



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 Telstra Enterprise 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 the Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.0 when used to connect the Telstra Enterprise SIP Trunking Service available from Telstra (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. The Avaya Session Border Controller for Enterprise 8.0 is the point of connection between the Enterprise and the Telstra 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.

Telstra 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	9
5.	Configure Avaya Aura® Communication Manager	10
5.1	System-Parameters Customer-Options	10
5.2	System-Parameters Features	11
5.3	Dial Plan.....	12
5.4	IP Node Names.....	13
5.5	IP Interface for Procr.....	13
5.6	IP Network Regions	14
5.7	IP Codec Parameters	16
5.8	SIP Trunks.....	17
5.8.1	Signaling Group.....	17
5.8.2	Trunk Group.....	18
5.9	Calling Party Information.....	22
5.10	Incoming Call Handling Treatment.....	22
5.11	Outbound Routing.....	23
5.12	Avaya G450 Media Gateway Provisioning.....	25
5.13	Avaya Aura® Media Server Provisioning	26
5.14	Save Communication Manager Translations	27
6.	Configure Avaya Aura® Session Manager	28
6.1	Configure SIP Domain	29
6.2	Configure Locations.....	29
6.3	Configure SIP Entities.....	30
6.3.1	Configure Session Manager SIP Entity	30
6.3.2	Configure Communication Manager SIP Entity.....	31
6.3.3	Configure Avaya SBCE SIP Entity	32
6.4	Configure Entity Links.....	32
6.4.1	Configure Entity Link to Communication Manager.....	33
6.4.2	Configure Entity Link for Avaya SBCE.....	34
6.5	Configure Routing Policies	34
6.5.1	Configure Routing Policy for Communication Manager.....	34
6.5.2	Configure Routing Policy for Avaya SBCE	35
6.6	Configure Dial Patterns.....	36
7.	Configure Avaya Session Border Controller for Enterprise	38
7.1	Device Management – Status.....	39
7.2	Server Interworking Profiles	40
7.2.1	Server Interworking – Session Manager.....	40

7.2.2	Server Interworking – Telstra	44
7.3	Signaling Manipulation Script	46
7.4	SIP Server Profiles	47
7.4.1	SIP Server – Session Manager	47
7.4.2	SIP Server – Telstra	49
7.5	Routing Profiles.....	56
7.5.1	Routing – To Session Manager.....	56
7.5.2	Routing – To Telstra	57
7.6	Topology Hiding Profiles.....	58
7.6.1	Topology Hiding – Session Manager	58
7.6.2	Topology Hiding – Telstra.....	58
7.7	Domain Policies	59
7.7.1	Application Rules.....	59
7.7.2	Border Rules	60
7.7.3	Media Rules	60
7.7.4	Signaling Rules	61
7.7.5	Endpoint Policy Groups.....	61
7.8	Networks & Flows	62
7.8.1	Network Management.....	62
7.8.2	Media Interfaces.....	62
7.8.3	Signaling Interface	63
7.8.4	Endpoint Flows – For Session Manager	64
7.8.5	Endpoint Flows – For Telstra	65
8.	Verification Steps.....	67
8.1	Avaya Session Border Controller for Enterprise.....	67
8.2	Avaya Aura® Communication Manager	70
8.3	Avaya Aura® Session Manager Status	70
8.4	Telephony Services	71
9.	Conclusion	72
10.	Additional References.....	73

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 the Avaya Session Border Controller for Enterprise (Avaya SBCE) when used to connect the Telstra Enterprise SIP Trunking Service available from Telstra (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. The Avaya SBCE is the point of connection between the Enterprise and the Telstra Enterprise SIP Trunking Service, and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The enterprise SIP Trunking Service available from Telstra is one of the SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The Telstra Enterprise 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 the 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, the Avaya SBCE is also configured as a SIP entity and has associated SIP entity links assigned within the 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 the Avaya SBCE utilizing TCP transport. The Avaya SBCE is connected to the Telstra Enterprise SIP Trunking Service, and the SIP signaling connectivity from the Avaya SBCE toward Telstra uses TCP.

The 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 Telstra Enterprise 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.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Telstra Enterprise SIP Trunking Service and the Customer Premises Equipment (CPE) containing Communication Manager, Session Manager, and the 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 did not include 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.

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

- SIP trunking (incoming and outgoing calls)
- 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
- EC500 – call extending to mobile
- G.711A, G.729A and G.722-64K high definition audio
- Network Call Redirection
- Basic Call Center scenarios
- Faxing (G.711 pass-through)
- Remote Worker scenarios
- Telstra Enterprise Trunking Redundancy

2.2 Test Results

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

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

- **Faxing** – Telstra Enterprise Trunking Service only supports FAX G.711 pass-through mode.
- **Call Transfer** – Upon blind transfer completion, PSTN transferee user does not receive ring back tone treatment, and keeps receiving hold treatment (with music if enabled). This may be resolved by disabling “Music (or Silence) on Transferred Trunk Calls” in Communication Manager system parameter.
- **Call Transfer** – one-way voice when Avaya One-X Communicator H.323 phone does blind transfer Telstra TIPT phone to Avaya 96x1 SIP phone. This issue is specific to the use case where Avaya One-X Communicator H.323 phone is the transferor and TIPT is the transferee. The SIP trace was showing that at the latest step of media renegotiation, audio stream was supposed to be between Telstra SBC and Avaya SBCE. However, the actual incoming RTP packets were from the Telstra TIPT phone, while Avaya SBCE is properly sending RTP packets to Telstra SBC. This audio issue might be eliminated by toggling the SIP signaling group settings of “Direct IP to IP Audio Connection” or “Initial IP-IP Direct Media” in Communication Manager.
- **Network Call Redirection** – SIP Network Call Redirection (NCR) using SIP 302 is not supported in the trunk used for testing, but NCR using REFER was successfully tested.
- **EC500 service with Confirmed Answer enabled** - With Initial IP-IP Direct Media enabled on the SIP signaling group toward to Telstra Enterprise Trunking, the EC500 call leg is established with two-way voice as soon as EC500 user answers the call on mobile without pressing a key to confirm. 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.
- **IP-IP Direct Media (Call Shuffling)** – During testing with Telstra Emergency Simulator (an IVR system), it is observed that when Avaya Communication Manager sends SIP reINVITE (without SDP) to do call shuffling, Telstra SIP Enterprise Trunking Service terminates the call. Enabling **Initial IP-IP Direct Media** and **H.323 Station Outgoing Direct Media** helped to eliminate the call shuffling (reINVITE without SDP), and thus helped to avoid the call drop.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>
- **Telstra:** Customers should contact their Telstra Business representative or follow the support links available on <http://telstra.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 VMware ESXi 6.0.
- Avaya Aura® Session Manager running on VMware ESXi 6.0.
- Avaya Aura® System Manager running on VMware ESXi 6.0.
- Avaya Aura® Messaging running on VMware ESXi 6.0.
- Avaya G450 Media Gateway.
- Avaya Aura® Media Server running on VMware ESXi 6.0. The Media Server can act as a media gateway Gxxx series.
- Avaya IP phones are represented with Avaya 96x1 Series IP Telephones running SIP software.
- Avaya one-X® Communicator 6.2
- Avaya Equinox for Windows 3.5
- The Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Telstra Enterprise SIP Trunking Service and the enterprise internal network.
- Outbound calls were originated from a phone provisioned on Avaya Aura® Communication Manager. Signaling passed from Avaya Aura® Communication Manager and Avaya Aura® Session Manager to the Avaya SBCE, before being sent to the Telecom network for termination.
- Inbound calls were sent from Telstra, through the Avaya SBCE to the Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Communication Manager terminated the call to the appropriate phone extension.

