



Application Notes for Configuring Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2 to support Clearcom SIP Trunk Service using TLS – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service on an enterprise solution consisting of Avaya Aura® Communication Manager Rel. 7.1, Avaya Aura® Session Manager Rel. 7.1 and Avaya Session Border Controller for Enterprise Rel. 7.2, to interoperate with the Clearcom SIP Trunk service using TLS.

The Clearcom SIP Trunk service provide customers with PSTN access via a SIP trunk between the enterprise and the service provider's network, as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	7
2.3.	Support	8
3.	Reference Configuration.....	9
4.	Equipment and Software Validated	12
5.	Configure Avaya Aura® Communication Manager.....	13
5.1.	Licensing and Capacity	13
5.2.	System Features.....	14
5.3.	IP Node Names.....	16
5.4.	Codecs	17
5.5.	IP Network Regions	19
5.6.	Signaling Group	20
5.7.	Trunk Group.....	23
5.8.	Calling Party Information.....	27
5.9.	Inbound Routing.....	28
5.10.	Outbound Routing	29
6.	Configure Avaya Aura® Session Manager	33
6.1.	System Manager Login and Navigation.....	34
6.2.	SIP Domain	35
6.3.	Locations	35
6.4.	Adaptations.....	38
6.5.	SIP Entities.....	40
6.6.	Entity Links	43
6.7.	Routing Policies	45
6.8.	Dial Patterns	46
7.	Configure Avaya Session Border Controller for Enterprise.....	49
7.1.	System Access.....	49
7.2.	System Management	51
7.3.	Network Management	55
7.4.	Media Interfaces.....	56
7.5.	Signaling Interfaces.....	58
7.6.	Server Interworking.....	60
7.6.1.	Server Interworking Profile – Enterprise.....	60
7.6.2.	Server Interworking Profile – Service Provider.....	62
7.7.	Signaling Manipulation	62
7.8.	Server Configuration	64
7.8.1.	Server Configuration Profile – Enterprise	64
7.8.2.	Server Configuration Profile – Service Provider	66
7.9.	Routing.....	70
7.9.1.	Routing Profile – Enterprise	70

7.9.2.	Routing Profile – Service Provider	71
7.10.	Topology Hiding.....	72
7.10.1.	Topology Hiding Profile – Enterprise.....	72
7.10.2.	Topology Hiding Profile – Service Provider.....	74
7.11.	Domain Policies.....	75
7.11.1.	Application Rules.....	75
7.11.2.	Media Rules.....	76
7.11.3.	Signaling Rules	79
7.12.	End Point Policy Groups	80
7.12.1.	End Point Policy Group – Enterprise	80
7.12.2.	End Point Policy Group – Service Provider.....	81
7.13.	End Point Flows.....	82
7.13.1.	End Point Flow – Enterprise	83
7.13.2.	End Point Flow – Service Provider.....	84
8.	Clearcom SIP Trunk Service Configuration	85
9.	Verification and Troubleshooting	85
9.1.	General Verification Steps	85
9.2.	Communication Manager Verification.....	85
9.3.	Session Manager Verification	86
9.4.	Avaya SBCE Verification	88
10.	Conclusion	93
11.	References.....	93
12.	Appendix A: SigMa Script.....	94

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunk Service between the Clearcom network and an Avaya SIP-enabled enterprise solution using Transport Layer Security (TLS). The Avaya solution consists of Avaya Aura® Communication Manager Rel. 7.1 (Communication Manager), Avaya Aura® Session Manager Rel. 7.1 (Session Manager), Avaya Session Border Controller for Enterprise (Avaya SBCE) Rel. 7.2 and various Avaya endpoints, listed in **Section 4**.

For privacy, TLS for Signaling was used inside of the enterprise (private network side) and outside of the enterprise (public network side). SRTP for media encryption was used inside of the enterprise (private network side). Outside of the enterprise (public network side) RTP was used.

The Clearcom SIP Trunking service referenced within these Application Notes is designed for business customers. Customers using this service with this Avaya enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

The terms “Service Provider” and “Clearcom” will be used interchangeably throughout these Application Notes.

2. General Test Approach and Test Results

A simulated CPE site containing all the equipment for the Avaya SIP-enabled enterprise solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Clearcom network via a broadband connection to the public Internet.

