



Avaya Solution & Interoperability Test Lab

Application Notes for OneAccess-Telstra SIP Business SIP Trunking with Avaya Aura® Communication Manager 7.1.2, Avaya Aura® Session Manager 7.1.2 and Avaya Session Border Controller for Enterprise 7.2.1 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Aura® Communication Manager Release 7.1.2 and Avaya Aura® Session Manager 7.1.2 with SIP trunks to the Avaya Session Border Controller for Enterprise 7.2.1 SP1 (Avaya SBCE) when used to connect to the OneAccess-Telstra Business SIP (Australia).

OneAccess-Telstra Business SIP provides PSTN access via SIP trunks between the enterprise and the Telstra Business SIP as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

OneAccess-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 OneAccess test lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1	Interoperability Compliance Testing.....	4
2.2	Test Results	5
2.3	Support	6
3.	Reference Configuration.....	6
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager.....	9
5.1	System-Parameters Customer-Options	9
5.2	System-Parameters Features	10
5.3	Dial Plan.....	12
5.4	IP Node Names.....	12
5.5	IP Interface for Procr.....	13
5.6	IP Network Regions	14
5.7	IP Codec Parameters	17
5.8	SIP Trunks.....	18
5.8.1	Signaling Group.....	18
5.8.2	Trunk Group.....	20
5.9	Calling Party Information.....	23
5.10	Incoming Call Handling Treatment.....	23
5.11	Outbound Routing	24
5.12	Avaya G450 Media Gateway Provisioning	26
5.13	Avaya Aura® Media Server Provisioning.....	28
5.13.1	Signaling Group for Media Server.....	28
5.13.2	Adding Media Server.....	29
5.14	Save Communication Manager Translations.....	29
6.	Configure Avaya Aura® Session Manager	30
6.1	Configure SIP Domain	31
6.2	Configure Locations	32
6.3	Configure SIP Entities.....	33
6.3.1	Configure Session Manager SIP Entity	33
6.3.2	Configure Communication Manager SIP Entity.....	35
6.3.3	Configure Avaya SBCE SIP Entity	36
6.4	Configure Entity Links.....	36
6.4.1	Configure Entity Link to Communication Manager.....	37
6.4.2	Configure Entity Link for Avaya SBCE.....	38
6.5	Configure Routing Policies	38
6.5.1	Configure Routing Policy for Communication Manager.....	38
6.5.2	Configure Routing Policy for Avaya SBCE	39
6.6	Configure Dial Patterns.....	40

7.	Configure Avaya Session Border Controller for Enterprise	43
7.1	System Management – Status	45
7.2	Global Profiles.....	45
7.2.1	Uniform Resource Identifier (URI) Groups.....	45
7.2.2	Server Interworking – Avaya.....	46
7.2.3	Server Interworking – OneAccess	49
7.2.4	Signaling Manipulation – OneAccess.....	51
7.2.5	Server Configuration – Avaya	53
7.2.6	Server Configuration – OneAccess.....	56
7.2.7	Routing – To Avaya.....	59
7.2.8	Routing – To OneAccess	60
7.2.9	Topology Hiding – Avaya	61
7.2.10	Topology Hiding – OneAccess	62
7.2.11	Domain Policies	62
7.2.12	Application Rules.....	62
7.2.13	Border Rules	62
7.2.14	Media Rules	62
7.2.15	Signaling Rules	63
7.2.16	Endpoint Policy Groups.....	63
7.3	Device Specific Settings.....	63
7.3.1	Network Management.....	63
7.3.2	Media Interfaces.....	64
7.3.3	Signaling Interface	65
7.3.4	Endpoint Flows – For Avaya	66
7.3.5	Endpoint Flows – For OneAccess.....	68
8.	Verification Steps.....	70
8.1	Avaya Session Border Controller for Enterprise.....	70
8.2	Avaya Aura® Communication Manager	73
8.3	Avaya Aura® Session Manager Status	74
8.4	Telephony Services	75
9.	Conclusion	75
10.	Additional References.....	75

1. Introduction

These Application Notes illustrate a sample configuration Avaya Aura® Communication Manager Release 7.1.2 and Avaya Aura® Session Manager 7.1.2 with SIP trunks to the Avaya Session Border Controller for Enterprise 7.2.1 (Avaya SBCE) when used to connect to the OneAccess-Telstra Business SIP.

Session Manager 7.1.2 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Communication Manager 7.1.2 is a telephony application server and is the point of connection between the enterprise endpoints and Session Manager 7.1.2. The Avaya SBCE 7.2.1 is the point of connection between Session Manager 7.1.2 and the OneAccess-Telstra Business SIP and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The OneAccess-Telstra Business SIP allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

2. General Test Approach and Test Results

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

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

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

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Session Manager, Communication Manager, the Avaya SBCE, and the OneAccess-Telstra Business SIP.

The compliance testing was based on the Avaya DevConnect Generic SIP Trunk test plan and the Telstra Business SIP Accreditation test plan. The testing covered functionality required for compliance as a solution supported on the OneAccess-Telstra Business SIP. Calls were made to and from the PSTN across the OneAccess-Telstra Business SIP. The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including SIP, H.323, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunks from OneAccess-Telstra Business SIP.
- Outbound PSTN calls from various phone types including SIP, H323, digital and analog telephone at the enterprise. All outbound PSTN calls are routed from the enterprise across the SIP trunks from OneAccess-Telstra Business SIP.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) and Avaya Equinox for Windows soft phones. The 1XC Computer Mode (where 1XC is used for call control as well as audio path) was tested.
- Dialing plans including local, outbound local call, emergency calls.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.729A, G.711A and G.711MU.
- Fax using pass-through mode.
- Media and Early Media transmissions.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound calls.
- User features such as hold and resume, transfer, forward and conference.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.

2.2 Test Results

Interoperability testing of OneAccess-Telstra Business SIP 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.

- **User-Agent header** - As OneAccess SIP NTU requires User-Agent header in the SIP messages sent to it, a Sigma script must be used on Avaya SBCE to insert User-Agent header into SIP messages before Avaya SBCE sends those messages to OneAccess SIP NTU.
- **Contact header** - OneAccess SIP NTU does not accept SIP INVITE which has too long URI in the Contact header. Therefore, a Sigma script must be used on Avaya SBCE to remove unnecessary parameters in the URI of the Contact header before Avaya SBCE sends SIP INVITE to OneAccess SIP NTU.

- **SIP REFER** – OneAccess SIP NTU does not support SIP REFER sent from Avaya, hence Network Call Redirection field of the SIP trunks on the Communication Manager which are used for the connection to OneAccess SIP NTU must be set to **n** (refer to **Section 5.8.2** for details).

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>
- **OneAccess-Telstra Business SIP:** Customers should contact their OneAccess-Telstra representative or follow the support links available on <https://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 5.5.
- Avaya Aura® Session Manager running on VMware ESXi 5.5.
- Avaya Session Border Controller for Enterprise running on VMware ESXi 5.5.
- Avaya Aura® System Manager running on VMware ESXi 5.5.
- Avaya Aura® Messaging running on VMware ESXi 5.5.
- Avaya G450 Media Gateway.
- Avaya Aura® Media Server running on VMware ESXi 5.5. The Media Server can act as a media gateway Gxxx series in providing tones, announcements or music on hold.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running H.323/SIP software.
- Avaya 2400 series digital phone.
- Analog phone.
- Avaya one-X® Communicator 6.2.
- Avaya Equinox™ Experience 3.2.
- OneAccess-Telstra Business SIP provided one trunk group and DID range for this testing is 0285xxx4xx (10 digits). Enterprise network is connected to Telstra network via OneAccess SIP Network Termination Unit (NTU).

