                n      user
                                n      user
                                n      user
                                n      user
                                n      user
                                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
2: y y y y y n  n      rest      none
3: y y y y y n  n      rest      none
4: y y y y y n  n      rest      none
5: y y y y y n  n      rest      none
6: y y y y y n  n      rest      none

```

5.12 Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateways is provisioned. The G430 is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below.

1. SSH to the G430 (not shown). Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., **g430-???(*super*)#**).
2. Enter the **show system** command and note the G430 serial number (e.g., **10IS2xxxxxxx**).
3. Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **192.168.1.12**).
4. Enter the **copy run copy start command** to save the G430 configuration.
5. On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown).

Enter the following parameters:

- Set **Type = G430**.
- Set **Name** = Enter a descriptive name (e.g., **g430**).
- Set **Serial Number** = Enter the serial number copied from **Step 2** (e.g., **10IS2xxxxxxx**).
- Set the **Encrypt Link** parameter as desired (**n** was used in the reference configuration).
- Set **Network Region = 1**.

When the Media Gateway registers, the SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., **g430-001(*super*)#**).

6. Enter the **display media-gateway 1** command, and verify that the G430 has registered.

```
display media-gateway 1                                     Page 1 of 2
MEDIA GATEWAY 1

      Type: g430
      Name: g430
      Serial No: 10IS2xxxxxxx
Link Encryption Type: any-ptls/tls      Enable CF? n
      Network Region: 1                  Location: 1
                                          Site Data: 1

      Recovery Rule: none

      Registered? y
FW Version/HW Vintage: 37 .21 .0 /1
      MGP IPV4 Address: 192.168.1.12
      MGP IPV6 Address:
Controller IP Address: 192.168.1.13
      MAC Address: 00:1b:4f:3f:14:48

Mutual Authentication? optional
```

5.13 Avaya Aura® Media Server Provisioning

Starting from release 7.0 of Avaya Aura®, Media Server can be used as VOIP resources for tones, announcements and music on hold in conjunction with Avaya Aura® Communication Manager.

5.13.1 Signaling Group for Media Server

This section describes the steps for administering the SIP connection to Media Server.

Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **1**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **Peer Detection Enabled?** is set to **n**. Set the **Peer Server** to **AMS**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of the Media Server as administered in **Section 5.4** (e.g., **ve4-ams**).
- **Near-end Listen Port** – Set to **5061**.
- **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set to **1**.