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

2.1. Interoperability Compliance Testing

To verify SIP Trunk interoperability, the following features and functionality were covered during the interoperability compliance test:

- SIP Trunk Registration (Dynamic Authentication).
- Response to SIP OPTIONS queries.
- Incoming calls from the PSTN were routed to DID numbers assigned by Clearcom. Incoming PSTN calls were terminated to the following endpoints: Avaya 96x1 Series IP Deskphones (H.323 and SIP), Avaya 2420 Digital Deskphones, Avaya one-X® Communicator softphone (H.323 and SIP), Avaya Equinox softphone (SIP) and analog Deskphones.
- Inbound and outbound PSTN calls to/from Remote Workers using Avaya 96x1 Deskphones (SIP).
- Outgoing calls to the PSTN were routed via Clearcom's network to various PSTN destinations.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.729A, G.711A and G.711MU.
- No matching codecs.
- Voicemail and DTMF tone support (leaving and retrieving voice mail messages, etc.).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- Calling number blocking (Privacy).
- Call Hold/Resume (long and short duration).
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call Transfers.
- Station Conference.
- EC500 (Extension to Cellular) calls.
- Simultaneous active calls.
- Long duration calls (over one hour).
- Proper response/error treatment to all trunks busy.
- Proper response/error treatment when disabling SIP connection.

Note – Remote Worker was tested as part of this solution. The configuration necessary to support remote workers is beyond the scope of these Application Notes and is not included in these Application Notes.

The following items were not tested:

- Inbound toll-free calls, outbound Toll-Free calls, 911 calls (emergency), “0” calls (Operator) and 0+10 digits calls (Operator Assisted) were not tested.

- The SIP REFER method for call redirection was not tested for reasons noted in **Section 2.2**.
- T.38 fax is not currently supported by Clearcom and it was not tested.

2.2. Test Results

Interoperability testing of the Clearcom SIP Trunk Service with the Avaya SIP-enabled enterprise solution was completed with successful results for all test cases with the observations/limitations noted below:

- **Avaya Equinox softphone:** Calls originated from the Avaya Equinox softphone to the PSTN failed to complete, the Service Provider (Clearcom) responded with “400 Bad Request” to the SIP messages sent by Communication Manager. This issue was not seen with any other Avaya softphones/end-points, only with the Equinox. Preliminary investigation indicates that the Equinox softphone is failing to negotiate media type from encrypted media (SRTP) to non-encrypted media (RTP). This issue is currently under investigation by Avaya.
- **SIP REFER method:** PSTN calls that were transferred back to the network using the SIP REFER method did not work properly. Attended call transfers dropped. On blind transfers, the REFER message was accepted by Clearcom with a 202 message, but the trunks were not released after the call transfer was completed. For these reasons testing was done with REFER disabled in Communication Manager (**Network Call Redirection** set to “n” under the **trunk-group**, refer to **Section 5.7**). With REFER disabled, blind and attended call transfers to the PSTN completed successfully, with the caveat that Communication Manager trunk channels were not released from the call path after the call was transferred, two trunk channels remained busy/connected for the entire duration of the call.
- **Outbound Calling Party Number (CPN) Blocking:** To support user privacy on outbound calls (calling party number blocking), when enabled by the user, Communication Manager sends “anonymous” as the calling number in the SIP “From” header and includes “Privacy: id” in the INVITE message, while the actual number of the caller is sent in the “P-Asserted-Identity” header. On the called PSTN phone, the calling party number was not blocked, the first DID number assigned to the SIP trunk (5528810001) was always displayed, instead of “anonymous”.
- **Caller ID on incoming calls from U.S. based PSTN numbers:** Calls originating from PSTN telephones based in the U.S. to Communication Manager displayed “Unavailable”. During the compliance test, Clearcom provided a local PSTN test number in Mexico, a SIP softphone was registered to this local PSTN number and was used to originate and terminate local PSTN calls to and from Communication Manager. The correct Caller ID was displayed at the Communication Manager extensions when calling from this local PSTN number. This behavior is not necessarily indicative of a limitation of the combined Avaya/Clearcom solution, this seems to be the expected behavior for international calls from the U.S., which is ultimately controlled by the PSTN providers, it is listed here simply as an observation.
- **Caller ID display on Outbound Calls, Call Forwards and Call transfers to the local PSTN in Mexico:** For outbound calls, calls from the local PSTN in Mexico to Communication Manager that were Forwarded or Transferred back out to the local PSTN in Mexico, the caller ID number displayed at the SIP softphone (local PSTN in Mexico) was always of the first DID number assigned to the SIP Trunk (5528810001), regardless of the PSTN number being used to originate the call.