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

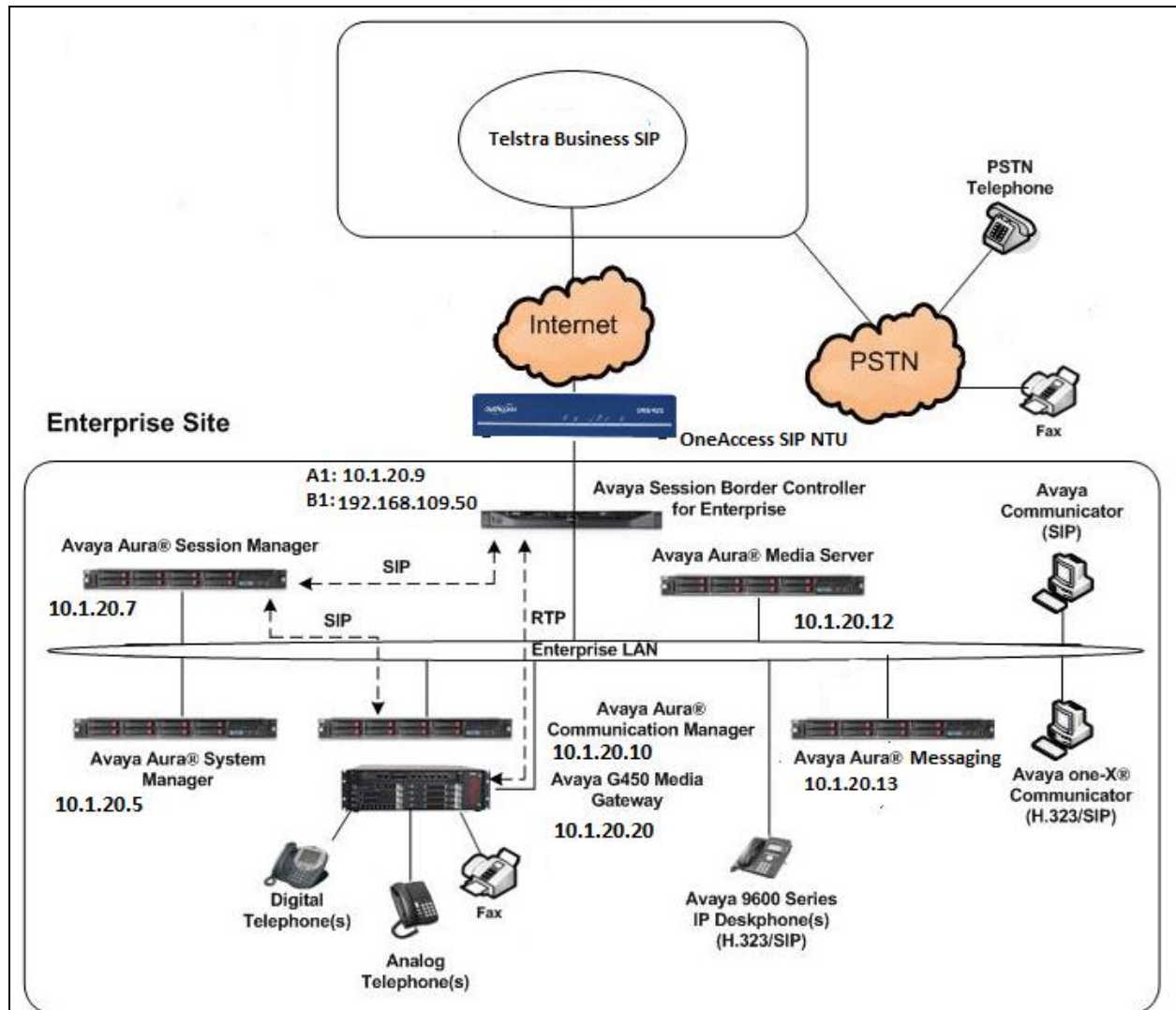


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® System Manager	System_Manager_7.1.2.0_r712007353
Avaya Aura® Session Manager	Session_Manager_7.1.2.0.712004
Avaya Aura® Communication Manager	CM-Simplex-07.1.0.0.532-e65-0.ova Patch: 01.0.532.0-24184.tar
Avaya Aura® Media Server	7.8.0.333_2017.07.17
Avaya Aura® Messaging	MSG-00.0.441.0-017_0004
Avaya G450 Media Gateway	g450_sw_38_21_0
Avaya SBCE	7.2.1.0-05-14222
Avaya One-X® Communicator	6.2.12.20-sp12p10
Avaya Equinox™ Experience	3.3.0.135.22
Avaya 9600 Series IP Deskphones - SIP	96x1-IPT-SIP-R7_1_1_0-091817
Avaya 9600 Series IP Deskphones – H323	96x1-IPT-H323-R6_6_5_06-080917
Avaya 2400 Series Digital phones	R6
Analog phone	N/A
Service Provider	
OneAccess-Telstra Business SIP	Broadworks Version R19 SP1 SIP NTU: V5.2R2C3_KE3

5. Configure Avaya Aura® Communication Manager

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

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

5.1 System-Parameters Customer-Options

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

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

Follow the steps shown below:

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

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
	Maximum Administered H.323 Trunks: 4000	0	
	Maximum Concurrently Registered IP Stations: 2400	4	
	Maximum Administered Remote Office Trunks: 2400	0	
	Maximum Concurrently Registered Remote Office Stations: 2400	0	
	Maximum Concurrently Registered IP eCons: 0	0	
	Max Concur Registered Unauthenticated H.323 Stations: 0	0	
	Maximum Video Capable Stations: 2400	1	
	Maximum Video Capable IP Softphones: 2400	2	
	Maximum Administered SIP Trunks: 4000	10	
	Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0	
	Maximum 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? n	Station as Virtual Extension? y	
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? n	
Port Network Support? y	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): 1		
Off-Premises Tone Detect Timeout Interval (seconds): 20		
AAR/ARS Dial Tone Required? y		
Music (or Silence) on Transferred Trunk Calls? no		
DID/Tie/ISDN/SIP Intercept Treatment: attendant		
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred		
Automatic Circuit Assurance (ACA) Enabled? n		
Abbreviated Dial Programming by Assigned Lists? n		
Auto Abbreviated/Delayed Transition Interval (rings): 2		
Protocol for Caller ID Analog Terminals: Bellcore		
Display Calling Number for Room to Room Caller ID Calls? n		

2. On **Page 9** verify that a text string has been defined to replace the **Calling Party Number (CPN)** for restricted or unavailable calls. The compliance test used the value of **Restricted** for restricted calls and **Unavailable** for unavailable calls.

```
display system-parameters features                                     Page 9 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: Restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: Unavailable

DISPLAY TEXT
                                Identity When Bridging: principal
                                User Guidance Display? n
  Extension only label for Team button on 96xx H.323 terminals? n

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

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

3. On **Page 19** verify that **Direct IP-IP Audio Connections** field is set to **y** and **SIP Endpoint Managed Transfer** field is set to **n**.

