



Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

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

Table of Contents

| | | |
|-------|---|----|
| 1. | Introduction..... | 4 |
| 2. | General Test Approach and Test Results..... | 5 |
| 2.1 | Interoperability Compliance Testing..... | 5 |
| 2.2 | Test Results | 6 |
| 2.3 | Support | 6 |
| 3. | Reference Configuration | 7 |
| 4. | Equipment and Software Validated | 8 |
| 5. | Configure Avaya Aura® Communication Manager | 9 |
| 5.1 | System-Parameters Customer-Options | 9 |
| 5.2 | System-Parameters Features | 10 |
| 5.3 | Dial Plan..... | 11 |
| 5.4 | IP Node Names..... | 12 |
| 5.5 | IP Interface for Procr..... | 12 |
| 5.6 | IP Network Regions | 13 |
| 5.7 | IP Codec Parameters | 15 |
| 5.8 | SIP Trunks..... | 16 |
| 5.8.1 | SIP Trunk for Evolve Voice SIP Trunking service access | 16 |
| 5.8.2 | SIP Trunk for Internal CPE access (Avaya SIP clients) | 19 |
| 5.9 | Calling Party Information..... | 22 |
| 5.10 | Incoming Call Handling Treatment..... | 23 |
| 5.11 | Outbound Routing..... | 23 |
| 5.12 | Avaya SIP Client Routing | 26 |
| 5.13 | Automatic Alternate Routing (AAR) Dialing | 27 |
| 5.14 | Avaya G450 Media Gateway Provisioning..... | 28 |
| 5.15 | Avaya Aura® Media Server Provisioning | 29 |
| 5.16 | Save Communication Manager Translations | 30 |
| 6. | Configure Avaya Aura® Session Manager | 31 |
| 6.1 | Configure SIP Domain | 32 |
| 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 – Outbound SIP Trunk | 34 |
| 6.3.3 | Configure Communication Manager SIP Entity – CPE Access | 35 |
| 6.3.4 | Configure Avaya SBCE SIP Entity | 36 |
| 6.4 | Configure Entity Links | 37 |
| 6.3.5 | Configure Entity Link to Communication Manager – Outbound SIP Trunk | 37 |
| 6.3.6 | Configure Entity Link to Communication Manager – CPE Access | 38 |
| 6.3.7 | Configure Entity Link for Avaya SBCE..... | 39 |
| 6.4 | Configure Routing Policies | 39 |
| 6.4.1 | Configure Routing Policy for Communication Manager..... | 40 |
| 6.4.2 | Configure Routing Policy for Avaya SBCE | 40 |
| 6.5 | Configure Dial Patterns..... | 41 |

| | | |
|-------|--|----|
| 7. | Configure Avaya Session Border Controller for Enterprise | 44 |
| 7.1 | Device Management – Status | 45 |
| 7.2 | Server Interworking Profiles | 47 |
| 7.2.1 | Server Interworking – Session Manager | 47 |
| 7.2.2 | Server Interworking – Optus EV | 51 |
| 7.3 | SIP Server Profiles | 53 |
| 7.3.1 | SIP Server – Session Manager | 53 |
| 7.3.2 | SIP Server – Optus EV | 55 |
| 7.4 | Routing Profiles..... | 57 |
| 7.4.1 | Routing – To Session Manager..... | 57 |
| 7.4.2 | Routing – To Optus EV | 58 |
| 7.5 | Topology Hiding | 59 |
| 7.5.1 | Topology Hiding – Session Manager | 59 |
| 7.5.2 | Topology Hiding – Optus EV | 59 |
| 7.6 | Domain Policies | 60 |
| 7.6.1 | Application Rules..... | 60 |
| 7.6.2 | Border Rules | 60 |
| 7.6.3 | Media Rules | 61 |
| 7.6.4 | Signaling Rules | 61 |
| 7.6.5 | Endpoint Policy Groups..... | 62 |
| 7.7 | Network & Flows | 63 |
| 7.7.1 | Network Management..... | 63 |
| 7.7.2 | Media Interfaces..... | 63 |
| 7.7.3 | Signaling Interface | 64 |
| 7.7.4 | Endpoint Flows – For Session Manager | 65 |
| 7.7.5 | Endpoint Flows – For Optus EV..... | 66 |
| 8. | Verification Steps..... | 67 |
| 8.1 | Avaya Session Border Controller for Enterprise..... | 67 |
| 8.2 | Avaya Aura® Communication Manager | 70 |
| 8.3 | Avaya Aura® Session Manager Status | 70 |
| 8.4 | Telephony Services | 71 |
| 9. | Conclusion | 72 |
| 10. | Additional References..... | 73 |

1. Introduction

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

Avaya Aura® Session Manager 8.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 8.1 is a telephony application. The Avaya SBCE is the point of connection between the Enterprise and the Optus Evolve Voice SIP Trunking Service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The Evolve Voice SIP Trunking Service available from Optus is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The Optus Evolve Voice SIP Trunking Service allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

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

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

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

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

2. General Test Approach and Test Results

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

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

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

2.1 Interoperability Compliance Testing

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

- Incoming calls to Avaya SIP and H.323 phones on the enterprise site from PSTN phone via the Optus Evolve Voice SIP Trunk.
- Outgoing calls from Avaya SIP and H.323 phones on the enterprise site via Optus Evolve Voice SIP trunk to PSTN destination
- Calls using G.711A and G.729A audio codecs.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls Incoming and Outgoing PSTN calls to/from Avaya One-X® Communicator and Avaya Equinox™ for Windows soft phones.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Place and receive calls on EC500 mobile client to/from Avaya SIP and H.323 phones as well as PSTN phones
- Network Call Redirection – Inbound vector call to call center agent queues
- Fax calls from/to other enterprise fax machine via the Optus evolve Voice SIP Trunk using T.38 (with fallback to G.711 is enabled).Incoming and outgoing calls between Avaya Remote Worker phones and PSTN phones

2.2 Test Results

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

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

- **Faxing** – Optus Evolve Voice supports Fax t.38 fallback to G.711 mode. At the time of compliance testing, there are circumstances t.38 was successfully negotiated between Optus Evolve Voice and Avaya Aura, but there is no t.38 fax data transmitted toward Avaya Aura. Optus should continue investigating the issue from Optus Evolve Voice network to understand the issue.
- **Call Forward** – If original calling number is not part of DID range assigned to the SIP Trunk, the pilot number will be presented to the forward target.
- **EC500 service with Confirmed Answer enabled** - With Initial IP-IP Direct Media enabled on the SIP signaling group toward to Optus Evolve Voice SIP Trunking Service, the ec500 call leg is established with no voice as soon as EC500 user answers the call on mobile. This results in a call drop after the confirmation timeout (default to 10 seconds). If EC500 service with Confirmed Answer setting is required, the **Initial IP-IP Direct Media** must be disabled on the signaling group which is used for (or shared with) EC500 service.
- **Emergency ‘000’ Services Limitations and Restrictions** - Although Optus provides Emergency Services dialing on ‘000’, Optus does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with Optus Evolve SIP Trunking Service to complete ‘000’ calls; therefore, it is the customer’s responsibility to ensure proper operation with its equipment/software vendor.
While the Optus Evolve SIP Trunking Service does support ‘000’ calling capabilities under certain Calling Plans, there are circumstances when that ‘000’ service may not be available. Such circumstances include, but are not limited to, relocation of the end user’s CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer’s location in the automatic location information database.
- **Avaya Network Call Redirection (NCR) must be disabled** (default) on the Avaya Aura® Communication Manager SIP trunk to the Optus Evolve Voice SIP Trunking Service as Optus Evolve Voice does not support REFER.

2.3 Support

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

3. Reference Configuration

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

- Avaya Aura® Communication Manager running on VMware ESXi 6.0.
- Avaya Aura® Session Manager running on VMware ESXi 6.0.
- Avaya Aura® System Manager running on VMware ESXi 6.0.
- Avaya Aura® Messaging running on VMware ESXi 6.0.
- Avaya G450 Media Gateway.
- Avaya Aura® Media Server running on VMware ESXi 6.0. The Media Server can act as a media gateway Gxxx series.
- Avaya IP phones are represented with Avaya 9600/1600 Series IP Telephones running H.323/SIP software.
- Avaya one-X® Communicator 6.2
- Avaya Equinox for Windows 3.5
- The Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Optus Evolve Voice SIP Trunking Service and the enterprise internal network.

