



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1 and Avaya Session Border Controller for Enterprise 8.0 with AAPT SIP Voice SIP Trunking Service - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Aura® Communication Manager Release 8.1 and Avaya Aura® Session Manager 8.1 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.0 when used to connect the AAPT SIP Voice SIP Trunking Service available from AAPT (Australia).

Avaya Aura® Session Manager 8.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 8.1 is a telephony application server. Avaya Session Border Controller for Enterprise 8.0 is the point of connection between the Enterprise and the AAPT SIP Voice SIP Trunking service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

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.

AAPT 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.....	5
2.1	Interoperability Compliance Testing.....	5
2.2	Test Results	6
2.3	Support	6
3.	Reference Configuration	7
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	SIP Trunk for SIP Voice SIP Trunking service access.....	16
5.8.2	SIP Trunk for Internal CPE access (Avaya SIP clients).....	19
5.9	Calling Party Information.....	22
5.10	Incoming Call Handling Treatment.....	23
5.11	Outbound Routing	24
5.12	Avaya SIP Client Routing	26
5.13	Automatic Alternate Routing (AAR) Dialing	26
5.14	Avaya G450 Media Gateway Provisioning.....	27
5.15	Avaya Aura® Media Server Provisioning.....	28
5.16	Save Communication Manager Translations.....	29
6.	Configure Avaya Aura® Session Manager	30
6.1	Configure SIP Domain	31
6.2	Configure Locations.....	31
6.3	Configure SIP Entities.....	32
6.3.1	Configure Session Manager SIP Entity	32
6.3.2	Configure Communication Manager SIP Entity – Outbound SIP Trunk	33
6.3.3	Configure Communication Manager SIP Entity – CPE Access	34
6.3.4	Configure Avaya SBCE SIP Entity	35
6.4	Configure Entity Links.....	36
6.4.1	Configure Entity Link to Communication Manager – Outbound SIP Trunk	37
6.4.2	Configure Entity Link to Communication Manager – CPE Access	37
6.4.3	Configure Entity Link for Avaya SBCE.....	38
6.5	Configure Routing Policies	38
6.5.1	Configure Routing Policy for Communication Manager.....	38
6.5.2	Configure Routing Policy for Avaya SBCE	39

6.6	Configure Dial Patterns	40
7.	Configure Avaya Session Border Controller for Enterprise	43
7.1	Device Management – Status	44
7.2	Server Interworking Profiles	46
7.2.1	Server Interworking – Session Manager	46
7.2.2	Server Interworking – AAPT	50
7.3	Signaling Manipulation Script	52
7.4	SIP Server Profiles	54
7.4.1	SIP Server – Session Manager	54
7.4.2	SIP Server – AAPT	56
7.5	Routing Profiles.....	59
7.5.1	Routing – To Session Manager	59
7.5.2	Routing – To AAPT	60
7.6	Topology Hiding	61
7.6.1	Topology Hiding – Session Manager	61
7.6.2	Topology Hiding – AAPT	61
7.7	Domain Policies	62
7.7.1	Application Rules.....	62
7.7.2	Border Rules	62
7.7.3	Media Rules	63
7.7.4	Signaling Rules	63
7.7.5	Endpoint Policy Groups	64
7.8	Network & Flows	65
7.8.1	Network Management.....	65
7.8.2	Media Interfaces.....	66
7.8.3	Signaling Interface	67
7.8.4	Endpoint Flows – For Session Manager	68
7.8.5	Endpoint Flows – For AAPT	69
8.	Verification Steps.....	70
8.1	Avaya Session Border Controller for Enterprise.....	70
8.2	Avaya Aura® Communication Manager	73
8.3	Avaya Aura® Session Manager Status	73
8.4	Telephony Services	74
9.	Conclusion	75
10.	Additional References.....	76

1. Introduction

These Application Notes illustrate a sample configuration Avaya Aura® Communication Manager Release 8.1 and Avaya Aura® Session Manager 8.1 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) when used to connect the AAPT SIP Voice SIP Trunking Service available from AAPT (Australia).

Avaya Aura® Session Manager 8.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 8.1 is a telephony application. Avaya SBCE is the point of connection between the Enterprise and the AAPT SIP Voice 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 Voice SIP Trunking Service available from AAPT is one of the SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The AAPT SIP Voice 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.

Purely as an example, the lab setup is configured in a non-redundant configuration (single Avaya Aura® Communication Manager, single Avaya Aura® Session Manager and a single Avaya SBCE). Additional resiliency could be built in as per the standard supported configurations documented in other Avaya publications.

On the private (enterprise) side, the Avaya Aura® Communication Manager "Processor Ethernet" or "procr" interface of Avaya Aura® Communication Manager is configured for SIP Trunking and is a SIP entity with associated SIP entity links in Avaya Aura® Session Manager. Additionally, Avaya SBCE is also configured as a SIP entity and has associated SIP entity links assigned within Avaya Aura® Session Manager.

In the documented example, the "Processor Ethernet" of the Avaya server running Avaya Aura® Communication Manager 8.1 is configured for SIP Trunking to Avaya Aura® Session Manager and Avaya SBCE is utilizing TCP transport. Avaya SBCE is connected to the AAPT SIP Voice SIP Trunking Service, and the SIP signaling connectivity from Avaya SBCE toward AAPT uses UDP.

Avaya SBCE performs security and topology-hiding at the enterprise edge. In the sample configuration, all SIP signaling and RTP media between the enterprise and the AAPT SIP Voice SIP Trunking Service solution flow through the Avaya SBCE.

2. General Test Approach and Test Results

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

The interoperability compliance testing focused on verifying inbound and outbound call flows between AAPT SIP Voice and Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, and Avaya SBCE (see **Section 3** for lab diagram).

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

2.1 Interoperability Compliance Testing

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

- PSTN incoming and outgoing calls to/from various phone types supported by Avaya IP Office including H.323, SIP, analog and digital stations; and Avaya Equinox Softphone
- Passing of DTMF events and their recognition by navigating automated menus (interacting with Avaya Aura® Messaging 7.1)
- PBX features such as hold, resume, conference and transfer
- G.711A audio
- Network Call Redirection
- Dialing plan including local 8-digit number and 10-digit Full Nation Number (FNN), international number
- Caller ID presentation and restriction
- Basic Call Center scenarios
- Faxing (G.711 pass-through)
- EC500 – call extending to mobile
- Remote Worker scenarios

2.2 Test Results

Interoperability testing of AAPT SIP Voice 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.

- **Calling / Called Party Identity:** In untrusted / authentication required configuration, AAPT may send hexadecimal string in **Contact** header, and may not send **P-Asserted-Identity**. This results in improper calling / called party identity displayed on Avaya clients. This also causes ec500 mapping failure, e.g., Communication Manager could not associate the mobile number with the host extension. An Avaya SBCE Signaling Manipulation (SigMa) script was used to overcome the issues. The purpose of the script is to add the **P-Asserted-Identity** header (if not existed) to the SIP requests/responses from/to AAPT SIP Voice Service. The content of the **P-Asserted-Identity** header is copied from **From/To** headers. See **Section 7.3** for how to create the script.
- **Call Forward** – No ring back tone on PSTN phone when Aura SIP extension set forward all call to another extension. The SIP trace is showing that Communication Manager firstly sends **181 Call is being forwarded** with **100rel** in **Require** header. Therefore, AAPT SIP Voice sends **PRACK**, and is expecting **200OK** for that **PRACK**. However, before sending **200OK** for the **PRACK**, Communication Manager sends **180 Ringing** with **100rel** in the **Require** header. AAPT SIP Voice could not handle this out-of-order **180 Ringing** at this point to generate the ringback tone to the PSTN caller. The issue is being investigated by both AAPT and Avaya.
- **EC500 service with Confirmed Answer enabled** - With Initial IP-IP Direct Media enabled on the SIP signaling group toward to AAPT SIP Voice SIP Trunking Service, the EC500 call leg is established with no voice as soon as EC500 user answers the call on mobile. This results in a call drop after the confirmation timeout (default to 10 seconds). If EC500 service with Confirmed Answer setting is required, the **Initial IP-IP Direct Media** must be disabled on the signaling group which is used for (or shared with) EC500 service.
- **Avaya Network Call Redirection (NCR) is recommended to be disabled** (default) on the Communication Manager SIP trunk group to the AAPT SIP Voice SIP Trunking Service. With NCR is enabled, in call transfer / conference scenarios, AAPT stops media by sending a re-INVITE, followed immediately by a BYE, and does not wait for a complete dialog. No obvious end-user impact was observed during compliance test. However, race condition issues are expected (e.g., Avaya endpoint does not get notified of transfer status properly).

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>
- **AAPT:** Customers should contact their AAPT Business representative or follow the support links available on <http://www.aapt.com.au>

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 Virtualized Environment.
- Avaya Aura® Session Manager running on Virtualized Environment.
- Avaya Aura® System Manager running on Virtualized Environment.
- Avaya Aura® Messaging running on Virtualized Environment.
- Avaya G450 Media Gateway.
- Avaya Aura® Media Server running on Virtualized Environment. The Media Server can act as a media gateway Gxxx series.
- Avaya IP phones are represented with Avaya 9600/1600 Series IP Telephones running H.323/SIP software.
- Avaya one-X® Communicator 6.2
- Avaya Equinox for Windows 3.5
- Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the AAPT SIP Voice SIP Trunking Service and the enterprise internal network.