```
display system-parameters features                                     Page 19 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

IP PARAMETERS
  Direct IP-IP Audio Connections? y      IP Audio Hairpinning? n
  Synchronization over IP? n Allow SIP-H323 Video in SDES? n

  SIP Endpoint Managed Transfer? n

  Expand ISDN Numbers to International for 1XCES? n

CALL PICKUP
  Maximum Number of Digits for Directed Group Call Pickup: 4
    Call Pickup on Intercom Calls? y      Call Pickup Alerting? n
  Temporary Bridged Appearance on Call Pickup? y      Directed Call Pickup? n
    Extended Group Call Pickup: none
    Enhanced Call Pickup Alerting? n

  Call Pickup for Call to Coverage Answer Group? n
    Display Information With Bridged Call? n
  Keep Bridged Information on Multiline Displays During Calls? y
    PIN Checking for Private Calls? n
```

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.
 - 3-digit extensions with a **Call Type** of **ext** beginning with 4 (which is a subset of DID numbers 0285xxx4xx) assigned by OneAccess-Telstra Business SIP).
 - 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code * for SIP Trunk Access Codes (TAC).

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

5.4 IP Node Names

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

Follow the steps shown below:

- Enter the **change node-names ip** command, and add node names and IP addresses for the following:
 - Session Manager SIP signaling interface (e.g., **asm** and **10.1.20.7**).
 - Media Server (e.g., **ams** and **10.1.20.12**).

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

5.5 IP Interface for Procr

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

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

display ip-interface pro		Page 1 of 2	
IP INTERFACES			
Type: PROCR		Target socket load: 19660	
Enable Interface? y	Allow H.323 Endpoints? y		
	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.net**. This domain name appears in the “From” header of SIP message originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to **yes**. Shuffling can be further restricted at the trunk level under the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.7**.
- Default values can be used for all other fields.

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

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: sipinterop.net
Name: Sydney     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: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 34
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
Subnet Mask: /24
```

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

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

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		Target socket load: 19660
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	
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.

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

      Type: g450
      Name: g450
      Serial No: 10Nxxxxxxxxx
Link Encryption Type: any-ptls/tls      Enable CF? n
      Network Region: 1                  Location: 1
                                          Site Data: 1
      Recovery Rule: none

      Registered? y
FW Version/HW Vintage: 38 .21 .0 /1
      MGP IPV4 Address: 10.1.20.20
      MGP IPV6 Address:
Controller IP Address: 10.1.20.10
      MAC Address: 00:1b:xx:xx:xx:48

Mutual Authentication? optional
```


5.7 IP Codec Parameters

Follow the steps shown below:

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

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

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

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

5.8.1 Signaling Group

This section describes the steps for administering the SIP trunk to Session Manager. This trunk corresponds to the **communication-manager** 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 **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **IP Video?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **asm**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6**.
- **Far-end Domain** – Enter **sipinterop.net**. This is the domain provisioned for Session Manager in **Section 6.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**.
- **Initial IP-IP Direct Media** – Set to **y**.
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- Default values may be used for all other fields.

```

add signaling-group 1                                     Page 1 of 2
SIGNALING GROUP

Group Number: 1          Group Type: sip
IMS Enabled? n          Transport Method: tls
Q-SIP? n
IP Video? n              Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr          Far-end Node Name: asm
Near-end Listen Port: 5061         Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain: sipinterop.net

Incoming Dialog Loopbacks: eliminate          Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                    RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3           Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y                       IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n       Initial IP-IP Direct Media? y
                                              Alternate Route Timer(sec): 600

```

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 Name** – Enter a descriptive name.
- **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**).
- Default values may be used for all other fields.

add trunk-group 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: TO-SM	COR: 1	TN: 1	TAC: *01
Direction: two-way	Outgoing Display? y		
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. This time interval (in milliseconds) should be equal to the time interval defined by the **Alternate Route Timer** on the signaling group form described in **Section 5.8.1**.

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 **90** seconds was used.

<code>add trunk-group 1</code>	Page 2 of 22
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): 90	
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.

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.

<code>add trunk-group 1</code>	Page 3 of 22
TRUNK FEATURES	
ACA Assignment? n	Measured: none
Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private
UI Treatment: service-provider	
Replace Restricted Numbers? y	
Replace Unavailable Numbers? y	
Hold/Unhold Notifications? y	
Modify Tandem Calling Number: no	

On **Page 5**, the **Network Call Redirection?** field must be set to **n**. Setting the **Network Call Redirection?** flag to **y** enables the use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer.

Set the **Send Transferring Party Information?** field to **n**, the **Send Diversion Header?** field to **y** and the **Support Request History?** field to **y**. 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.

Set the **Always Use re-INVITE for Display Updates** field to **y** and the **Identity for Calling Party Display** field to **P-Asserted-Identity**.

add trunk-group 1	Page 5 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? y	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? y	
Enable Q-SIP? n	

5.9 Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Use the **change private-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 0285xxx4xx DID numbers provided for testing were assigned to the extensions 4xx. 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. Note that real number is replaced by x for security reason.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
3	4	1	285xxx	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. DID number sent by OneAccess-Telstra Business SIP can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 1					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	9	285xxx	6		
public-ntwrk					

5.11 Outbound Routing

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

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

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

change feature-access-codes									
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:									
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).

change ars analysis 0							Page	1 of	2
ARS DIGIT ANALYSIS TABLE									
							Location: all		
							Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI		
	String	Min	Max	Pattern	Type	Num	Reqd		
02		10	10	1	pubu		n		
04		10	10	1	pubu		n		
0011		12	20	1	pubu		n		
000		3	3	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 5.9**.

change route-pattern 1													Page	1 of	3	
Pattern Number: 1													Pattern Name: sip			
SCCAN? n				Secure SIP? n				Used for SIP stations? n								
													DCS/	IXC		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						QSIG			
No			Mrk	Lmt	List	Del	Digits						Intw			
1:	1	0											n	user		
2:													n	user		
3:													n	user		
4:													n	user		
5:													n	user		
6:													n	user		

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., **10Nxxxxxxxx**).
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 running-config startup-config** 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** (e.g., **10Nxxxxxxxx**).
- Set the **Encrypt Link** parameter as desired (**n** was used in the reference configuration).
- Set **Network Region** = **1**.

When the Media Gateway registers, the SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., **g450-001(*super*)#**).

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

display media-gateway 1
MEDIA GATEWAY 1

Page 1 of 2

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

 Recovery Rule: none

 Registered? y
FW Version/HW Vintage: 38 .21 .0 /1
 MGP IPV4 Address: 10.1.20.20
 MGP IPV6 Address:
Controller IP Address: 10.1.20.10
 MAC Address: 00:1b:xx:xx:xx:e0

Mutual Authentication? optional

5.13 Avaya Aura® Media Server Provisioning

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

5.13.1 Signaling Group for Media Server

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

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **Peer Detection Enabled?** is set to **n**. Set the **Peer Server** to **AMS**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of the Media Server as administered in **Section 5.4** (e.g., **ams**).
- **Near-end Listen Port** – Set to **9061**.
- **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set to **1**.