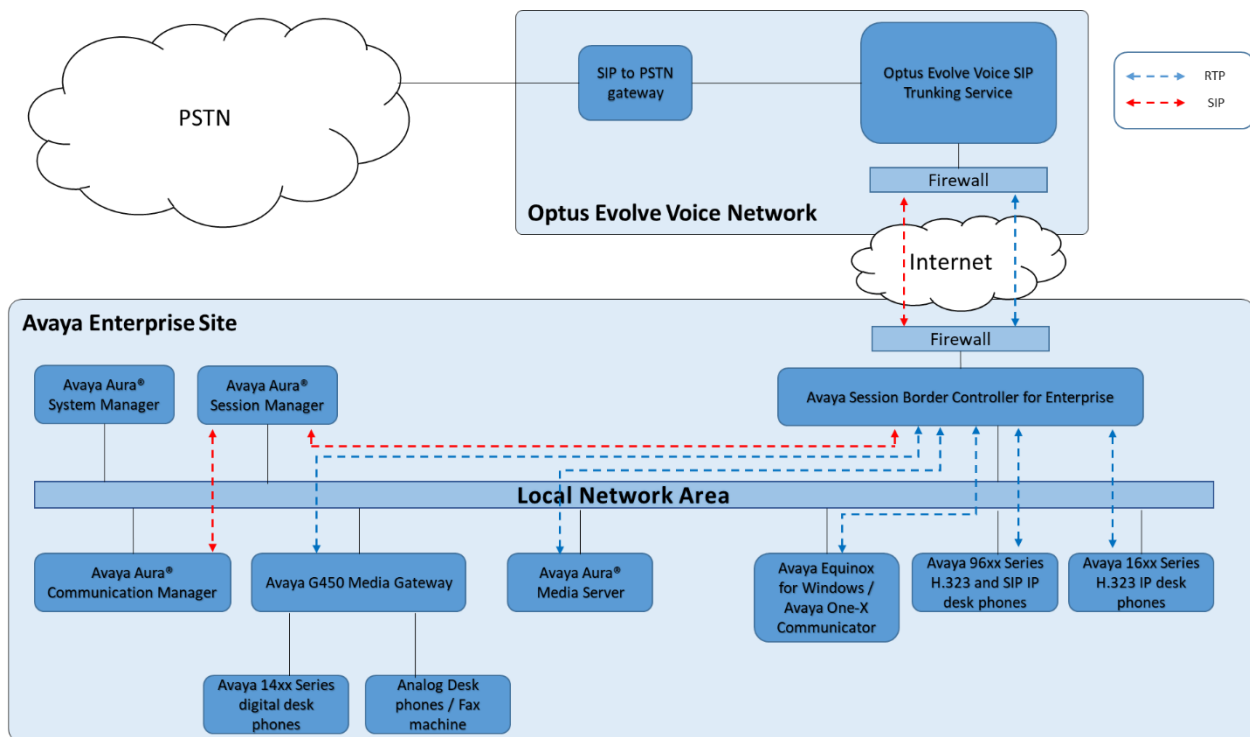


Figure 1: Test Setup Optus Evolve Voice to Avaya Enterprise

4. Equipment and Software Validated

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

| Component | Version |
|--|--|
| Avaya | |
| Avaya Aura Communication Manager 8.1 SP1 | 8.1.0.0.890-25393 |
| Avaya Aura Session Manager 8.1 | 8.1.0.0.810007 |
| Avaya Aura System Manager 8.1 | Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.9814 |
| Avaya Aura Messaging 7.1 | 7.1.0.0.532 |
| Avaya Session Border Controller for Enterprise 8.0 | 8.0.0.0-19-16991 |
| Avaya Media Gateway G450 | g450_sw_41_9_0 |
| Avaya Aura Media Server 8.0 | 8.0.0.205 |
| Avaya One-X Communicator 6.2 | 6.2.13.2 |
| Avaya Equinox for Windows 3.5 | 3.5.7.30.1 |
| Avaya One-X Agent H323 2.5.8 | 2.5.60313.0 |
| Avaya 96x1 series – SIP phone | 7.1.5 |
| Avaya 96xx series – H.323 phone | 3.2.8 |
| Avaya 16xx series – H.323 phone | 1.3.12 |
| Service Provider – Optus Evolve Voice | |
| Genband CS2000 | Release 18 |
| Acme Packet SBC | SCZ7.2.0 MR-2 GA (Build 252) |

5. Configure Avaya Aura® Communication Manager

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

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these Application Notes. Other parameter values may or may not match based on local configurations. The Communication Manager SAT console, the Avaya SMGR Web UI and the Avaya SBCE Web UI captured in this sections are displaying the configuration those have been configured earlier. The actual Communication Manager SAT commands, Avaya SMGR Web UI and Avaya SBCE Web UI to create/add the configurations may vary.

5.1 System-Parameters Customer-Options

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

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

Follow the steps shown below:

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

| display system-parameters customer-options | | | Page | 2 of | 12 |
|---|--|--|-------------|-----------|----|
| OPTIONAL FEATURES | | | | | |
| IP PORT CAPACITIES | | | USED | | |
| Maximum Administered H.323 Trunks: | | | 4000 | 0 | |
| Maximum Concurrently Registered IP Stations: | | | 1000 | 1 | |
| Maximum Administered Remote Office Trunks: | | | 4000 | 0 | |
| Max Concurrently Registered Remote Office Stations: | | | 1000 | 0 | |
| Maximum Concurrently Registered IP eCons: | | | 68 | 0 | |
| Max Concur Reg Unauthenticated H.323 Stations: | | | 100 | 0 | |
| Maximum Video Capable Stations: | | | 2400 | 0 | |
| Maximum Video Capable IP Softphones: | | | 1000 | 1 | |
| Maximum Administered SIP Trunks: | | | 4000 | 10 | |
| Max Administered Ad-hoc Video Conferencing Ports: | | | 4000 | 0 | |
| Max Number of DS1 Boards with Echo Cancellation: | | | 80 | 0 | |

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

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

5.2 System-Parameters Features

Follow the steps shown below:

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

| display system-parameters features | | Page 1 of 19 |
|--|--|--------------|
| FEATURE-RELATED SYSTEM PARAMETERS | | |
| Self Station Display Enabled? n | | |
| Trunk-to-Trunk Transfer: all | | |
| Automatic Callback with Called Party Queuing? n | | |
| Automatic Callback - No Answer Timeout Interval (rings): 3 | | |
| Call Park Timeout Interval (minutes): 10 | | |
| Off-Premises Tone Detect Timeout Interval (seconds): 20 | | |
| AAR/ARS Dial Tone Required? y | | |
| Music (or Silence) on Transferred Trunk Calls? no | | |
| DID/Tie/ISDN/SIP Intercept Treatment: attendant | | |
| Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred | | |
| Automatic Circuit Assurance (ACA) Enabled? n | | |
| Abbreviated Dial Programming by Assigned Lists? n | | |
| Auto Abbreviated/Delayed Transition Interval (rings): 2 | | |
| Protocol for Caller ID Analog Terminals: Bellcore | | |
| Display Calling Number for Room to Room Caller ID Calls? n | | |

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

```

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

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

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

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

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

```

5.3 Dial Plan

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

Follow the steps shown below:

- Enter the **change dialplan analysis** command to provision the following dial plan.
 - 4-digit extensions with a **Call Type** of **ext** beginning with:
 - The digits **83** for Communication Manager extensions (which is assigned by Optus as DID numbers).
 - 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code * for SIP Trunk Access Codes (TAC).

| change dialplan analysis | | | | | | Page 1 of 12 | | |
|--------------------------|--------------|-----------|---------------|--------------|-----------|-----------------|--------------|-----------|
| DIAL PLAN ANALYSIS TABLE | | | | | | | | |
| Location: all | | | | | | Percent Full: 2 | | |
| Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type |
| 000 | 3 | udp | | | | | | |
| 13 | 6 | udp | | | | | | |
| 1300 | 10 | udp | | | | | | |
| 18 | 10 | udp | | | | | | |
| 9 | 1 | fac | | | | | | |
| # | 4 | fac | | | | | | |
| 83 | 4 | ext | | | | | | |
| * | 3 | dac | | | | | | |

5.4 IP Node Names

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

Follow the steps shown below:

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

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

5.5 IP Interface for Procr

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

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

| display ip-interface procr | | Page 1 of 2 |
|----------------------------|---------------------------------|-------------|
| IP INTERFACES | | |
| Type: PROCR | | |
| Target socket load: 4800 | | |
| Enable Interface? y | Allow H.323 Endpoints? y | |
| Network Region: 1 | Allow H.248 Gateways? y | |
| | Gatekeeper Priority: 5 | |
| IPV4 PARAMETERS | | |
| Node Name: procr | IP Address: 10.1.20.10 | |

5.6 IP Network Regions

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

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

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

                                IP NETWORK REGION
Region: 1                NR Group: 1
Location: 1              Authoritative Domain: sipinterop.net
                        Name: optus                Stub Network Region: n
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
                        Codec Set: 1              Inter-region IP-IP Direct Audio: yes
                        UDP Port Min: 2048        IP Audio Hairpinning? n
                        UDP Port Max: 53999
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS      AUDIO RESOURCE RESERVATION PARAMETERS
                        RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic in region 1. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, the Avaya Media Server, IP/SIP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields.

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

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

| | | | | | |
|---------------------------|--|------|--------------------------|----|---|
| change ip-interface procr | | Page | 1 | of | 2 |
| IP INTERFACES | | | | | |
| Type: PROCr | | | | | |
| Target socket load: 19660 | | | | | |
| Enable Interface? y | | | Allow H.323 Endpoints? y | | |
| Network Region: 1 | | | Allow H.248 Gateways? y | | |
| | | | Gatekeeper Priority: 5 | | |
| IPV4 PARAMETERS | | | | | |
| Node Name: procr | | | IP Address: 10.1.20.10 | | |
| Subnet Mask: /24 | | | | | |

To define network region 1 for the 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: | 10IS11367055 | |
| Link Encryption Type: | any-ptls/tls | Enable CF? n |
| Network Region: 1 | | Location: 1 |
| | | Site Data: |
| Recovery Rule: | none | |
| Registered? | y | |
| FW Version/HW Vintage: | 41 .9 .0 /2 | |
| MGP IPV4 Address: | 10.1.20.20 | |
| MGP IPV6 Address: | | |
| Controller IP Address: | 10.1.20.10 | |
| MAC Address: | 00:1b:4f:3e:a5:e0 | |
| Mutual Authentication? | optional | |

5.7 IP Codec Parameters

Follow the steps shown below:

1. Enter the **change ip-codec-set x** command, where **x** is the number of the IP codec set specified in **Section 5.6**. On **Page 1** of the **ip-codec-set** form, ensure that **G.711A**, **G.729A** 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 MEDIA PARAMETERS | | |
| Codec Set: 1 | | |
| Audio | Silence | Frames |
| Codec | Suppression | Per Pkt |
| | | Size(ms) |
| 1: G.711A | n | 20 |
| 2: G.729 | n | 20 |
| 3: G.711MU | n | 20 |
| 5: | | |
| 6: | | |
| 7: | | |

2. On **Page 2** of the ip-codec-set form, set **t.38-G711-fallback**.

| | | | |
|--|---------------------------|-----------------|---------------------|
| change ip-codec-set 1 | | Page 2 of 2 | |
| IP MEDIA PARAMETERS | | | |
| Allow Direct-IP Multimedia? y | | | |
| Maximum Call Rate for Direct-IP Multimedia: 15360:Kbits | | | |
| Maximum Call Rate for Priority Direct-IP Multimedia: 15360:Kbits | | | |
| | Mode | Redun- dancy | Packet Size (ms) |
| FAX | t.38-G711-fallback | 0 | ECM: y FB-Timer: 4 |
| Modem | off | 0 | |
| TDD/TTY | US | 3 | |
| H.323 Clear-channel | n | 0 | |
| SIP 64K Data | n | 0 | 20 |

5.8 SIP Trunks

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group. Two SIP trunks are defined on Communication Manager in the reference configuration:

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

5.8.1 SIP Trunk for Evolve Voice SIP Trunking service access

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

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **sm-ve**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6**.
- **Far-end Domain** – Enter **sipinterop.net**. This is the domain provisioned for Session Manager in **Section 6.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.