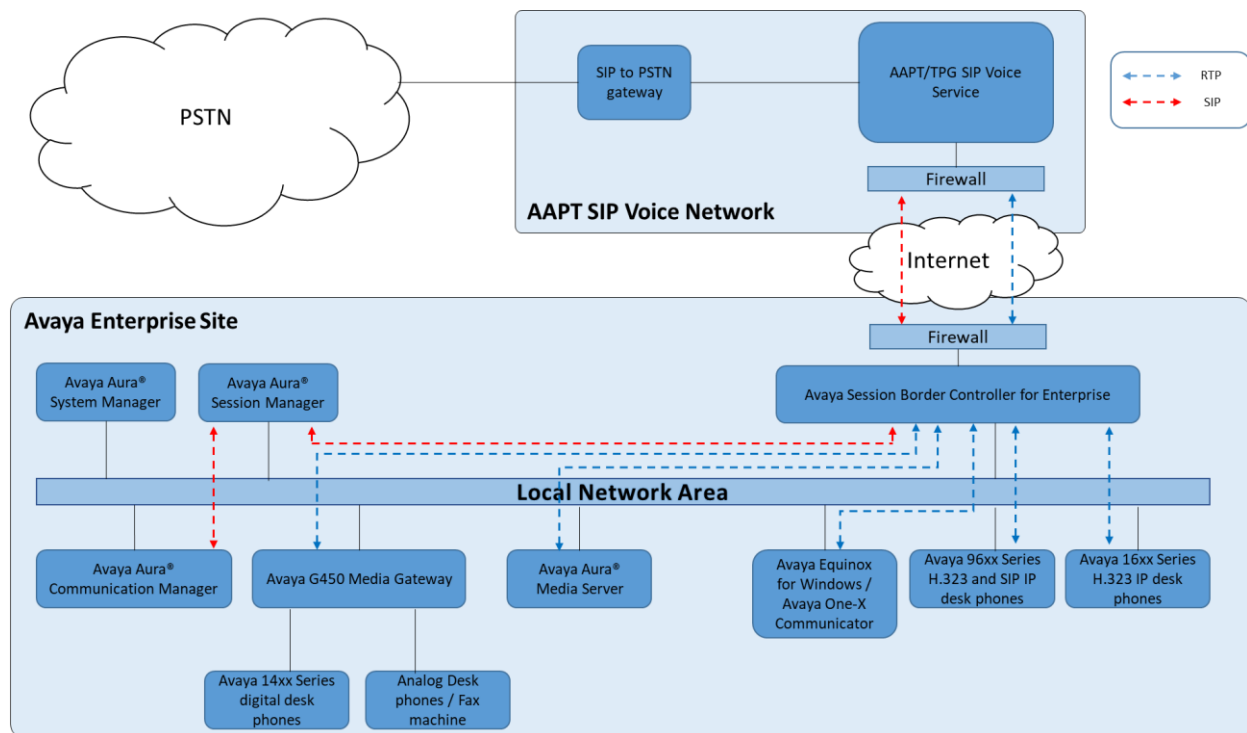


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	8.1.0.0.890-25393
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya Aura® System Manager	Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.9814
Avaya Aura® Messaging	7.1.0.0.532
Avaya Session Border Controller for Enterprise	8.0.0.0-19-16991
Avaya G450 Media Gateway	g450_sw_41_9_0
Avaya Aura Media Server	8.0.0.205
Avaya one-X® Communicator	6.2.13.2
Avaya Equinox for Windows	3.5.7.30.1
Avaya one-X® Agent H323	2.5.60313.0
Avaya 96x1 series – SIP Deskphones	7.1.5
Avaya 96xx series – H.323 Deskphones	3.2.8
Avaya 16xx series – H.323 Deskphones	1.3.12
Service Provider – AAPT SIP Voice	
Metaswitch cCFS (Softswitch)	V9.4.10_SU5_P90.00
Metaswitch Perimera ISC (SBC)	V4.3.20_SU4_P1203

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. The Communication Manager SAT console, the System Manager Web UI and the Avaya SBCE Web UI captured in this sections are displaying the configuration those have been configured earlier. The actual Communication Manager SAT commands, the System Manager Web UI and the Avaya SBCE Web UI to create/add the configurations may vary.

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:			4000		0
Maximum Concurrently Registered IP Stations:			1000		1
Maximum Administered Remote Office Trunks:			4000		0
Max Concurrently Registered Remote Office Stations:			1000		0
Maximum Concurrently Registered IP eCons:			68		0
Max Concur Reg Unauthenticated H.323 Stations:			100		0
Maximum Video Capable Stations:			2400		0
Maximum Video Capable IP Softphones:			1000		1
Maximum Administered SIP Trunks:			4000		10
Max Administered Ad-hoc Video Conferencing Ports:			4000		0
Max Number of DS1 Boards with Echo Cancellation:			80		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? n	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
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): 10		
Off-Premises Tone Detect Timeout Interval (seconds): 20		
AAR/ARS Dial Tone Required? y		
Music (or Silence) on Transferred Trunk Calls? no		
DID/Tie/ISDN/SIP Intercept Treatment: attendant		
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred		
Automatic Circuit Assurance (ACA) Enabled? n		
Abbreviated Dial Programming by Assigned Lists? n		
Auto Abbreviated/Delayed Transition Interval (rings): 2		
Protocol for Caller ID Analog Terminals: Bellcore		
Display Calling Number for Room to Room Caller ID Calls? n		

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:
 - The digits **68** for Communication Manager extensions (which is assigned by AAPT as DID numbers).
 - 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	
000	3	udp							
1300	10	udp							
18	10	udp							
68	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 Entity in **Section 6.3.2**.

Follow the steps shown below:

- Enter the **change node-names ip** command, and add a node name and IP address for the following:
 - Session Manager SIP signaling interface (e.g., **sm-ve** and **10.1.20.7**).
 - Avaya Media Server interface (e.g., **ams-ve** and **10.1.20.12**).

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ams-ve	10.1.20.12	
default	0.0.0.0	
procr	10.1.20.10	
procr6	::	
sm-ve	10.1.20.7	

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 fields.

display ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR	Target socket load: 4800	
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: 10.1.20.10	

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 Avaya Media Gateway / Avaya Media Server. 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                NR Group: 1
Location: 1              Authoritative Domain: sipinterop.net
Name: AAPT                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: 2048           IP Audio Hairpinning? n
                          UDP Port Max: 53999
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
H.323 IP ENDPOINTS        AUDIO RESOURCE RESERVATION PARAMETERS
                          RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic in region 1. In the compliance testing, Communication Manager, the G450 Media Gateway, Media Server, IP/SIP extensions, Session Manager and 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		M
										G	A	t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c			
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e		
1	1										all	
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												

Non-IP telephones (e.g., analog, digital) derive their network region from the IP interface of the G450 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.

change 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: 10.1.20.10		
Subnet Mask: /24				

To define network region 1 for the G450 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: g450
                                     Name: g450
                                     Serial No: 10IS11367055
Link Encryption Type: any-ptls/tls      Enable CF? n
Network Region: 1                               Location: 1
                                     Site Data:

Recovery Rule: none

Registered? y
FW Version/HW Vintage: 41 .9 .0 /2
MGP IPV4 Address: 10.1.20.20
MGP IPV6 Address:
Controller IP Address: 10.1.20.10
MAC Address: 00:1b:4f:3e:a5:e0

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** and **G.711MU** are included in the codec list. Note that the packet interval size will default to 20ms.

```
display ip-codec-set 1                                     Page 1 of 2
                                     IP MEDIA PARAMETERS

Codec Set: 1

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

- On **Page 2** of the ip-codec-set form, set **pass-through** for G.711 pass-through mode.

display ip-codec-set 1		Page 2 of 2	
IP MEDIA PARAMETERS			
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	Redun- dancy	Packet Size (ms)
FAX	pass-through	0	
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. Two SIP trunk groups are defined on Communication Manager in the reference configuration:

- SIP Voice SIP Trunking service access – SIP Trunk group 1
- Internal CPE access (ie: Avaya SIP extension) – SIP Trunk group 3

5.8.1 SIP Trunk for SIP Voice SIP Trunking service access

This section describes the steps for administering the SIP trunk to Session Manager. This trunk corresponds to the **cm-ve** 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., **1**), and provision the following:

- Group Type** – Set to **sip**.
- Transport Method** – Set to **tcp**.
- Verify that **IMS Enabled?** 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., **sm-ve**).
- Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**
- 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 / Avaya Media Server when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **Initial IP-IP Direct Media** – Set to **y**, indicating that the RTP paths should be initially direct between Avaya SIP stations and the internal interface of ASBCE, to reduce the use of media resources on the Avaya Media Gateway / Avaya Media Server.
- **H.323 Station Outgoing Direct Media** – Set to **y**, indicating that the RTP paths should be also initially direct for the H.323 stations, to avoid the use of media resources on the Avaya Media Gateway / Avaya Media Server.
- Default values may be used for all other fields.

display signaling-group 1		Page 1 of 3
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? y	Priority Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
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: sm-ve	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	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? y	Initial IP-IP Direct Media? y	
	Alternate Route Timer(sec): 6	

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

- **Group Type** – Set to **sip**.
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***01**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Section 5.8.1** (e.g., **1**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

```

display trunk-group 1                                     Page 1 of 4
                                     TRUNK GROUP

Group Number: 1                Group Type: sip           CDR Reports: y
  Group Name: AAPT-Trunk        COR: 1                 TN: 1         TAC: *01
  Direction: two-way           Outgoing Display? n
  Dial Access? n                Night Service:
  Queue Length: 0
  Service Type: public-ntwrk    Auth Code? n
                                   Member Assignment Method: auto
                                   Signaling Group: 1
                                   Number of Members: 10

```

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 1                                     Page 3 of 4
TRUNK FEATURES
  ACA Assignment? n                Measured: none
                                   Maintenance Tests? y

  Suppress # Outpulsing? n        Numbering Format: public
                                   UI Treatment: service-provider

                                   Replace Restricted Numbers? y
                                   Replace Unavailable Numbers? y

                                   Hold/Unhold Notifications? y
                                   Modify Tandem Calling Number: no

```

On **Page 4**, set the **Network Call Redirection** field should be set to **n**. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer. Refer **Section 2.2** for observations with **Network Call Redirection** / SIP REFER enabled.

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.

```

display trunk-group 1
                                Page 4 of 4
                                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? y
                                Identity for Calling Party Display: From
Block Sending Calling Party Location in INVITE? n
                                Accept Redirect to Blank User Destination? y
                                Enable Q-SIP? n

Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits

```

5.8.2 SIP Trunk for Internal CPE access (Avaya SIP extensions)

This section describes the steps for administering the SIP trunk to Session Manager. This trunk corresponds to the **cm-ve-optim** SIP Entity defined in **Section 6.3.3**.