```
add signaling-group 2                                     Page 1 of 2
                                     SIGNALING GROUP
Group Number: 1                Group Type: sip
                               Transport Method: tls
Peer Detection Enabled? n    Peer Server: AMS
Near-end Node Name: procr      Far-end Node Name: ams
Near-end Listen Port: 9061     Far-end Listen Port: 5061
                               Far-end Network Region: 1
Far-end Domain: 10.1.20.12
```

5.13.2 Adding Media Server

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

- **Signaling Group** – Set to signaling group administered in **Section 5.13.1** (e.g., **2**).
- **Voip Channel License Limit** – Set to desired number. In the compliance test, **10** was used.
- **Dedicated Voip Channel Licenses** – Set to desired number. In the compliance test, **10** was used.
- **Network Region** – Set to the network region administered in **Section 5.6** (e.g., **1**).

add media-server 1	MEDIA SERVER	Page 1 of 1
Media Server ID: 1		
Signaling Group: 2		
Voip Channel License Limit: 10		
Dedicated Voip Channel Licenses: 10		

5.14 Save Communication Manager Translations

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

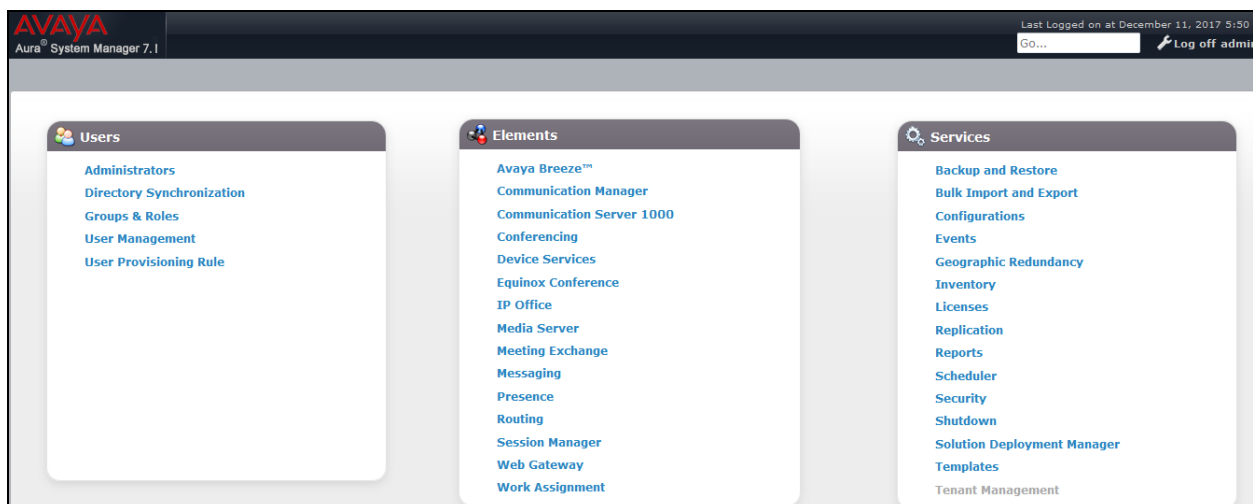
6. Configure Avaya Aura® Session Manager

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

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

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

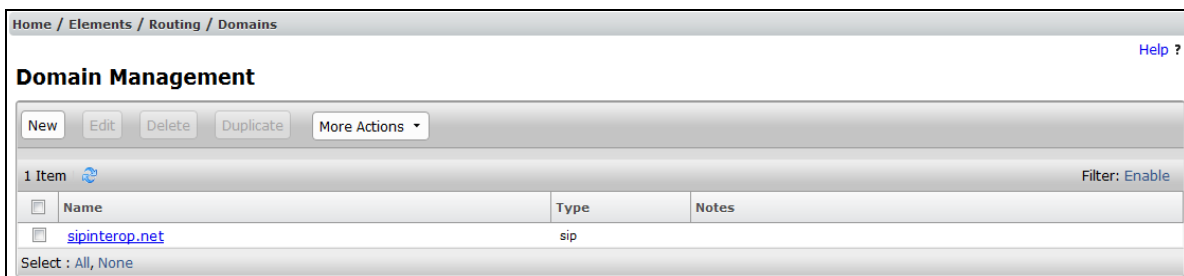
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the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



6.1 Configure SIP Domain

Follow the steps shown below:

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



The screenshot displays the 'Domain Management' interface. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. A 'Help ?' link is located in the top right corner. Below the title, there is a toolbar with buttons for 'New', 'Edit', 'Delete', 'Duplicate', and a 'More Actions' dropdown menu. A status bar indicates '1 Item' with a refresh icon and a 'Filter: Enable' link. The main content is a table with three columns: 'Name', 'Type', and 'Notes'. The table contains one row with the domain 'sipinterop.net' and type 'sip'. At the bottom left, there is a 'Select : All, None' option.

	Name	Type	Notes
<input type="checkbox"/>	sipinterop.net	sip	

6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **Sydney** 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., **Sydney**).
 - **Notes:** Add a brief description.
 - Select and enter desired numbers for **Overall Managed Bandwidth**.
2. Click **Commit** to save.

The screenshot displays the 'Location Details' configuration page. The left sidebar shows the 'Routing' menu with 'Locations' selected. The main content area is titled 'Location Details' and includes a 'Commit' button. The 'General' section contains the following fields:

- Name:** Sydney
- Notes:**

The 'Dial Plan Transparency in Survivable Mode' section includes an 'Enabled' checkbox and a 'Listed Directory Number' field. The 'Associated CM SIP Entity' field is also present. The 'Overall Managed Bandwidth' section is highlighted with a red box and contains the following fields:

- Managed Bandwidth Units:** Kbit/sec
- Total Bandwidth:** 2048
- Multimedia Bandwidth:** 1024

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., **session-manager**).
 - **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.1.20.7**).
 - **Type** – Verify **Session Manager** is selected.
 - **Location** – Select location **Sydney**.
 - **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.
 - Click **Commit** to save.

SIP Entity Details

Commit

Cancel

General

* Name: session-manager

* FQDN or IP Address: 10.1.20.7

Type: Session Manager

Notes:

Location: Sydney

Outbound Proxy:

Time Zone: Australia/Sydney

Minimum TLS Version: Use Global Setting

Credential name:

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

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. **communication-manager**).
 - **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 **Sydney** administered in **Section 6.2**.
 - **Time Zone** – Select the time zone in which Communication Manager resides.
 - Use the default values for the remaining parameters.
3. Click on **Commit**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: communication-manager

*** FQDN or IP Address:** 10.1.20.10

Type: CM

Notes:

Adaptation:

Location: Sydney

Time Zone: Australia/Sydney

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

Commit **Cancel**

6.3.3 Configure Avaya SBCE SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **SBCE-A1**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.1.20.9**).
- **Type** – Verify **SIP Trunk** is selected.

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* **Name:** SBCE-A1

* **FQDN or IP Address:** 10.1.20.9

Type: SIP Trunk

Notes:

Adaptation:

Location: Sydney

Time Zone: Australia/Sydney

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress

6.4 Configure Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager defined in **Section 6.3.1**.
- **Protocol:** Select the transport protocol used for this link, **TLS** for the Entity Link to Communication Manager and **TLS** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager.

- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.3.2**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section 6.3.3**
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.4.1 Configure Entity Link to Communication Manager

Follow the steps shown below:

1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name (or have it created automatically) for this link to Communication Manager (e.g., **session-manager_communication-manager_5061_TLS**).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.3.1** for Session Manager (e.g., **session-manager**).
 - **SIP Entity 1 Port** – Enter **5061**.
 - **Protocol** – Select **TLS**.
 - **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.2** for the Communication Manager internal entity (e.g., **communication-manager**).
 - **SIP Entity 2 Port** – Enter **5061**.
 - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel Help

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override
<input type="checkbox"/>	* session-manager_comm	* session-manager	TLS	* 5061	* communication-manager	* 5061	<input type="checkbox"/>

Select: All None

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., **session-manager_SBCE-A1_5061_TLS**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.3** for the Avaya SBCE entity (e.g., **SBCE-A1**).

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override
session-manager_SBCE	session-manager	TLS	5061	SBCE-A1	5061	<input type="checkbox"/>

6.5 Configure Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. Two routing policies were added, one for Communication Manager and another for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click the **New** button in the right pane (not shown). The following screen is displayed.

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

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

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

6.5.1 Configure Routing Policy for Communication Manager

This Routing Policy is used for inbound calls from OneAccess-Telstra Business SIP.

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 OneAccess-Telstra Business SIP calls to Communication Manager (e.g., **to_cm**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.

4. In the **SIP Entity List** page, select the SIP Entity administered in **Section 6.3.2** for the Communication Manager SIP Entity (**communication-manager**), 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**.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit **Cancel**

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type
communication-manager	10.1.20.10	CM

6.5.2 Configure Routing Policy for Avaya SBCE

This Routing Policy is used for outbound calls to the OneAccess-Telstra Business SIP. Repeat the steps in **Section 6.6.1**, 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**).

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit **Cancel**

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type
SBCE-A1	10.1.20.9	SIP Trunk

6.6 Configure Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to OneAccess-Telstra Business SIP 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.

Two examples of the dial patterns used for the compliance testing are shown below, one for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise.

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	-ALL-		to_SBCE	0	<input type="checkbox"/>	SBCE-A1