```
add signaling-group 1                                     Page 1 of 2
                                     SIGNALING GROUP
Group Number: 1                Group Type: sip
                               Transport Method: tls
Peer Detection Enabled? n    Peer Server: AMS
Near-end Node Name: procr      Far-end Node Name: ve4-ams
Near-end Listen Port: 5061     Far-end Listen Port: 5061
                               Far-end Network Region: 1
Far-end Domain: 192.168.1.15
```


5.13.2 Adding Media Server

Enter the **add media-server x** command, where **x** is the number of an unused media server (e.g., **1**), and provision the following:

- **Signaling Group** – Set to signaling group administered in **Section 5.13.1** (e.g., **1**).
- **Voip Channel License Limit** – Set to **10**.
- **Dedicated Voip Channel Licenses** – Set to **10**.
- **Network Region** – Set to the network region administered in **Section 5.6** (e.g., **1**).

add media-server 1		Page 1 of 1
MEDIA SERVER		
Media Server ID: 1		
Signaling Group: 1		
Voip Channel License Limit: 10		
Dedicated Voip Channel Licenses: 10		
Node Name: ve4-ams		
Network Region: 1		
Location: 1		
Announcement Storage Area: ANNC-638363a6-f0d7-41e5-913d-000c29d72adf		

5.14 Save Communication Manager Translations

After the Communication Manager provisioning is completed, enter the command **save translation**.

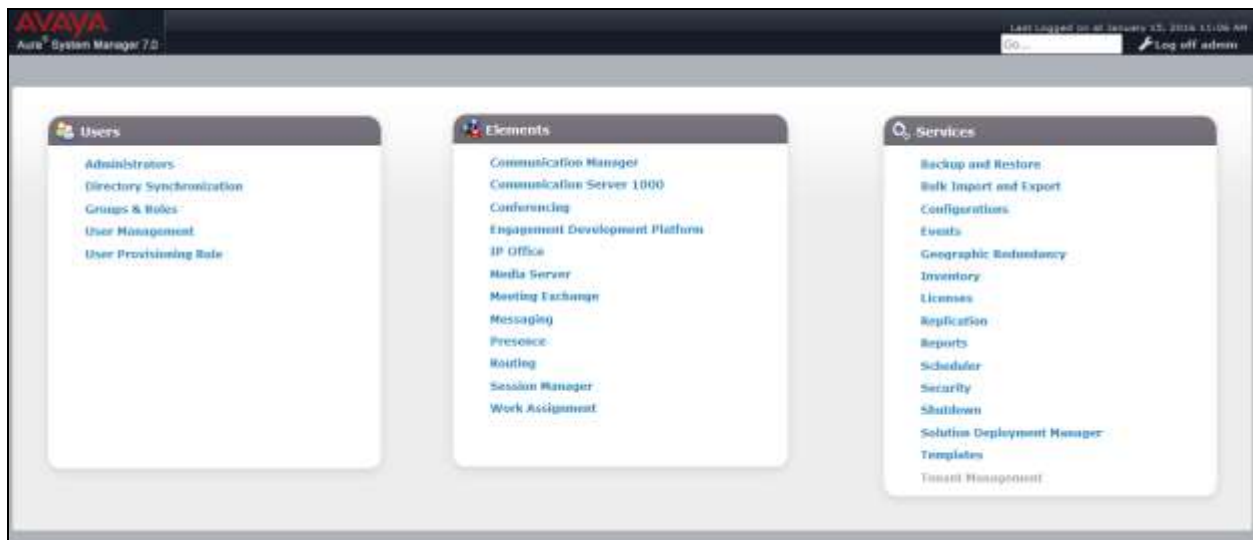
6. Configure Avaya Aura® Session Manager

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

- SIP domain.
- Logical/physical Location that can be used by SIP Entities.
- 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.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

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

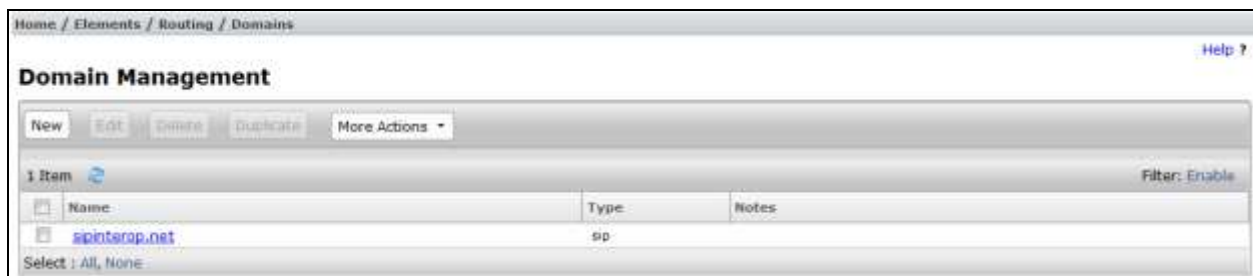
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



6.1 Configure SIP Domain

Follow the steps shown below:

1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.net** was defined.
2. Click **New** (not shown). Enter the following values and use default values for remaining fields.
 - **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **sipinterop.net** is shown.
 - **Type:** Verify **sip** is selected.
 - **Notes:** Add a brief description.
3. Click **Commit** to save (not shown).

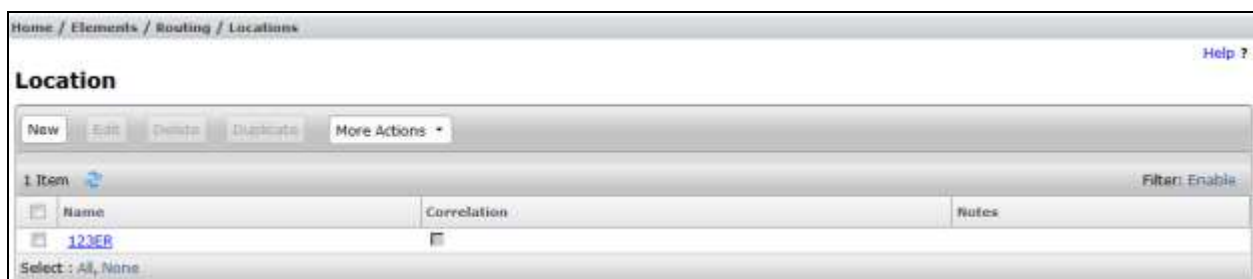


6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **123ER** is configured.

Follow the steps shown below:

1. Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.
 - **Name:** Enter a descriptive name for the Location (e.g., **123ER**).
 - **Notes:** Add a brief description.
2. Click **Commit** to save.



6.3 Configure 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 Avaya SBCE.

6.3.1 Configure Session Manager SIP Entity

Follow the steps shown below

1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g., **ve3-sm**).
 - **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (not the management interface), provisioned during installation (e.g., **192.168.1.11**).
 - **Type** – Verify **Session Manager** is selected.
 - **Location** – Select location **123ER**.
 - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
 - **Time Zone** – Select the time zone in which Session Manager resides.
3. In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
 - Use the default values for the remaining parameters.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

6.3.2 Configure Communication Manager SIP Entity

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g. **ve3-cm**).

- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) (e.g. **192.168.1.12**).
- **Type** – Select **CM**.
- **Location** – Select a Location **123ER** administered in **Section 6.2**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.

3. Click on **Commit**.

SIP Entity Details

General

*** Name:**

*** FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Credential name:

Securable: ☐

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

SIP Link Monitoring

SIP Link Monitoring:

6.3.3 Configure Avaya SBCE SIP Entity

Repeat the steps in **Section 6.3.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **sbce_A1**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **192.168.1.16**).
- **Type** – Verify **SIP Trunk** is selected.
- **Location** – Select location **123ER** (**Section 6.2**).

SIP Entity Details

CommitCancel

General

* Name: sbce_A1

* FQDN or IP Address: 192.168.1.16

Type: SIP Trunk

Notes:

Adaptation:

Location: 123ER

Time Zone: Australia/Sydney

* 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

6.4 Configure Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and another one for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click 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 defined in **Section 6.3.1**.
- **Protocol:** Select the transport protocol used for this link, **TLS** for the Entity Link to Communication Manager and **TLS** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.3.2**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section 6.3.3**
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.4.1 Configure Entity Link to Communication Manager

Follow the steps shown below:

1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name (or have it created automatically) for this link to Communication Manager (e.g., **ve3-sm_ve3-cm_5061_TLS**).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.3.1** for Session Manager (e.g., **ve3-sm**).