- **Caller ID display on EC500 extension to cellular:** For EC500 extension to cellular calls the Caller ID display at the Mobile/cellular station was always of the first DID number assigned to the SIP Trunk (5528810001), regardless of the PSTN number being used to originate the call.
- **From Header Manipulation:** Clearcom uses SIP trunk registration and digest authentication in order to accept calls from the enterprise into their network. Additionally, Clearcom requires the username associated with the SIP trunk credentials to be present in the “From” header of all outbound calls from the enterprise. Otherwise, the call is rejected with a “403 Username from not allowed” message. A Signaling Script was created in the Avaya SBCE to include the SIP trunk credential’s username in the “From” header of all outbound calls. (**Section 7.7** and **Section 12**).
- **Request-URI Header Manipulation:** Clearcom sends the username associated with the SIP trunk credentials in the “Request URI” header of all inbound calls, while the actual DID number of the party dialed is sent in the “To” header. Since the routing decision in Session Manager is based on Dial Patterns, by inspecting the number present in the “Request URI” header of the incoming call, a Signaling Script was created in the Avaya SBCE to populate the “Request URI” header with the number present in the “To” header of inbound calls. (**Section 7.7** and **Section 12**).
- **SIP header optimization:** There are multiple SIP headers and parameters used by Communication Manager and Session Manager, some of them Avaya proprietary, that had no significance in the service provider’s network. These headers were removed with the purpose of blocking enterprise information from being propagated outside of the enterprise boundaries, to reduce the size of the packets entering the service provider’s network and to improve the solution interoperability in general. The following headers were removed from outbound messages using an Adaptation in Session Manager: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-id, P-Charging-Vector and P-Location (**Section 6.4**). Additionally, the parameters “gsid” and “epv” were removed from outbound Contact headers using a Signaling Script in the Avaya SBCE (**Section 7.7** and **Section 12**).

2.3. Support

For support on Clearcom SIP Trunk Service visit the corporate Web page at:

<http://www.clearcom.mx/>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Clearcom SIP Trunk Service through a public Internet WAN connection.