The second example shows that a 10-digit pattern that starts with 0285xxx is used for inbound calls from OneAccess-Telstra Business SIP to DID numbers on Communication Manager.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 0285 

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1


Emergency Type:

SIP Domain: -ALL- ▼

Notes: to ddi number

Originating Locations and Routing Policies

Add Remove

1 Item 

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Rou Not
<input type="checkbox"/>	-ALL-		to_cm	0	<input type="checkbox"/>	communication-manager	

7. Configure Avaya Session Border Controller for Enterprise

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

As described in Section 3, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (10.1.20.9), with access to the **Sydney** location. The connection to OneAccess-Telstra Business SIP uses the Avaya SBCE public interface B1 (IP address **192.168.109.50**). The following provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

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



The screenshot shows the Avaya Session Border Controller for Enterprise login page. On the left is the Avaya logo and the text 'Session Border Controller for Enterprise'. On the right, under the heading 'Log In', there is a 'Username' field with a text input box and a 'Continue' button. Below the input fields, there is a disclaimer: 'This system is intended solely for authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of the system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the substance of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets. © 2011 - 2013 Avaya Inc. All rights reserved.'

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



This screenshot shows the same login page as the previous one, but with an additional 'Password' field. The 'Username' field now contains the text 'xxxxxxxx'. Below the 'Password' field is a 'Log In' button. The disclaimer text at the bottom remains the same: 'This system is intended solely for authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modification of the system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the substance of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets. © 2011 - 2013 Avaya Inc. All rights reserved.'

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.

[Alarms](#) [Incidents](#) [Status ▾](#) [Logs ▾](#) [Diagnostics](#) [Users](#)

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management

- Global Parameters
- Global Profiles
- PPM Services
- Domain Policies
- TLS Management
- Device Specific Settings

Dashboard

Information	
System Time	06:59:11 PM AEDT Refresh
Version	7.2.1.0-05-14222
Build Date	Tue Oct 31 00:06:46 UTC 2017
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	12/11/2017 21:37:33 AEDT
Failed Login Attempts	1

Installed Devices

EMS
sbce

7.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned** (not shown).
2. Click on **View** to display the **System Information** screen.

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

Requested: 100

100

Advanced Sessions

Requested: 100

100

Scopia Video Sessions

Requested: 100

100

CES Sessions

Requested: 100

100

Transcoding Sessions

Requested: 100

100

Encryption

☒

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
10.239.192.234	10.239.192.234	255.255.255.248	10.239.192.233	B1

DNS Configuration

Primary DNS

10.1.20.3

Secondary DNS

DNS Location

DMZ

DNS Client IP

10.1.20.9

Management IP(s)

IP #1 (IPv4)

10.1.20.8

7.2 Global Profiles

7.2.1 Uniform Resource Identifier (URI) Groups

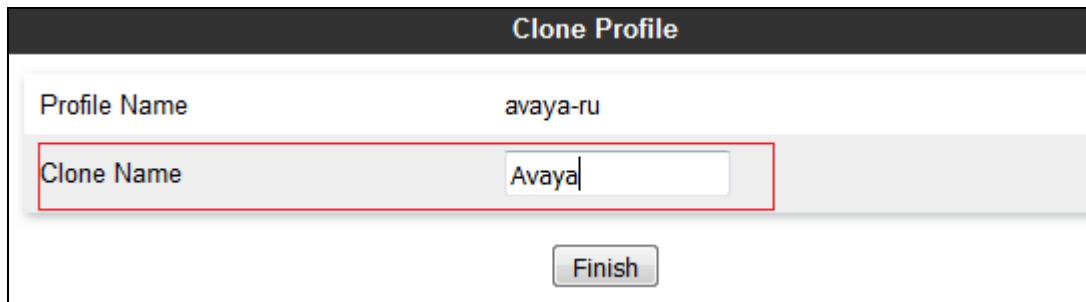
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a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

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

7.2.2 Server Interworking – Avaya

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

1. Navigate to **Global Profiles > Server Interworking** from the left-hand menu.
2. Select **avaya-ru** then click on **Clone** button.
3. Enter profile name: (e.g., **Avaya**), and click on **Finish**.



The screenshot shows a 'Clone Profile' dialog box. It has a dark header bar with the title 'Clone Profile'. Below the header, there are two input fields. The first field is labeled 'Profile Name' and contains the text 'avaya-ru'. The second field is labeled 'Clone Name' and contains the text 'Avaya'. This second field is highlighted with a red rectangular border. Below these fields is a 'Finish' button.

4. Click on **Edit** in the **General** tab (not shown).
- Uncheck **T38 Support** box.
 - Click on **Finish**.

The screenshot shows a window titled "Editing Profile: Session Manager" with a close button (X) in the top right corner. The "General" tab is selected. The window contains various configuration options for a session manager profile. The "T.38 Support" checkbox is highlighted with a red rectangle. Below the "T.38 Support" checkbox is the "URI Scheme" section, which has three radio buttons: "SIP" (selected), "TEL", and "ANY". At the bottom of the window is a "Finish" button.

Editing Profile: Session Manager	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Delayed Offer	<input 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
Finish	

5. Click on **Edit** in the **Advanced** tab (not shown).
- **Record Routes:** Choose **None**.
 - Check to **Has Remote SBC**.
 - Click on **Finish**.

Editing Profile: Session Manager

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 Avaya

Diversion Manipulation ☐

Diversion Condition None

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

☒ None
☐ SIP Notify
☐ SIP Info
☐ Inband

Finish

7.2.3 Server Interworking – OneAccess

Navigate to **Global Profiles > Server Interworking** from the left-hand menu to add an Interworking Profile for the connection to OneAccess-Telstra Business SIP.

- Click on **Add** (not shown) then enter **OneAccess** as the **profile name** and click on **Next** (not shown).
- In **General** window: Uncheck **T.38 Support** then click on **Next**.

The screenshot shows the 'Interworking Profile' configuration window with the 'General' tab selected. The window contains the following settings:

- Hold Support:** ☒ None, ☐ RFC2543 - c=0.0.0.0, ☐ RFC3264 - a=sendonly
- 180 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- 181 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- 182 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- 183 Handling:** ☒ None, ☐ SDP, ☐ No SDP
- Refer Handling:** ☐
- URI Group:** None (dropdown)
- Send Hold:** ☒
- Delayed Offer:** ☒
- 3xx Handling:** ☐
- Diversion Header Support:** ☐
- Delayed SDP Handling:** ☐
- Re-Invite Handling:** ☐
- Prack Handling:** ☐
- Allow 18X SDP:** ☐
- T.38 Support:** ☐ (highlighted with a red box)
- URI Scheme:** ☒ SIP, ☐ TEL, ☐ ANY
- Via Header Format:** ☒ RFC3261, ☐ RFC2543

At the bottom, there are 'Back' and 'Next' buttons. The 'Next' button is highlighted with a red box.

- Leave default values in **SIP Timers** window and **Privacy** window (not shown).
- In **Advance** window: Select **None** for **Record Routes** and check to **Has Remote SBC** then click on **Finish**.

Interworking Profile [X]

Record Routes: ☒ None
☐ Single Side
☐ Both Sides
☐ Dialog-Initiate Only (Single Side)
☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup: ☐

Extensions:

Diversion Manipulation: ☐

Diversion Condition:

Diversion Header URI:

Has Remote SBC: ☒

Route Response on Via Port: ☐

Relay INVITE Replace for SIPREC: ☐

DTMF

DTMF Support: ☒ None
☐ SIP Notify
☐ SIP Info
☐ Inband

Back

7.2.4 Signaling Manipulation – OneAccess

As OneAccess SIP NTU requires User-Agent header in the SIP messages sent to it, a Sigma script must be used on Avaya SBCE to insert User-Agent header into SIP messages before Avaya SBCE sends those messages to OneAccess SIP NTU.

OneAccess SIP NTU also does not accept SIP INVITE which has too long URI of the Contact header. Therefore, a Sigma script must be used on Avaya SBCE to remove unnecessary parameters in the URI of the Contact header before Avaya SBCE sends SIP INVITE to OneAccess SIP NTU.

1. Navigate to **Global Profiles > Signaling Manipulation** from the left-hand menu.
2. Click on **Add** button to add a Sigma script as shown below.

Signaling Manipulation Scripts: OneAccess

Upload

Add

Signaling Manipulation Scripts

OneAccess

Click here to add a description.

Signaling Manipulation

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["User-Agent"][1] = "Avaya-SBC-v7.2.1";
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

Edit

Text version of the script:

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["User-Agent"][1] = "Avaya-SBC-v7.2.1";
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);

}
}
```