 - **SIP Entity 1 Port** – Enter **5061**.
 - **Protocol** – Select **TLS**.
 - **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.2** for the Communication Manager internal entity (e.g., **ve3-cm**).
 - **SIP Entity 2 Port** - Enter **5061**.
 - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.

The screenshot shows a web-based configuration interface for 'Entity Links'. At the top, it says '1 Item' and 'Filter: Enable'. Below is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The table contains one row with the following values: Name: 've3-sm_ve3-cm_5061_tls', SIP Entity 1: 've3-sm', Protocol: 'TLS', Port: '5061', SIP Entity 2: 've3-cm', DNS Override: (unchecked), Port: '5061', and Connection Policy: 'trusted'. Below the table, there is a 'Select: All, None' dropdown and 'Commit' and 'Cancel' buttons at the bottom right.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* ve3-sm_ve3-cm_5061_tls	* ve3-sm	TLS	* 5061	* ve3-cm	<input type="checkbox"/>	* 5061	trusted

Select: All, None

Commit Cancel

6.4.2 Configure Entity Link for Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.4.1**, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., **ve3-sm_sbce_A1_5061_TLS**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.3** for the Avaya SBCE entity (e.g., **sbce_A1**).

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	BRS Override	Port	Connect Policy
* ve3-sm_sbce_A1_5061_	* Q:ve3-sm	TLS	* 5061	* Q:sbce_A1	<input type="checkbox"/>	* 5061	trusted

Select: All, None

Commit Cancel

6.5 Configure Routing Policies

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

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

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

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

6.5.1 Configure Routing Policy for Communication Manager

This Routing Policy is used for inbound calls from AT&T.

1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **ve3-cm**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
4. In the **SIP Entity List** page, select the SIP Entity administered in **Section 6.3.2** for the Communication Manager SIP Entity (**ve3-cm**), and click on **Select**.

- Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.
- No **Regular Expressions** were used in the reference configuration.
- Click on **Commit**.

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ve3-cm	192.168.1.12	CM	

6.5.2 Configure Routing Policy for Avaya SBCE

This Routing Policy is used for outbound calls to the service provider. Repeat the steps in **Section 6.5.1**, with the following changes:

- Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sbce**).
- SIP Entity List** – Select the SIP Entity administered in **Section 6.3.3** for the Avaya SBCE entity (e.g., **sbce_A1**).

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sbce_A1	192.168.1.16	SIP Trunk	

6.6 Configure Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to AT&T and vice versa. Dial Patterns define which routing 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 **New** button in the right pane (not shown).

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.
- **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.

Three examples of the dial patterns used for the compliance testing were shown below, one for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise and another one for Avaya SIP extension.

The first example shows that 10-digit dialed numbers that has a destination domain of “sipinterop.net” uses route policy to Avaya SBCE as defined in **Section 6.5.2**.

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: 02

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: sipinterop.net

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
123ER		sbce	0	<input type="checkbox"/>	sbce_A1	

Select : All, None

The second example shows that outbound 12-digit to 20-digit numbers that start with 0011 uses route policy to Avaya SBCE as defined in **Section 6.5.2** for PSTN International calls.

Dial Pattern Details Commit Cancel

General

* Pattern: 0011

* Min: 12

* Max: 20

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: sipinterop.net

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"/>	123ER		sbce	0	<input type="checkbox"/>	sbce_A1	

Select : All, None

The third example shows that 10-digit pattern that start with 028059 is used for inbound calls from AT&T to DID numbers on Avaya Aura® Communication Manager.

Dial Pattern Details Commit Cancel

General

* Pattern: 028059

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: sipinterop.net

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"/>	123ER		ve3-cm	0	<input type="checkbox"/>	ve3-cm	

Select : All, None

The fourth example shows that 000 dialed number is used for emergency service in Australia.

Dial Pattern Details

Commit

Cancel

General

* Pattern:

000

* Min:

3

* Max:

3

Emergency Call:

☒

* Emergency Priority:

1

* Emergency Type:

all

SIP Domain:

sipinterop.net

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"/>	123ER		sbce	0	<input type="checkbox"/>	sbce_A1	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

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