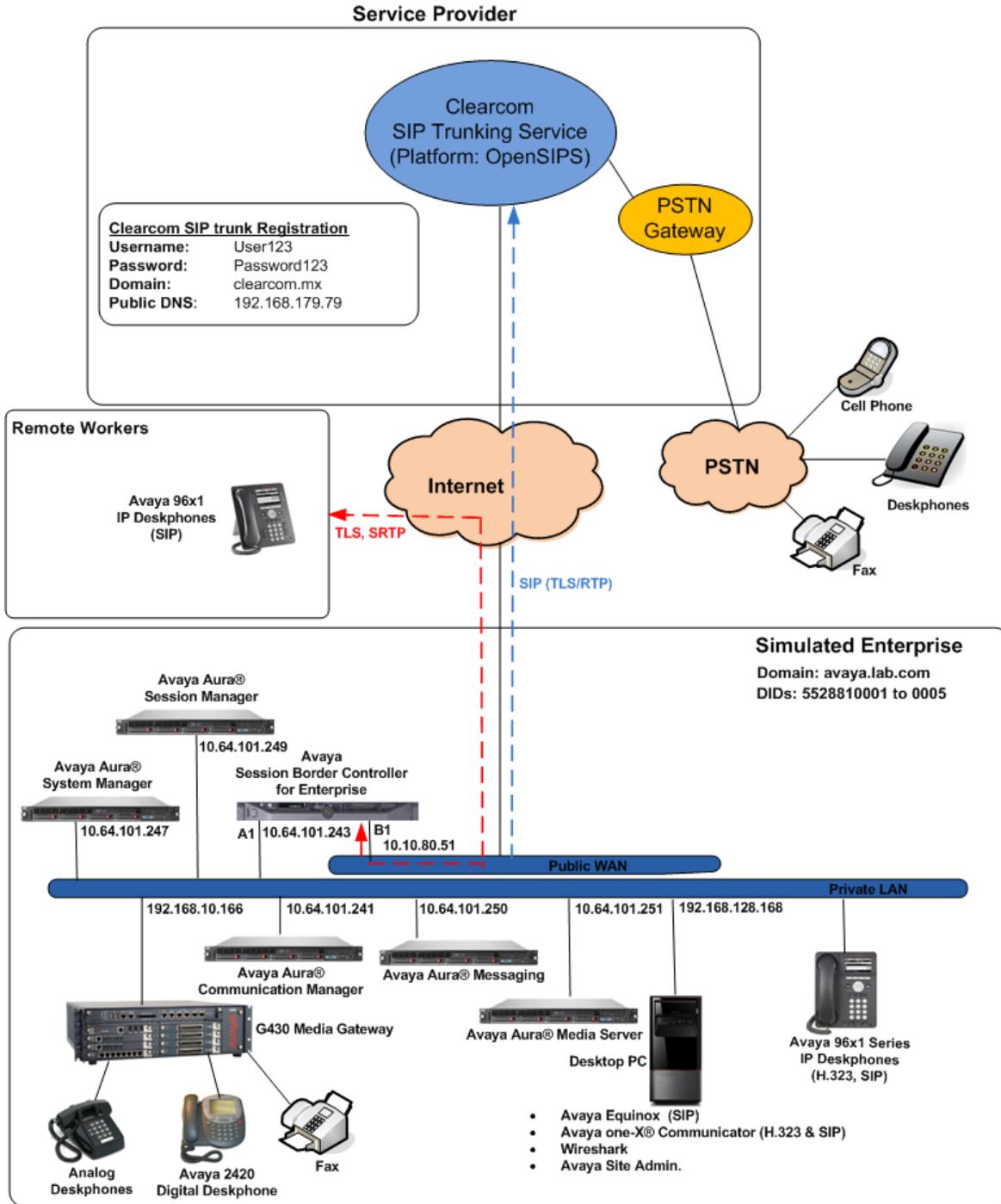


Figure 1: Avaya SIP Enterprise Solution connected to Clearcom SIP Trunk Service

The Avaya components used to create the simulated enterprise customer site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya Aura® Messaging.
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya 96x1 Series IP Deskphones (H.323 and SIP).
- Avaya one-X® Communicator softphones (H.323 and SIP).
- Avaya Equinox softphone (SIP).
- Avaya digital and analog telephones.

Additionally, the reference configuration included remote worker functionality. A remote worker is a SIP endpoint that resides in the untrusted network, registered to the Session Manager at the enterprise via the Avaya SBCE. Remote workers offer the same functionality as any other endpoint at the enterprise. This functionality was successfully tested during the compliance test using only the Avaya 96x1 SIP Deskphones. For signaling, Transport Layer Security (TLS) and for media, Secure Real-time Transport Protocol (SRTP) was used on Avaya 96x1 SIP Deskphones used to test remote worker functionality. Other Avaya SIP endpoints that are supported in a Remote Worker configuration deployment were not tested.

The configuration tasks required to support remote workers are beyond the scope of these Application Notes; hence they are not discussed in this document. Consult [9] in the **References** section for additional information on this topic.

The Avaya SBCE was located at the edge of the enterprise. Its public side was connected to the public Internet, while its private side was connected to the enterprise infrastructure. All signaling and media traffic entering or leaving the enterprise flowed through the Avaya SBCE, protecting in this way the enterprise against any SIP-based attacks. The Avaya SBCE also performed network address translation at both the IP and SIP layers.

For inbound calls, the calls flowed from the service provider to the Avaya SBCE then to Session Manager. Session Manager used the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrived at Communication Manager, further incoming call treatment, such as incoming digit translation was performed.

Outbound calls to the PSTN were first processed by Communication Manager for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns (or regular expressions) and routing policies to determine the route to the Avaya SBCE for egress to the Clearcom network.

A separate SIP trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec settings required by the service provider could be applied only to this trunk without affecting other enterprise SIP traffic. This trunk carried both inbound and outbound traffic.

As part of the Avaya Aura® version 7.1 release, Communication Manager incorporates the ability to use the Avaya Aura® Media Server (AAMS) as a media resource. The AAMS is a software-based, high density media server that provides DSP resources for IP-based sessions. Media resources from both the AAMS and a G430 Media Gateway were utilized during the compliance test. The configuration of the AAMS is not discussed in this document. For more information on the installation and administration of the AAMS in Communication Manager refer to the AAMS documentation listed in the **References** section.