7.2.5 Server Configuration – Avaya

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

1. Navigate to **Global Profiles > Server Configuration** from the left-hand menu.
2. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Avaya**) and click on **Next** (not shown).
3. The **Edit Server Configuration Profile - General** window will open.
 - Select **Server Type: Call Server**.
 - **SIP Domain:** Leave blank.
 - **IP Address / FQDN:** **10.1.20.7** (Session Manager signaling IP Address as configured in Section 6.3.1).
 - **Transport:** Select **TLS**.
 - **Port:** **5061**.
 - **TLS Client Profile:** Select **clientA1**. Certificates and TLS profiles configuration are out of scope of this Application Notes.
 - Click on **Next**.

Edit Server Configuration Profile - General X

Server Type: Call Server ▼

SIP Domain:

TLS Client Profile: ClientA1 ▼

Add

IP Address / FQDN	Port	Transport
10.1.20.7	5061	TLS ▼

Delete

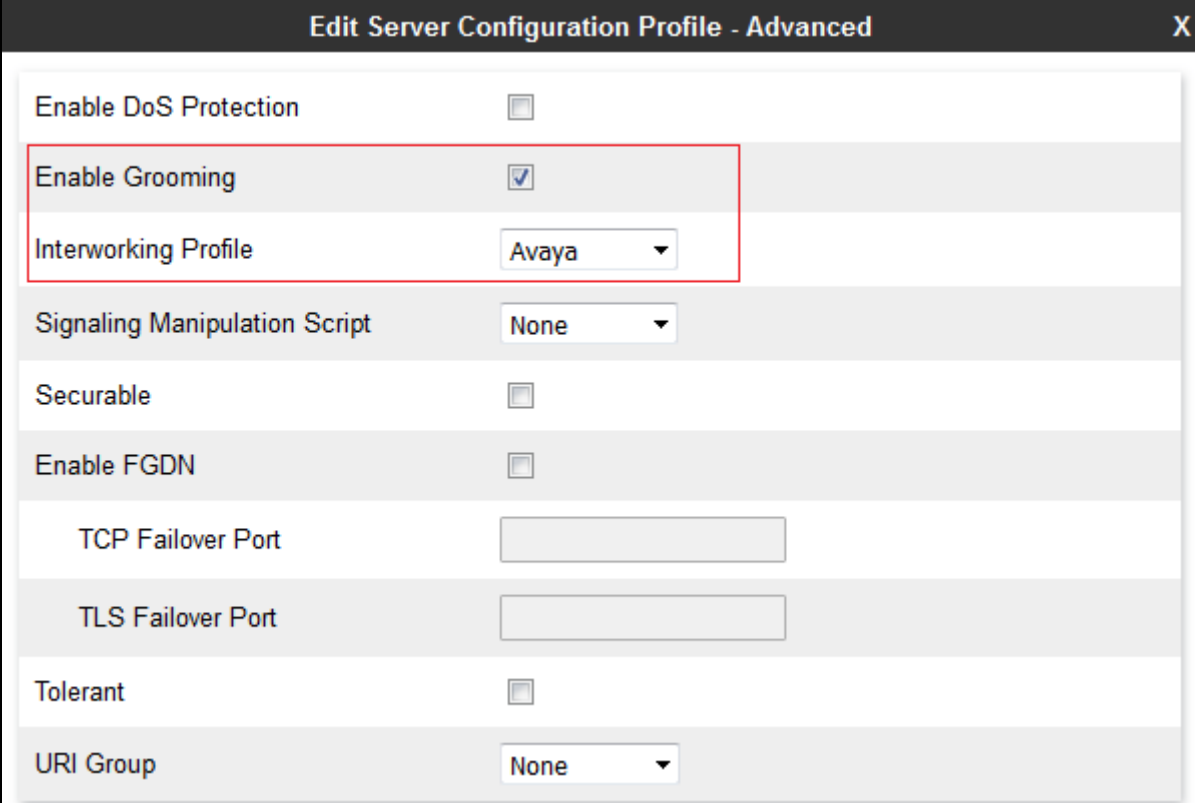
Back Next

4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
 - Click on **Next** to accept default values.
5. The **Add Server Configuration Profile - Heartbeat** window will open.
 - Check **Enable Heartbeat** box.
 - **Method**: Select **OPTIONS**.
 - **Frequency**: Enter **30**.
 - **From URI** and **To URI**: Enter **ping@sipinterop.net**.
 - Click on **Next** button.