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

| display signaling-group 1 | | Page 1 of 3 |
|---|------------------------------------|------------------------------|
| SIGNALING GROUP | | |
| Group Number: 1 | Group Type: sip | |
| IMS Enabled? n | Transport Method: tcp | |
| Q-SIP? n | | |
| IP Video? y | Priority Video? n | Enforce SIPS URI for SRTP? y |
| Peer Detection Enabled? y | Peer Server: SM | Clustered? n |
| Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y | | |
| Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n | | |
| Alert Incoming SIP Crisis Calls? n | | |
| Near-end Node Name: procr | Far-end Node Name: sm-ve | |
| Near-end Listen Port: 5060 | Far-end Listen Port: 5060 | |
| | Far-end Network Region: 1 | |
| Far-end Domain: sipinterop.net | | |
| Incoming Dialog Loopbacks: eliminate | Bypass If IP Threshold Exceeded? n | |
| DTMF over IP: rtp-payload | RFC 3389 Comfort Noise? n | |
| Session Establishment Timer(min): 3 | Direct IP-IP Audio Connections? y | |
| Enable Layer 3 Test? y | IP Audio Hairpinning? n | |
| H.323 Station Outgoing Direct Media? y | Initial IP-IP Direct Media? y | |
| | Alternate Route Timer(sec): 6 | |

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

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

```

display trunk-group 1                                     Page 1 of 4
                                     TRUNK GROUP
Group Number: 1                Group Type: sip                CDR Reports: y
  Group Name: Optus-EV-Trunk      COR: 1                TN: 1                TAC: *01
  Direction: two-way            Outgoing Display? n
  Dial Access? n                Night Service:
  Queue Length: 0
  Service Type: public-ntwrk      Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 10

```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end.

Note - Optus Evolve Voice SIP Trunking service screens the calling party number for valid DID numbers. At the time of testing, Full National Number (FNN) format (10-digit number starting with 0) is required to be sent to Optus network for properly presenting calling party number to called party. Otherwise, pilot number will be presented. Setting the **Numbering Format** field to public may result in “+” to be inserted to the calling number, and thus fails the screening.

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

```

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

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

                                     Replace Restricted Numbers? y
                                     Replace Unavailable Numbers? y

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

```

On **Page 4**, set the **Network Call Redirection** field should be set to **n**. Setting the **Network Call Redirection** flag to **y** enables SIP REFER for call transfer.

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

| | |
|---|--------------------|
| display trunk-group 1 | Page 4 of 4 |
| PROTOCOL VARIATIONS | |
| Mark Users as Phone? n | |
| Prepend '+' to Calling/Alerting/Diverting/Connected Number? n | |
| Send Transferring Party Information? y | |
| Network Call Redirection? n | |
| Send Diversion Header? y | |
| Support Request History? n | |
| Telephone Event Payload Type: 101 | |
| Convert 180 to 183 for Early Media? n | |
| Always Use re-INVITE for Display Updates? n | |
| Identity for Calling Party Display: P-Asserted-Identity | |
| Block Sending Calling Party Location in INVITE? n | |
| Accept Redirect to Blank User Destination? y | |
| Enable Q-SIP? n | |
| Interworking of ISDN Clearing with In-Band Tones: keep-channel-active | |
| Request URI Contents: may-have-extra-digits | |

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

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

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **sm-ve**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6**.
- **Far-end Domain** – Enter **sipinterop.net**. This is the domain provisioned for Session Manager in **Section 6.1**.

- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway / Avaya Media Server when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- **Initial IP-IP Direct Media** – Set to **y**, indicating that the RTP paths should be initially direct between Avaya SIP stations and the internal interface of ASBCE, to the use of media resources on the Avaya Media Gateway / Avaya Media Server.
- **H.323 Station Outgoing Direct Media** – Set to **y**, indicating that the RTP paths should be also initially direct for the H.323 stations, to avoid the use of media resources on the Avaya Media Gateway / Avaya Media Server.
- Default values may be used for all other fields.

```

display signaling-group 3                                     Page 1 of 3
                                SIGNALING GROUP

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

Far-end Domain: sipinterop.net

Incoming Dialog Loopbacks: eliminate                      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                      RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3                      Direct IP-IP Audio Connections? y
                                                IP Audio Hairpinning? n
Enable Layer 3 Test? y                      Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? y                      Alternate Route Timer(sec): 6

```

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

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

| | | | |
|------------------------------|------------------------|---------------------------------------|-----------------|
| display trunk-group 3 | | Page 1 of 4 | |
| TRUNK GROUP | | | |
| Group Number: 3 | Group Type: sip | CDR Reports: y | |
| Group Name: SIP-OPTIM | COR: 1 | TN: 1 | TAC: *01 |
| Direction: two-way | Outgoing Display? n | Night Service: | |
| Dial Access? n | | | |
| Queue Length: 0 | | | |
| Service Type: tie | Auth Code? n | | |
| | | Member Assignment Method: auto | |
| | | Signaling Group: 3 | |
| | | Number of Members: 10 | |

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Default values may be used for all other fields.

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

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

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

5.9 Calling Party Information

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

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

In the sample configuration, the 02xxxxx3xx DID numbers provided for testing were assigned to the extensions 83xx. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk (trunk 1) when calls were originated from these extensions.

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

| | | | | | | | |
|----------------------------|------|--------|---------|--|-------|-----------------------|---|
| Change private-numbering 0 | | | | | Page | 1 of | 2 |
| NUMBERING - PRIVATE FORMAT | | | | | | | |
| Ext | | Trk | Private | | Total | | |
| Len | Code | Grp(s) | Prefix | | Len | | |
| 4 | 83 | 1 | 02xxxx | | 10 | Total Administered: 2 | |
| 4 | 83 | 3 | | | 4 | Maximum Entries: 540 | |

Note: the actual number in above example configuration is masked with **xxxx**

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 Optus 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 | 3 |
| INCOMING CALL HANDLING TREATMENT | | | | | | |
| Service/ | Number | Number | Del | Insert | | |
| Feature | Len | Digits | | | | |
| public-ntwrk | 10 | 02xxxx | 6 | | | |

Note: the actual number in above example configuration is masked with **xxxx**

5.11 Outbound Routing

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

| | | | | | | |
|---------------------------------|----------|------------|--------|-----------------|-------------|-----------|
| change dialplan analysis | | | | Page | 1 of | 12 |
| DIAL PLAN ANALYSIS TABLE | | | | | | |
| Location: all | | | | Percent Full: 2 | | |
| Dialed | Total | Call | Dialed | Total | Call | Dialed |
| String | Length | Type | String | Length | Type | String |
| 000 | 3 | udp | | | | |
| 13 | 6 | udp | | | | |
| 1300 | 10 | udp | | | | |
| 18 | 10 | udp | | | | |
| 83 | 4 | ext | | | | |
| * | 3 | dac | | | | |
| # | 4 | fac | | | | |
| 9 | 1 | fac | | | | |

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

| | |
|--|-----------------------|
| change feature-access-codes | Page 1 of 12 |
| FEATURE ACCESS CODE (FAC) | |
| Abbreviated Dialing List1 Access Code: | |
| Abbreviated Dialing List2 Access Code: | |
| Abbreviated Dialing List3 Access Code: | |
| Abbreviated Dial - Prgm Group List Access Code: | |
| Announcement Access Code: | |
| Answer Back Access Code: | |
| Attendant Access Code: | |
| Auto Alternate Routing (AAR) Access Code: | |
| Auto Route Selection (ARS) - Access Code 1: 9 | Access Code 2: |
| 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 String | Total | | Route | Call | Node | ANI |
| | Min | Max | Pattern | Type | Num | Reqd |
| 000 | 3 | 3 | 1 | emer | | n |
| 0011 | 12 | 20 | 1 | pubu | | n |
| 02 | 10 | 10 | 1 | pubu | | n |
| 03 | 10 | 10 | 1 | pubu | | n |
| 04 | 10 | 10 | 1 | pubu | | n |
| 06 | 10 | 10 | 1 | pubu | | n |
| 07 | 10 | 10 | 1 | pubu | | n |
| 08 | 10 | 10 | 1 | pubu | | n |
| 13 | 6 | 6 | 1 | pubu | | n |
| 1300 | 10 | 10 | 1 | pubu | | n |
| 18 | 10 | 10 | 1 | pubu | | n |
| 8399 | 4 | 4 | 1 | pubu | | n |
| xxxxxxxx | 8 | 8 | 1 | pubu | | n |

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for **route pattern 1** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **1** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** **unk-unk**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.8.1**.

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

5.12 Avaya SIP Client Routing

Route Patterns are used to direct calls to the Local SIP trunk for access to SIP phones or other destinations in the CPE. Use the **change route-pattern** command to configure the parameters for **route pattern 3** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **3** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** **lev0-pvt**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.8.2**.

| | | | | | | | | | | | | |
|-----------------------|-----|---------------|--------|--------------------------|---------------|-----------------|----------|------|-----------|-------------------------|------|---|
| chage route-pattern 3 | | | | | | | | | | Page | 1 of | 4 |
| Pattern Number: 3 | | | | | | | | | | Pattern Name: SIP-OPTIM | | |
| SCCAN? n | | Secure SIP? n | | Used for SIP stations? y | | | | | | | | |
| Primary SM: sm-ve | | | | | Secondary SM: | | | | | | | |
| Grp | FRL | NPA | Pfx | Hop | Toll | No. | Inserted | | | DCS/ | IXC | |
| No | | Mrk | Lmt | List | Del | Digits | | | QSIG | | | |
| | | | | | | | Dgts | | | Intw | | |
| 1: | 3 | 0 | | | | | | | | n | user | |
| 2: | | | | | | | | | | n | user | |
| 3: | | | | | | | | | | n | user | |
| 4: | | | | | | | | | | n | user | |
| 5: | | | | | | | | | | n | user | |
| 6: | | | | | | | | | | n | user | |
| BCC VALUE | | TSC | CA-TSC | ITC BCIE | | Service/Feature | PARM | Sub | Numbering | LAR | | |
| 0 | 1 | 2 | M | 4 | W | Request | Dgts | | Format | | | |
| 1: | y | y | y | y | y | n | n | rest | lev0-pvt | none | | |
| 2: | y | y | y | y | y | n | n | rest | | none | | |
| 3: | y | y | y | y | y | n | n | rest | | none | | |
| 4: | y | y | y | y | y | n | n | rest | | none | | |
| 5: | y | y | y | y | y | n | n | rest | | none | | |

5.13 Automatic Alternate Routing (AAR) Dialing

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

| | | | | | | | |
|--------------------------|---------|---------|------|------|------|--|-----------------|
| change aar analysis 0 | | | | | | | Page 1 of 2 |
| AAR DIGIT ANALYSIS TABLE | | | | | | | |
| Location: all | | | | | | | Percent Full: 0 |
| Dialed | Total | Route | Call | Node | ANI | | |
| String | Min Max | Pattern | Type | Num | Reqd | | |
| 83xx | 4 4 | 3 | lev0 | | n | | |
| | | | | | n | | |

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for **route pattern 1** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **1** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** unk-unk. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.8.2**.