Avaya Aura® Messaging was used during the compliance test to verify voice mail redirection and navigation, as well as the delivery of Message Waiting Indicator (MWI) messages to the enterprise telephones. Since the configuration tasks for Messaging are not directly related to the interoperability tests with the Clearcom network SIP Trunk service, they are not included in these Application Notes.

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 only (private network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the compliance testing associated with this Application Note, TLS transport for Signaling was used inside of the enterprise (private network side) and outside of the enterprise (public network side). SRTP for media encryption was used inside of the enterprise (private network side), RTP was used outside of the enterprise (public network side).

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Communication Manager	7.1.1.0.0 (01.0.532.0-23985)
Avaya Aura® Session Manager	7.1.1.0 (7.1.1.0.711008)
Avaya Aura® System Manager	7.1.1.0 Build No. 7.1.0.0.1125193 Software Update Rev. No. 7.1.1.0.046931
Avaya Session Border Controller for Enterprise	ASBCE 7.2 7.2.0.0-18-13712
Avaya Aura® Messaging	7.0 Service Pack 0 (MSG-00.0.441.0-017_0004)
Avaya Aura® Media Server	7.8.0.333 SP5 7.8.0.333_2017.07.17
Avaya G430 Media Gateway	G430_sw_38_20_1
Avaya 96x1 Series IP Deskphones (SIP)	Version 7.1.1.0.9
Avaya 96x1 Series IP Deskphones (H.323)	Version 6.6506
Avaya one-X® Communicator (H.323, SIP)	6.2.12.04-SP12
Avaya Equinox (SIP)	3.2.2.2
Avaya 2420 Series Digital Deskphones	N/A
Avaya 6210 Analog Deskphones	N/A
Clearcom	
OpenSIPS Softswitch	1.9
OpenSIPS Session Border Controller	1.9

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Servers and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

Note – The Avaya Aura® servers and the Avaya SBCE used in the reference configuration and shown on the previous table were deployed on a virtualized environment. These Avaya components ran as virtual machines over VMware® (ESXi 6.0.0) platforms. Consult the installation documentation on the **References** section for more information.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to work with the Clearcom network SIP Trunk service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from the service provider. It is assumed that the general installation of Communication Manager, the Avaya G430 Media Gateway and the Avaya Aura® Media Server has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Some screens captures will show the use of the **change** command instead of the **add** command, since the configuration used for the testing was previously added.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **120** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

```
display system-parameters customer-options Page 2 of 12
OPTIONAL FEATURES

IP PORT CAPACITIES                                USED
Maximum Administered H.323 Trunks: 12000 0
Maximum Concurrently Registered IP Stations: 18000 1
Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
Maximum Concurrently Registered IP eCons: 414 0
Max Concur Registered Unauthenticated H.323 Stations: 100 0
Maximum Video Capable Stations: 41000 0
Maximum Video Capable IP Softphones: 18000 7
Maximum Administered SIP Trunks: 24000 120
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
Maximum Number of DS1 Boards with Echo Cancellation: 522 0

(NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons incoming calls should not be allowed to transfer back to the PSTN, then leave the field set to **none**.

```
change 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
```

On **Page 9** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of *restricted* for restricted calls and *unavailable* for unavailable calls.

```
change 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
```


5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Enter the corresponding codec in the **Audio Codec** column of the table. Clearcom supports audio codecs *G.729*, *G.711A* and *G.711MU*.

```
change ip-codec-set 2 Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 2

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.729          n          2          20
2: G.711A        n          2          20
3: G.711MU       n          2          20
4: _____    -            -            -
5: _____    -            -            -
6: _____    -            -            -
7: _____    -            -            -

Media Encryption                                Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: none
3: _____
4: _____
5: _____
```

On Page 2, set the Fax Mode to *off* (refer to Section 2.1).

```
change ip-codec-set 2                                     Page 2 of 2
                                                         IP MEDIA PARAMETERS
                                                         Allow Direct-IP Multimedia? n

                                                         Mode
                                                         Redun-
                                                         dancy
                                                         Packet
                                                         Size (ms)
FAX off _____ 0
Modem off _____ 0
TDD/TTY US _____ 3
H.323 Clear-channel n _____ 0
SIP 64K Data n _____ 0 20

Media Connection IP Address Type Preferences
1: IPv4
2: _____
```

5.5. IP Network Regions

Create a separate IP network region for the service provider trunk group. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP Network Region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is *avaya.lab.com* as assigned to the shared test environment in the Avaya test lab. This domain name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to *yes*, the default setting. This will 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 and Media Server. Shuffling can be further restricted at the trunk level on the Signaling Group form if needed.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values may be used for all other fields.