The screenshot shows a window titled "Edit Server Configuration Profile - Heartbeat". Inside the window, there are the following elements:

- Enable Heartbeat**: A checkbox that is checked.
- Method**: A dropdown menu currently displaying "OPTIONS".
- Frequency**: A text input field containing the number "30", followed by the unit "seconds".
- From URI**: A text input field containing the value "ping@sipinterop.net".
- To URI**: A text input field containing the value "ping@sipinterop.net".
- Finish**: A button located at the bottom right of the configuration area.

6. The **Add Server Configuration Profile - Advanced** window will open.
- Check **Enable Grooming** box.
 - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.



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

7.2.6 Server Configuration – OneAccess

Repeat the steps in **Section 7.2.5**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to OneAccess-Telstra Business SIP network.

1. Select **Add Profile** and enter a Profile Name (e.g., **OneAccess**) and click on **Next** (not shown).
2. On the **Edit Server Configuration Profile - General** window, enter the following.
 - Select **Server Type: Trunk Server**.
 - **SIP Domain:** Leave blank.
 - **IP Address / FQDN: 192.168.109.1** (OneAccess SIP NTU IP address).
 - **Transport:** Select **UDP**.
 - **Port: 5062**.
 - Click on **Next**.

Edit Server Configuration Profile - General X

Server Type: Trunk Server

SIP Domain:

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport	
192.168.109.1	5062	UDP	Delete

Back Next

3. On the **Edit Server Configuration Profile – Authentication** window, enter the following.
 - Select **Enable Authentication**.
 - Enter trunk Pilot number into **User Name**.
 - Enter assigned password into **Password** and **Confirm Password**.

Edit Server Configuration Profile - Authentication X

Enable Authentication ☒

User Name 2857...

Realm
(Leave blank to detect from server challenge)

Password
(Leave blank to keep existing password)

Confirm Password

Finish

4. On the **Edit Server Configuration Profile – Heartbeat** window, enter the following.
 - Select **Enable Heartbeat**.
 - **Method**: Select **REGISTER**.
 - **Frequency**: Enter desired number. In the compliance test, 600 was used.
 - **From URI** and **To URI**: Enter trunk pilot number provided, such as 285xxx4xx@192.168.109.50.

Edit Server Configuration Profile - Heartbeat X

Enable Heartbeat ☒

Method REGISTER ▼

Frequency 600 seconds

From URI 2857...4xx@192.168.109.50

To URI 2857...4xx@192.168.109.50

Finish

5. On the **Edit Server Configuration Profile – Advanced** window, enter the following.
- **Interworking Profile:** Select **OneAccess** created in **Section 7.2.3**.
 - **Signaling Manipulation Script:** Select **OneAccess** created in **Section 7.2.4**.

Add Server Configuration Profile - Advanced X

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

7.2.7 Routing – To Avaya

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

1. Navigate to **Global Profiles > Routing** from the left-hand menu, and click on **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Avaya**) and click **Next** (not shown).
3. The **Routing Profile** window will open. Using the default values shown, click on **Add**.
4. Populate the following fields:
 - **Priority/Weight = 1.**
 - **Server Configuration = Session Manager.**
 - **Next Hop Address:** Verify that the **10.1.20.7:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
 - Click on **Finish**.

The screenshot shows the 'Profile : Avaya - Edit Rule' window. The top section contains fields for 'URI Group' (set to '*') and 'Time of Day' (set to 'default'). Below these are several rows of configuration options: 'Load Balancing' (Priority) and 'NAPTR' (unchecked), 'Transport' (None) and 'Next Hop Priority' (checked), 'Next Hop In-Dialog' (unchecked) and 'Ignore Route Header' (unchecked), and 'ENUM' (unchecked) and 'ENUM Suffix' (empty). An 'Add' button is at the bottom right of this section. Below is a table with four columns: 'Priority / Weight', 'Server Configuration', 'Next Hop Address', and 'Transport'. The first row contains the values '1', 'Avaya', '10.1.20.7:5061 (TLS)', and 'None'. A 'Delete' button is at the end of this row. At the bottom of the window is a 'Finish' button.

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Avaya	10.1.20.7:5061 (TLS)	None	Delete

7.2.8 Routing – To OneAccess

Repeat the steps in **Section 7.2.7**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to OneAccess-Telstra Business SIP.

1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **OneAccess**).
2. On the **Routing Profile** window, populate the following fields:
 - **Server Configuration: OneAccess.**
 - **Next Hop Address:** Verify that the **192.168.109.1:5062 (UDP)** entry from the drop down menu is selected.
3. Click on **Finish**.

URI Group	Time of Day
*	default

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

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

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

ENUM	ENUM Suffix
<input type="checkbox"/>	

[Add](#)

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	OneAccess	192.168.109.1:5062 (UDP)	None

[Delete](#)

[Finish](#)

7.2.9 Topology Hiding – Avaya

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. Navigate to **Global Profiles > Topology Hiding** from the left-hand side menu.
2. Click on **Add** button (not shown), enter **Profile Name:** (e.g., **Avaya**), and click **Next** (not shown).
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button (not shown) repeatedly to add headers. Note that the **Overwrite Value** is **sipinterop.net**.
4. Populate the fields as shown below, and click on **Finish** (not shown).

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

Edit

7.2.10 Topology Hiding – OneAccess

Repeat the steps in **Section 7.2.9**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to OneAccess-Telstra Business SIP.

1. Enter a **Profile Name**: (e.g., **OneAccess**).
2. Click on the **Add Header** button (not shown) repeatedly to add headers.
3. Populate the fields as shown below, and click on **Finish** (not shown). Note that the **Overwrite Value** is **192.168.109.1**.

Topology Hiding			
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	192.168.109.1
SDP	IP/Domain	Auto	---
To	IP/Domain	Overwrite	192.168.109.1
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	192.168.109.1
Record-Route	IP/Domain	Auto	---
<div>Edit</div>			

7.2.11 Domain Policies

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

7.2.12 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 default rule was used.

Note: It is not recommended to edit default rules. New rules should be added or cloned from default rules.

7.2.13 Border Rules

The Border rules specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses. In the solution as tested, the **default** rule was utilized. No customization was required.

7.2.14 Media Rules

The Media rules will be applied to both directions. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

7.2.15 Signaling Rules

Signaling rules are a mechanism on the Avaya SBCE to manipulate the signaling beyond simple header manipulation. Signaling rules allow action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. In the solution as tested, the **default** rule was used.

7.2.16 Endpoint Policy Groups

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

7.3 Device Specific Settings

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

7.3.1 Network Management

1. Select **Device Specific Settings > Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

Network Management: sbce

Devices	Interfaces	Networks
sbce		

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
A1	10.1.20.1	255.255.255.0	A1	10.1.20.9	Edit	Delete
B1	192.168.109.1	255.255.255.0	B1	192.168.109.50	Edit	Delete

7.3.2 Media Interfaces

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Med_A1.
 - **IP Address:** 10.1.20.9 (Avaya SBCE A1 address).
 - **Port Range:** 35000-40000.
4. Click on **Finish** (not shown).
5. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Med_B1.
 - **IP Address:** 192.168.109.50 (Avaya SBCE B1 address).
 - **Port Range:** 35000-40000.
6. Click on **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.