As described in Section 3, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (**192.168.1.16**), with access to the **123ER** location. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address **10.240.249.130**). The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

1. Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.

3. Enter the password and click on **Log In**.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

Dashboard

Information	
System Time	04:45:01 PM AEST 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	5

Installed Devices
EMS
asbce7

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
asbce7: No Subscriber Flow Matched
asbce7: No Subscriber Flow Matched
asbce7: No Subscriber Flow Matched
asbce7: No Subscriber Flow Matched
asbce7: No Subscriber Flow Matched

7.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.

System Management

Devices Updates SSL VPN Licensing

Device Name	Management IP	Version	Status	
asbce7	192.168.2.10	7.0.0-21-6602	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

2. Click on **View** (shown above) to display the **System Information** screen.

System Information: asbce7

X

General Configuration

Appliance Name

asbce7

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 100

100

Advanced Sessions

Requested: 100

100

Scopia Video Sessions

Requested: 100

100

CES Sessions

Requested: 10

10

Encryption

☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
192.168.1.16	192.168.1.16	255.255.255.0	192.168.1.1	A1
10.240.249.130	10.240.249.130	255.255.255.240	10.240.249.129	B1
10.240.249.131	10.240.249.131	255.255.255.240	10.240.249.129	B1

DNS Configuration

Primary DNS

135.10.209.250

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.240.249.130

Management IP(s)

IP

192.168.2.10

7.2 Global Profiles

7.2.1 Uniform Resource Identifier (URI) Groups

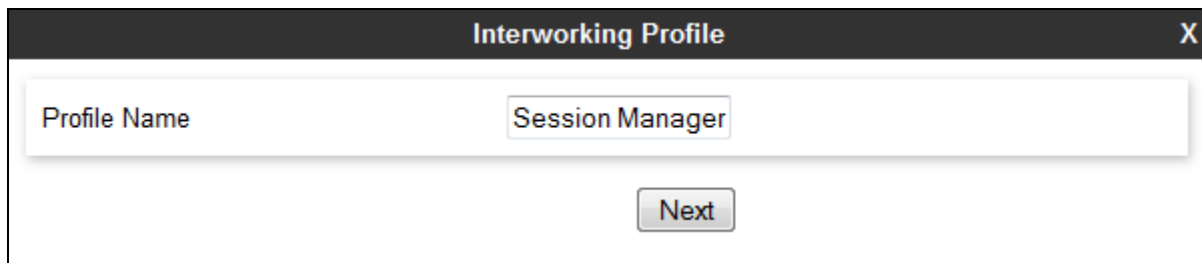
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.

7.2.2 Server Interworking – Session Manager

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to Session Manager.

1. Select **Global Profiles → Server Interworking** from the left-hand menu.
2. Click the **Add** button.
3. Enter profile name: (e.g., **Session Manager**), and click **Next**.



The screenshot shows a web-based configuration window titled "Interworking Profile". It features a close button (X) in the top right corner. The main content area contains a text input field with the label "Profile Name" and the text "Session Manager" entered. Below the input field is a "Next" button.

4. The **General** screen will open.
- Check **T38 Support**.
 - All other options can be left with default values, and click **Next**.

General	
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	<input type="text" value="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
<input type="button" value="Back"/> <input type="button" value="Next"/>	

5. On the **Timers** and **Privacy** windows, select **Next** to accept default values.
6. On the **Advanced** window, configure as below while other field left as default:
 - Record Routes: choose **None**.
 - Include End Point IP for Context Lookup: choose **Yes**.
 - Extension: choose **Avaya**.
 - Has Remote SBC: choose **Yes**.

The screenshot displays the 'Advanced' configuration window with the following settings:

- Record Routes:** Radio buttons for None (selected), Single Side, Both Sides, Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup:** Checkmark is checked.
- Extensions:** Dropdown menu set to 'Avaya'.
- Diversion Manipulation:** Checkmark is unchecked.
- Diversion Condition:** Dropdown menu set to 'None'.
- Diversion Header URI:** Empty text field.
- Has Remote SBC:** Checkmark is checked.
- Route Response on Via Port:** Checkmark is unchecked.
- DTMF:** Section header.
- DTMF Support:** Radio buttons for None (selected), SIP NOTIFY, and SIP INFO.

At the bottom, there are 'Back' and 'Finish' buttons.

7.2.3 Server Interworking – AT&T

Repeat the steps shown in **Section 7.2.2** to add an Interworking Profile for the connection to AT&T via the VPN network, with the following changes:

1. Click **Add** to add a new profile, enter **ATT** then click **Next** (not shown)
2. The **General** screen will open:
 - Check **T38 Support**.
 - All other options can be left as default.
 - Click **Next**.
 - The **Timers** then **Privacy** screens will open (not shown), accept default values for all the screens by clicking **Next**.

General	
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
<div>Back Next</div>	

Advanced window is configured as below, click **Finish** to save the profile:

- **Record Routes:** choose **None**
- **Extensions:** choose **Nortel**
- Check **Has Remote SBC**

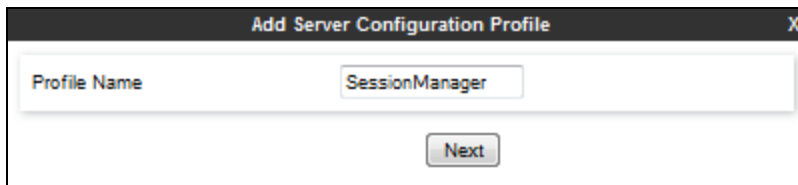
The screenshot shows a window titled "Editing Profile: ATT" with a close button (X) in the top right corner. The window contains several configuration sections:

- Record Routes:** A group box containing five radio buttons: "None" (selected), "Single Side", "Both Sides", "Dialog-Initiate Only (Single Side)", and "Dialog-Initiate Only (Both Sides)".
- Include End Point IP for Context Lookup:** A checkbox that is currently unchecked.
- Extensions:** A dropdown menu showing "Nortel".
- Diversion Manipulation:** A checkbox that is currently unchecked.
- Diversion Condition:** A dropdown menu showing "None".
- Diversion Header URI:** An empty text input field.
- Has Remote SBC:** A checkbox that is checked.