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 **IMS Enabled?** 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., **sm-ve**).
- **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 Media Gateway / Media Server when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **Initial IP-IP Direct Media** – Set to **y**, indicating that the RTP paths should be initially direct between Avaya SIP stations and the internal interface of ASBCE, to the use of media resources on the Media Gateway / Media Server.
- **H.323 Station Outgoing Direct Media** – Set to **y**, indicating that the RTP paths should be also initially direct for the H.323 stations, to avoid the use of media resources on the Avaya Media Gateway / Avaya Media Server.
- Default values may be used for all other fields.

```

display signaling-group 3                                     Page 1 of 3
                                SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
    Q-SIP? n
    IP Video? y                      Priority Video? n          Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM                      Clustered? n
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: sm-ve
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
                                                RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload                      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
Enable Layer 3 Test? y                      Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? y                      Alternate Route Timer(sec): 6

```

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

- **Group Type** – Set to **sip**.
- **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 **tie**.
- **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 4	
TRUNK GROUP			
Group Number: 3	Group Type: sip	CDR Reports: y	
Group Name: SIP-OPTIM	COR: 1	TN: 1	TAC: *03
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 3	
		Number of Members: 10	

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. Default values may be used for all other fields.

display trunk-group 1		Page 3 of 4	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private	UI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
		Hold/Unhold Notifications? y	
Modify Tandem Calling Number: no			

On **Page 4**, Set **Telephone Event Payload Type** to **101** to be consistent with the **Telephone Event Payload Type** of the SIP Trunk (Trunk 1) toward AAPT SIP Voice. Default values may be used for all other fields

display trunk-group 3	Page 4 of 4
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? n	
Support Request History? y	
Telephone Event Payload Type: 101	
Overwrite Calling Identity? n	
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? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.9 Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers.

Use the **change private-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the service provider. It is used to authenticate the caller.

In the sample configuration, the DID numbers provided for testing were assigned to the extensions 68xx. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk (trunk 1) when calls were originated from these extensions.

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. AAPT will accept the full E.164 string including + prefix. The following example is to construct an E.164 11-digit calling number from 4-digit extension, '+' will be automatically inserted if the SIP Signaling group is connected to Session Manager. The actual number is masked with 'x' for security reason.

display public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	68	1	612xxxx	11	
					Total Administered: 3
					Maximum Entries: 240
					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.

In order to presenting calling party number to Avaya SIP extension in 4-digit internal format, an additional private-numbering entry is administered for the SIP extension access trunk (trunk group 3).

display private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total CPN Len	
4	68	1		4	
					Total Administered: 2
					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. The DID numbers sent by AAPT can be mapped to Communication Manager extensions 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.

display inc-call-handling-trmt trunk-group 1					Page 1 of 3
INCOMING CALL HANDLING TREATMENT					
Service/Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10 02xxxx		6		

Note: the actual number is masked with “xxxx” for security reason.

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			DIAL PLAN ANALYSIS TABLE						Page	1 of	12
			Location: all			Percent Full: 2					
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type			
000	3	udp									
1300	10	udp									
18	10	udp									
68	4	ext									
*	3	dac									
#	4	fac									
9	1	fac									

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

display feature-access-codes			FEATURE ACCESS CODE (FAC)						Page	1 of	12
			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 **1** for an outbound call which contains the SIP trunk to the service provider (as defined next).

display ars analysis 0							Page	1 of	2
ARS DIGIT ANALYSIS TABLE							Percent Full: 0		
Location: all									
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd			
000	3	3	1	emer		n			
0011	12	20	1	pubu		n			
02	10	10	1	pubu		n			
03	10	10	1	pubu		n			
04	10	10	1	pubu		n			
06	10	10	1	pubu		n			
07	10	10	1	pubu		n			
08	10	10	1	pubu		n			
1300	10	10	1	pubu		n			
18	10	10	1	pubu		n			
xxxxxxxx	8	8	1	pubu		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 1** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the service provider. For the compliance testing, trunk group **1** 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:** **pub-unk**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.9**.

display route-pattern 1										Page	1 of	4
Pattern Number: 1										Pattern Name: AAPT-EV-Route		
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:	1	0									n	user
2:											n	user
3:											n	user
4:											n	user
5:											n	user
6:											n	user
	BCC VALUE		TSC	CA-TSC		ITC BCIE Service/Feature			PARM	Sub	Numbering	LAR
	0	1 2 M 4 W		Request						Dgts	Format	
1:	y	y y y y y n	n			rest					pub-unk	none
2:	y	y y y y y n	n			rest						none
3:	y	y y y y y n	n			rest						none

5.12 Avaya SIP Extension Routing

Route Patterns are used to direct calls to the local SIP trunk for access to SIP extensions or other destinations in the CPE. 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 trunk group for the Avaya SIP Extension Routing. 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:** **lev0-pvt**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.9**.

display route-pattern 3											Page	1 of	4					
Pattern Number: 3											Pattern Name: SIP-OPTIM							
SCCAN? n											Secure SIP? n			Used for SIP stations? y				
Primary SM: sm-ve											Secondary SM:							
Grp FRL NPA Pfx Hop Toll No.											Inserted			DCS/ IXC				
No											Mrk Lmt List Del Digits			QSIG				
											Dgts			Intw				
1: 3 0											n			user				
2:											n			user				
3:											n			user				
4:											n			user				
5:											n			user				
6:											n			user				
BCC VALUE											TSC	CA-TSC	ITC BCIE Service/Feature PARM Sub			Numbering	LAR	
0 1 2 M 4 W											Request			Dgts			Format	
1: y y y y y n n											rest			lev0-pvt			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	

5.13 Automatic Alternate Routing (AAR) Dialing

Use the **change aar analysis** command to configure the routing for Avaya SIP Extensions. The example below shows a subset of the SIP extensions used as part of the compliance testing.

display aar analysis 0										Page	1 of	2
AAR DIGIT ANALYSIS TABLE												
Location: all										Percent Full: 0		
Dialed		Total		Route		Call		Node		ANI		
String		Min Max		Pattern		Type		Num		Reqd		
68xx		4 4		3		lev0				n		
										n		

5.14 Avaya G450 Media Gateway Provisioning

In the reference configuration, a G450 Media Gateways is provisioned. The G450 Media Gateway is used for local DSP resources, announcements, Music On Hold, etc.

Note – Only the Media Gateway provisioning associated with the G450 registration to Communication Manager is shown below.

1. SSH to the G450 (not shown). Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., **g450-??? (super)#**).
2. Enter the **show system** command and note the G450 serial number (e.g., **10IS11367055**).
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., **10.1.20.10**).
4. Enter the **copy run copy start command** to save the G450 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** = **G450**.
- Set **Name** = Enter a descriptive name (e.g., **g450**).
- Set **Serial Number** = Enter the serial number copied from **Step 2**.
- Set the **Encrypt Link** parameter as desired (**any-ptls/tls** 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., **g450-001 (super)#**).

6. Enter the **display media-gateway 1** command, and verify that the G450 has registered.

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

                                Type: g450
                                Name: g450
                                Serial No: 10IS11367055
                                Link Encryption Type: any-ptls/tls
                                Network Region: 1
                                Enable CF? n
                                Location: 1
                                Site Data:

                                Recovery Rule: none

                                Registered? y
                                FW Version/HW Vintage: 41 .9 .0 /2
                                MGP IPV4 Address: 10.1.20.20
                                MGP IPV6 Address:
                                Controller IP Address: 10.1.20.10
                                MAC Address: 00:1b:4f:3e:a5:e0

                                Mutual Authentication? optional
```

5.15 Avaya Aura® Media Server Provisioning

In the reference configuration, a Media Server is provisioned. The Media Server is located in the enterprise and is used, along with the G450 Media Gateway, for local DSP resources, announcements, and Music On Hold.

Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **2**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **Peer Detection Enabled?** is set to **n**.
- **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 Media Server as administered in **Section 5.4** (e.g., **ams-ve**).
- **Near-end Listen Port** – Set to **9061**.
- **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** – Automatically populated with the IP address of the Media Server.

```
display signaling-group 2                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 2                Group Type: sip
                               Transport Method: tls

Peer Detection Enabled? n    Peer Server: AMS

Near-end Node Name: procr                Far-end Node Name: ams-ve
Near-end Listen Port: 9061              Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain: 10.1.20.12
```

Enter the **add media-server x** command where **x** is an available Media Server identifier (e.g., **1**), and provision the followings:

- **Signaling Group** – Enter the signaling group previously configured for Media Server (e.g., **2**).
- **Voip Channel License Limit** – Enter the number of VoIP channels for this Media Server (based on licensing) (e.g., **10**).
- **Dedicated Voip Channel Licenses** – Enter the number of VoIP channels licensed to this Media Server (e.g., **10**).
- Remaining fields are automatically populated based on the signaling group provisioning for the Media Server.

```
display media-server 1

                                MEDIA SERVER

Media Server ID: 1

    Signaling Group: 2
    Voip Channel License Limit: 10
    Dedicated Voip Channel Licenses: 10