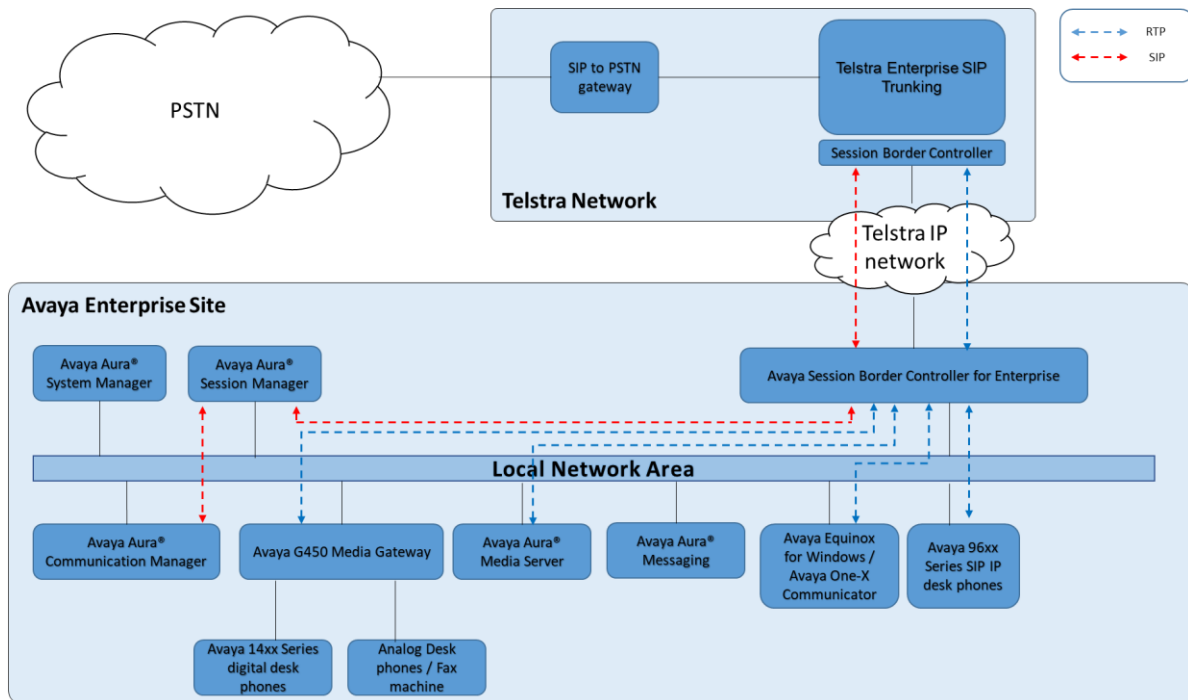


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura Communication Manager 8.1 SP1	8.1.0.0.890-25393
Avaya Aura Session Manager 8.1	8.1.0.0.810007
Avaya Aura System Manager 8.1	Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.9814
Avaya Aura Messaging 7.1	7.1.0.0.532
Avaya Session Border Controller for Enterprise 8.0	8.0.0.0-19-16991
Avaya Media Gateway G450	g450_sw_41_9_0
Avaya Aura Media Server 8.0	8.0.0.205
Avaya One-X Communicator 6.2	6.2.13.2
Avaya Equinox for Windows 3.5	3.5.7.30.1
Avaya One-X Agent H323 2.5.8	2.5.60313.0
Avaya 96x1 series – SIP phone	7.1.5
Service Provider – Telstra	
Telstra Enterprise SIP Trunking Service	BroadWorks 21.x

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 that has been configured earlier. The actual Communication Manager SAT commands, System Manager Web UI and 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.
 - 5-digit extensions with a **Call Type** of **ext** beginning with:
 - The digits **506** for Communication Manager extensions (which is assigned by Telstra 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
119	4	udp						
13	6	udp						
1300	10	udp						
506	5	ext						
6	1	fac						
9	1	fac						
*	3	dac						
#	4	fac						

5.4 IP Node Names

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

Follow the steps shown below:

- Enter the **change node-names ip** command, and add 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 parameters.

display ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		
		Target socket load: 4800
Enable Interface? y	Allow H.323 Endpoints? y	
	Allow H.248 Gateways? y	
Network Region: 1	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.com**. 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.com
Name: telstra            Stub Network Region: n
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
Codec Set: 1              Inter-region IP-IP Direct Audio: yes
                           IP Audio Hairpinning? n
  UDP Port Min: 2048
  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 Avaya G450 Media Gateway, the Avaya Media Server, IP/SIP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields.

display ip-network-region 1										Page	4 of	20
Source Region: 1 Inter Network Region Connection Management										I		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												

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

display ip-interface procr										Page	1 of	2
IP INTERFACES												
Type: PROCR												
19660										Target socket load:		
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 Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

```

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

```

5.7 IP Codec Parameters

Follow the steps shown below:

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

```

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: G.729       n              2             20
                                4:
                                5:
                                6:
                                7:

```


2. On **Page 2** of the ip-codec-set form, set **FAX Mode** to **pass-through**.

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. In the below example, the same signaling group and trunk group are administered for both trunking to SIP Service Provider, and Avaya SIP client access. However, it is possible to administer separate signaling groups and trunk groups to better tweaking the settings as required.

5.8.1 Signaling Group

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.com**. 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.com		
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	

5.8.2 Trunk Group

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** – enter **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 **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: Telstra-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 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **900** seconds was used.

```

display trunk-group 1                                     Page 2 of 4
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 30000

  SCCAN? n                          Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 900

  Disconnect Supervision - In? y Out? y

  XOIP Treatment: auto              Delay Call Setup When Accessed Via IGAR? n

```

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.

Note – Telstra Enterprise SIP Trunking service screens the calling party number for valid DID numbers. At the time of testing, 9-digit number format (without leading 0) of calling party number is sent to Telstra network for validation. Setting the **Numbering Format** field to public may result in “+” to be inserted to the calling number, and may result in call origination failure.

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: private
                                                         UI Treatment: service-provider

                                                         Replace Restricted Numbers? y
                                                         Replace Unavailable Numbers? y

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

On **Page 4**, setting the **Network Call Redirection** field to **n** disables use of the SIP REFER message for call transfer, re-INVITE will be used instead. Setting the **Network Call Redirection** flag to **y** enables use of the SIP REFER message for call transfer. In compliance test, both mechanisms were tested and successful.

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.

PROTOCOL VARIATIONS

```
Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
Send Transferring Party Information? y
Network Call Redirection? n

Send Diversion Header? y
Support Request History? n
Telephone Event Payload Type: 101

Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
Accept Redirect to Blank User Destination? y
Enable Q-SIP? n

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 SIP service provider. It is used to authenticate the caller.

In the sample configuration, the 3539506xx DID numbers provided for testing were assigned to the extensions 506xx. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

display private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	506	1	3539	9	Total Administered: 1
					Maximum Entries: 540

5.10 Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. The DID numbers sent by Telstra 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/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	9	3539		4	

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.

display 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
119	4	udp						
13	6	udp						
1300	10	udp						
1800	10	udp						
1902	10	udp						
500	5	ext						
506	5	ext						
6	1	fac						
9	1	fac						
*	3	dac						
#	4	fac						

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

display feature-access-codes		Page 1 of 12	
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialing List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code:			
Answer Back Access Code:			
Attendant Access Code:			
Auto Alternate Routing (AAR) Access Code:			
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2: 6	
Automatic Callback Activation: #002		Deactivation: #003	
Call Forwarding Activation Busy/DA: #004 All: #005		Deactivation: #006	
Call Forwarding Enhanced Status: #007 Act: #008		Deactivation: #009	
Call Park Access Code: #010			
Call Pickup Access Code: #011			
CAS Remote Hold/Answer Hold-Unhold Access Code: #012			
CDR Account Code Access Code: #013			
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation:		Deactivation:	
Contact Closure Open Code:		Close Code:	

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance testing. All dialed strings are mapped to route pattern **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	Max	Route Pattern	Call Type	Node Num	ANI Req'd			
000	3	3	1	pubu		n			
0011	10	18	1	pubu		n			
03	10	10	1	pubu		n			
04	10	10	1	pubu		n			
13	6	6	1	pubu		n			
1300	10	10	1	pubu		n			
1800	10	10	1	pubu		n			
1902	10	10	1	pubu		n			
50000	5	5	1	pubu		n			
*67	11	16	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 SIP 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:** **unk-unk**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.8.2**.

display route-pattern 1													Page	1 of	4									
Pattern Number: 1													Pattern Name: sip											
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: 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 n													n			rest			unk-unk			none		
2: y y y y y n													n			rest						none		
3: y y y y y n													n			rest						none		
4: y y y y y n													n			rest						none		

5.12 Avaya G450 Media Gateway Provisioning

In the reference configuration, a G450 Media Gateways is provisioned. The G450 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
```