```
change ip-network-region 2                                     Page 1 of 20
                                     IP NETWORK REGION
Region: 2      NR Group: 2
Location: 1    Authoritative Domain: avaya.lab.com
Name: SP Region      Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048    IP Audio Hairpinning? n
UDP Port Max: 3349
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
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The following example shows the settings used for the compliance test. It indicates that codec set **2** will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 2 was used and was configured using the parameters highlighted below, shown on the screen on the next page:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the transport protocol to be used between Communication Manager and Session Manager. For the compliance test, *tls* was used.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to *SM* once Communication Manager detects its peer is a Session Manager.

Note: Once the **Peer-Server** field is updated to *SM*, the system changes the default values of the following fields, setting them to display-only:

- **Prepend ‘+’ to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?** is changed to *y*.
- **Remove ‘+’ from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?** is changed to *n*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *SM*. This node name maps to the IP address of Session Manager, as defined in **Section 5.3**
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to *5071*.
- Set the **Far-end Network Region** to the IP network region defined for the Service Provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the Avaya SBCE and the enterprise endpoint. If this value is set to *n*, then the Avaya Media Gateway or Media Server will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway and Media Server, these resources may be depleted during high call volume preventing additional calls from completing.
- Default values may be used for all other fields

```

change signaling-group 2                                     Page 1 of 2
                                SIGNALING GROUP

Group Number: 2
IMS Enabled? n
Q-SIP? n
IP Video? n
Peer Detection Enabled? y
Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr
Near-end Listen Port: 5071
Far-end Node Name: SM
Far-end Listen Port: 5071
Far-end Network Region: 2
Far-end Domain: avaya.lab.com
Incoming Dialog Loopbacks: eliminate
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
H.323 Station Outgoing Direct Media? n
Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
Initial IP-IP Direct Media? n
Alternate Route Timer(sec): 6

```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 2 was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
change trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                         Group Type: sip
Group Name: Service Provider                           COR: 1      TN: 1      TAC: 602
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
Signal Group: 2
Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. The default value of **600** seconds was used.

```
change trunk-group 2                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
  Redirect On OPTIM Failure: 5000
  SCCAN? n                                             Digital Loss Group: 18
  Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
  XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 1xC: station-extension
```

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. When *public* format is used, Communication Manager automatically inserts a “+” sign, preceding the numbers in the “From”, “Contact” and “P-Asserted Identity” (PAI) headers. To keep uniformity with the format used by Clearcom, the **Numbering Format** was set to *private* and the **Numbering Format** in the route pattern was set to *unk-unk* (see **Section 5.10**).
- 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 has enabled CPN block.

```
change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                         Maintenance Tests? y

Suppress # Outpulsing? n   Numbering Format: private
                                                         UII Treatment: service-provider
                                                         Replace Restricted Numbers? y
                                                         Replace Unavailable Numbers? y
                                                         Hold/Unhold Notifications? y
Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

On Page 4:

- Set the **Network Call Redirection** field to *n*. With this setting, Communication Manager will not use the REFER method, which is not supported by Clearcom, for the redirection of PSTN calls that are transferred back to the SIP trunk (refer to **Section 2.1**)
- Set the **Send Diversion Header** field to *n* and **Support Request History** to *n*.
- Set the **Telephone Event Payload Type** to **101**, the value preferred by Clearcom.
- Set the **Convert 180 to 183 for Early Media?** to *y*.
- Verify that **Identity for Calling Party Display** is set to *P-Asserted-Identity*.
- Default values were used for all other fields.

```
change trunk-group 2                                     Page 4 of 21
PROTOCOL VARIATIONS
Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
Send Transferring Party Information? n
Network Call Redirection? n
Send Diversion Header? n
Support Request History? n
Telephone Event Payload Type: 101
Convert 180 to 183 for Early Media? y
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. Inbound Routing

In general, the “incoming call handling treatment” form for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Clearcom is left unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 2
```

Page 1 of 30

INCOMING CALL HANDLING TREATMENT				
Service/ Feature	Number Len	Number Digits	Del	Insert
public-ntwrk	10	5528810001	10	3042
public-ntwrk	10	5528810002	10	3225
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—
public-ntwrk	—	—	—	—

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an “outside line”. This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1, as a feature access code (*fac*).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	13	udp						
1	4	dac						
2	4	ext						
3	4	ext						
4	4	udp						
5	4	ext						
6	3	dac						
7	4	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	2	dac						

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