Node Name: ams-ve
Network Region: 1
Location: 1
Announcement Storage Area: ANNC-b2bf4c0a-205a-41e8-84c1-000c2963b6c0
```

5.16 Save Communication Manager Translations

After the Communication Manager provisioning is completed, enter the command **save translation** (not shown).

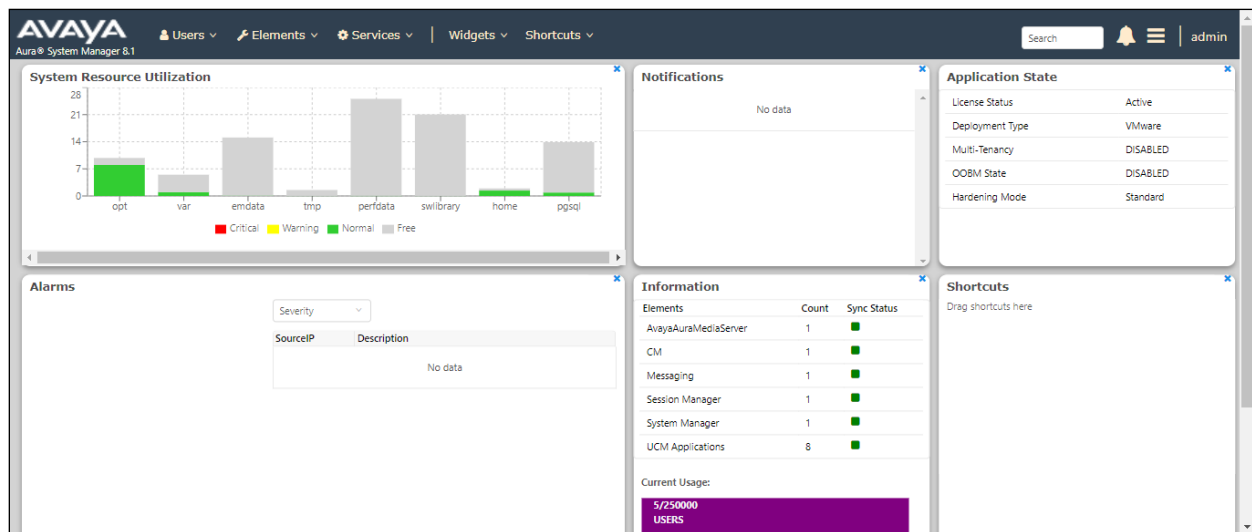
6. Configure Avaya Aura® Session Manager

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 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.

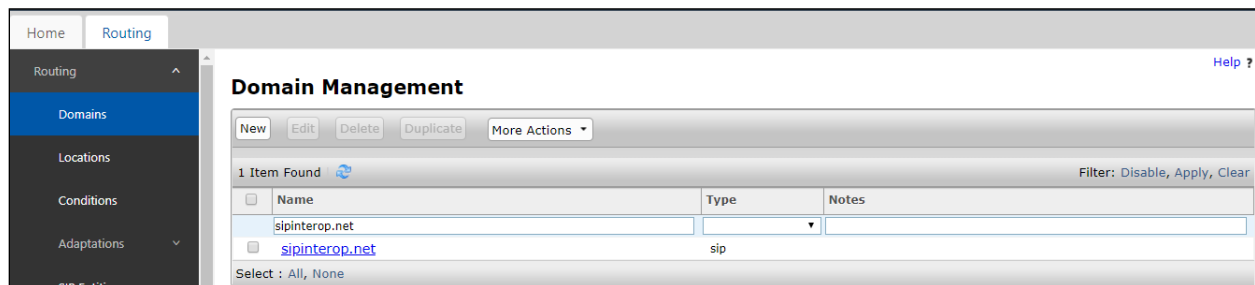
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **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).

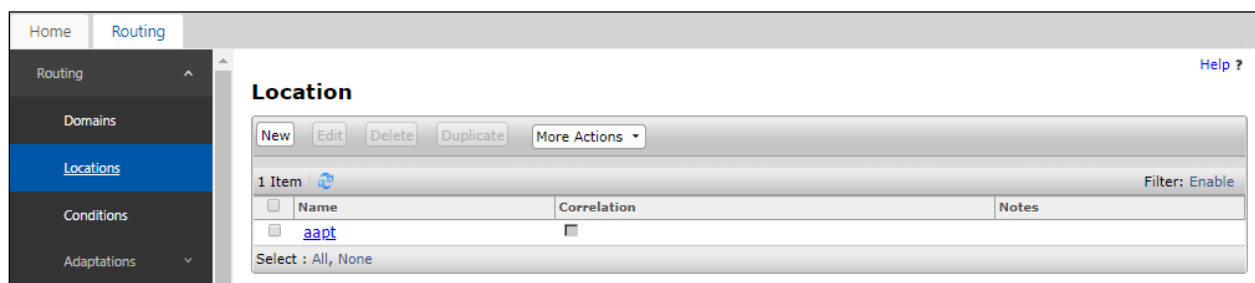


6.2 Configure Locations

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

Follow the steps shown below:

1. Select **Locations** from the left navigational menu. Click **New**. In the **General** section (not shown), enter the following values and use default values for remaining fields.
 - **Name:** Enter a descriptive name for the Location (e.g., **aapt**).
 - **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., **sm-ve**).
 - **IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.1.20.7**).
 - **SIP FQDN** – (Optional) Leave blank or enter the SIP FQDN of Session Manager signaling interface (e.g., **sm-ve-sm100.sipinterop.net**)
 - **Type** – Verify **Session Manager** is selected.
 - **Location** – Select location **aapt**.
 - **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.

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar has 'SIP Entities' selected. The main area has two tabs: 'General' and 'Monitoring'. The 'General' tab contains the following fields:

- Name:** sm-ve
- IP Address:** 10.1.20.7
- SIP FQDN:** sm-ve-sm100.sipinterop.net
- Type:** Session Manager
- Location:** aapt
- Outbound Proxy:** (empty)
- Time Zone:** Australia/Melbourne
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)

The 'Monitoring' tab contains the following fields:

- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located at the top right of the 'General' tab.

6.3.2 Configure Communication Manager SIP Entity – Outbound SIP Trunk

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. **cm-ve**).
 - **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) (e.g. **10.1.20.10**).
 - **Type** – Select **CM**.
 - **Location** – Select a Location **aapt** administered in **Section 6.2**.
 - **Time Zone** – Select the time zone in which Communication Manager resides.
3. In the **Monitoring** section of the **SIP Entity Details** page select:
 - a. Select **Use Session Manager Configuration** for **SIP Link Monitoring** field
 - b. Use the default values for the remaining parameters.
4. Click on **Commit**.

The screenshot displays the 'SIP Entity Details' configuration page. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is divided into three sections: 'General', 'Loop Detection', and 'Monitoring'. The 'General' section includes fields for Name (cm-ve), FQDN or IP Address (10.1.20.10), Type (CM), Notes, Adaptation, Location (aapt), Time Zone (Australia/Sydney), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (checkbox), and Call Detail Recording (none). The 'Loop Detection' section includes Loop Detection Mode (On), Loop Count Threshold (5), and Loop Detection Interval (200). The 'Monitoring' section includes SIP Link Monitoring (Use Session Manager Configuration) and CRLF Keep Alive Monitoring (Use Session Manager Configuration). At the top right of the main content area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

6.3.3 Configure Communication Manager SIP Entity – CPE Access

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

- **Name** – Enter a different CM descriptive name (e.g., **cm-ve-optim**).
- **FQDN or IP Address** – Enter the same IP address of Communication Manager Processor Ethernet (procr) (e.g. **10.1.20.10**).
- Other fields as same as in **Section 6.3.2**.

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar contains a navigation menu with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into three sections: 'General', 'Loop Detection', and 'Monitoring'. The 'General' section includes fields for 'Name' (cm-ve-optim), 'FQDN or IP Address' (10.1.20.10), 'Type' (CM), 'Notes', 'Adaptation', 'Location' (aapt), 'Time Zone' (Australia/Sydney), 'SIP Timer B/F (in seconds)' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name', 'Securable' (checkbox), and 'Call Detail Recording' (none). The 'Loop Detection' section includes 'Loop Detection Mode' (On), 'Loop Count Threshold' (5), and 'Loop Detection Interval (in msec)' (200). The 'Monitoring' section includes 'SIP Link Monitoring' and 'CRLF Keep Alive Monitoring', both set to 'Use Session Manager Configuration'.

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

SIP Entity Details

Commit Cancel

Help ?

General

* Name: cm-ve-optim

* FQDN or IP Address: 10.1.20.10

Type: CM

Notes:

Adaptation:

Location: aapt

Time Zone: Australia/Sydney

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

6.3.4 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., **10.1.20.9**).
- **Type** – Verify **SIP Trunk** is selected.
- **Location** – Select location **aapt** (**Section 6.2**).

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into three sections: 'General', 'Loop Detection', and 'Monitoring'. In the 'General' section, fields include Name (sbce_A1), FQDN or IP Address (10.1.20.9), Type (SIP Trunk), Notes, Adaptation, Location (aapt), Time Zone (Australia/Sydney), SIP Timer B/F (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (unchecked), Call Detail Recording (egress), and Loop Detection (On). The 'Loop Detection' section includes Loop Count Threshold (5) and Loop Detection Interval (200). The 'Monitoring' section includes SIP Link Monitoring (Use Session Manager Configuration), CRLF Keep Alive Monitoring (Use Session Manager Configuration), Supports Call Admission Control (unchecked), Shared Bandwidth Manager (unchecked), Primary Session Manager Bandwidth Association, and Backup Session Manager Bandwidth Association.

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

SIP Entity Details

Commit Cancel

Help ?

General

* Name: sbce_A1

* FQDN or IP Address: 10.1.20.9

Type: SIP Trunk

Notes:

Adaptation:

Location: aapt

Time Zone: Australia/Sydney

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

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, **TCP** for the Entity Link to Communication Manager and **TCP** 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 6.3.4**.
- **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 – Outbound SIP Trunk

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., **sm-ve_cm-ve_5060_TCP**).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.3.1** for Session Manager (e.g., **sm-ve**).
 - **SIP Entity 1 Port** – Enter **5060**.
 - **Protocol** – Select **TCP**.
 - **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.2** for the Communication Manager entity (e.g., **cm-ve**).
 - **SIP Entity 2 Port** - Enter **5060**.
 - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.

The screenshot shows the 'Entity Links' configuration page in a web interface. The left sidebar has a menu with 'Routing' selected, and 'Entity Links' is highlighted under it. The main area shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The values in the table are: Name: sm-ve_cm-ve_5060_TCP, SIP Entity 1: sm-ve, Protocol: TCP, Port: 5060, SIP Entity 2: cm-ve, Port: 5060, DNS Override: (checkbox), Connection Policy: trusted, Deny New Service: (checkbox), Notes: (empty). There are 'Commit' and 'Cancel' buttons at the top right of the table area. A 'Filter: Enable' link is also present.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
sm-ve_cm-ve_5060_TCP	sm-ve	TCP	5060	cm-ve	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.4.2 Configure Entity Link to Communication Manager – CPE Access

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., **sm-ve_cm-ve-optim_5061_TLS**).
- **SIP Entity 1 Port** – Enter **5061**.
- **Protocol** – Select **TLS**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.3** for the Communication Manager entity (e.g., **cm-ve-optim**).
- **SIP Entity 2 Port** - Enter **5061**.
- Click on **Commit**.

The screenshot shows the 'Entity Links' configuration page in a web interface, similar to the previous one but with different values. The left sidebar has 'Entity Links' highlighted. The main area shows a table with one item. The values in the table are: Name: sm-ve_cm-ve-optim_5061_TLS, SIP Entity 1: sm-ve, Protocol: TLS, Port: 5061, SIP Entity 2: cm-ve-optim, Port: 5061, DNS Override: (checkbox), Connection Policy: trusted, Deny New Service: (checkbox), Notes: (empty). There are 'Commit' and 'Cancel' buttons at the top right of the table area. A 'Filter: Enable' link is also present.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
sm-ve_cm-ve-optim_5061_TLS	sm-ve	TLS	5061	cm-ve-optim	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.4.3 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., **sm-ve_sbce_A1_5060_TCP**).
- **SIP Entity 1 Port** – Enter **5060**.
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.4** for the Avaya SBCE entity (e.g., **sbce_A1**).
- **SIP Entity 2 Port** - Enter **5060**.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
sm-ve_sbce_A1_5060_TCP	sm-ve	TCP	5060	sbce_A1	5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.5 Configure Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. 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 AAPT.

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 AAPT calls to Communication Manager (e.g., **to cm-ve**), 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 (**cm-ve**), and click on **Select**.
5. Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.
6. No **Regular Expressions** were used in the reference configuration.
7. Click on **Commit**.

The screenshot shows the 'Routing Policy Details' page in a web interface. The left sidebar has a menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and has 'Commit' and 'Cancel' buttons. Under the 'General' tab, there are fields for 'Name' (set to 'cm-ve'), 'Disabled' (checkbox), 'Retries' (set to 0), and 'Notes'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table. The table has columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. It contains one entry: 'cm-ve' with FQDN or IP Address '10.1.20.10' and Type 'CM'. At the bottom, there is a 'Time of Day' section.

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., **to sbce**).
- **SIP Entity List** –Select the SIP Entity administered in **Section 6.3.4** for the Avaya SBCE entity (e.g., **sbce_A1**).