5.13 Avaya Aura® Media Server Provisioning

In the reference configuration, an Avaya Aura® Media Server is provisioned. The Media Server is located in the Main site 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
```

5.14 Save Communication Manager Translations

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

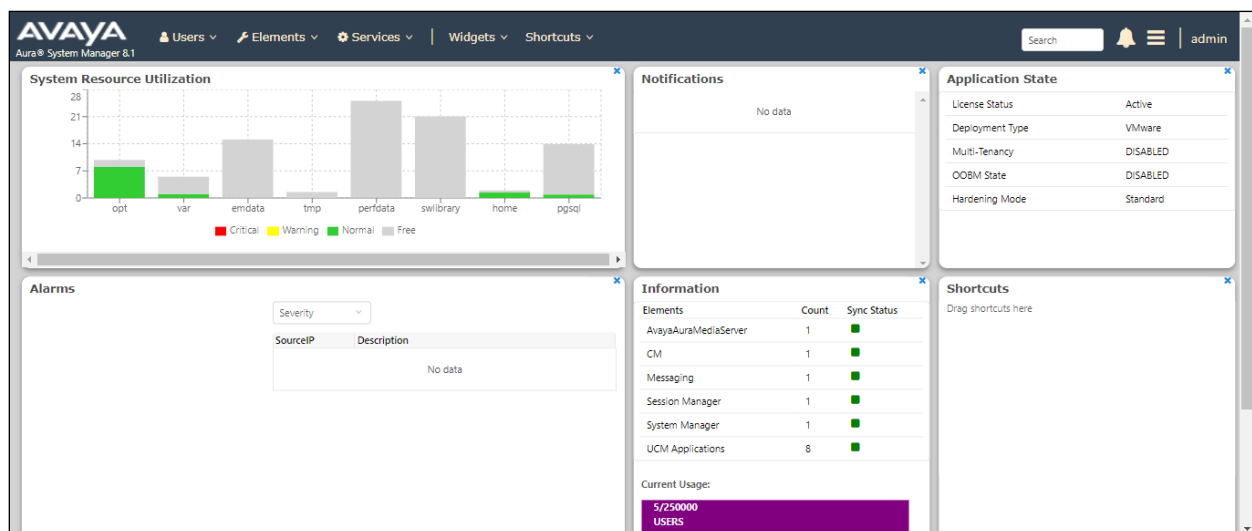
6. Configure Avaya Aura® Session Manager

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 the Avaya SBCE
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager server to be managed by System Manager

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

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



6.1 Configure SIP Domain

Follow the steps shown below:

1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.com** 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.com** is shown.
 - **Type:** Verify **sip** is selected.
 - **Notes:** Add a brief description.
3. Click **Commit** to save (not shown).

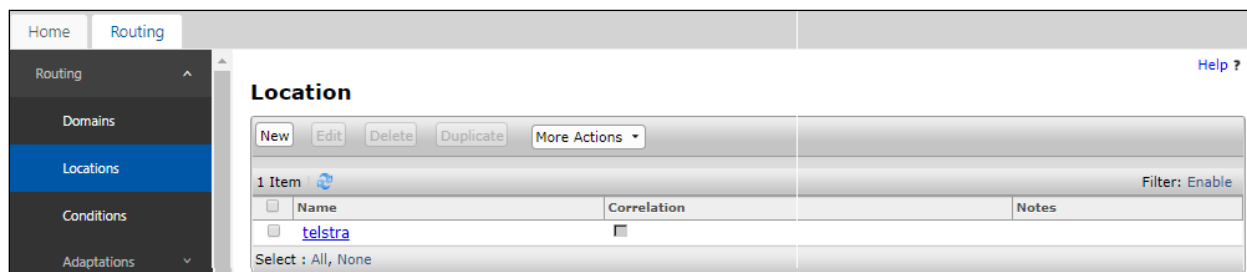


6.2 Configure Locations

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

Follow the steps shown below:

1. Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.
 - **Name:** Enter a descriptive name for the Location (e.g., **telstra**).
 - **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** – Optionally, 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 **Telstra**.
 - **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 'Routing' expanded and 'SIP Entities' selected. The main area is titled 'SIP Entity Details' with a 'General' tab. Fields include: Name (sm-ve), IP Address (10.1.20.7), SIP FQDN (sm-ve-sm100.sipinterop.net), Type (Session Manager), Notes, Location (telstra), Outbound Proxy, Time Zone (Australia/Melbourne), Minimum TLS Version (Use Global Setting), and Credential name. The Monitoring section shows SIP Link Monitoring and CRLF Keep Alive Monitoring both set to 'Use Session Manager Configuration'. Buttons for 'Commit' and 'Cancel' are at the top right.

6.3.2 Configure Communication Manager SIP Entity

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g. **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 **Telstra** administered in **Section 6.2**.
 - **Time Zone** – Select the time zone in which Communication Manager resides.
 - In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.
3. Click on **Commit**.

Home Routing

SIP Entity Details

Commit Cancel Help ?

General

* Name: cm-ve

* FQDN or IP Address: 10.1.20.10

Type: CM

Notes:

Adaptation:

Location: telstra

Time Zone: Australia/Melbourne

* 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

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

6.3.3 Configure Avaya SBCE SIP Entity

Repeat the steps in **Section 6.3.1** 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 **telstra** (**Section 6.2**).

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar has a navigation menu with 'SIP Entities' selected. The main content area is divided into three sections: 'General', 'Loop Detection', and 'Monitoring'. The 'General' section contains fields for Name (sbce_A1), FQDN or IP Address (10.1.20.9), Type (SIP Trunk), Notes, Adaptation, Location (telstra), Time Zone (Australia/Melbourne), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name, Securable (checkbox), and Call Detail Recording (egress). The 'Loop Detection' section contains fields for Loop Detection Mode (On), Loop Count Threshold (5), and Loop Detection Interval (in msec) (200). The 'Monitoring' section contains fields for SIP Link Monitoring (Use Session Manager Configuration) and CRLF Keep Alive Monitoring (Use Session Manager Configuration). There are 'Commit' and 'Cancel' buttons at the top right.

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 6.3.3**
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.4.1 Configure Entity Link to Communication Manager

Follow the steps shown below:

1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name (or have it created automatically) for this link to Communication Manager (e.g., **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**.

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 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 6.3.3** for the Avaya SBCE entity (e.g., **SBCE_A1**).
- **SIP Entity 2 Port** - Enter **5060**

The screenshot shows the 'Entity Links' configuration page. On the left is a navigation pane with options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), and Time Ranges. The main area is titled 'Entity Links' and contains 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 row shows: Name: sm-ve_sbce_A1_5060_T, SIP Entity 1: sm-ve, Protocol: TCP, Port: 5060, SIP Entity 2: sbce_A1, Port: 5060, DNS Override: unchecked, Connection Policy: trusted, Deny New Service: unchecked, and Notes: empty. Below the table is a 'Select: All, None' dropdown. At the top right of the main area is a 'Help ?' link. At the bottom right are 'Commit' and 'Cancel' buttons.

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 Telstra.

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 Telstra 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 for a policy named 'cm-ve'. The left sidebar contains a menu with 'Routing Policies' selected. The main content area has a 'General' tab. Under 'General', there is a 'Name' field with 'cm-ve', a 'Disabled' checkbox, a 'Retries' field with '0', and a 'Notes' field. 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 6.3.3** for the Avaya SBCE entity (e.g., **sbce_A1**).

The screenshot shows the 'Routing Policy Details' page for a policy named 'to sbce'. The left sidebar contains a menu with 'Routing Policies' selected. The main content area has a 'General' tab. Under 'General', there is a 'Name' field with 'to sbce', a 'Disabled' checkbox, a 'Retries' field with '0', and a 'Notes' field. 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: 'sbce_A1' with FQDN or IP Address '10.1.20.9' and Type 'SIP Trunk'. At the bottom, there is a 'Time of Day' section.

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 Telstra and vice versa. Dial Patterns define which routing policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click **New** button in the right pane (not shown).

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

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

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

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

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

The first example shows that 10-digit dialed numbers starting with 0353950 use route policy **to sbce** as defined in **Section 6.5.2**