- Route Response on Via Port:** A checkbox that is currently unchecked.
- DTMF:** A section header with a dark background.
- DTMF Support:** A group box containing three radio buttons: "None" (selected), "SIP NOTIFY", and "SIP INFO".
- Finish:** A button at the bottom center of the window.

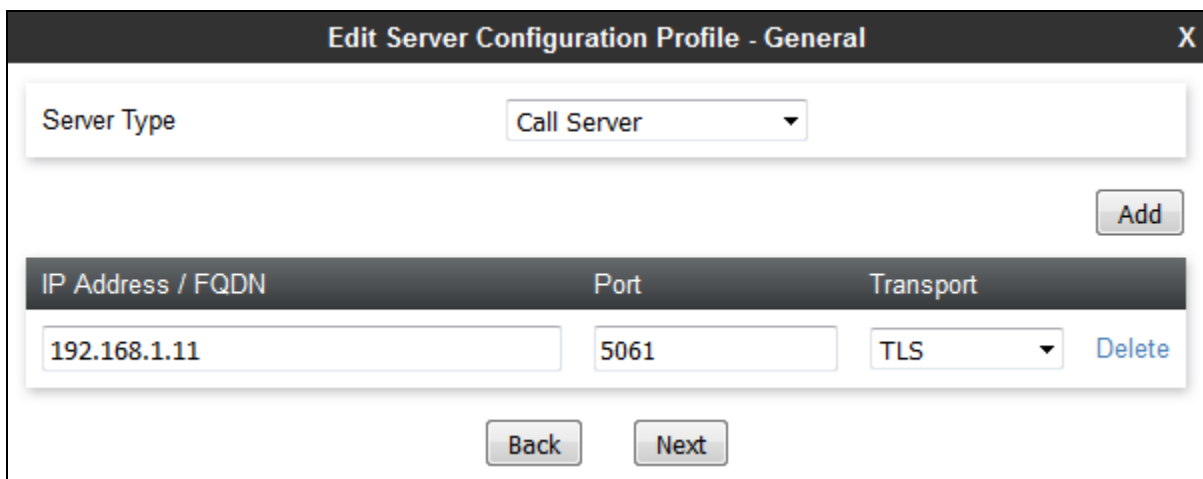
7.2.4 Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

1. Select **Global Profiles → Server Configuration** from the left-hand menu.
2. Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click **Next**.



3. The **Add Server Configuration Profile** window will open.
 - Select **Server Type: Call Server**.
 - **IP Address / FQDN: 192.168.1.11** (Session Manager signaling IP Address).
 - **Transport:** Select **TLS**.
 - **Port: 5061**.
 - Select **Next**.



4. The **Authentication** window will open (not shown).
 - Select **Next** to accept default values.

5. The **Heartbeat** window will open.
 - Check to **Enable Heartbeat**
 - **Method**: select **OPTIONS**
 - **Frequency**: enter **30** (or more)
 - **From URI** and **To URI**: enter **ping@sipinterop.net**

Add Server Configuration Profile - Heartbeat

Enable Heartbeat ☒

Method **OPTIONS**

Frequency seconds

From URI

To URI

Back **Next**

6. The **Advanced** window will open.
 - Check to **Enable Grooming**
 - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.
 - **TLS Client Profile**: select proper provisioned profile (please refer to *Administering Avaya Session Border Controller for Enterprise* document for TLS management). In this example select **SMclient2**.
 - Select **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile **Session Manager**

TLS Client Profile **SMclient2**

Signaling Manipulation Script **None**

Connection Type **SUBID**

Securable ☐

Back **Finish**

7.2.5 Server Configuration – AT&T

Repeat the steps in **Section 7.2.4**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to AT&T.

1. Select **Add Profile** and enter a Profile Name (e.g., **ATT**) and select **Next**.
2. On the **General** window (not shown), enter the following.
 - Select Server Type: **Trunk Server**.
 - **IP Address / FQDN**: **10.56.65.242** (AT&T's SBC IP address)
 - **Transport**: Select **TLS**.
 - **Port**: **5061**.
 - Select **Next** (not shown).

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

Add

IP Address / FQDN	Port	Transport
10.56.65.242	5061	TLS

Delete

Finish

3. Just select **Next** under **Authentication** window (not shown).

4. Under **Heartbeat** window:
 - Select **Enable Heartbeat**.
 - **Method**: choose **OPTIONS**.
 - **Frequency**: enter **30** (or more).
 - **From URI** and **To URI**: enter **ping@10.56.65.242**.

Enable Heartbeat ☒

Method OPTIONS ▾

Frequency seconds

From URI

To URI

Finish

5. Under **Advanced** window:
 - Select **ATT** for **Interworking Profile**.
 - Select **ATTClient** for **TLS Client Profile**.

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile ATT ▾

TLS Client Profile ATTclient ▾

Signaling Manipulation Script None ▾

Connection Type SUBID ▾

Securable ☐

Finish

7.2.6 Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

1. Select **Global Profiles** → **Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Session Manager**) and click **Next**.
3. The Routing Profile window will open. Using the default values shown, click on **Add**.
4. The Next-Hop Address window will open. Populate the following fields:
 - **Priority/Weight = 1.**
 - **Server Configuration = Session Manager.**
 - **Next Hop Address:** Verify that the **192.168.1.11:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
 - Click on **Finish**.

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manager	192.168.1.11:5061 (TLS)	None

7.2.7 Routing – To AT&T

Repeat the steps in **Section 7.2.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AT&T.

1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **ATT**).
2. On the **Next-Hop Address** window (not shown), populate the following fields:
 - **Server Configuration** = **ATT**.
 - **Next Hop Address**: Verify that the **10.56.65.242:5061** entry from the drop down menu is selected.
 - Use default values for the rest of the parameters.
3. Click **Finish**.

The screenshot shows the 'Profile : ATT - Edit Rule' window. It contains several configuration fields and a table of rules.

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

[Add](#)

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	ATT	10.56.65.242:5061 (TLS)	None	Delete

[Finish](#)

7.2.8 Topology Hiding – Session Manager

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

1. Select **Global Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name:** (e.g., **Session Manager**), and click **Next**.
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until **Via** header is added.
4. Populate the fields as shown below, and click **Finish**. Note that **sipinterop.net** is the domain used.

The screenshot shows the 'Topology Hiding Profiles: Session Manager' configuration window. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Session Manager' (selected), and 'ATT'. The main area has a blue header bar with 'Click here to add a description'. Below it, a table titled 'Topology Hiding' contains the following data:

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	sipinterop.net
Request-Line	IP/Domain	Overwrite	sipinterop.net