The screenshot shows the 'Routing Policy Details' page in a web interface, similar to the previous one but with different values. The 'Name' field is set to 'to sbce'. The 'SIP Entity as Destination' section shows a table with one entry: 'sbce_A1' with FQDN or IP Address '10.1.20.9' and Type 'SIP Trunk'. The 'Time of Day' section is also visible at the bottom.

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 AAPT 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.

Four examples of the dial patterns used for the compliance testing were shown below, two for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise and another one for outbound calls to emergency number.

The first example shows that 10-digit dialed numbers starting with 02 that has a destination domain of “All” uses route policy to **sbce** as defined in **Section 6.5.2**

Dial Pattern Details

General

- * Pattern: 02
- * Min: 10
- * Max: 10
- Emergency Call: ☐
- SIP Domain: -ALL-
- Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

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

Select : All, None

The second example shows that outbound any 8-digit numbers uses route policy **to sbce** as defined in **Section 6.5.2** for PSTN calls.

Dial Pattern Details

General

* Pattern: xxxxxxx

* Min: 8

* Max: 8

Emergency Call: ☐

SIP Domain: -ALL-

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
<input type="checkbox"/> aapt		to sbce	0	<input type="checkbox"/>	sbce_A1	

Select : All, None

The third example shows that 10-digit pattern that starts with 02xxxx68 is used for inbound calls from AAPT to DID numbers on Avaya Aura® Communication Manager.

Dial Pattern Details

General

* Pattern: 02xxxx68xx

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

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
<input type="checkbox"/> -ALL-		to cm-ve	0	<input type="checkbox"/>	cm-ve	

Select : All, None

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

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:** 000

* **Min:** 3

* **Max:** 3

Emergency Call: ☒

* **Emergency Priority:** 1

* **Emergency Type:** All

SIP Domain: -ALL-

Notes: emergency simulator

Originating Locations and Routing Policies

Add Remove Filter: Enable

1 Item

<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"/>	aapt		to sbce	0	<input type="checkbox"/>	sbce_A1	

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.

As described in **Section 3**, the reference configuration places the private interface (A1) of Avaya SBCE in the Common site, (10.1.20.9), with access to the **AAPT** site. The connection to AAPT uses the Avaya SBCE public interface B1 (IP address 10.239.192.234). The following 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**.



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field containing the placeholder text "username". Below the input field is a "Continue" button. Further down, there is a "WELCOME TO AVAYA SBC" message, a warning about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2019 Avaya Inc. All rights reserved."

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



This screenshot shows the same login page as the previous one, but with the "Password:" label added below the "Username:" label. The password input field now contains a series of dots. The "Log In" button has replaced the "Continue" button. The rest of the page content, including the Avaya logo, the "WELCOME TO AVAYA SBC" message, the warning, the consent statement, and the copyright notice, remains the same.

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

Device: sbceAlarmsIncidentsStatusLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for EnterpriseAVAYA

EMS Dashboard

Device ManagementBackup/RestoreSystem ParametersDoS / DDoSScrubberUser AgentsConfiguration ProfilesServicesDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & Logging

Dashboard

Information

System Time	08:21:01 PM AEST	Refresh
Version	8.0.0.0-19-16991	
Build Date	Sat Jan 26 21:58:11 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	06/25/2019 19:47:08 AEST	
Failed Login Attempts	0	

Active Alarms (past 24 hours)
None found.

Installed Devices

EMS

sbce

Incidents (past 24 hours)

sbce: Heartbeat Successful, Server is UP

sbce: Heartbeat Successful, Server is UP

sbce: Heartbeat Successful, Server is UP

sbce: Heartbeat Successful, Server is UP

7.1 Device Management – Status

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

Device: sbceAlarmsIncidentsStatusLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for EnterpriseAVAYA

EMS Dashboard

Device ManagementBackup/RestoreSystem ParametersDoS / DDoSScrubberUser AgentsConfiguration Profiles

Device Management

DevicesUpdatesSSL VPNLicensingKey Bundles

Device Name	Management IP	Version	Status	
sbce	10.1.20.8	8.0.0.0-19-16991	Commissioned	RebootShutdownRestart ApplicationViewEditUninstall

- Click on **View** (shown above) to display the **System Information** screen. Note that DNS servers are AAPT DNS servers and DNS client must be B1 IP address that is used for SIP trunk with AAPT.

System Information: sbce

X

General Configuration

Appliance Name	sbce
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: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
CLID	---
Encryption Available: Yes	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.1.20.9	10.1.20.9	255.255.255.0	10.1.20.1	A1
10.1.20.19	10.1.20.19	255.255.255.0	10.1.20.1	A1
135.27.78.6	135.27.78.6	255.255.255.248	135.27.78.1	A2
10.239.192.234	10.239.192.234	255.255.255.248	10.239.192.233	B1
10.239.192.235	10.239.192.235	255.255.255.248	10.239.192.233	B1

DNS Configuration

Primary DNS	10.1.20.3
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.239.192.234

Management IP(s)

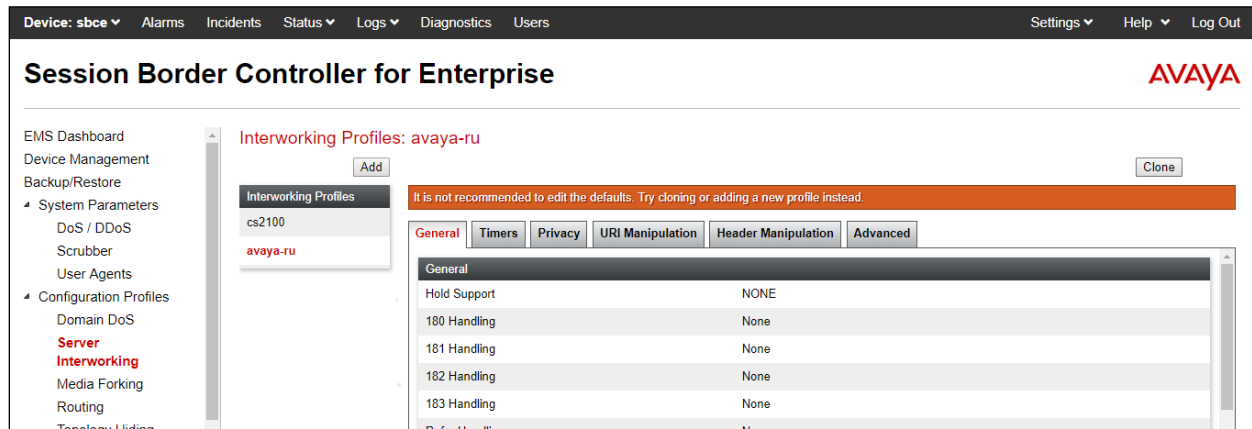
IP #1 (IPv4)	10.1.20.8
--------------	-----------

7.2 Server Interworking Profiles

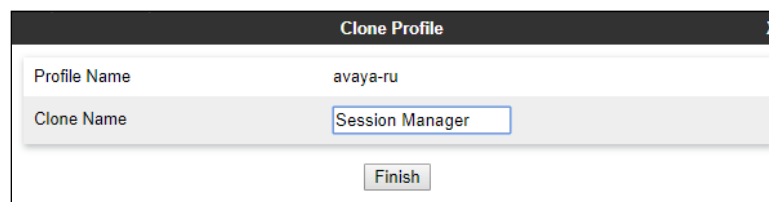
7.2.1 Server Interworking – Session Manager

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 **Configuration Profiles → Server Interworking** from the left-hand menu.
2. Select the pre-defined **avaya-ru** profile and click the **Clone** button.



3. Enter profile name: (e.g., **Session Manager**), and click **Finish**.



- The new Session Manager profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.

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

On the left, a sidebar menu lists various configuration options under "Configuration Profiles", including "Domain DoS", "Server Interworking" (highlighted in red), "Media Forking", "Routing", "Topology Hiding", "Signaling Manipulation", "URI Groups", "SNMP Traps", "Time of Day Rules", "FGDN Groups", and "Reverse Proxy Policy".

The main content area is titled "Interworking Profiles: Session Manager". It features a list of profiles on the left: "cs2100", "avaya-ru", and "Session Manager" (highlighted in red). An "Add" button is located above the list. To the right of the list, there are buttons for "Rename", "Clone", and "Delete".

The "Session Manager" profile is selected, and its configuration is displayed in a tabbed interface. The tabs are "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of configuration parameters:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

5. The **General** screen will open.

- Uncheck **T.38 Support**.
- All other options can be left with default values, and click **Finish**.

The screenshot shows a dialog box titled "Editing Profile: Session Manager" with a close button (X) in the top right corner. The "General" tab is selected. The dialog contains the following settings:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input 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 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

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

6. On the **Privacy, URI Manipulation, Header Manipulation** windows as, select **Finish** to accept default values.
7. On the **Advanced** window, configure;
 - **Record Routes**: choose **Both Sides**.
 - **Include End Point IP for Context Lookup**: choose **Yes**.
 - **Has Remote SBC**: choose **Yes**.

The screenshot shows the 'Editing Profile: Session Manager' window with the following configuration options:

- Record Routes**: Radio buttons for None, Single Side, Both Sides (selected), Dialog-Initiate Only (Single Side), and Dialog-Initiate Only (Both Sides).
- Include End Point IP for Context Lookup**: Checkmark (checked).
- Extensions**: Dropdown menu showing 'Avaya'.
- Diversion Manipulation**: Checkmark (unchecked).
- Diversion Condition**: Dropdown menu showing 'None'.
- Diversion Header URI**: Text input field.
- Has Remote SBC**: Checkmark (checked).
- Route Response on Via Port**: Checkmark (unchecked).
- Relay INVITE Replace for SIPREC**: Checkmark (unchecked).
- MOBX Re-INVITE Handling**: Checkmark (unchecked).
- DTMF**: Section header.
- DTMF Support**: Radio buttons for None (selected), SIP Notify, RFC 2833 Relay & SIP Notify, SIP Info, RFC 2833 Relay & SIP Info, and Inband.
- Finish**: Button at the bottom.

7.2.2 Server Interworking – AAPT

Repeat the steps shown in **Section 7.2.1** to add an Interworking Profile for the connection to AAPT via the public network, with the following changes:

1. Click **Add** to add a new profile, enter **AAPT** then click **Next** (not shown)
2. The **General** screen will open:
 - Uncheck **T.38 Support**.
 - All other options can be left as default.
 - Click **Next**.
 - The **Privacy/DTMF**, **SIP Timers/Transport Timers** screens will open (not shown), accept default values for all the screens by clicking **Next**.

The screenshot shows a dialog box titled "Editing Profile: AAPT" with a close button (X) in the top right corner. The "General" tab is selected. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None (dropdown menu)
Send Hold	<input 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 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

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

Editing Profile: AAPT

Record Routes

☒ None

☐ Single Side

☐ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☐

Extensions

None

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

Relay INVITE Replace for SIPREC

☐

MOBX Re-INVITE Handling

☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ RFC 2833 Relay & SIP Notify

☐ SIP Info

☐ RFC 2833 Relay & SIP Info

☐ Inband

Finish

7.3 Signaling Manipulation Script

Signaling Manipulation Script **Add-PAI-header** is required to:

- If not existed, add PAI header to SIP requests and responses from/to AAPT SIP Voice
- The PAI header content is copied from From/To headers

Follow below steps to create Signaling Manipulation Script **Add-PAI-header**:

1. Select **Configuration Profiles → Signaling Manipulation** from the left-hand menu
2. Select **Add** and the **Signaling Manipulation Editor** window will open
3. Enter the script name into **Title** (e.g., **Add-PAI-header**)
4. Copy and paste the content in the below text box into the editor, and click **Save**