Home

Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Dial Patterns

Help ?

Dial Pattern Details

Commit

Cancel

General

* Pattern:

0353950xxx

* Min:

10

* Max:

10

Emergency Call:

☐

SIP Domain:

-ALL-

Notes:

10 digit TIPT phones

Add

Remove

1 Item

Filter: Enable

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

Select : All, None

The second example shows that 9-digit pattern that start with 3539506 is used for inbound calls from Telstra to DID numbers on Avaya Aura® Communication Manager.

Home Routing

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 35395060x

* Min: 9

* Max: 9

Emergency Call: ☐

SIP Domain: -ALL-

Notes: DID Range

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

Select : All, None

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

Home Routing

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

1 Item

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

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

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

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

As described in Section 3, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (10.1.20.9), with access to the **Telstra** site. The connection to Telstra uses the Avaya SBCE public interface B1 (IP address 10.2.2.30). 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, the Avaya logo is in red, and below it, the text "Session Border Controller for Enterprise" is displayed. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field containing "username". Below the input field is a "Continue" button. Further down, there is a "WELCOME TO AVAYA SBC" message, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Below this is a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, it says "© 2011 - 2019 Avaya Inc. All rights reserved."

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page, similar to the previous one, but with an additional "Password:" label and a password input field containing "*****". Below the password field is a "Log In" button. The rest of the page content, including the Avaya logo, "Session Border Controller for Enterprise" text, disclaimer, consent statement, and 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**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Device: sbce', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main content area is divided into three sections:

- EMS Dashboard** (left sidebar):
 - Device Management
 - Backup/Restore
 - System Parameters
 - DoS / DDoS
 - Scrubber
 - User Agents
 - Configuration Profiles
 - Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging
- Dashboard** (center):
 - Information** table:

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** (right):
 - EMS
 - sbce
- Incidents (past 24 hours)** (bottom right):
 - 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.

The screenshot shows the 'Device Management' page. The top navigation bar is the same as the dashboard. The main content area is divided into two sections:

- EMS Dashboard** (left sidebar):
 - Device Management
 - Backup/Restore
 - System Parameters
 - DoS / DDoS
 - Scrubber
 - User Agents
 - Configuration Profiles
- Device Management** (center):
 - Tabs: **Devices**, Updates, SSL VPN, Licensing, Key Bundles
 - Devices** table:

Device Name	Management IP	Version	Status	
sbce	10.1.20.8	8.0.0.0-19-16991	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

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

System Information: sbce

General Configuration

Appliance Name	sbce
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions	100
Requested: 100	
Advanced Sessions	100
Requested: 100	
Scopia Video Sessions	0
Requested: 0	
CES Sessions	0
Requested: 0	
Transcoding Sessions	0
Requested: 0	
CLID	---
Encryption	<input checked="" type="checkbox"/>
Available: Yes	

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
10.2.2.30	10.2.2.30	255.255.255.128	10.2.2.1	B1

DNS Configuration

Primary DNS	10.86.113.20
Secondary DNS	10.86.114.20
DNS Location	DMZ
DNS Client IP	10.2.2.30

Management IP(s)

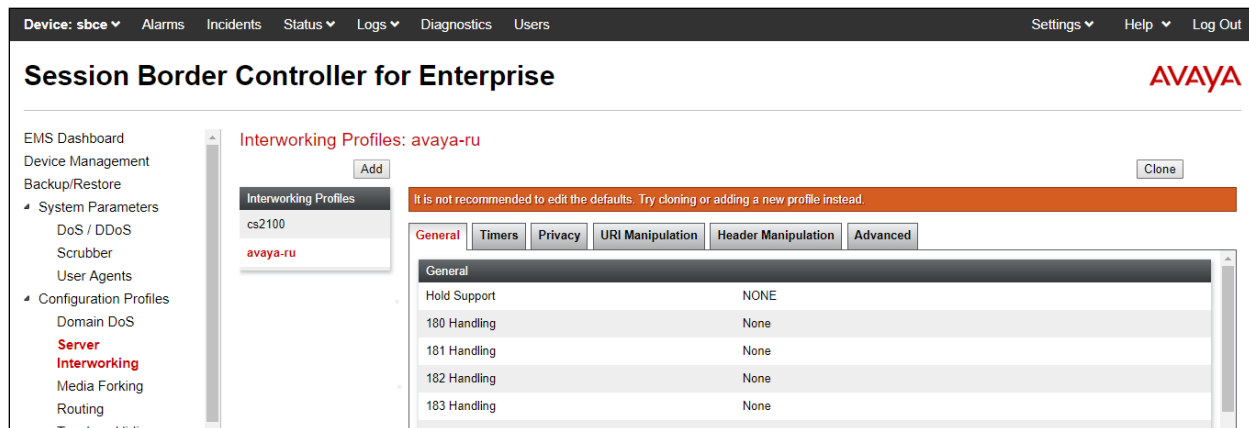
IP #1 (IPv4)	10.1.20.8
--------------	-----------

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.

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



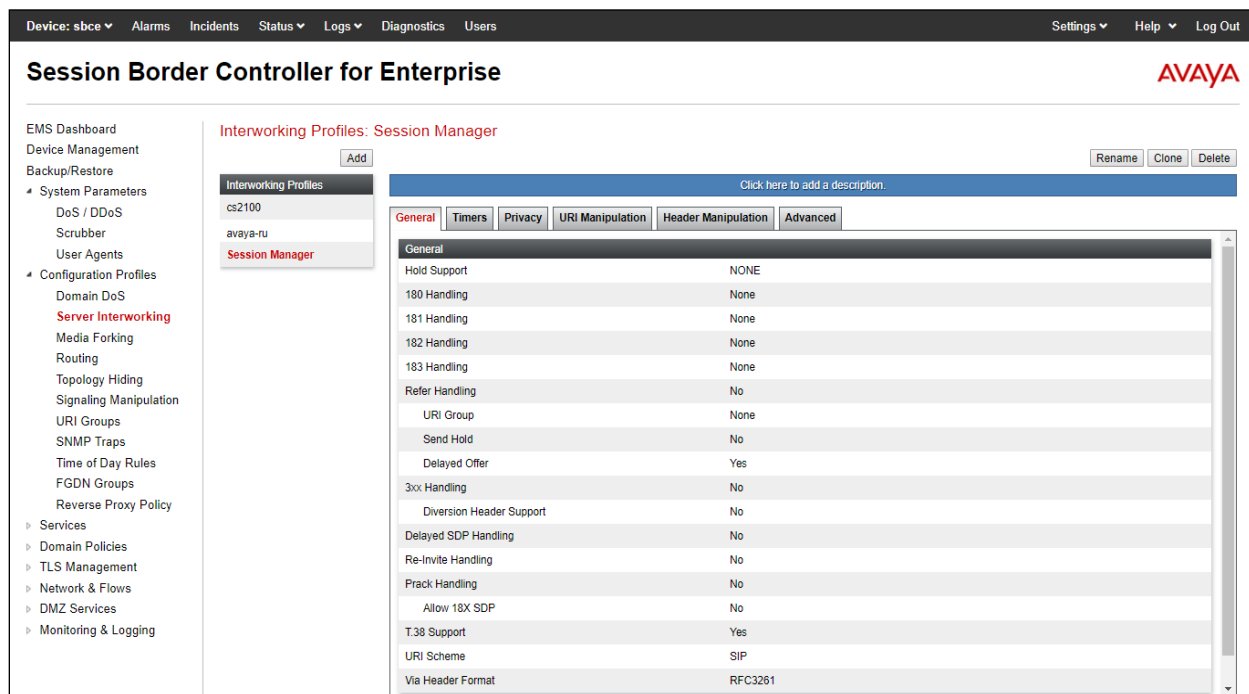
3. Enter profile name: (e.g., **Session Manager**), and click **Finish**.

Clone Profile X

Profile Name: avaya-ru

Clone Name:

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



5. The **General** screen will open.
 - Check **T38 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 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)
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 checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

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

6. Leave settings in the **Timer, Privacy, URI Manipulation, Header Manipulation** windows as default.

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 set to 'Avaya'.
- Diversion Manipulation:** Checkmark (unchecked).
- Diversion Condition:** Dropdown menu set to '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 – Telstra

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

1. Click **Add** to add a new profile, enter **Telstra** then click **Next** (not shown)
2. The **General** screen will open:
 - All 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: Telstra" with a close button (X) in the top right corner. The "General" tab is selected. The dialog contains various settings for SIP interworking, most of which are set to their default values. 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

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

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

Editing Profile: Telstra

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

A Signaling Manipulation Script is required to:

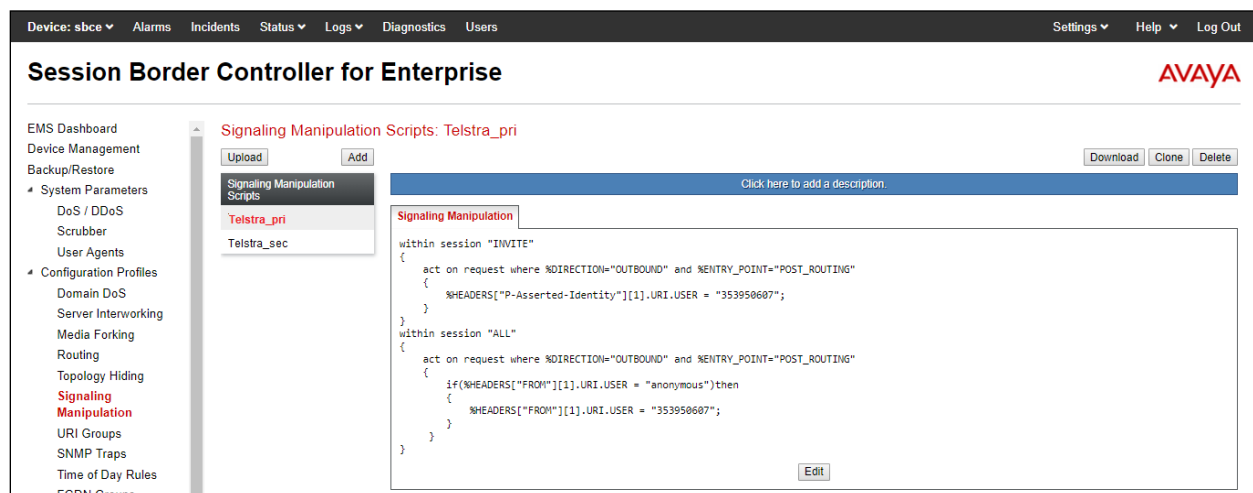
- Add the primary Trunk Pilot number into the PAI Header on outgoing calls
- If the FROM header is 'anonymous', then re-write the FROM with the primary Trunk Pilot number

Follow below steps to create Signaling Manipulation Script **Telstra_pri**. This script will be used in SIP Server configuration for Telstra primary server.

1. Select **Configuration Profiles → Signaling Manipulation** from the left-hand menu (not shown)
2. Select **Add** and the **Signaling Manipulation Editor** window will open (not shown)
3. Enter the script name into **Title** (e.g., **Telstra_Pri**) (not shown)
4. Copy and paste the content in the below text box into the editor, and click **Save**