Record-Route	IP/Domain	Auto	—
To	IP/Domain	Overwrite	sipinterop.net
Via	IP/Domain	Auto	—

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

7.2.9 Topology Hiding – AT&T

Repeat the steps in **Section 7.2.8**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AT&T.

1. Enter a **Profile Name:** (e.g., **ATT**).
2. Click on the **Add Header** button repeatedly until **Refer-By** header is added.
3. Populate the fields as shown below, and click **Finish**.

The screenshot shows the 'Topology Hiding Profiles: ATT' configuration window. On the left, a sidebar lists 'Topology Hiding Profiles' with options: 'default', 'cisco_th_profile', 'Session Manager', and 'ATT' (selected). The main area has a blue header bar with 'Click here to add a description'. Below it, a table titled 'Topology Hiding' contains the following data:

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

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

7.2.10 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.2.11 Application Rules

Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 100 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.

Application Rules: default

Filter By Device...

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	10
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support: None

RTCP Keep-Alive: No

Edit

7.2.12 Border Rules

The Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses.

Border Rules: default

Filter By Device...

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Border Rule

Enable NATing	<input checked="" type="checkbox"/>
Use SIP Published IP	<input checked="" type="checkbox"/>
Use SDP Published IP	<input checked="" type="checkbox"/>

Edit

7.2.13 Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

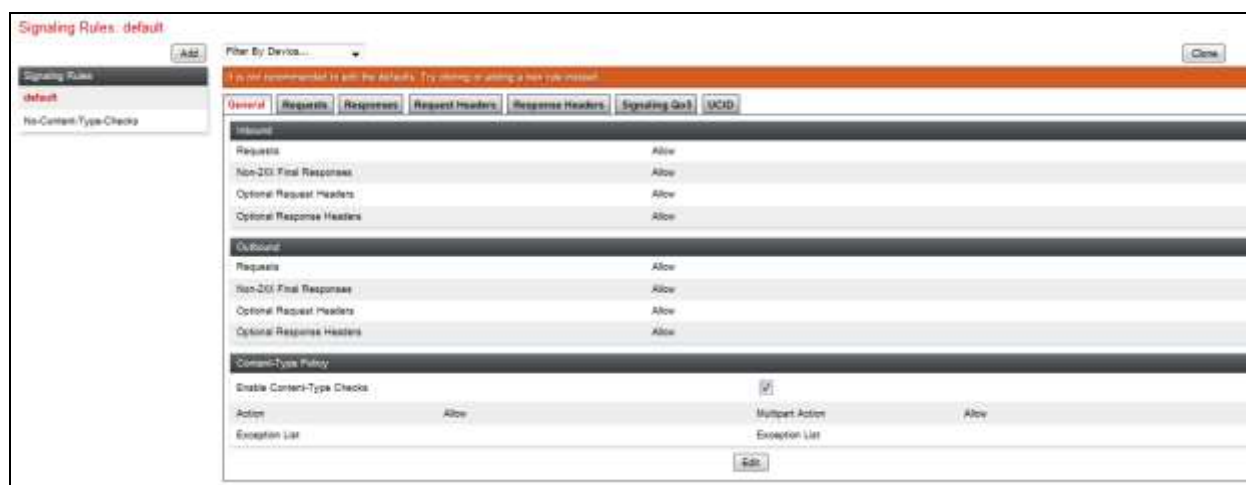
The screenshot shows the 'Media Rules: default-low-med' configuration page. On the left is a sidebar with a list of media rules: 'default-low-med' (highlighted), 'default-low-med-enc', 'default-high', 'default-high-enc', 'evsyle-low-med-enc', and 'default-low-med-MR'. The main area has a 'Filter By Device...' dropdown and a 'Close' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this are tabs for 'Media Encryption', 'Media Silencing', 'Media QoS', 'Media BFCP', and 'Media FEC'. The 'Media Encryption' tab is active, showing settings for 'Audio Encryption' and 'Video Encryption'. Both have 'Preferred Formats' set to 'RTP', 'Interworking' checked, and 'Mandatory' unchecked. 'Capability Negotiation' is also unchecked. An 'Edit' button is at the bottom right.

This screenshot shows the 'Media Rules: default-low-med' configuration page with the 'Media Silencing' tab selected. The sidebar and warning message are the same. The 'Media Silencing' tab shows a single setting: 'Media Silencing' which is unchecked. An 'Edit' button is located at the bottom right.

This screenshot shows the 'Media Rules: default-low-med' configuration page with the 'Media QoS' tab selected. The sidebar and warning message are the same. The 'Media QoS' tab contains settings for 'Media QoS Reporting' (RTCP Enabled, unchecked), 'Media QoS Marking' (Enabled, checked), 'QoS Type' (DSCP), 'Audio QoS' (Audio DSCP, EF), and 'Video QoS' (Video DSCP, EF). An 'Edit' button is at the bottom right.

7.2.14 Signaling Rules

The default Signaling Rule was utilized. No customization was required.



7.2.15 Endpoint Policy Groups

In the solution as tested, the **default-low** rule was utilized. This rule incorporated the media and Signaling Rules specified above, as well as other policies.



7.3 Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

7.3.1 Network Management

1. Select **Device Specific Settings** → **Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by

selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

Note: B1 has two IP Addresses configured for each interface. One is used for SIP trunking, another one is used for Remote worker. Configuration for Remote worker is out of scope of this document.

Network Management: asbce7

Devices	Interfaces	Networks
asbce7		

Name	Gateway	Subnet Mask	Interface	IP Address	Edit	Delete
A1	192.168.1.16	255.255.255.0	A1	192.168.1.1	Edit	Delete
B1	10.240.249.129	255.255.255.240	B1	10.240.249.130 10.240.249.131	Edit	Delete

7.3.2 Media Interfaces

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name: Media_A1.**
 - **IP Address: 192.168.1.16** (Avaya SBCE A1 address).
 - **Port Range: 35000-40000.**
4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name: Media_B1_trunking.**
 - **IP Address: 10.240.249.130** (Avaya SBCE B1 address).
 - **Port Range: 35000-40000.**
6. Click **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.

Media Interface: asbce7

Devices	Media Interface
asbce7	

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

Name	Media IP Address	Port Range	Edit	Delete
Media_A1	192.168.1.16 A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
Media_B1_trunking	10.240.249.130 B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
Media_B1_rw	10.240.249.131 B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

7.3.3 Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
 - **Name: Sig_A1.**
 - **IP Address: 192.168.1.16** (Avaya SBCE A1 address).
 - **TLS Port: 5061.**
 - **TCP Port: 5060.**
 - **TLS Profile: SMserver2.**
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