Media Interface: sbce

Devices
sbce

Media Interface

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

Add

Name	Media IP Network	Port Range	
Med_A1	10.1.20.9 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Med_B1	192.168.109.50 B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

7.3.3 Signaling Interface

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Click on **Add** (not shown) and enter the following:
 - **Name: Sig_A1.**
 - **IP Address: 10.1.20.9** (Avaya SBCE A1 address).
 - **TCP/UDP Port: 5060.**
 - **TLS Port: 5061.**
 - **TLS Profile: ServerA1.** Certificates and TLS profiles configuration are out of scope of this Application Notes.
4. Click on **Finish** (not shown).
5. Click on **Add** again, and enter the following:
 - **Name: Sig_B1.**
 - **IP Address: 192.168.109.50** (Avaya SBCE B1 address).
 - **UDP Port: 5060.**
6. Click on **Finish** (not shown). Note that changes to these values require an application restart.

Signaling Interface: sbce

Devices
sbce

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_B1	192.168.109.50 B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete
Sig_A1	10.1.20.9 A1 (A1, VLAN 0)	5060	5060	5061	ServerA1	Edit Delete

7.3.4 Endpoint Flows – For Avaya

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:
 - **Flow Name: Avaya.**
 - **Server Configuration: Avaya.**
 - **URI Group: *.**
 - **Transport: *.**
 - **Remote Subnet: *.**
 - **Received Interface: Sig_B1.**
 - **Signaling Interface: Sig_A1.**
 - **Media Interface: Med_A1.**
 - **End Point Policy Group: default-low.**
 - **Routing Profile: OneAccess.**
 - **Topology Hiding Profile: Avaya.**
 - Let other values default.
4. Click **Finish**.

Edit Flow: Avaya

X

Flow Name	Avaya
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_B1
Signaling Interface	Sig_A1
Media Interface	Med_A1
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	OneAccess
Topology Hiding Profile	Avaya
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

7.3.5 Endpoint Flows – For OneAccess

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

- **Flow Name: OneAccess.**
- **Server Configuration: OneAccess.**
- **Received Interface: Sig_A1.**
- **Signaling Interface: Sig_B1.**
- **Media Interface: Med_B1.**
- **Endpoint Policy Groups: default-low.**
- **Routing Profile: Avaya.**
- **Topology Hiding Profile: OneAccess.**

Edit Flow: OneAccessX

Flow Name	<input type="text" value="OneAccess"/>
Server Configuration	<input type="text" value="OneAccess"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="Sig_A1"/>
Signaling Interface	<input type="text" value="Sig_B1"/>
Media Interface	<input type="text" value="Med_B1"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="default-low"/>
Routing Profile	<input type="text" value="Avaya"/>
Topology Hiding Profile	<input type="text" value="OneAccess"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

Finish

8. Verification Steps

The following steps may be used to verify the configuration.

8.1 Avaya Session Border Controller for Enterprise

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

Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **B1**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **3000**).
 - 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.

Trace: sbce

Devices
sbce

Packet Capture

Captures

Packet Capture Configuration

StatusReady

InterfaceB1

Local Address
IP:Port192.168.109.90:

Remote Address
*, *.Port, IP, IP:Port*

ProtocolAll

Maximum Number of Packets to Capture3000

Capture Filename
Using the name of an existing capture will overwrite it.test.pcap

Start CaptureClear

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

Trace: sbce

Devices
sbce

Packet Capture

Captures

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

Packet Capture Configuration

Status

In Progress

Interface

B1

Local Address

10.2.2.135

Remote Address

*

Protocol

All

Maximum Number of Packets to Capture

3000

Capture Filename

test.pcap

Stop Capture

- Run the test.
- When the test is completed, select the **Stop Capture** button shown above.
- 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**.
- Click on the **File Name** link to download the file and use Wireshark to open the trace.

Trace: sbce

Devices	Packet Capture	Captures	Refresh
sbce			
File Name	File Size (bytes)	Last Modified	
test_20160405184126.pcap	0	April 5, 2016 6:41:26 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 OneAccess-Telstra Business SIP and the customer SIP PABX is the customer SBC. On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the OneAccess-Telstra Business SIP.
- Ping from the SBC to the Session Manager.
- Ping from the OneAccess-Telstra Business SIP towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

Full Diagnostic

Ping Test

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

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)	Error: Unable to reach 10.1.20.1 from 10.1.20.9 [A1].
✓ Ping: SBC (A1) to Primary DNS (10.1.20.3)	Average ping from 10.1.20.9 [A1] to 10.1.20.3 is 0.492ms.
✓ Ping: SBC (B1) to Gateway (192.168.109.1)	Average ping from 192.168.109.50 [B1] to 192.168.109.1 is 1.385ms.
🔄 Ping: SBC (B1) to Primary DNS (10.1.20.3)	Running...

Incident Viewer

AVAYA

Device All
Category All

Clear Filters

Refresh

Generate Report

Displaying results 1 to 15 out of 44.

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

8.2 Avaya Aura® Communication Manager

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

- Verify signaling status, trunk status.

```
status signaling-group 1
STATUS SIGNALING GROUP

Group ID: 1
Group Type: sip

Group State: in-service
```

```
status trunk 1
TRUNK GROUP STATUS

Member    Port    Service State    Mtce Connected Ports
              Busy
0001/001 T00001  in-service/idle  no
0001/002 T00002  in-service/idle  no
0001/003 T00003  in-service/idle  no
0001/004 T00004  in-service/idle  no
0001/005 T00005  in-service/idle  no
0001/006 T00006  in-service/idle  no
0001/007 T00007  in-service/idle  no
0001/008 T00008  in-service/idle  no
0001/009 T00009  in-service/idle  no
0001/010 T00010  in-service/idle  no
```

8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

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

Home / Elements / Session Manager / Dashboard Help ?

Session Manager Dashboard

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

Session Manager Instances

Service State EASG

1 Item All

<input type="checkbox"/>	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
<input type="checkbox"/>	session-manager	Core	✓	0/0/0	Up	Accept New Service	1/3	0	1/1	✓	✓	Normal	Disabled	7.1.2.0.712004

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.
3. Clicking on the **1/3** entry in the **Entity Monitoring** column, results in the following display, please make sure Conn. Status of communication-manager and SBCE-A1 is UP. This status proves that communication-manager and SBCE-A1 are alive and responding to session-manager.

All Entity Links for Session Manager: [session-manager](#)

Summary View

Status Details for the selected Session Manager:

3 Items

	SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SBCE-A1	IPv4	10.1.20.9	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	communication-manager	IPv4	10.1.20.10	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	messaging-server	IPv4	10.1.20.13	5060	TCP	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN

8.4 Telephony Services

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

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.1.2, Avaya Aura® Session Manager 7.1.2, and Avaya Session Border Control for Enterprise 7.2.1 can be configured to interoperate successfully with OneAccess-Telstra Business SIP. This solution allows enterprise users access to the PSTN using the OneAccess-Telstra Business SIP. Please refer to **Section 2.2** for exceptions.

10. Additional References

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

- [1] *Deploying Avaya Aura® System Manager Release 7.1.2.*
- [2] *Administering Avaya Aura® System Manager for Release 7.1.2.*
- [3] *Administering Avaya Aura® Session Manager Release 7.1.2.*
- [4] *Deploying Avaya Aura Session Manager Release 7.1.2.*
- [5] *Deploying Avaya SBCE on VMware in Virtualized Environment Release 7.2.1.*
- [6] *Administering Avaya Session Border Controller Release 7.2.1*
- [7] *Document Library for Avaya Aura Communication Manager 7.1.x.*
- [8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [9] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [10] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for OneAccess-Telstra Business SIP is available from Telstra.

©2018 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.