```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
    %HEADERS["P-Asserted-Identity"][1].URI.USER = "353950607";
}
}

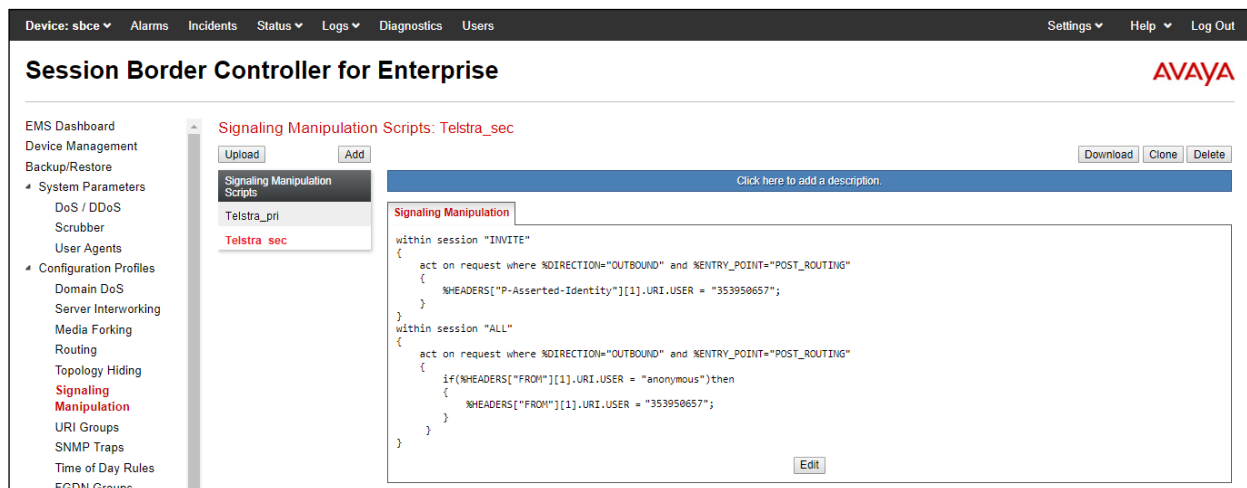
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
    if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
    {
        %HEADERS["FROM"][1].URI.USER = "353950607";
    }
}
}
```



Repeat the above steps to create Signaling Manipulation Script **Telstra_sec**. This script will be used in SIP Server configuration for Telstra secondary server.