 - **Name: Sig_B1_trunking.**
 - **IP Address: 10.240.249.130** (Avaya SBCE B1 address).
 - **TLS Port: 5061.**
 - **TLS Profile: ATTserver.**
6. Click **Finish** (not shown). Note that changes to these values require an application restart.

Signaling Interface: asbce7

Devices
asbce7

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_A1	192.168.1.16 A1 (A1, VLAN 0)	5060	—	5061	SMserver2	Edit Delete
Sig_B1_trunking	10.240.249.130 B1 (B1, VLAN 0)	—	—	5061	ATTserver	Edit Delete
Sig_B1_rw	10.240.249.131 B1 (B1, VLAN 0)	5060	5060	5061	SMserver2	Edit Delete

7.3.4 Endpoint Flows – For Session Manager

1. Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
 - **Name:** Session Manager.
 - **Server Configuration:** Session Manager.
 - **URI Group:** *.
 - **Transport:** TLS.
 - **Remote Subnet:** *.
 - **Received Interface:** Sig_B1_trunking.
 - **Signaling Interface:** Sig_A1.
 - **Media Interface:** Med_A1.
 - **End Point Policy Group:** default-low.
 - **Routing Profile:** ATT.
 - **Topology Hiding Profile:** Session Manager.
 - Let other values default.
4. Click **Finish**.

Edit Flow: Session Manager	
Flow Name	Session Manager
Server Configuration	Session Manager
URI Group	*
Transport	TLS
Remote Subnet	*
Received Interface	Sig_B1_trunking
Signaling Interface	Sig_A1
Media Interface	Media_A1
End Point Policy Group	default-low
Routing Profile	ATT
Topology Hiding Profile	Session Manager
Signaling Manipulation Script	None
Remote Branch Office	Any
Finish	

7.3.5 Endpoint Flows – For AT&T

Repeat step **1** through **4** from **Section 7.3.4**, with the following changes:

- **Name:** ATT.
- **Server Configuration:** ATT.
- **Received Interface:** Sig_A1.
- **Signaling Interface:** Sig_B1_trunking.
- **Media Interface:** Med_B1_trunking.
- **Routing Profile:** Session Manager.
- **Topology Hiding Profile:** ATT.

Edit Flow: ATT	
Flow Name	ATT
Server Configuration	ATT
URI Group	*
Transport	TLS
Remote Subnet	*
Received Interface	Sig_A1
Signaling Interface	Sig_B1_trunking
Media Interface	Media_B1_trunking
End Point Policy Group	default-low
Routing Profile	Session Manager
Topology Hiding Profile	ATT
Signaling Manipulation Script	None
Remote Branch Office	Any
Finish	

8. Verification Steps

The following steps may be used to verify the configuration.

8.1 Avaya Session Border Controller for Enterprise

Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **All**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
 - Specify a **Capture Filename** (e.g., **TEST.pcap**).
 - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
 - Click **Start Capture** to begin the trace.

The screenshot shows the 'Packet Capture Configuration' window in the Avaya SBCE interface. The window has a sidebar with 'Devices' and 'sbce' selected. The main area has tabs for 'Packet Capture' and 'Captures'. The configuration fields are as follows:

Field	Value
Status	Ready
Interface	All
Local Address (IP Port)	10.2.2.125
Remote Address (IP Port)	*
Protocol	All
Maximum Number of Packets to Capture	3000
Capture Filename (Using the name of an existing device will overwrite it)	test.pcap

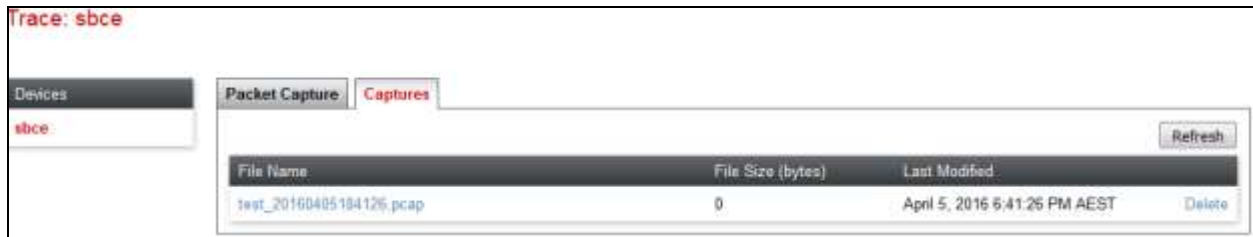
At the bottom of the configuration area are 'Start Capture' and 'Clear' buttons.

The capture process will initialize and then display the following **In Progress** status window:

The screenshot shows the 'Packet Capture Configuration' window with the status changed to 'In Progress'. A blue banner at the top reads: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.' The configuration fields are the same as in the previous screenshot, but the 'Start Capture' button has been replaced with a 'Stop Capture' button.

Field	Value
Status	In Progress
Interface	All
Local Address (IP Port)	10.2.2.125
Remote Address (IP Port)	*
Protocol	All
Maximum Number of Packets to Capture	3000
Capture Filename (Using the name of an existing device will overwrite it)	test.pcap

3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.



The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the VNGS SIP Trunk Service and the customer SIP PABX is the customer SBC.

On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the AT&T network gateway.
- Ping from the SBC to the Session Manager.
- Ping from the AT&T network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

Full Diagnostic
Ping Test

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Start Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (192.168.1.1)	Average ping from 192.168.1.16[A1] to 192.168.1.1 is 1.469ms.
✓ Ping: SBC (A1) to Primary DNS (135.10.209.250)	Average ping from 192.168.1.16[A1] to 135.10.209.250 is 111.287ms.
✓ Ping: SBC (B1) to Gateway (10.240.249.129)	Average ping from 10.240.249.130 [B1] to 10.240.249.129 is 0.268ms.

Incident Viewer

AVAYA

Device: All Category: All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 44

Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	729881580397602	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580396121	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580393451	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881402194116	4/4/16	7:40 PM	Policy	sbce	Heartbeat Successful, Server is UP

8.2 Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager.

- Verify signaling status, trunk status.

status signaling-group 3
STATUS SIGNALING GROUP
Group ID: 3
Group Type: sip
Group State: in-service