| | | | | | | | | | | | | | | | | | | | | |
|------------------------|--|---------------|-----|--------------------------|-----|----------|---|---|----------|---|------|-------------------------|--------|-----|------|-----------------|------|--------|-----------|-----|
| change route-pattern 3 | | | | | | | | | | | | Page | 1 of | 4 | | | | | | |
| Pattern Number: 3 | | | | | | | | | | | | Pattern Name: SIP-OPTIM | | | | | | | | |
| SCCAN? n | | Secure SIP? n | | Used for SIP stations? y | | | | | | | | | | | | | | | | |
| Primary SM: sm-ve | | | | Secondary SM: | | | | | | | | | | | | | | | | |
| Grp FRL NPA | | Pfx | Hop | Toll | No. | Inserted | | | DCS/ IXC | | | | | | | | | | | |
| No | | Mrk | Lmt | List | Del | Digits | | | QSIG | | | | | | | | | | | |
| | | | | | | | | | | | | Intw | | | | | | | | |
| 1: 3 | | 0 | | | | | | | | | | n | user | | | | | | | |
| 2: | | | | | | | | | | n | user | | | | | | | | | |
| 3: | | | | | | | | | | n | user | | | | | | | | | |
| 4: | | | | | | | | | | n | user | | | | | | | | | |
| 5: | | | | | | | | | | n | user | | | | | | | | | |
| 6: | | | | | | | | | | n | user | | | | | | | | | |
| BCC VALUE | | | | | | | | | | | | TSC | CA-TSC | ITC | BCIE | Service/Feature | PARM | Sub | Numbering | LAR |
| 0 1 2 M 4 W | | | | | | | | | | | | Request | | | | Dgts | | Format | | |
| 1: | | Y | Y | Y | Y | Y | n | n | rest | | | lev0-pvt | | | none | | | | | |
| 2: | | Y | Y | Y | Y | Y | n | n | rest | | | | | | none | | | | | |
| 3: | | Y | Y | Y | Y | Y | n | n | rest | | | | | | none | | | | | |
| 4: | | Y | Y | Y | Y | Y | n | n | rest | | | | | | none | | | | | |
| 5: | | Y | Y | Y | Y | Y | n | n | rest | | | | | | none | | | | | |
| 6: | | Y | Y | Y | Y | Y | n | n | rest | | | | | | none | | | | | |

5.14 Avaya G450 Media Gateway Provisioning

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

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

1. SSH to the G450 (not shown). Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., **g450-???(*super*)#**).
2. Enter the **show system** command and note the G450 serial number (e.g., **10IS11367055**).
3. Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.1.20.10**).
4. Enter the **copy run copy start command** to save the G450 configuration.
5. On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown).

Enter the following parameters:

- Set **Type** = **G450**.
- Set **Name** = Enter a descriptive name (e.g., **g450**).
- Set **Serial Number** = Enter the serial number copied from **Step 2**.
- Set the **Encrypt Link** parameter as desired (**any-ptls/tls** was used in the reference configuration).
- Set **Network Region** = **1**.

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

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

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

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

      Recovery Rule: none

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

Mutual Authentication? optional
```

5.15 Avaya Aura® Media Server Provisioning

In the reference configuration, an Avaya Aura® Media Server is provisioned. The Media Server is located in the Main site and is used, along with the G450 Media Gateway, for local DSP resources, announcements, and Music On Hold.

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **Peer Detection Enabled?** is set to **n**.
- **Peer Server** to **AMS**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Media Server as administered in **Section 5.4** (e.g., **ams-ve**).
- **Near-end Listen Port** – Set to **9061**.
- **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6**.
- **Far-end Domain** – Automatically populated with the IP address of the Media Server.

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

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

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

```
display media-server 1

                                MEDIA SERVER

                                Media Server ID: 1

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

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

5.16 Save Communication Manager Translations

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

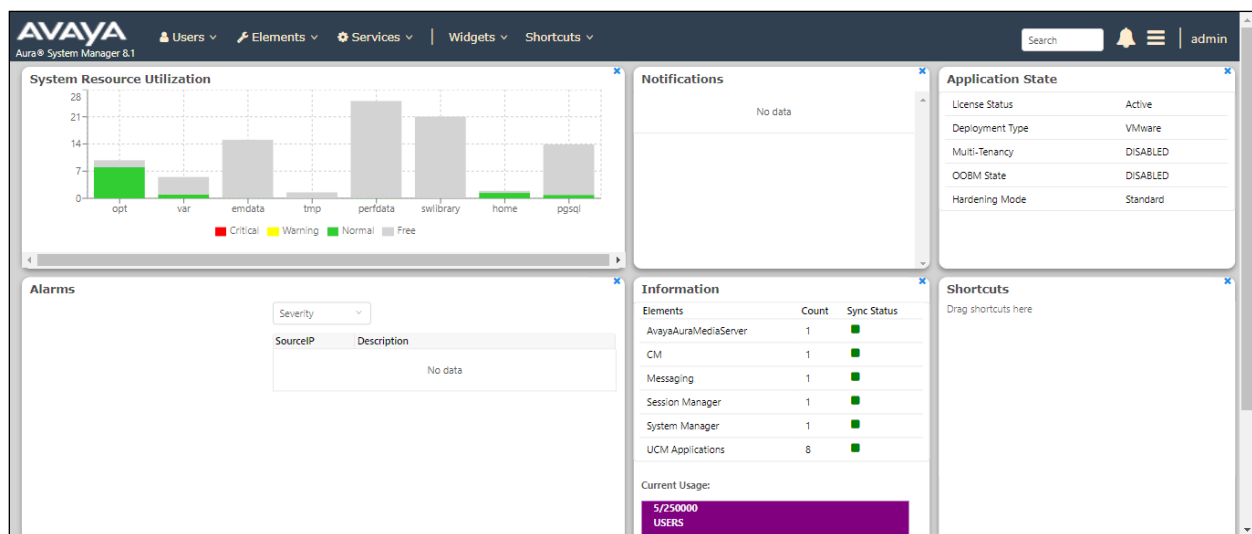
6. Configure Avaya Aura® Session Manager

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

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

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

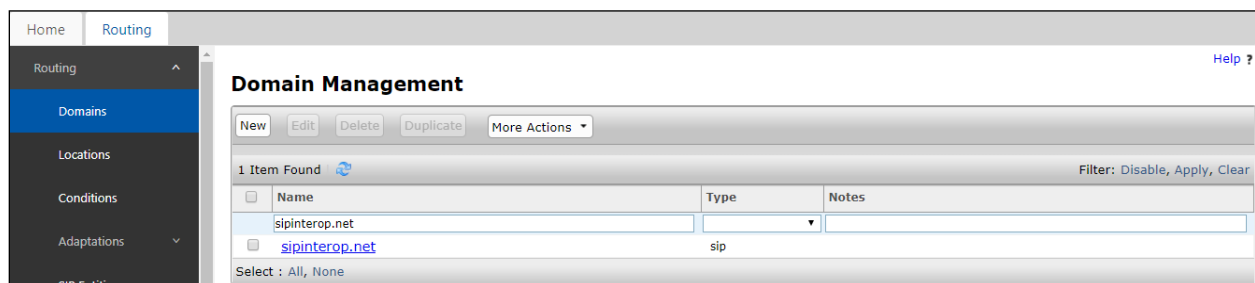
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the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



6.1 Configure SIP Domain

Follow the steps shown below:

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

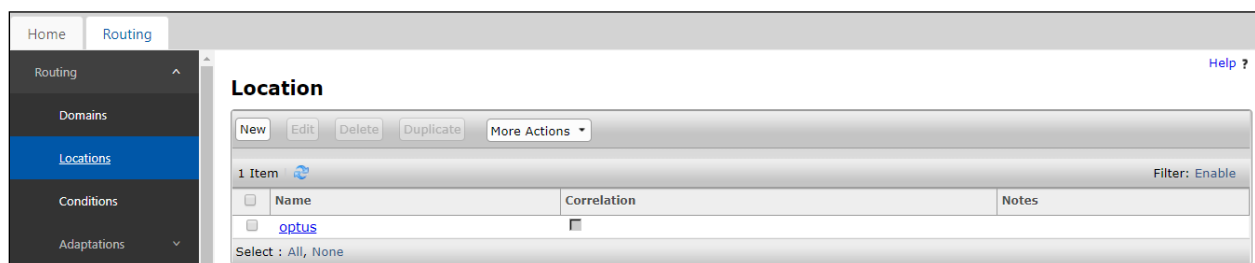


6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **optus** 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., **optus**).
 - **Notes:** Add a brief description.
2. Click **Commit** to save.



6.3 Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE.

6.3.1 Configure Session Manager SIP Entity

Follow the steps shown below

1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g., **sm-ve**).
 - **IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.1.20.7**).
 - **SIP FQDN** – (Optional) Leave blank or enter the SIP FQDN of Session Manager signaling interface (e.g., **sm-ve-sm100.sipinterop.net**)
 - **Type** – Verify **Session Manager** is selected.
 - **Location** – Select location **optus**.
 - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
 - **Time Zone** – Select the time zone in which Session Manager resides.
3. In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
 - Use the default values for the remaining parameters.

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar has 'SIP Entities' selected under the 'Routing' section. The main content area has two tabs: 'General' and 'Monitoring'. The 'General' tab is active, displaying the following fields:

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

The 'Monitoring' tab is also visible, showing:

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

Buttons for 'Commit' and 'Cancel' are located at the top right of the main content area.

6.3.2 Configure Communication Manager SIP Entity – Outbound SIP Trunk

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g. **cm-ve**).
 - **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) (e.g. **10.1.20.10**).
 - **Type** – Select **CM**.
 - **Location** – Select a Location **Optus** administered in **Section 6.2**.
 - **Time Zone** – Select the time zone in which Communication Manager resides.
3. In the **Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field
 - Use the default values for the remaining parameters.
4. Click on **Commit**.

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

6.3.3 Configure Communication Manager SIP Entity – CPE Access

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

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

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

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

SIP Entity Details

Commit Cancel

Help ?

General

* Name: cm-ve-optim

* FQDN or IP Address: 10.1.20.10

Type: CM

Notes:

Adaptation:

Location: optus

Time Zone: Australia/Sydney

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

6.3.4 Configure Avaya SBCE SIP Entity

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

- **Name** – Enter a descriptive name (e.g., **sbce_A1**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.1.20.9**).
- **Type** – Verify **SIP Trunk** is selected.
- **Location** – Select location **optus** (**Section 6.2**).