```
within session "ALL"
{
act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{
    if(exists(%HEADERS["P-Asserted-Identity"][1]))then
    {
        print "P-Asserted-Identity header already exists: ";
    }
    else
    {
        %ToHeader = %HEADERS["To"][1];
        %HEADERS["P-Asserted-Identity"][1] = %ToHeader;
        remove(%HEADERS["P-Asserted-Identity"][1].PARAMS["tag"]);
    }
}

act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{
    if(!exists(%HEADERS["P-Asserted-Identity"][1]))then
    {
        print "P-Asserted-Identity header already exists: ";
    }
    else
    {
        %FromHeader = %HEADERS["From"][1];
        %HEADERS["P-Asserted-Identity"][1] = %FromHeader;
        remove(%HEADERS["P-Asserted-Identity"][1].PARAMS["tag"]);
    }
}
}
```

Device: sbce Alarms Incidents Status Logs Diagnostics Users
Settings Help Log Out

Session Border Controller for Enterprise

EMS Dashboard

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Domain DoS

Server Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy

Policy

Services

Domain Policies

TLS Management

Network & Flows

DMZ Services

Relay

Signaling Manipulation Scripts: Add-PAI-header

Upload

Add

Download

Clone

Delete

Signaling Manipulation Scripts

Add-PAI-header

Click here to add a description.

Signaling Manipulation