```
status trunk 3
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0003/001	T00001	in-service/idle	no
0003/002	T00002	in-service/idle	no
0003/003	T00003	in-service/idle	no
0003/004	T00004	in-service/idle	no
0003/005	T00005	in-service/idle	no
0003/006	T00006	in-service/idle	no
0003/007	T00007	in-service/idle	no
0003/008	T00008	in-service/idle	no
0003/009	T00009	in-service/idle	no
0003/010	T00010	in-service/idle	no

8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

1. Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.

Session Manager Dashboard
This page provides the overall status and health summary of each administered Session Manager.

Service State: Shutdown System: As of 2:09 PM

1 Item Show All Filter: Enable

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	Version
<input type="checkbox"/> ve3-sm	Core	✓	0/0/0	Up	Accept New Service	0/3	1	1/1	✓	✓	Normal	7.0.0.2.700201

Select: All, None

2. The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status. In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **3** Entities defined.
3. Clicking on the **0/3** entry in the **Entity Monitoring** column, results in the following display:

Session Manager Entity Link Connection Status
This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: ve3-sm

Summary View

Status Details for the selected Session Manager:

3 Items Refresh Filter: Enable

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> shce-A1	192.168.1.16	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/> ve3-sm	192.168.1.12	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/> ve3-nam	192.168.1.14	5060	TCP	FALSE	UP	200 OK	UP

Options messages between Avaya SBCE and Session Manager:

```
ve3-sm - traceSM - Captured: 36 Displayed: 8

sbce_A1      SM100

-----
14:12:58.400 | --OPTIONS-> | (2) sip:sipinterop.net
14:12:58.401 | <--200 OK-- | (2) 200 OK (OPTIONS)
14:13:09.487 | --OPTIONS-> | (4) sip:sipinterop.net
14:13:09.489 | <--200 OK-- | (4) 200 OK (OPTIONS)
14:13:28.401 | --OPTIONS-> | (2) sip:sipinterop.net
14:13:28.402 | <--200 OK-- | (2) 200 OK (OPTIONS)
14:13:29.606 | --OPTIONS-> | (7) sip:sipinterop.net
14:13:29.608 | <--200 OK-- | (7) 200 OK (OPTIONS)
```

8.4 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Control for Enterprise 7.0 can be configured to interoperate successfully with AT&T SIP Trunking Service. This solution allows enterprise users access to the PSTN using the AT&T SIP Trunking Service connection. Please refer to **Section 2.2** for exceptions.

10. Additional References

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

- [1] *What's New in Avaya Aura Release 7.0*, Release 7.0, 03-601818, Issue 1, August 2015.
- [2] *Deploying Avaya Aura® System Manager*, Release 7.0, Issue 1, October 2015.
- [3] *Administering Avaya Aura® System Manager for Release 7.0*, Issue 1, August 2015.
- [4] *Administering Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015.
- [5] *Deploying Avaya Aura Communication Manager in Virtualized Environment*, Release 7.0, Issue 1, August 2015.
- [6] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0, Issue 1, August 2015.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.
- [8] *Deploying Avaya Session Border Controller in Virtualized Environment*, Release 7.0, Issue 1, August 2015.
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.

- [10] *Deploying and Updating Avaya Aura Media Server Appliance, Release 7.7, Issue 1, August 2015.*
- [11] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager, Release 7.7, August 2015.*
- [12] *Deploying Avaya Aura® Messaging for Single Server Systems 6.3.3, Release 6.3.3, August 2015.*
- [13] *Administering Avaya Aura® Messaging 6.3.3, Release 6.3.3, August 2015.*
- [14] *9600 Series IP Deskphones Overview and Specification, Release 7.0, Issue 1, August 2015.*
- [15] *Installing and Maintaining Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP, Release 7.0, Issue 1, August 2015.*
- [16] *Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP, Release 7.0, Issue 2, August 2015.*
- [17] *Administering Avaya one-X® Communicator, Release 6.2, April 2015.*
- [18] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura® Communication Manager Rel. 6.3 and Avaya Aura® Session Managers Rel. 6.3. Issue 1.*
- [19] *RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>*
- [20] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method, <http://www.ietf.org/>*
- [21] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>*
- [22] *Configuration Note 88100 – Version L (05/11/2015) AVAYA S8730/S8800/CS1/CS2/1006r SIP Integration with AVAYA Aura Session Manager.*

Product documentation for AT&T SIP Trunking service is available from AT&T.

©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.