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

| Section | Field | Value |
|----------------|-----------------------------------|-----------------------------------|
| General | Name | sbce_A1 |
| | FQDN or IP Address | 10.1.20.9 |
| | Type | SIP Trunk |
| | Notes | |
| | Adaptation | |
| | Location | optus |
| | Time Zone | Australia/Sydney |
| | SIP Timer B/F (in seconds) | 4 |
| | Minimum TLS Version | Use Global Setting |
| | Credential name | |
| Loop Detection | Securable | <input type="checkbox"/> |
| | Call Detail Recording | egress |
| | Loop Detection Mode | On |
| Monitoring | Loop Count Threshold | 5 |
| | Loop Detection Interval (in msec) | 200 |
| | SIP Link Monitoring | Use Session Manager Configuration |
| Monitoring | CRLF Keep Alive Monitoring | Use Session Manager Configuration |

6.4 Configure Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager defined in **Section 6.3.1**.
- **Protocol:** Select the transport protocol used for this link, **TCP** for the Entity Link to Communication Manager and **TCP** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager.
- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.3.2**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section 6.3.4**
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.3.5 Configure Entity Link to Communication Manager – Outbound SIP Trunk

Follow the steps shown below:

1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name (or have it created automatically) for this link to Communication Manager (e.g., **sm-ve_cm-ve_5060_TCP**).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.3.1** for Session Manager (e.g., **sm-ve**).
 - **SIP Entity 1 Port** – Enter **5060**.
 - **Protocol** – Select **TCP**.
 - **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.2** for the Communication Manager entity (e.g., **cm-ve**).
 - **SIP Entity 2 Port** – Enter **5060**.
 - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.

6.3.6 Configure Entity Link to Communication Manager – CPE Access

To configure this Entity Link, repeat the steps in **Section 6.3.5**, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., **sm-ve_cm-ve-optim_5061_TLS**).
- **SIP Entity 1 Port** – Enter **5061**.
- **Protocol** – Select **TLS**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.3** for the Communication Manager entity (e.g., **cm-ve-optim**).
- **SIP Entity 2 Port** - Enter **5061**.
- Click on **Commit**.

6.3.7 Configure Entity Link for Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.3.5**, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., **sm-ve_sbce_A1_5060_TCP**).
- **SIP Entity 1 Port** – Enter **5060**.
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.4** for the Avaya SBCE entity (e.g., **sbce_A1**).
- **SIP Entity 2 Port** - Enter **5060**.

The screenshot shows the 'Entity Links' configuration page. The left navigation pane has 'Entity Links' selected. The main area displays a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The values in the table are: Name: sm-ve_sbce_A1_5060_TCP, SIP Entity 1: sm-ve, Protocol: TCP, Port: 5060, SIP Entity 2: sbce_A1, Port: 5060, DNS Override: unchecked, Connection Policy: trusted, Deny New Service: unchecked, and Notes: empty. There are 'Commit' and 'Cancel' buttons at the top and bottom right of the table area.

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

6.4 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.

6.4.1 Configure Routing Policy for Communication Manager

This Routing Policy is used for inbound calls from Optus.

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 Optus calls to Communication Manager (e.g., **to cm-ve**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
4. In the **SIP Entity List** page, select the SIP Entity administered in **Section 6.3.2** for the Communication Manager SIP Entity (**cm-ve**), and click on **Select**.
5. Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.
6. No **Regular Expressions** were used in the reference configuration.
7. Click on **Commit**.

The screenshot shows the 'Routing Policy Details' page for a policy named 'to cm-ve'. The left sidebar is under the 'Routing' tab, with 'Routing Policies' selected. The main content area has a 'General' section with fields for 'Name' (to cm-ve), 'Disabled' (unchecked), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table. The table has columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. One entry is visible: 'cm-ve' with IP '10.1.20.10' and Type 'CM'. At the bottom, there is a 'Time of Day' section.

| Name | FQDN or IP Address | Type | Notes |
|-------|--------------------|------|-------|
| cm-ve | 10.1.20.10 | CM | |

6.4.2 Configure Routing Policy for Avaya SBCE

This Routing Policy is used for outbound calls to the service provider. Repeat the steps in **Section 6.4.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **to sbce**).
- **SIP Entity List** – Select the SIP Entity administered in **Section 6.3.4** for the Avaya SBCE entity (e.g., **sbce_A1**).

The screenshot shows the 'Routing Policy Details' page for a policy named 'to sbce'. The left sidebar is under the 'Routing' tab, with 'Routing Policies' selected. The main content area has a 'General' section with fields for 'Name' (to sbce), 'Disabled' (unchecked), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table. The table has columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. One entry is visible: 'sbce_A1' with IP '10.1.20.9' and Type 'SIP Trunk'. At the bottom, there is a 'Time of Day' section.

| Name | FQDN or IP Address | Type | Notes |
|---------|--------------------|-----------|-------|
| sbce_A1 | 10.1.20.9 | SIP Trunk | |

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

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

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

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

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

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

The first example shows that 10-digit dialed numbers starting with 02 that has a destination domain of “All” uses route policy to **sbce** as defined in **Section 6.4.2**.

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 02

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

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

Select : All, None

The second example shows that outbound any 8-digit numbers uses route policy to Avaya SBCE as defined in **Section 6.4.2** for PSTN calls.

The screenshot shows the 'Dial Pattern Details' configuration page. The left sidebar lists navigation options: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main content area is titled 'Dial Pattern Details' and includes a 'General' section with the following fields:

- * Pattern: xxxxxxxx
- * Min: 8
- * Max: 8
- Emergency Call: ☐
- SIP Domain: -ALL-
- Notes: (empty)

 Below the 'General' section is the 'Originating Locations and Routing Policies' section, which contains a table with 1 item. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The single row shows 'optus' as the Originating Location Name, 'to sbce' as the Routing Policy Name, and 'sbce_A1' as the Routing Policy Destination. The Rank is 0. There are 'Add' and 'Remove' buttons above the table, and a 'Filter: Enable' link on the right.

The third example shows that 10-digit pattern that start with 02xxxxx3 (the actual number is masked with “x”) is used for inbound calls from Optus to DID numbers on Avaya Aura® Communication Manager.

The screenshot shows the 'Dial Pattern Details' configuration page. The left sidebar is the same as the previous screenshot. The main content area is titled 'Dial Pattern Details' and includes a 'General' section with the following fields:

- * Pattern: 02xxxxx3
- * Min: 10
- * Max: 10
- Emergency Call: ☐
- SIP Domain: -ALL-
- Notes: (empty)

 Below the 'General' section is the 'Originating Locations and Routing Policies' section, which contains a table with 1 item. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The single row shows '-ALL-' as the Originating Location Name, 'to cm-ve' as the Routing Policy Name, and 'cm-ve' as the Routing Policy Destination. The Rank is 0. There are 'Add' and 'Remove' buttons above the table, and a 'Filter: Enable' link on the right.

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

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:** 000

* **Min:** 3

* **Max:** 3

Emergency Call: ☒

* **Emergency Priority:** 1

* **Emergency Type:** All

SIP Domain: -ALL-

Notes: emergency simulator

Originating Locations and Routing Policies

Add Remove Filter: Enable

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

7. Configure Avaya Session Border Controller for Enterprise

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

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

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (10.1.20.9), with access to the **Optus** site. The connection to Optus uses the Avaya SBCE public interface B1 (IP address 192.168.1.2). The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

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



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

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



This screenshot shows the same login page as the previous one, but now with a "Password:" label and a password input field containing eight dots. A "Log In" button has appeared below the password field. The rest of the page content, including the Avaya logo, disclaimer, and copyright notice, remains the same.

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

Session Border Controller for Enterprise AVAYA

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

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
 - DoS / DDoS
 - Scrubber
 - User Agents
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Dashboard

Information

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

Installed Devices

| Device Name |
|-------------|
| sbce |

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

| |
|--|
| sbce: Heartbeat Successful, Server is UP |
| sbce: Heartbeat Successful, Server is UP |
| sbce: Heartbeat Successful, Server is UP |
| sbce: Heartbeat Successful, Server is UP |

7.1 Device Management – Status

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

Session Border Controller for Enterprise AVAYA

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

Device Management

EMS Dashboard

- Device Management**
- Backup/Restore
- System Parameters
 - DoS / DDoS
 - Scrubber
 - User Agents
- Configuration Profiles

Devices | Updates | SSL VPN | Licensing | Key Bundles

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

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

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: 0

0

CES Sessions

Requested: 0

0

Transcoding Sessions

Requested: 0

0

CLID

Encryption

Available: Yes

☒

Network Configuration

| IP | Public IP | Network Prefix or Subnet Mask | Gateway | Interface |
|-------------|-------------|-------------------------------|-------------|-----------|
| 10.1.20.9 | 10.1.20.9 | 255.255.255.0 | 10.1.20.1 | A1 |
| 10.1.20.19 | 10.1.20.19 | 255.255.255.0 | 10.1.20.1 | A1 |
| 192.168.1.2 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 | B1 |
| 192.168.1.3 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | B1 |
| 135.27.78.6 | 135.27.78.6 | 255.255.255.248 | 135.27.78.1 | A2 |

DNS Configuration

Primary DNS

10.1.20.3

Secondary DNS

DNS Location

DMZ

DNS Client IP

192.168.1.2

Management IP(s)

IP #1 (IPv4)

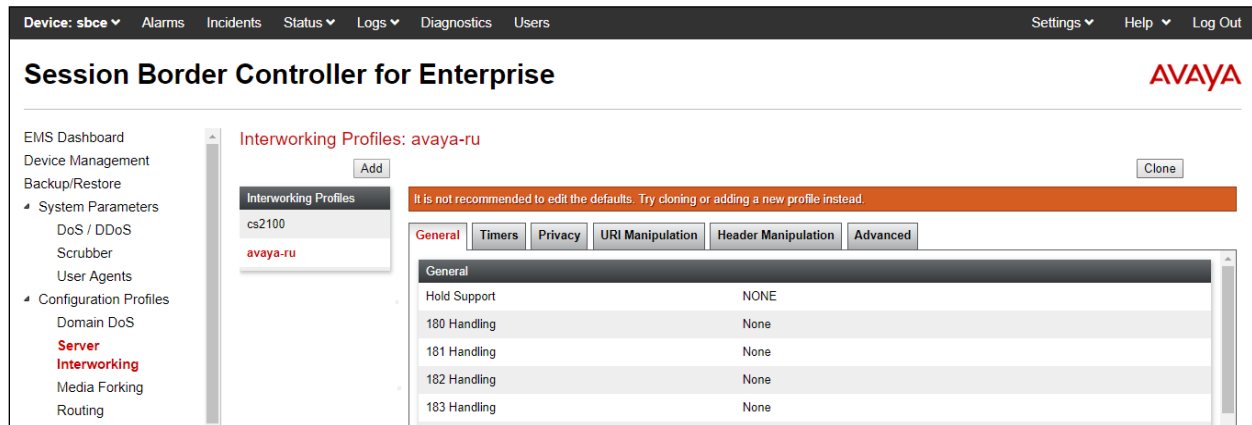
10.1.20.8

7.2 Server Interworking Profiles

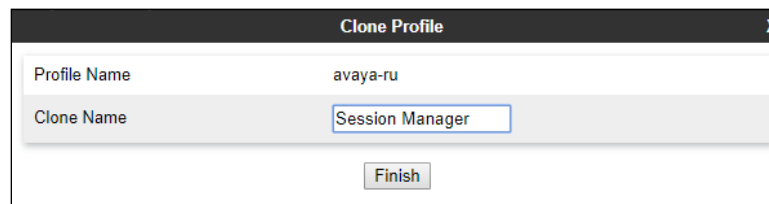
7.2.1 Server Interworking – Session Manager

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

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



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



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

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

On the left, a sidebar menu lists various configuration options, including EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, and Services. The "Session Manager" profile is highlighted in the "Interworking Profiles" section.