```

within session "ALL"
{
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    if(exists(%HEADERS["P-Asserted-Identity"][1]))then
    {
      print "P-Asserted-Identity header already exists: ";
    }
    else
    {
      %ToHeader = %HEADERS["To"][1];
      %HEADERS["P-Asserted-Identity"][1] = %ToHeader;
      remove(%HEADERS["P-Asserted-Identity"][1].PARAMS["tag"]);
    }
  }
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    if(!exists(%HEADERS["P-Asserted-Identity"][1]))then
    {
      print "P-Asserted-Identity header already exists: ";
    }
    else
    {
      %FromHeader = %HEADERS["From"][1];
      %HEADERS["P-Asserted-Identity"][1] = %FromHeader;
      remove(%HEADERS["P-Asserted-Identity"][1].PARAMS["tag"]);
    }
  }
}

```

DNA; Reviewed:
SPOC 9/17/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

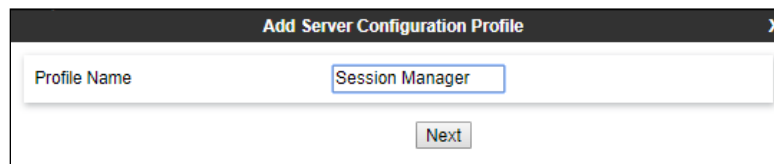
53 of 77
aaptASBCEaura81

7.4 SIP Server Profiles

7.4.1 SIP Server – Session Manager

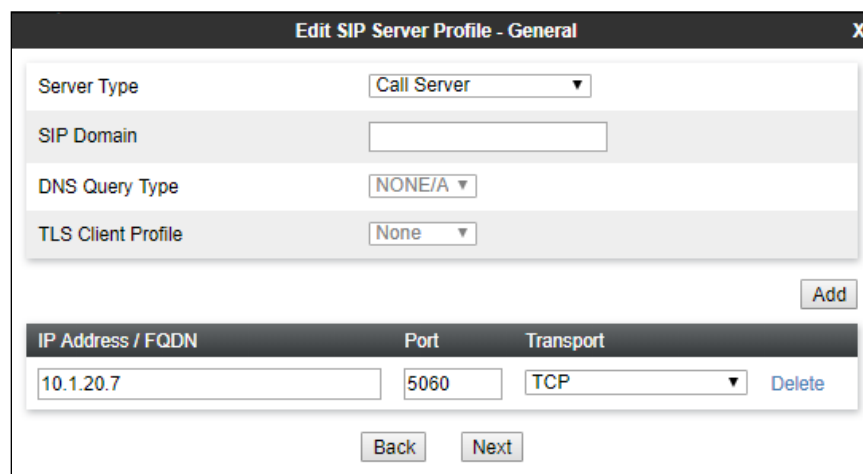
This section defines the SIP Server Profile for the Avaya SBCE connection to Session Manager.

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



The screenshot shows a window titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "Session Manager". Below the input field is a "Next" button.

3. The **Add SIP Server Profile** window will open.
 - Select **Server Type: Call Server**.
 - **IP Address / FQDN: 10.1.20.7** (Session Manager signaling IP Address)
 - **Transport: Select TCP**.
 - **Port: 5060**.
 - Select **Next**.



The screenshot shows a window titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. The window contains several fields and a table.

Server Type	Call Server ▼		
SIP Domain	<input type="text"/>		
DNS Query Type	NONE/A ▼		
TLS Client Profile	None ▼		

Add

IP Address / FQDN	Port	Transport	
10.1.20.7	5060	TCP ▼	Delete

Back **Next**

4. The **Authentication** and **Heartbeat** windows will open (not shown).
 - Select **Next** to accept default values.
5. The **Advanced** window will open.
 - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.1**.
 - Check **Enable Grooming**.
 - Select **Finish**.

Edit SIP Server Profile - Advanced X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Session Manager ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Finish

7.4.2 SIP Server – AAPT

Repeat the steps in **Section 7.4.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to AAPT Trunk Group. AAPT supports both trusted network / static IP address configuration and untrusted network / authentication required configuration.

Step 3 and 5 in below example are for untrusted network configuration only.

1. Select **Add Profile** and enter a Profile Name (e.g., **AAPT**) and select **Next**.
2. On the **General** window (not shown), enter the following.
 - Select **Server Type: Trunk Server**.
 - **IP Address / FQDN: 192.10.26.33** (outbound proxy of AAPT).
 - **Transport:** Select **UDP**.
 - **Port: 5060**.
 - Select **Next**.

IP Address / FQDN	Port	Transport
192.10.26.33	5060	UDP

3. Under Authentication window:
 - Select **Enable Authentication**, if requested by AAPT. Otherwise, skip all the settings in this window.
 - **User Name:** enter Authentication name for outbound proxy.
 - **Realm:** enter SIP realm provided by AAPT.
 - **Password** and **Confirm Password:** enter Password provided by AAPT.

User Name	612 68
Realm (Leave blank to detect from server challenge)	sipvoice.syd.aapt.com.au
Password
Confirm Password

4. Under Heartbeat window:
- Select **Enable Heartbeat**.
 - **Method**: choose **OPTIONS**.
 - **Frequency**: enter **60**.
 - **From URI** and **To URI**: enter **sbc@sipinterop.net**.

Edit SIP Server Profile - Heartbeat

Enable Heartbeat ☒

Method OPTIONS ▼

Frequency seconds

From URI

To URI

Finish

5. Under Registration window:
- Select **Register with All Servers**, if requested by AAPT. Otherwise, skip all the settings in this window.
 - **Refresh Interval**: enter **3600**.
 - **From URI** and **To URI**: enter SIP URI provided by AAPT.

Edit SIP Server Profile - Registration

Register with All Servers ☒

Register with Priority Server ☐

Refresh Interval seconds

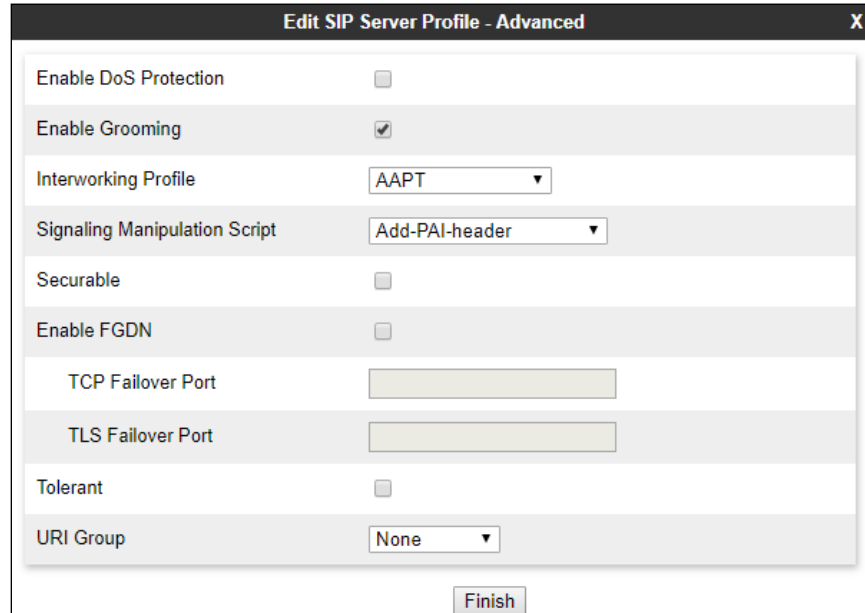
From URI

To URI

Finish

6. Under **Advanced** window:

- Check **Enable Grooming**.
- Select **AAPT** for Interworking Profile
- Select **Add-PAI-header** for the Signaling Manipulation Script (see **Section 7.3**)



The screenshot shows a window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several configuration options, each with a label and a control element:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	AAPT ▼
Signaling Manipulation Script	Add-PAI-header ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

At the bottom right of the window is a "Finish" button.

7.5 Routing Profiles

7.5.1 Routing – To Session Manager

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

1. Select **Configuration 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.
 - **SIP Server Profile** = **Session Manager**.
 - **Next Hop Address**: Verify that the **10.1.20.7:5060 (TCP)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
 - Click on **Finish**.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session Manager	10.1.20.7:5060 (TCP)	None	Delete

7.5.2 Routing – To AAPT

Repeat the steps in **Section 7.5.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to AAPT.

1. On the **Configuration Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **AAPT**).
2. **Load Balancing**: select **Priority**.
3. On the **Next-Hop Address** window (not shown), populate the following fields:
 - **SIP Server Profile = AAPT**.
 - **Next Hop Address**: Verify that the **192.10.26.33:5060** entry from the drop down menu is selected. Also note that the **Transport** field is grayed out.
 - Use default values for the rest of the parameters.
4. Click **Finish**.

Profile : AAPT - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

AAPT

192.10.26.33:5060

None

Delete

Finish

7.6 Topology Hiding

7.6.1 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 network.

1. Select **Configuration 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 all headers are added.
4. Populate the fields as shown below, and click **Finish**.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left-hand side menu is expanded to 'Configuration Profiles', and 'Topology Hiding' is selected. The 'Add' button is visible. The 'Topology Hiding Profiles: Session Manager' window is open, showing a table of headers and their replacement actions.

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

7.6.2 Topology Hiding – AAPT

Repeat the steps in **Section 7.6.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to AAPT.

1. Enter a **Profile Name**: (e.g., **AAPT**).
2. Click on the **Add Header** button repeatedly until all headers are added.
3. Populate the fields as shown below, and click **Finish**.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left-hand side menu is expanded to 'Configuration Profiles', and 'Topology Hiding' is selected. The 'Add' button is visible. The 'Topology Hiding Profiles: AAPT' window is open, showing a table of headers and their replacement actions.

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

7.7 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. Avaya SBCE has pre-defined / default Rules and Policies under Domain Policies. Although the default Rules and Policies are editable, it is highly recommended to clone the Rules and/or Policies before modification as needed. The compliance test was commenced using the default rules and policies without any modification.

7.7.1 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, Avaya SBCE was licensed for 200 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration options, with "Domain Policies" expanded to show "Application Rules". The main content area is titled "Application Rules: default" and features a list of rules on the left and a detailed configuration table on the right. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." The configuration table is as follows:

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Below the table, a "Miscellaneous" section contains the following settings:

CDR Support	Off
RTCP Keep-Alive	No

7.7.2 Border Rules

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

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface, specifically the "Border Rules" configuration page. The top navigation bar and main header are consistent with the previous screenshot. The sidebar menu shows "Domain Policies" expanded to "Border Rules". The main content area is titled "Border Rules: default" and includes a list of rules on the left and a configuration table on the right. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." The configuration table is as follows:

NAT Traversal	
Enable Natting	<input checked="" type="checkbox"/>
Use SIP Published IP	<input checked="" type="checkbox"/>
Use SDP Published IP	<input checked="" type="checkbox"/>

7.7.3 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 in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules (selected), Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, and TLS Management. The main content area has a title 'Media Rules: default-low-med' and an 'Add' button. Below the title is a list of media rules: default-low-med, default-low-med-enc, default-high, default-high-enc, and avaya-low-med-enc. The 'default-low-med' rule is selected. The main configuration area shows a warning: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below the warning are tabs for Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing sections for Audio Encryption, Video Encryption, and Miscellaneous. Audio Encryption has Preferred Formats set to RTP and Interworking checked. Video Encryption has Preferred Formats set to RTP and Interworking checked. Miscellaneous has Capability Negotiation set to off.

7.7.4 Signaling Rules

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

The screenshot shows the 'Signaling Rules: default' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (selected), Charging Rules, End Point Policy Groups, Session Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area has a title 'Signaling Rules: default' and an 'Add' button. Below the title is a list of signaling rules: default and No-Content-Type-Checks. The 'default' rule is selected. The main configuration area shows a warning: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below the warning are tabs for General, Requests, Responses, Request Headers, Response Headers, Signaling QoS, and UCID. The 'General' tab is active, showing sections for Inbound, Outbound, and Content-Type Policy. Inbound has Non-2XX Final Responses set to Allow, Optional Request Headers set to Allow, and Optional Response Headers set to Allow. Outbound has Requests set to Allow, Non-2XX Final Responses set to Allow, Optional Request Headers set to Allow, and Optional Response Headers set to Allow. Content-Type Policy has Enable Content-Type Checks checked, Action set to Allow, Multipart Action set to Allow, and Exception List set to Exception List.

7.7.5 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.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: sbce, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar lists navigation options: System Parameters, Configuration Profiles, Services, and Domain Policies (with sub-items: Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Charging Rules, and End Point Policy Groups). The main content area is titled "Policy Groups: default-low" and features an "Add" button. Below this is a list of policy groups: default-low (highlighted), default-low-enc, default-med, default-med-enc, default-high, default-high-enc, and avaya-def-low-enc. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new group instead." Below the warning is a blue bar with the text "Click here to add a row description." A "Policy Group" form is visible, containing a table with the following data:

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
1	default	default	default-low-med	default-low	default	None	Off

The table also includes a "Summary" button and an "Edit" link for the first row.

7.8 Network & Flows

The **Network & Flows** 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.

7.8.1 Network Management

1. Select **Networks & Flows** → **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.

Device: sbce Alarms 2 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows

Network Management

Interfaces Networks

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
A1	10.1.20.1	255.255.255.0	A1	10.1.20.9, 10.1.20.19	Edit	Delete
A2	135.27.78.1	255.255.255.248	A2	135.27.78.6	Edit	Delete
B1-AAPT	10.239.192.233	255.255.255.248	B1	10.239.192.234, 10.239.192.235	Edit	Delete

7.8.2 Media Interfaces

1. Select **Networks & Flows** 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:** Med_A1.
 - **IP Address:** 10.1.20.9 (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:** Med_B1.
 - **IP Address:** 10.239.192.234 (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.

Device: sbce Alarms 2 Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows
Advanced Options
DMZ Services

Media Interface

Add

Name	Media IP Network	Port Range	
remote access	135.27.78.6 A2 (A2, VLAN 0)	35000 - 40000	Edit Delete
Med_B1	10.239.192.234 B1-AAAPT (B1, VLAN 0)	35000 - 40000	Edit Delete
Med_A1	10.1.20.9 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_A1_RW	10.1.20.19 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_B1_RW	10.239.192.235 B1-AAAPT (B1, VLAN 0)	35000 - 40000	Edit Delete

7.8.3 Signaling Interface

1. Select **Networks & Flows** 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:** 10.1.20.9 (Avaya SBCE A1 address).
 - **TCP Port:** 5060.
 - **UDP Port:** 5060.
 - **TLS Port:** 5060.
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
 - **Name:** Sig_B1.
 - **IP Address:** 10.239.192.234 (Avaya SBCE B1 address).
 - **TCP Port:** 5060.
 - **UDP Port:** 5060.
6. Click **Finish** (not shown). Note that changes to these values require an application restart.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: sbce', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar contains a menu with options like 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', 'Media Interface', 'Signaling Interface' (highlighted in red), 'End Point Flows', 'Session Flows', and 'Advanced Options'. The main content area is titled 'Signaling Interface' and features a table with columns: Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, TLS Profile, and Edit/Delete links. The table lists several interfaces, including 'remote access', 'Sig_B1', 'Sig_A1', 'Sig_A1_RW', and 'Sig_B1_RW'. An 'Add' button is located in the top right corner of the table area.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
remote access	135.27.78.6 A2 (A2, VLAN 0)	5060	5060	5061	ServerA1	Edit	Delete
Sig_B1	10.239.192.234 B1-AAPT (B1, VLAN 0)	5060	5060	---	None	Edit	Delete
Sig_A1	10.1.20.9 A1 (A1, VLAN 0)	5060	5060	5061	ServerA1	Edit	Delete
Sig_A1_RW	10.1.20.19 A1 (A1, VLAN 0)	5060	5060	5061	ServerA1	Edit	Delete
Sig_B1_RW	10.239.192.235 B1-AAPT (B1, VLAN 0)	5060	5060	5061	ServerB1	Edit	Delete

7.8.4 Endpoint Flows – For Session Manager

1. Select **Networks & Flows** → **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.
 - **SIP Server Profile:** Session Manager.
 - **URI Group:** *.
 - **Transport:** *.
 - **Remote Subnet:** *.
 - **Received Interface:** Sig_B1.
 - **Signaling Interface:** Sig_A1.
 - **Media Interface:** Med_A1.
 - **End Point Policy Group:** default-low.
 - **Routing Profile:** AAPT.
 - **Topology Hiding Profile:** Session Manager.
 - Let other values default.
4. Click **Finish**.

Edit Flow: Session Manager	
Flow Name	Session Manager
SIP Server Profile	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_B1
Signaling Interface	Sig_A1
Media Interface	Med_A1
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	AAPT
Topology Hiding Profile	Session Manager
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
Finish	

7.8.5 Endpoint Flows – For AAPT

Repeat step 1 through 4 from Section 7.8.4, with the following changes:

- **Name:** AAPT.
- **SIP Server Profile:** AAPT.
- **URI Group:** *.
- **Transport:** *.
- **Remote Subnet:** *.
- **Received Interface:** Sig_A1.
- **Signaling Interface:** Sig_B1.
- **Media Interface:** Med_B1.
- **End Point Policy Group:** AAPT.
- **Routing Profile:** Session Manager.
- **Topology Hiding Profile:** AAPT.

Edit Flow: AAPT	
Flow Name	AAPT
SIP Server Profile	AAPT
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_A1
Signaling Interface	Sig_B1
Media Interface	Med_B1
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Session Manager
Topology Hiding Profile	AAPT
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
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

Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Monitoring & Logging → Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **B1**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **10000**).
 - 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 displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: sbce, Alarms (2), Incidents, Status, Logs, Diagnostics, and Users. The main header shows 'Session Border Controller for Enterprise' and the AVAYA logo. The left sidebar lists various management options, with 'Monitoring & Logging' expanded to show 'Trace' as the selected option. The main content area is titled 'Trace: sbce' and features a 'Packet Capture' tab. Below this, a 'Packet Capture Configuration' form is visible, containing fields for Status (Ready), Interface (B1), Local Address (10.239.192.234), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). The form includes 'Start Capture' and 'Clear' buttons at the bottom.

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: sbce', 'Alarms 2', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. The left sidebar lists various management options, with 'Monitoring & Logging' expanded and 'Trace' selected. The main content area is titled 'Trace: sbce' and contains a 'Packet Capture' tab and a 'Captures' tab. A blue banner states: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.' Below this is the 'Packet Capture Configuration' section with the following fields: Status (In Progress), Interface (B1), Local Address (10.239.192.234), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). A 'Stop Capture' button is at the bottom right.

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 screenshot shows the same Avaya Session Border Controller for Enterprise web interface, but now the 'Captures' tab is selected. The 'Packet Capture' tab is still visible. A 'Refresh' button is at the top right of the captures table. The table has three columns: 'File Name', 'File Size (bytes)', and 'Last Modified'. It contains one entry: 'test_20190722100412.pcap' with a size of 823,296 bytes and a last modified time of July 22, 2019 10:04:30 AM AEST. A 'Delete' button is next to the file name.

File Name	File Size (bytes)	Last Modified
test_20190722100412.pcap	823,296	July 22, 2019 10:04:30 AM AEST

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 AAPT 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 AAPT network gateway.

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

Device: sbce ▾ Help

Diagnostics

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.

Stop 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: A2	A2 is operating within normal parameters with a full duplex connection at 1Gb/s.
⚙ SBC Link Check: B1	Running...
⊖ Ping: SBC (A1) to Gateway (10.1.20.1)	
⊖ Ping: SBC (A1) to Primary DNS (10.1.20.3)	
⊖ Ping: SBC (A2) to Gateway (135.27.78.1)	
⊖ Ping: SBC (A2) to Primary DNS (10.1.20.3)	

Help

Incident Viewer

Device: sbce ▾ Category: All ▾ Clear Filters Refresh Generate Report

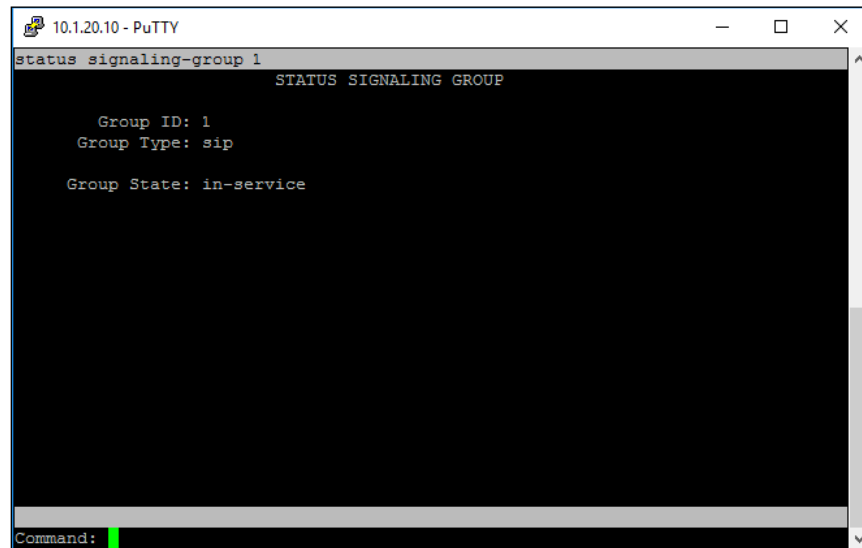
Displaying results 466 to 480 out of 2001.

ID	Device	Date & Time	Category	Type	Cause
781109652777372	sbce	Jul 4, 2019 3:48:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109502774320	sbce	Jul 4, 2019 3:43:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109352774351	sbce	Jul 4, 2019 3:38:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109202773624	sbce	Jul 4, 2019 3:33:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109148109554	sbce	Jul 4, 2019 3:31:36 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
781109148080928	sbce	Jul 4, 2019 3:31:36 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
781109084011121	sbce	Jul 4, 2019 3:29:28 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
781109084006174	sbce	Jul 4, 2019 3:29:28 PM	Policy	Server Heartbeat	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