```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.USER = "353950657";
}
}

within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
{
%HEADERS["FROM"][1].URI.USER = "353950657";
}
}
}
}
```

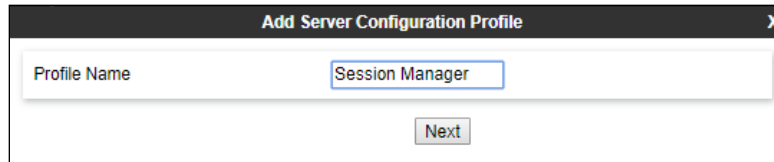


7.4 SIP Server Profiles

7.4.1 SIP Server – Session Manager

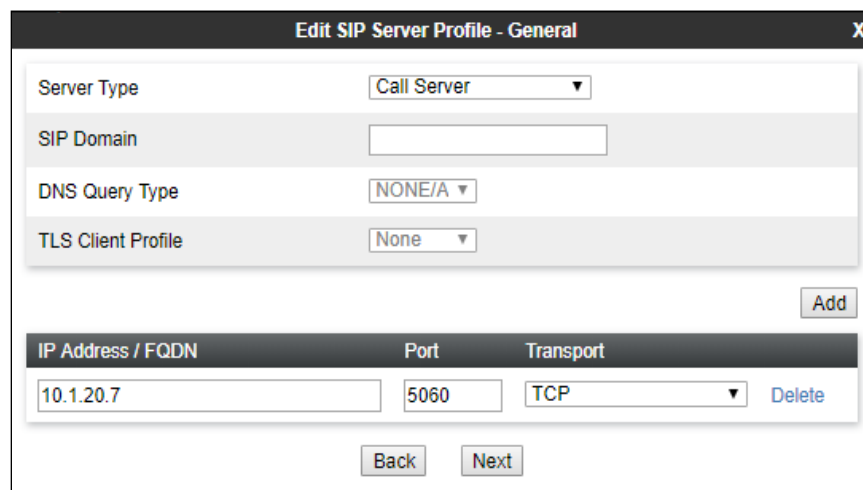
This section defines the SIP Server Profile for the Avaya SBCE connection to Session Manager.

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 dialog box titled "Add Server Configuration Profile" has a close button (X) in the top right corner. It contains a text field labeled "Profile Name" with the value "Session Manager" entered. Below the text 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 dialog box titled "Edit SIP Server Profile - General" has a close button (X) in the top right corner. It contains several fields and a table:

- Server Type:** Call Server (dropdown menu)
- SIP Domain:** (empty text field)
- DNS Query Type:** NONE/A (dropdown menu)
- TLS Client Profile:** None (dropdown menu)
- Add:** button

IP Address / FQDN	Port	Transport	
10.1.20.7	5060	TCP	Delete

At the bottom of the dialog box are "Back" and "Next" buttons.

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**.
 - Select **Finish**.

7.4.2 SIP Server – Telstra

Telstra provides two trunk groups for Enterprise SIP Trunking Service. These two trunk groups are connected to two outbound proxies. Telstra Enterprise SIP Trunking Service requires authentication so Enterprise Trunk credentials must be provided by Telstra.

7.4.2.1 Telstra primary

Repeat the steps in **Section 7.4.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Telstra Trunk Group 1.

1. Select **Add Profile** and enter a Profile Name (e.g., **Telstra_pri**) and select **Next**.

2. On the **General** window (not shown), enter the following.
 - Select **Server Type: Trunk Server**.
 - **IP Address / FQDN: sbc-cw.ipvs.net** (outbound proxy 1 of Telstra)
 - **Transport:** Select **TCP**.
 - **Port: 5060**
 - Select **Next**

Edit SIP Server Profile - General

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
sbc-cw.ipvs.net	5060	TCP

Delete

Back Next

3. Under **Authentication** window:

- Select **Enable Authentication**
- **User Name**: enter Authentication name for outbound proxy 1
- **Realm**: leave blank
- **Password** and **Confirm Password**: enter Password provided by Telstra

Add SIP Server Profile - Authentication

Enable Authentication: ☒

User Name: N3312101R

Realm: (Leave blank to detect from server challenge)

Password:

Confirm Password:

Back Next

4. Under **Heartbeat** window:
- Select **Enable Heartbeat**
 - **Method**: choose **OPTIONS**
 - **Frequency**: enter **600**
 - **From URI** and **To URI**: enter SIP URI provided by Telstra, e.g., **0353950607@sipconn.test1.com**

Add Server Configuration Profile - Heartbeat X

Enable Heartbeat ☒

Method **OPTIONS** ▼

Frequency 600 seconds

From URI 0353950607@sipconn.test1

To URI 0353950607@sipconn.test1

Back Next

5. Under **Registration** window:
- Select **Register with All Servers**
 - **Refresh Interval**: enter **600**
 - **From URI** and **To URI**: enter SIP URI provided by Telstra, e.g., **353950607@sipconn.test1.com**

Add SIP Server Profile - Registration X

Register with All Servers ☒

Register with Priority Server ☐

Refresh Interval 600 seconds

From URI 353950607@sipconn.test1

To URI 353950607@sipconn.test1

Back Next

6. Under **Advanced** window:

- Select **Telstra** for Interworking Profile
- Select **Telstra_pri** for Signaling Manipulation Script (see **Section 7.3**)

The screenshot shows a configuration window titled "Add SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings:

- Enable DoS Protection: ☐
- Enable Grooming: ☒
- Interworking Profile:
- Signaling Manipulation Script:
- Securable: ☐
- Enable FGDN: ☐
- TCP Failover Port:
- TLS Failover Port:
- Tolerant: ☐
- URI Group:

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

7.4.2.2 Telstra secondary

Repeat the steps in **Section 7.4.2.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Telstra Trunk Group 2.

1. Select **Add Profile** and enter a Profile Name (e.g., **Telstra_sec**) and select **Next**.

The screenshot shows a configuration window titled "Add Server Configuration Profile" with a close button (X) in the top right corner. The window contains a single text input field for the "Profile Name" with the value "Telstra_sec". Below the input field is a "Next" button.

2. On the **General** window (not shown), enter the following.
 - Select **Server Type: Trunk Server**.
 - **IP Address / FQDN: sbc-cw2.ipvs.net** (outbound proxy 2 of Telstra)
 - **Transport: Select TCP**.
 - **Port: 5060**
 - Select **Next** (not shown)

Edit SIP Server Profile - General

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
sbc-cw2.ipvs.net	5060	TCP

Delete

Back Next

3. Under **Authentication** window:
 - Select **Enable Authentication**
 - **User Name:** enter Authentication name for outbound proxy 2
 - **Realm:** leave blank
 - **Password and Confirm Password:** enter Password provided by Telstra

Add SIP Server Profile - Authentication

Enable Authentication: ☒

User Name: N3312202R

Realm: (Leave blank to detect from server challenge)

Password:

Confirm Password:

Back Next

4. Under **Heartbeat** window:
 - Select **Enable Heartbeat**
 - **Method**: choose **OPTIONS**
 - **Frequency**: enter **600**
 - **From URI** and **To URI**: enter SIP URI provided by Telstra, e.g., **35950657@sipconn.test1.com**

The screenshot shows a window titled "Add Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat**: A checkbox that is checked.
- Method**: A dropdown menu set to "OPTIONS".
- Frequency**: A text input field containing "600" followed by the unit "seconds".
- From URI**: A text input field containing "0353950657@sipconn.test1".
- To URI**: A text input field containing "0353950657@sipconn.test1".
- At the bottom, there are "Back" and "Next" buttons.

5. Under Registration window:
 - Select **Register with All Servers**
 - **Refresh Interval**: enter **600**
 - **From URI** and **To URI**: enter SIP URI provided by Telstra, e.g., **35950657@sipconn.test1.com**

The screenshot shows a window titled "Add SIP Server Profile - Registration". It contains the following fields and controls:

- Register with All Servers**: A checkbox that is checked.
- Register with Priority Server**: A checkbox that is unchecked.
- Refresh Interval**: A text input field containing "600" followed by the unit "seconds".
- From URI**: A text input field containing "353950657@sipconn.test1".
- To URI**: A text input field containing "353950657@sipconn.test1".
- At the bottom, there are "Back" and "Next" buttons.

6. Under **Advanced** window:

- Select **Telstra** for Interworking Profile
- Select **Telstra_sec** for Signaling Manipulation Script (see **Section 7.3**)

The screenshot shows a configuration window titled "Add SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Telstra ▼
Signaling Manipulation Script	Telstra_sec ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None ▼

At the bottom of the window, there are two buttons: "Back" and "Finish".

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

7.5.2 Routing – To Telstra

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

1. On the **Configuration Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Telstra**).