The main content area is titled "Interworking Profiles: Session Manager". It features a table of profiles with columns for Name, Description, and Actions (Rename, Clone, Delete). The "Session Manager" profile is selected, and its configuration is displayed in the "General" tab.

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

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

- Check **T38 Support**.
- All other options can be left with default values, and click **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 settings are as follows:

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

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

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

The screenshot shows the 'Editing Profile: Session Manager' window. The 'Record Routes' section has radio buttons for 'None', 'Single Side', 'Both Sides' (selected), 'Dialog-Initiate Only (Single Side)', and 'Dialog-Initiate Only (Both Sides)'. The 'Include End Point IP for Context Lookup' checkbox is checked. The 'Extensions' dropdown is set to 'Avaya'. The 'Diversion Manipulation' checkbox is unchecked. The 'Diversion Condition' dropdown is set to 'None'. The 'Diversion Header URI' field is empty. The 'Has Remote SBC' checkbox is checked. The 'Route Response on Via Port' checkbox is unchecked. The 'Relay INVITE Replace for SIPREC' checkbox is unchecked. The 'MOBX Re-INVITE Handling' checkbox is unchecked. The 'DTMF' section has radio buttons for 'None' (selected), 'SIP Notify', 'RFC 2833 Relay & SIP Notify', 'SIP Info', 'RFC 2833 Relay & SIP Info', and 'Inband'. A 'Finish' button is at the bottom.

7.2.2 Server Interworking – Optus EV

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

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

The screenshot shows a window titled "Editing Profile: Optus EV" with a close button (X) in the top right corner. The window contains a "General" tab with various configuration options. The options and their current states are as follows:

| Option | Value/State |
|--------------------------|--|
| Hold Support | <input type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input checked="" 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 type="radio"/> None <input checked="" type="radio"/> SDP <input type="radio"/> No SDP |
| Refer Handling | <input type="checkbox"/> |
| URI Group | None (dropdown menu) |
| Send Hold | <input type="checkbox"/> |
| Delayed Offer | <input checked="" type="checkbox"/> |
| 3xx Handling | <input type="checkbox"/> |
| Diversion Header Support | <input type="checkbox"/> |
| Delayed SDP Handling | <input type="checkbox"/> |
| Re-Invite Handling | <input type="checkbox"/> |
| Prack Handling | <input type="checkbox"/> |
| Allow 18X SDP | <input type="checkbox"/> |
| T.38 Support | <input checked="" type="checkbox"/> |
| URI Scheme | <input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY |
| Via Header Format | <input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543 |

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

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

Editing Profile: Optus EV

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

Nortel

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

Relay INVITE Replace for SIPREC

☐

MOBX Re-INVITE Handling

☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ RFC 2833 Relay & SIP Notify

☐ SIP Info

☐ RFC 2833 Relay & SIP Info

☐ Inband

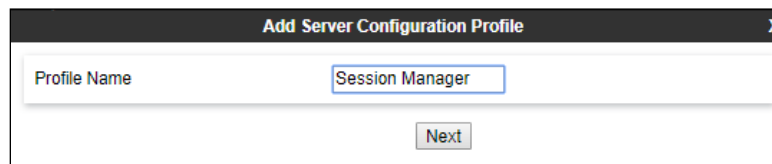
Finish

7.3 SIP Server Profiles

7.3.1 SIP Server – Session Manager

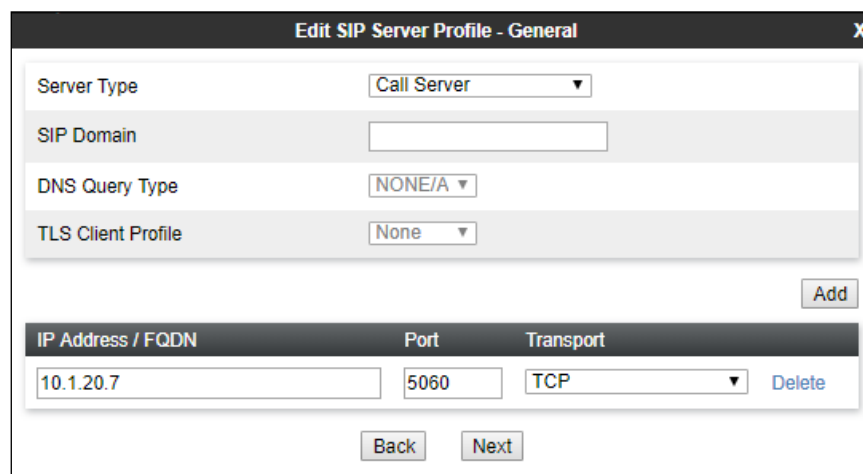
This section defines the SIP Server Profile for the Avaya SBCE connection to Session Manager.

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



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

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



The screenshot shows a window titled "Edit SIP Server Profile - General" with a close button (X) in the top right corner. The window contains several fields and a table. The fields are: "Server Type" (dropdown menu set to "Call Server"), "SIP Domain" (text input field), "DNS Query Type" (dropdown menu set to "NONE/A"), and "TLS Client Profile" (dropdown menu set to "None"). Below these fields is an "Add" button. At the bottom of the window is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "10.1.20.7", "5060", and "TCP". To the right of the table is a "Delete" button. Below the table are "Back" and "Next" buttons.

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| 10.1.20.7 | 5060 | TCP |

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

5. The **Advanced** window will open.
- For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.1**.
 - Check **Enable Grooming**.
 - Select **Finish**.

Edit SIP Server Profile - Advanced X

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

Finish

7.3.2 SIP Server – Optus EV

Repeat the steps in **Section 7.3.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Optus EV Trunk Group.

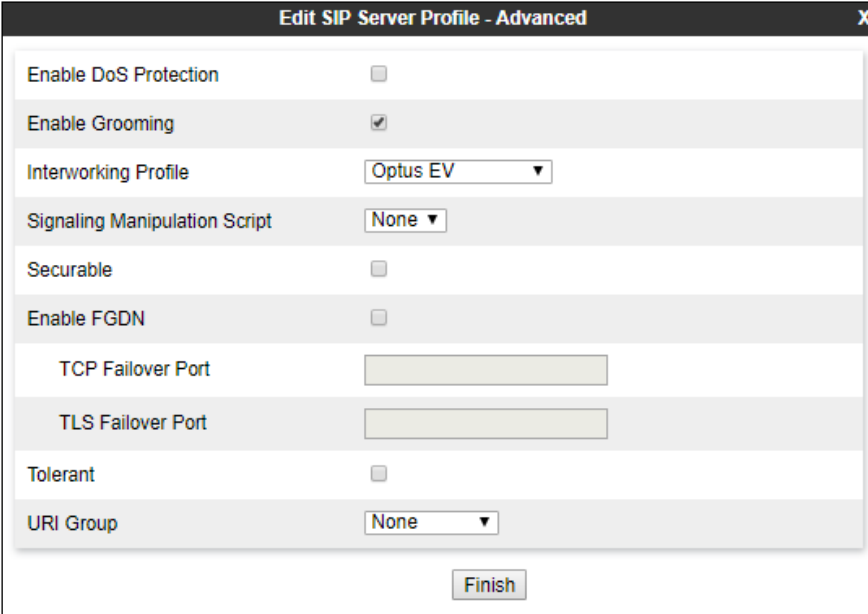
1. Select **Add Profile** and enter a Profile Name (e.g., **Optus EV**) and select **Next**.
2. On the **General** window (not shown), enter the following.
 - Select **Server Type: Trunk Server**.
 - **IP Address / FQDN: x.x.x.x** (outbound proxy of Optus).
 - **Transport: Select UDP**.
 - **Port: 5060**.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

| IP Address / FQDN | Port | Transport |
|-------------------|------|-----------|
| x.x.x.x | 5060 | UDP |

3. Under Heartbeat window:
 - Select **Enable Heartbeat**.
 - **Method:** choose **OPTIONS**.
 - **Frequency:** enter **60**.
 - **From URI** and **To URI:** enter **sbcsipinterop.net**.

| | |
|------------------|-------------------------------------|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method | OPTIONS |
| Frequency | 60 seconds |
| From URI | sbcsipinterop.net |
| To URI | sbcsipinterop.net |

4. Under **Advanced** window:
- Check **Enable Grooming**.
 - Select **Optus EV** for Interworking Profile.



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

| | |
|-------------------------------|-------------------------------------|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input checked="" type="checkbox"/> |
| Interworking Profile | Optus EV ▼ |
| 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 ▼ |

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

7.4 Routing Profiles

7.4.1 Routing – To Session Manager

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

1. Select **Configuration Profiles** → **Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Session Manager**) and click **Next**.
3. The **Routing Profile** window will open. Using the default values shown, click on **Add**.
4. The **Next-Hop Address** window will open. Populate the following fields:
 - **Priority/Weight** = **1**
 - **SIP Server Profile** = **Session Manager**.
 - **Next Hop Address**: Verify that the **10.1.20.7:5060 (TCP)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
 - Click on **Finish**.

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

7.4.2 Routing – To Optus EV

Repeat the steps in **Section 7.4.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Optus.

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

Profile : Optus EV - Edit Rule

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

Add

| Priority / Weight | LDAP Search Attribute | LDAP Search Regex Pattern | LDAP Search Regex Result | SIP Server Profile | Next Hop Address | Transport |
|-------------------|-----------------------|---------------------------|--------------------------|--------------------|------------------|-----------|
| 1 | | | | Optus EV | x.x.x.x:5060 | None |

Delete

Finish

7.5 Topology Hiding

7.5.1 Topology Hiding – Session Manager

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Configuration Profiles', and 'Topology Hiding' is selected. The 'Topology Hiding Profiles: Session Manager' window is open. The 'Add' button is visible. The 'Topology Hiding' table is populated with the following headers and values:

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

7.5.2 Topology Hiding – Optus EV

Repeat the steps in **Section 7.5.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Optus.