```
10.1.20.10 - PuTTY
status signaling-group 1

STATUS SIGNALING GROUP

Group ID: 1
Group Type: sip

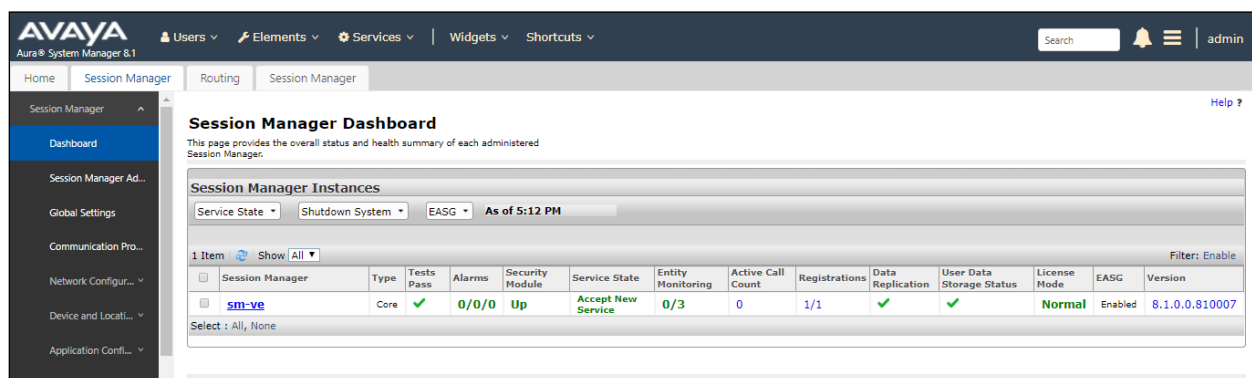
Group State: in-service

Command:
```

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**.



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.

- Clicking on the **0/3** entry in the **Entity Monitoring** column, results in the following display:

Session Manager Dashboard

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

Session Manager Instances

Service State: Shutdown System EASG As of 5:12 PM

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Version
sm-ve	Core	✓	0/0/0	Up	Accept New Service	0/3	0	1/1	✓	✓	Normal	Enabled	8.1.0.0.810007

Select: All, None

Options messages between Avaya SBCE and Session Manager:

EMS - traceSBC - Captured: 6026 Displayed: 1380

10.1.1.20.7

SBC

Time	Source	Destination	Message
15:52:17.181	10.1.1.20.7	10.1.1.20.9	SIP: 200 OK (OPTIONS)
15:52:21.185	10.1.1.20.9	10.1.1.20.7	SIP: sip:sipinterop.net
15:52:21.185	10.1.1.20.9	10.1.1.20.7	SIP: 200 OK (OPTIONS)
15:52:29.197	10.1.1.20.7	10.1.1.20.9	SIP: sip:sipinterop.net
15:52:29.197	10.1.1.20.7	10.1.1.20.9	SIP: 200 OK (OPTIONS)
15:52:42.216	10.1.1.20.9	10.1.1.20.7	SIP: sip:sipinterop.net
15:52:42.216	10.1.1.20.9	10.1.1.20.7	SIP: 200 OK (OPTIONS)
15:53:03.245	10.1.1.20.7	10.1.1.20.9	SIP: sip:sipinterop.net
15:53:03.245	10.1.1.20.7	10.1.1.20.9	SIP: 200 OK (OPTIONS)
15:53:16.264	10.1.1.20.9	10.1.1.20.7	SIP: sip:sipinterop.net
15:53:17.264	10.1.1.20.9	10.1.1.20.7	SIP: 200 OK (OPTIONS)
15:53:18.265	10.1.1.20.7	10.1.1.20.9	SIP: sip:10.1.20.9
15:53:18.266	10.1.1.20.7	10.1.1.20.9	SIP: 200 OK (OPTIONS)
15:53:24.275	10.1.1.20.9	10.1.1.20.7	SIP: sip:sipinterop.net
15:53:24.275	10.1.1.20.9	10.1.1.20.7	SIP: 200 OK (OPTIONS)

8.4 Telephony Services

- 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.
- Verify basic call functions such as hold, transfer, and conference.
- Verify the use of DTMF signaling.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, and Avaya Session Border Control for Enterprise 8.0 can be configured to interoperate successfully with AAPT SIP Voice SIP Trunking service. This solution allows enterprise users access to the PSTN using the AAPT SIP Voice SIP Trunking service connection. Please refer to **Section 2** for exceptions.

10. Additional References

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

- [1] *Deploying Avaya Aura® Communication Manager in Virtualized Environment R8.1*, Jun 2019
- [2] *Administering Avaya Aura® Communication Manager R8.1*, Jun 2019
- [3] *Upgrading Avaya Aura® Communication Manager R8.1*, Jun 2019
- [4] *Deploying Avaya Aura® System Manager in Virtualized Environment Release 8.1*, Jun 2019
- [5] *Upgrading Avaya Aura® System Manager to Release 8.1*, Jun 2019
- [6] *Administering Avaya Aura® System Manager Release 8.1*, Jun 2019
- [7] *Deploying Avaya Aura® Session Manager in Virtualized Environment Release 8.1*, Jun 2019
- [8] *Upgrading Avaya Aura® Session Manager Release 8.1*, Jun 2019
- [9] *Administering Avaya Aura® Session Manager Release 8.1*, Jun 2019
- [10] *Deploying Avaya Session Border Controller for Enterprise Release 8.0*, Mar 2019
- [11] *Upgrading Avaya Session Border Controller for Enterprise Release 8.0*, Feb 2019
- [12] *Administering Avaya Session Border Controller for Enterprise Release 8.0*, Feb 2018
- [13] *Deploying and Updating Avaya Aura Media Server Appliance Release 8.0*, Mar 2019
- [14] *Implementing and Administering Avaya Aura Media Server Release 8.0*, Apr 2019
- [15] *Deploying and Upgrading Avaya G450 Branch Gateway Release 8.1*, Jun 2019
- [16] *Administering Avaya G450 Branch Gateway Release 8.1*, Jun 2019
- [17] *Deploying Avaya Aura® Messaging using VMware® in the Virtualized Environment*, Mar 2019
- [18] *Administering Avaya Aura® Messaging*, Mar 2019
- [19] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©2019 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.