2. **Load Balancing**: select **Round-Robin**
3. On the **Next-Hop Address** window (not shown), populate the following fields:
 - **SIP Server Profile = Telstra_pri**.
 - **Next Hop Address**: Verify that the **sbc-cw.ipvs.net:5060** entry from the drop down menu is selected.
 - Click **Add** to enter another record for **Telstra_sec**. Verify that the entry for **sbc-cw2.ipvs.net:5060** is selected from the **Next Hop Address** drop down menu.
 - Use default values for the rest of the parameters.
4. Click **Finish**.

Profile : Telstra - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Round-Robin	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
0				Telstra_pr	sbc-cw.ipvs.net:5060	None	Delete
0				Telstra_se	sbc-cw2.ipvs.net:5060	None	Delete

Finish

7.6 Topology Hiding Profiles

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 networks.

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** (not shown).
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until the **Refer-To** header is added (not shown).
4. Populate the fields as shown below, and click **Finish**.

The screenshot shows 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 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, Domain DoS, Server Interworking, Media Forking, Routing, Topology Hiding (highlighted), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy, and Policy. The main content area is titled "Topology Hiding Profiles: Session Manager" and features an "Add" button. Below this, a list of profiles is shown: default, cisco_th_profile, Telstra, and Session Manager (highlighted). The "Session Manager" profile is selected, and its configuration is displayed in a table. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The headers listed are From, Via, Request-Line, Referred-By, Record-Route, SDP, To, and Refer-To. The criteria for all headers is "IP/Domain". The replace actions are "Overwrite" for From, Request-Line, To, and Refer-To, and "Auto" for Via, Referred-By, and Record-Route. The overwrite values are "sipinterop.com" for From, Request-Line, To, and Refer-To, and "---" for Via, Referred-By, and Record-Route. An "Edit" button is located at the bottom right of the table.

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

7.6.2 Topology Hiding – Telstra

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

1. Enter a **Profile Name:** (e.g., **Telstra**).
2. Click on the **Add Header** button repeatedly until **Refer-To** header is added (not shown).
3. Populate the fields as shown below, and click **Finish**. Note that **sipconn.test1.com** is the domain used.

Device: sbce
Alarms
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
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups

Topology Hiding Profiles: Telstra
Add

Topology Hiding Profiles
default
cisco_th_profile
Telstra
Session Manager

Click here to add a description.
Rename
Clone
Delete

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
From	Domain	Overwrite	sipconn.test1.com
Request-Line	Domain	Overwrite	sipconn.test1.com
Referred-By	Domain	Overwrite	sipconn.test1.com
SDP	Domain	Overwrite	sipconn.test1.com
To	Domain	Overwrite	sipconn.test1.com
Refer-To	Domain	Overwrite	sipconn.test1.com

Edit

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

Device: sbce
Alarms
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
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Charging Rules

Application Rules: default
Add

Application Rules
default
default-trunk
default-subscriber-low
default-subscriber-high
default-server-low
default-server-high

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

Application Rule

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"/>		

Miscellaneous
CDR Support
Off
RTCP Keep-Alive
No

DNA; Reviewed:
SPOC 8/31/2019

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

59 of 74
tASBCEaura8

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 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 displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules (highlighted), Media Rules, Security Rules, Signaling Rules, and Charging Rules. The main content area is titled "Border Rules: default" and features an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, the "NAT Traversal" tab is active, showing a table with three rows: "Enable Natting" (checked), "Use SIP Published IP" (checked), and "Use SDP Published IP" (checked). An "Edit" button is located at the bottom right of the table.

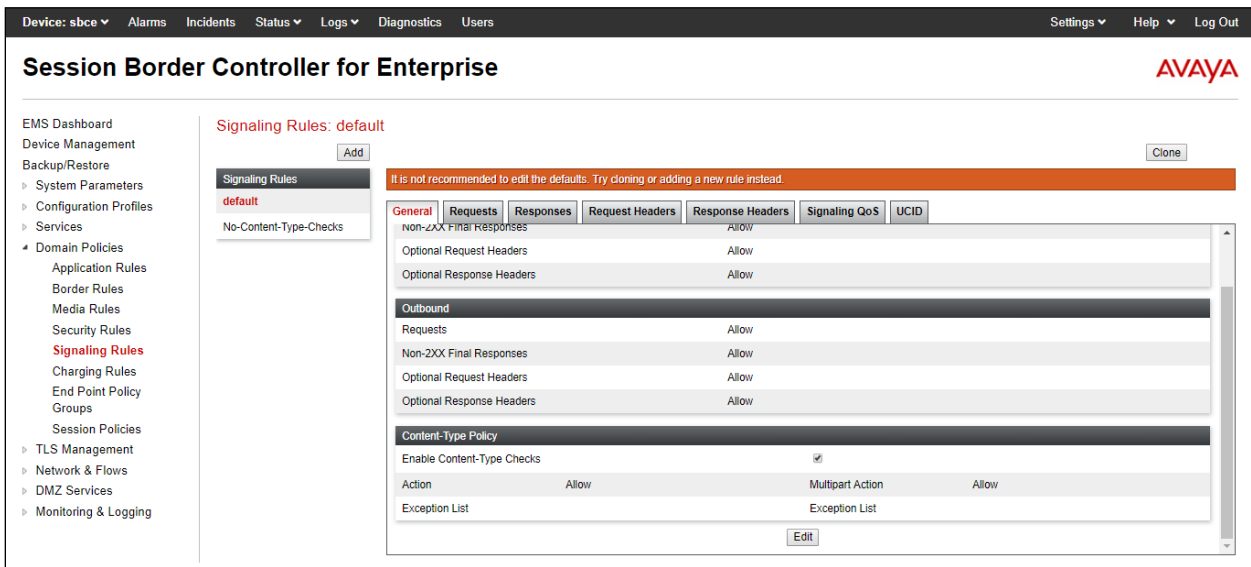
7.7.3 Media Rules

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 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 displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules (highlighted), Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, TLS Management, and Network & Flows. The main content area is titled "Media Rules: default-low-med" and features an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, the "Encryption" tab is active, showing a table with three rows: "Audio Encryption" (RTP), "Video Encryption" (RTP), and "Miscellaneous" (Capability Negotiation). The "Audio Encryption" and "Video Encryption" rows have a checked box in the "Interworking" column. The "Miscellaneous" row has an unchecked box in the "Capability Negotiation" column. An "Edit" button is located at the bottom right of the table.

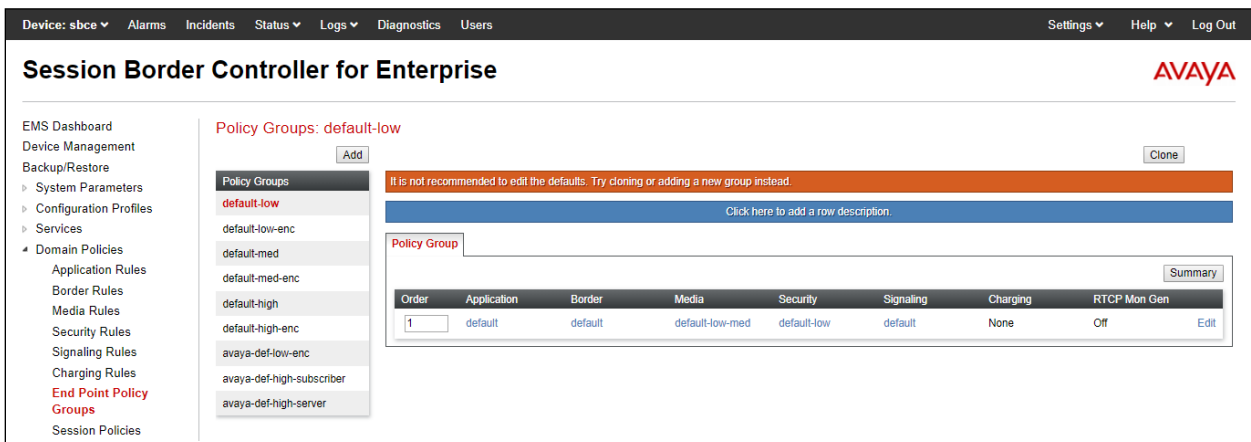
7.7.4 Signaling Rules

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



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.



7.8 Networks & Flows

The **Network & Flows** menus allow 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 **Network & 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.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1	10.1.20.1	255.255.255.0	A1	10.1.20.9	Edit Delete
B1	10.2.2.1	255.255.255.128	B1	10.2.2.30, 10.2.2.31	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:** Media_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: Media_B1_trunking.**
 - **IP Address: 10.2.2.30** (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.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: sbce', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists navigation options: 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', 'Media Interface', and 'Signaling Interface'. The main content area is titled 'Media Interface' and contains a table with the following data:

Name	Media IP Network	Port Range	
Media_A1	10.1.20.9 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Media_B1_trunking	10.2.2.30 B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

7.8.3 Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
 - **Name: Signaling_A1.**
 - **IP Address: 10.1.20.9** (Avaya SBCE A1 address).
 - **TCP Port: 5060.**
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
 - **Name: Signaling_B1_trunking.**
 - **IP Address: 10.2.2.30** (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 web interface. The top navigation bar includes 'Device: sbce', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists navigation options: 'EMS Dashboard', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Network & Flows', 'Network Management', 'Media Interface', and 'Signaling Interface'. The main content area is titled 'Signaling Interface' and contains a table with the following data:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Signaling_B1_trunking	10.2.2.30 B1 (B1, VLAN 0)	5060	---	---	None	Edit Delete