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Configuration Profiles', and 'Topology Hiding' is selected. The 'Topology Hiding Profiles: Optus EV' window is open. The 'Add' button is visible. The 'Topology Hiding' table is populated with the following headers and values:

| Header | Criteria | Replace Action | Overwrite Value |
|--------------|-----------|----------------|---------------------------|
| Refer-To | IP/Domain | Overwrite | sip201.ippbx.optus.com.au |
| Referred-By | IP/Domain | Overwrite | sip201.ippbx.optus.com.au |
| Record-Route | IP/Domain | Auto | --- |
| To | IP/Domain | Overwrite | sip201.ippbx.optus.com.au |
| SDP | IP/Domain | Overwrite | sip201.ippbx.optus.com.au |
| Via | IP/Domain | Auto | --- |
| From | IP/Domain | Overwrite | sip201.ippbx.optus.com.au |
| Request-Line | IP/Domain | Overwrite | sip201.ippbx.optus.com.au |

7.6 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. Avaya SBCE has pre-defined / default Rules and Policies under Domain Policies. Although the default Rules and Policies are editable, it is highly recommended to clone the Rules and/or Policies before modification as needed. The compliance test was commenced using the default rules and policies without any modification.

7.6.1 Application Rules

Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 200 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: sbce, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. The left sidebar contains a menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, and Domain Policies. Under Domain Policies, "Application Rules" is selected. The main content area shows "Application Rules: default" with an "Add" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, a table lists application rules. The "default" rule is selected, showing details for Audio and Video sessions. The Audio rule has a maximum of 200 concurrent sessions and 5 sessions per endpoint. The Video rule has a maximum of 5 concurrent sessions and 5 sessions per endpoint. A "Miscellaneous" section shows "CDR Support" as Off and "RTCP Keep-Alive" as No.

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

| Miscellaneous | |
|-----------------|-----|
| CDR Support | Off |
| RTCP Keep-Alive | No |

7.6.2 Border Rules

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface, specifically the Border Rules configuration page. The top navigation bar and main header are identical to the previous screenshot. The left sidebar shows "Domain Policies" expanded, with "Border Rules" selected. The main content area shows "Border Rules: default" with an "Add" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, a table lists border rules. The "default" rule is selected, showing details for NAT Traversal. The "default" rule has "Enable Natting" checked, "Use SIP Published IP" checked, and "Use SDP Published IP" checked.

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

7.6.3 Media Rules

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

The screenshot shows the 'Media Rules: default-low-med' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules (selected), Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies, and TLS Management. The main content area has a header 'Media Rules: default-low-med' with an 'Add' button and a 'Clone' button. Below this is a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration is divided into four tabs: Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Under 'Audio Encryption', 'Preferred Formats' is set to 'RTP' and 'Interworking' is checked. Under 'Video Encryption', 'Preferred Formats' is set to 'RTP' and 'Interworking' is checked. A 'Miscellaneous' section at the bottom shows 'Capability Negotiation' is unchecked.

7.6.4 Signaling Rules

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

The screenshot shows the 'Signaling Rules: default' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar is the same as in the previous screenshot, with 'Signaling Rules' selected. The main content area has a header 'Signaling Rules: default' with an 'Add' button and a 'Clone' button. Below this is a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration is divided into seven tabs: General, Requests, Responses, Request Headers, Response Headers, Signaling QoS, and UCID. The 'General' tab is active, showing 'Non-2XX Final Responses' set to 'Allow', 'Optional Request Headers' set to 'Allow', and 'Optional Response Headers' set to 'Allow'. An 'Outbound' section shows 'Requests' set to 'Allow', 'Non-2XX Final Responses' set to 'Allow', 'Optional Request Headers' set to 'Allow', and 'Optional Response Headers' set to 'Allow'. A 'Content-Type Policy' section shows 'Enable Content-Type Checks' checked, 'Action' set to 'Allow', 'Multipart Action' set to 'Allow', and an 'Exception List'.

7.6.5 Endpoint Policy Groups

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

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

On the left, a sidebar menu lists various configuration categories: System Parameters, Configuration Profiles, Services, and Domain Policies. Under Domain Policies, sub-items include Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Charging Rules, and End Point Policy Groups (highlighted in red).

The main content area is titled "Policy Groups: default-low" and features an "Add" button. Below this, a list of policy groups is shown: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, and avaya-def-low-enc. The "default-low" group is selected.

A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new group instead." Below this, a blue bar prompts the user to "Click here to add a row description."

The "Policy Group" configuration table is displayed with the following data:

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

7.7 Network & Flows

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

7.7.1 Network Management

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

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

| Name | Gateway | Subnet Mask / Prefix Length | Interface | IP Address | |
|----------|-------------|-----------------------------|-----------|--------------------------|-------------|
| A1 | 10.1.20.1 | 255.255.255.0 | A1 | 10.1.20.9, 10.1.20.19 | Edit Delete |
| B1-Optus | 192.168.1.1 | 255.255.255.0 | B1 | 192.168.1.2, 192.168.1.3 | Edit Delete |

7.7.2 Media Interfaces

1. Select **Network & Flows** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name: Media_A1.**
 - **IP Address: 10.1.20.9** (Avaya SBCE A1 address).
 - **Port Range: 35000-40000.**
4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name: Optus media.**
 - **IP Address: 192.168.1.2** (Avaya SBCE B1 address).
 - **Port Range: 35000-40000.**

- Click **Finish** (not shown). Note that changes to these values require an application restart.
The completed **Media Interface** screen is shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left-hand navigation menu is expanded to 'Network & Flows', and 'Media Interface' is selected. The main content area displays a table of configured Media Interfaces.

| Name | Media IP Network | Port Range | |
|---------------|--------------------------------------|---------------|-------------|
| Media_A1 | 10.1.20.9 A1 (A1, VLAN 0) | 35000 - 40000 | Edit Delete |
| Optus media | 192.168.1.2 B1-Optus (B1, VLAN 0) | 35000 - 40000 | Edit Delete |
| remote worker | 192.168.1.3 B1-Optus (B1, VLAN 0) | 35000 - 40000 | Edit Delete |
| remote access | 135.27.78.6 A2 (A2, VLAN 0) | 35000 - 40000 | Edit Delete |
| Media_A1_RW | 10.1.20.19 A1 (A1, VLAN 0) | 35000 - 40000 | Edit Delete |

7.7.3 Signaling Interface

- Select **Network & Flows** from the menu on the left-hand side (not shown).
- Select **Signaling Interface**.
- Select **Add** (not shown) and enter the following:
 - Name:** **Signaling_A1**.
 - IP Address:** **10.1.20.9** (Avaya SBCE A1 address).
 - TCP Port:** **5060**.
 - UDP Port:** **5060**.
 - TLS Port:** **5060**.
- Click **Finish** (not shown).
- Select **Add** again, and enter the following:
 - Name:** **Optus Signaling**.
 - IP Address:** **192.168.1.2** (Avaya SBCE B1 address).
 - UDP Port:** **5060**.
- Click **Finish** (not shown). Note that changes to these values require an application restart.

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left-hand navigation menu is expanded to 'Network & Flows', and 'Signaling Interface' is selected. The main content area displays a table of configured Signaling Interfaces.

| Name | Signaling IP Network | TCP Port | UDP Port | TLS Port | TLS Profile | |
|-----------------|--------------------------------------|----------|----------|----------|-------------|-------------|
| Optus Signaling | 192.168.1.2 B1-Optus (B1, VLAN 0) | 5060 | 5060 | --- | None | Edit Delete |
| remote worker | 192.168.1.3 B1-Optus (B1, VLAN 0) | 5060 | 5060 | 5061 | ServerB1 | Edit Delete |
| Signaling_A1 | 10.1.20.9 A1 (A1, VLAN 0) | 5060 | 5060 | 5061 | ServerA1 | Edit Delete |
| Signaling_A1_RW | 10.1.20.19 A1 (A1, VLAN 0) | 5060 | 5060 | 5061 | ServerA1 | Edit Delete |
| remote access | 135.27.78.6 A2 (A2, VLAN 0) | 5060 | 5060 | 5061 | ServerA1 | Edit Delete |

7.7.4 Endpoint Flows – For Session Manager

1. Select **Network & Flows** → **Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
 - **Name:** Session Manager.
 - **SIP Server Profile:** Session Manager.
 - **URI Group:** *.
 - **Transport:** *.
 - **Remote Subnet:** *.
 - **Received Interface:** Optus Signaling.
 - **Signaling Interface:** Signaling_A1.
 - **Media Interface:** Media_A1.
 - **End Point Policy Group:** default-low.
 - **Routing Profile:** Optus EV.
 - **Topology Hiding Profile:** Session Manager.
 - Let other values default.
4. Click **Finish** .

| Edit Flow: Session Manager | |
|-------------------------------|--------------------------|
| Flow Name | Session Manager |
| SIP Server Profile | Session Manager ▼ |
| URI Group | * ▼ |
| Transport | * ▼ |
| Remote Subnet | * |
| Received Interface | Optus Signaling ▼ |
| Signaling Interface | Signaling_A1 ▼ |
| Media Interface | Media_A1 ▼ |
| Secondary Media Interface | None ▼ |
| End Point Policy Group | default-low ▼ |
| Routing Profile | Optus EV ▼ |
| Topology Hiding Profile | Session Manager ▼ |
| Signaling Manipulation Script | None ▼ |
| Remote Branch Office | Any ▼ |
| Link Monitoring from Peer | <input type="checkbox"/> |
| Finish | |

7.7.5 Endpoint Flows – For Optus EV

Repeat step **1** through **4** from **Section 7.7.4**, with the following changes:

- **Name: Optus EV.**
- **SIP Server Profile : Optus EV.**
- **URI Group: *.**
- **Transport: *.**
- **Remote Subnet: *.**
- **Received Interface: Signaling_A1.**
- **Signaling Interface: Optus Signaling.**
- **Media Interface: Optus media.**
- **End Point Policy Group: default-low.**
- **Routing Profile: Session Manager.**
- **Topology Hiding Profile: Optus EV.**

| Edit Flow: Optus EV | |
|-------------------------------|--------------------------|
| Flow Name | Optus EV |
| SIP Server Profile | Optus EV |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Signaling_A1 |
| Signaling Interface | Optus Signaling |
| Media Interface | Optus media |
| Secondary Media Interface | None |
| End Point Policy Group | default-low |
| Routing Profile | Session Manager |
| Topology Hiding Profile | Optus EV |
| Signaling Manipulation Script | None |
| Remote Branch Office | Any |
| Link Monitoring from Peer | <input type="checkbox"/> |
| Finish | |

8. Verification Steps

The following steps may be used to verify the configuration.