Signaling_A1	10.1.20.9 A1 (A1, VLAN 0)	5060	---	---	None	Edit Delete

7.8.4 Endpoint Flows – For Session Manager

1. Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
 - **Name:** Session Manager.
 - **SIP Server Profile:** Session Manager.
 - **URI Group:** *
 - **Transport:** *
 - **Remote Subnet:** *
 - **Received Interface:** Signaling_B1_trunking.
 - **Signaling Interface:** Signaling_A1.
 - **Media Interface:** Media_A1.
 - **End Point Policy Group:** default-low.
 - **Routing Profile:** Telstra.
 - **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	Signaling_B1_trunking ▼
Signaling Interface	Signaling_A1 ▼
Media Interface	Media_A1 ▼
Secondary Media Interface	None ▼
End Point Policy Group	default-low ▼
Routing Profile	Telstra ▼
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 Telstra

7.8.5.1 Telstra primary

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

- **Name:** Telstra_pri.
- **SIP Server Profile:** Telstra_pri.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Signaling_A1.
- **Signaling Interface:** Signaling_B1_trunking.
- **Media Interface:** Media_B1_trunking
- **End Point Policy Group:** default_low.
- **Routing Profile:** Session Manager.
- **Topology Hiding Profile:** Telstra.

Field	Value
Flow Name	Telstra_pri
SIP Server Profile	Telstra_pri
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signaling_A1
Signaling Interface	Signaling_B1_trunking
Media Interface	Media_B1_trunking
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Session Manager
Topology Hiding Profile	Telstra
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

Finish

7.8.5.2 Telstra secondary

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

- **Name:** Telstra_sec.
- **SIP Server Profile:** Telstra_sec.
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Signaling_A1.
- **Signaling Interface:** Signaling_B1_trunking.
- **Media Interface:** Media_B1_trunking
- **End Point Policy Group:** default_low.
- **Routing Profile:** Session Manager.
- **Topology Hiding Profile:** Telstra.

Edit Flow: Telstra_sec	
Flow Name	Telstra_sec
SIP Server Profile	Telstra_sec
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signaling_A1
Signaling Interface	Signaling_B1_trunking
Media Interface	Media_B1_trunking
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Session Manager
Topology Hiding Profile	Telstra
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:

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **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 SBCE web interface. At the top, a navigation bar includes links for Device: sbce, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left sidebar lists various management options, with "Trace" highlighted under the "Monitoring & Logging" section. The main content area is titled "Trace: sbce" and features two tabs: "Packet Capture" (active) and "Captures". Below the tabs is a "Packet Capture Configuration" form. The form includes fields for Status (Ready), Interface (B1), Local Address (10.2.2.30), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). At the bottom of the form are "Start Capture" and "Clear" buttons.

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

Device: sbceAlarmsIncidentsStatus▼Logs▼DiagnosticsUsersSettings▼Help▼Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & LoggingSNMPSyslog ManagementDebuggingTraceLog CollectionDoS LearningCDR Adjunct

Trace: sbce

Packet CaptureCaptures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

StatusIn Progress

InterfaceB1▼

Local Address10.2.2.30▼:▼

Remote Address*▼

ProtocolAll▼

Maximum Number of Packets to Capture10000

Capture Filenametest.pcap

Stop Capture

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.

Device: sbceAlarmsIncidentsStatus▼Logs▼DiagnosticsUsersSettings▼Help▼Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & LoggingSNMPSyslog ManagementDebuggingTraceLog CollectionDoS LearningCDR Adjunct

Trace: sbce

Packet CaptureCaptures

Last Modified▼Descending▼SortResetRefresh

File Name	File Size (bytes)	Last Modified	
test_20190626005256.pcap	0	June 26, 2019 12:53:44 AM AEST	Delete
7_11_10_20190620042416.pcap	1,404,928	June 20, 2019 4:24:48 AM AEST	Delete
7_11_10_20190620042158.pcap	1,634,304	June 20, 2019 4:22:33 AM AEST	Delete
7_11_10_20190620034451.pcap	1,708,032	June 20, 2019 3:45:24 AM AEST	Delete
7_11_7_20190620030743.pcap	888,832	June 20, 2019 3:08:30 AM AEST	Delete
7_11_6_20190620030358.pcap	2,631,069	June 20, 2019 3:04:35 AM AEST	Delete
7_11_5_20190620030232.pcap	2,269,184	June 20, 2019 3:03:18 AM AEST	Delete
7_6_1_20190619220514.pcap	1,601,536	June 19, 2019 10:06:02 PM AEST	Delete
7_5_10_20190619204901.pcap	2,547,435	June 19, 2019 8:50:00 PM AEST	Delete
7_5_9_20190619204613.pcap	815,104	June 19, 2019 8:46:50 PM AEST	Delete

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 Telstra Enterprise SIP Trunk Service and the customer SIP PABX is the Avaya SBCE. 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 Telstra network gateway.

• Ping from the SBC to the Session Manager.

DNA; Reviewed:
SPOC 8/31/2019

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

68 of 74
tASBCEaura8

- Ping from the Telstra 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: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
🔄 Ping: SBC (A1) to Gateway (10.1.20.1)	Running...
✗ Ping: SBC (A1) to Primary DNS (10.86.113.20)	
✗ Ping: SBC (A1) to Secondary DNS (10.86.114.20)	
✗ Ping: SBC (B1) to Gateway (10.2.2.1)	
✗ Ping: SBC (B1) to Primary DNS (10.86.113.20)	
✗ Ping: SBC (B1) to Secondary DNS (10.86.114.20)	

Help

Incident Viewer

Device: All
Category: Policy
Clear Filters
Refresh
Generate Report

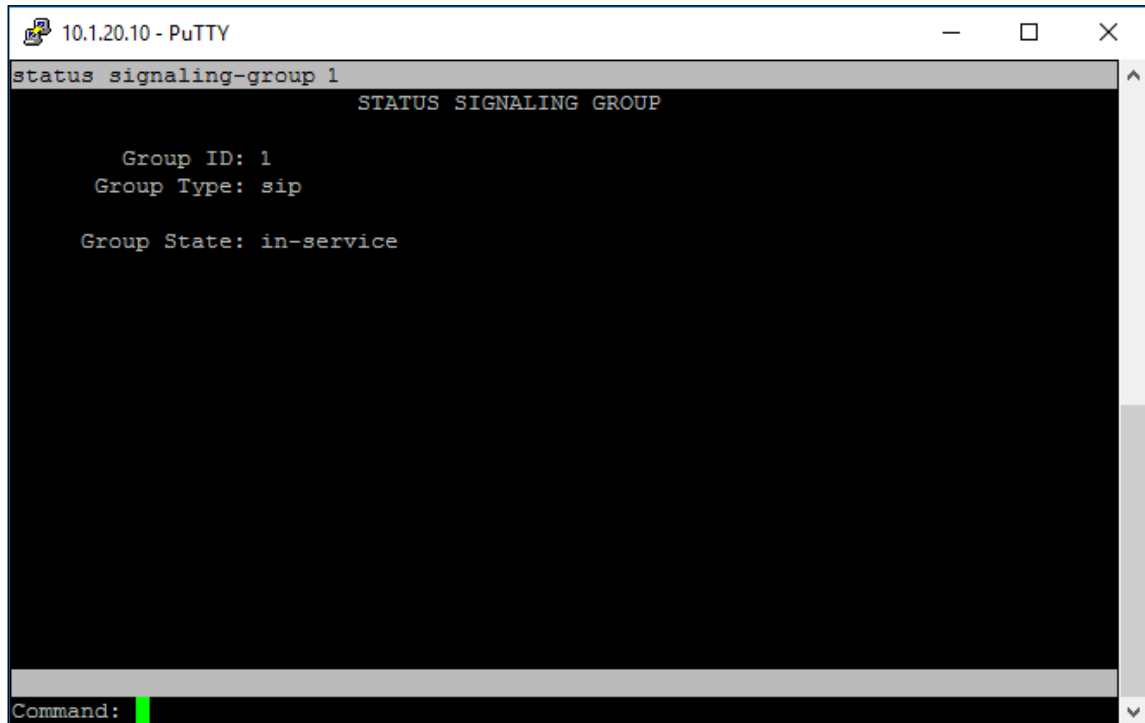
Displaying results 916 to 930 out of 948.

ID	Device	Date & Time	Category	Type	Cause
780506957835142	sbce	Jun 20, 2019 4:58:35 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
780506778123518	sbce	Jun 20, 2019 4:52:36 PM	Policy	Server Registration	Registration Successful, Server is UP
780506778096938	sbce	Jun 20, 2019 4:52:36 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
780506672856136	sbce	Jun 20, 2019 4:49:05 PM	Policy	Server Registration	Registration Successful, Server is UP
780506672833931	sbce	Jun 20, 2019 4:49:05 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

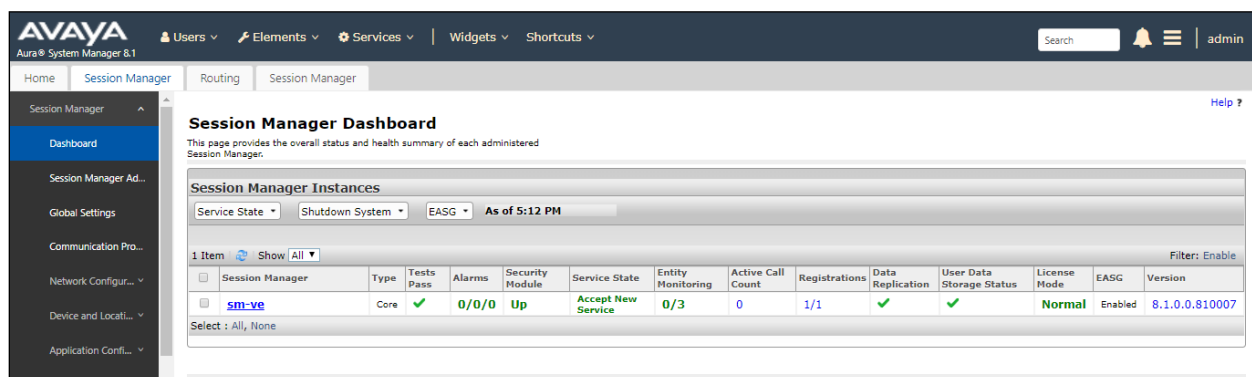
Group State: in-service

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**.



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

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

Select: All, None

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

Session Manager 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

8.4 Telephony Services

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

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 8.1, Avaya Aura® Session Manager 8.1, and Avaya Session Border Control for Enterprise 8.0 can be configured to interoperate successfully with Telstra Enterprise SIP Trunking service. This solution allows enterprise users access to the PSTN using the Telstra Enterprise SIP Trunking service connection. Please refer to **Section 2.2** for exceptions.

10. Additional References

This section references the documentation relevant to these Application Notes. 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.