8.1 Avaya Session Border Controller for Enterprise

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

Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Monitoring & Logging → Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **B1**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **10000**).
 - Specify a **Capture Filename** (e.g., **test.pcap**).
 - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
 - Click **Start Capture** to begin the trace.

The screenshot displays the Avaya SBCE web interface. The top navigation bar includes links for Device: sbce, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left sidebar lists various management options, with "Monitoring & Logging" expanded to show "Trace". The main content area is titled "Trace: sbce" and features a "Packet Capture" tab. Below this is a "Packet Capture Configuration" form with the following fields: Status (Ready), Interface (B1), Local Address (192.168.1.2), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). "Start Capture" and "Clear" buttons are at the bottom of the form.

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

Device: sbce ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

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

Trace: sbce

Packet CaptureCaptures

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

Packet Capture Configuration

StatusIn Progress

InterfaceB1 ▾

Local Address (IP:Port)192.168.1.2 ▾ : ▾

Remote Address *Port, IP, IP:Port

ProtocolAll ▾

Maximum Number of Packets to Capture10000

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

Stop Capture

3. Run the test.

4. When the test is completed, select the **Stop Capture** button shown above.

5. Click on the **Captures** tab and the packet capture is listed as a .pcap file with the date and time added to filename specified in **Step 2**.

6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

Device: sbce ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

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

Trace: sbce

Packet CaptureCaptures

Last Modified ▾Descending ▾SortResetRefresh

| File Name | File Size (bytes) | Last Modified | |
|--|-------------------|-------------------------------|--------|
| long_call_20190703182356.pcap | 962,560 | July 3, 2019 6:24:11 PM AEST | Delete |
| long_call_20190703171957.pcap | 2,373,471 | July 3, 2019 5:20:42 PM AEST | Delete |
| incoming_fax_from_Avaya_20190703110033.pcap | 2,335,680 | July 3, 2019 11:02:05 AM AEST | Delete |
| 7_4_6_20190703103026.pcap | 1,945,600 | July 3, 2019 10:31:03 AM AEST | Delete |
| 7_4_5_20190703102932.pcap | 2,224,128 | July 3, 2019 10:30:21 AM AEST | Delete |
| 7_4_2_20190703100118.pcap | 1,851,392 | July 3, 2019 10:02:09 AM AEST | Delete |
| 7_11_10_directMedia_networking_20190703093937.pcap | 1,404,928 | July 3, 2019 9:40:07 AM AEST | Delete |
| 7_11_10_directMedia_networking_20190703093832.pcap | 1,019,904 | July 3, 2019 9:38:57 AM AEST | Delete |
| 7_11_10_fail_20190702191328.pcap | 2,256,896 | July 2, 2019 7:14:10 PM AEST | Delete |
| 7_11_6_20190702191004.pcap | 274,432 | July 2, 2019 7:10:15 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 Optus Evolve Voice Service and the customer SIP PABX is the customer SBC. On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

• Ping from the SBC to the Optus network gateway.

• Ping from the SBC to the Session Manager.

DNA; Reviewed:
SPOC 8/31/2019

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

68 of 74
optusSBCEaura81

- Ping from the Optus network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

Device: sbce
Help

Diagnostics

Full Diagnostic
Ping Test

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

Stop Diagnostic

| Task Description | Status |
|---|--|
| ✓ EMS Link Check | M1 is operating within normal parameters with a full duplex connection at 1Gb/s. |
| ✓ SBC Link Check: A1 | A1 is operating within normal parameters with a full duplex connection at 1Gb/s. |
| ✓ SBC Link Check: A2 | A2 is operating within normal parameters with a full duplex connection at 1Gb/s. |
| 🔄 SBC Link Check: B1 | Running... |
| ✗ Ping: SBC (A1) to Gateway (10.1.20.1) | |
| ✗ Ping: SBC (A1) to Primary DNS (10.1.20.3) | |
| ✗ Ping: SBC (B1) to Gateway (192.168.1.1) | |
| ✗ Ping: SBC (B1) to Primary DNS (10.1.20.3) | |
| ✗ Ping: SBC (A2) to Gateway (135.27.78.1) | |
| ✗ Ping: SBC (A2) to Primary DNS (10.1.20.3) | |

Help

Incident Viewer

Device: sbce
Category: All
Clear Filters
Refresh
Generate Report

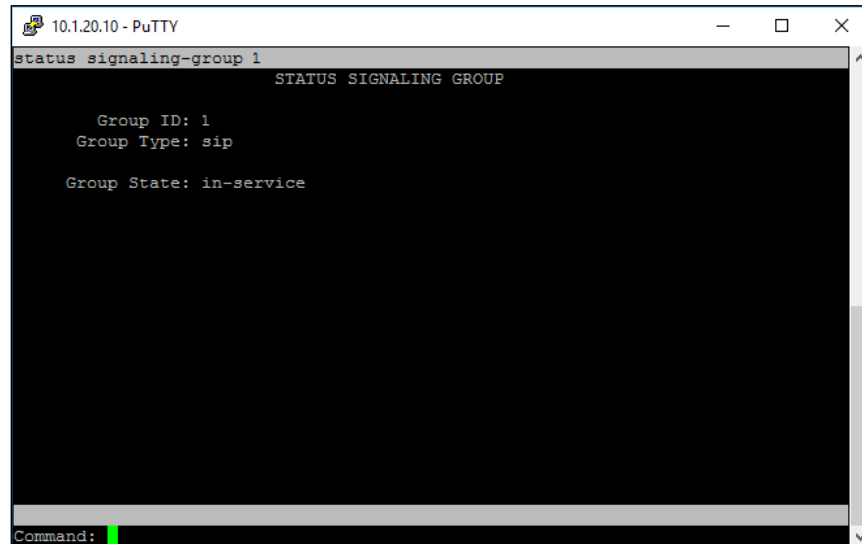
Displaying results 466 to 480 out of 2001.

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

8.2 Avaya Aura® Communication Manager

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

- Verify signaling status, trunk status



```
10.1.20.10 - PuTTY
status signaling-group 1
STATUS SIGNALING GROUP

Group ID: 1
Group Type: sip

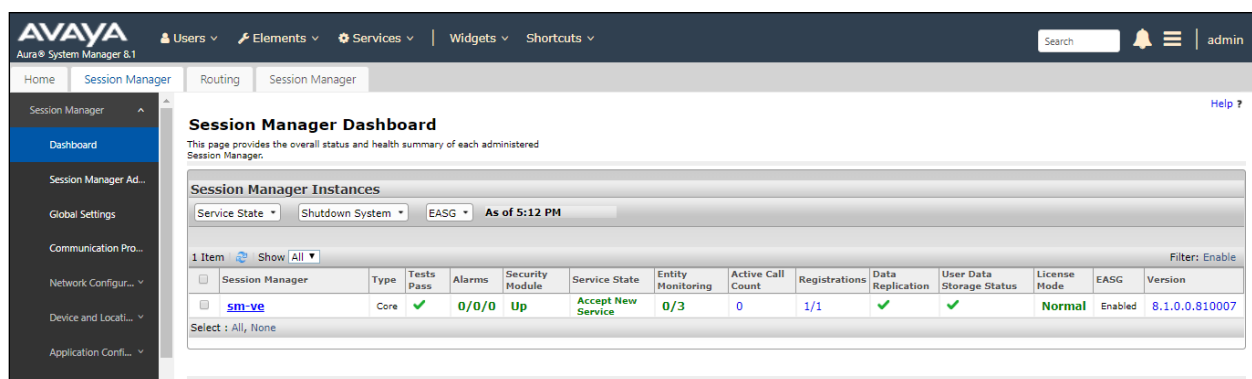
Group State: in-service

Command:
```

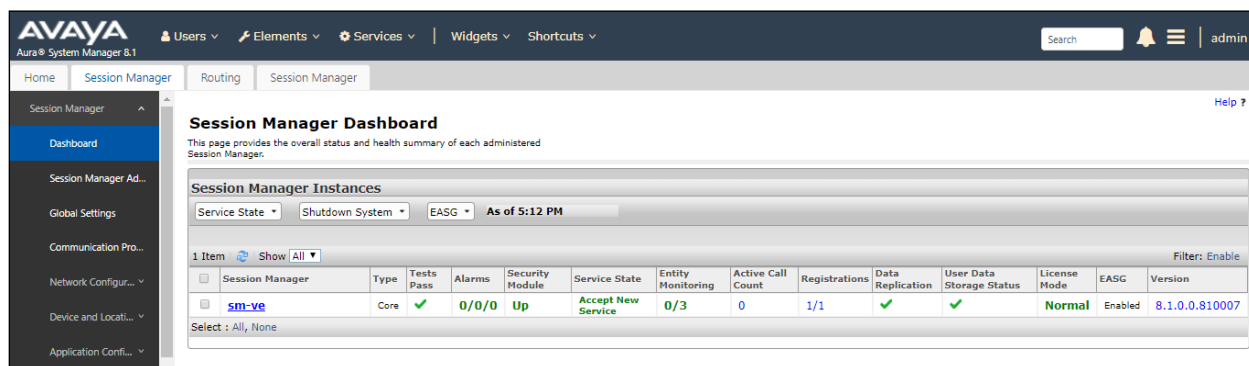
8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

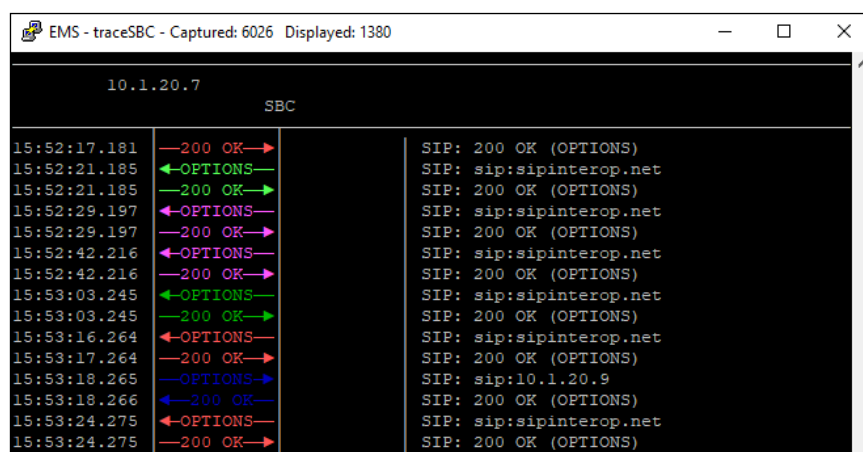
1. Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



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



Options messages between Avaya SBCE and Session Manager:



8.4 Telephony Services

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

9. Conclusion

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

10. Additional References

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

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

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.