```
change feature-access-codes Page 1 of 10
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: #7 ____
Answer Back Access Code: ____
Attendant Access Code: ____
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2: ____
Automatic Callback Activation: ____ Deactivation: ____
Call Forwarding Activation Busy/DA: ____ All: ____ Deactivation: ____
Call Forwarding Enhanced Status: ____ Act: ____ Deactivation: ____
Call Park Access Code: ____
Call Pickup Access Code: ____
CAS Remote Hold/Answer Hold-Unhold Access Code: ____
CDR Account Code Access Code: ____
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 test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2, which contains the SIP trunk group to the service provider.

```
change ars analysis 001
```

Page 1 of 2

ARS DIGIT ANALYSIS TABLE
Location: all Percent Full: 0

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
001	13	18	2	intl		n
01	12	12	2	natl		n
011	10	18	2	intl		n
040	3	3	2	svcl		n
045	13	13	2	natl		n
101xxxx0	8	8	deny	op		n
101xxxx0	18	18	deny	op		n
101xxxx01	16	24	deny	iop		n
101xxxx011	17	25	deny	intl		n
101xxxx1	18	18	deny	fnpa		n
10xxx0	6	6	deny	op		n
10xxx0	16	16	deny	op		n
10xxx01	14	22	deny	iop		n
10xxx011	15	23	deny	intl		n
10xxx1	16	16	deny	fnpa		n

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 in the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider.
- **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:** Set to *unk-unk*. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.

```

change route-pattern 2                                     Page 1 of 3
      Pattern Number: 2      Pattern Name: 3~rv. Provider
  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: 2__ 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          rest          _____  _____  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
  
```

Note - Enter the **save translation** command (not shown) to save all the changes made to the Communication Manager configuration in the previous sections.

6. Configure Avaya Aura® Session Manager

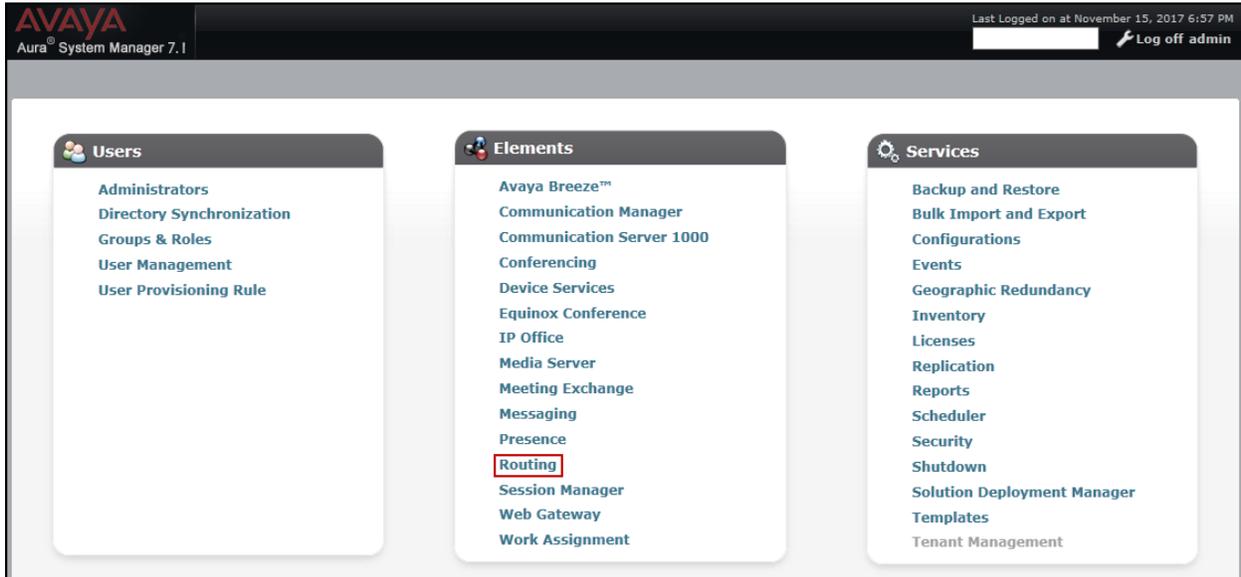
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Locations that can be occupied by SIP Entities.
- Adaptation module to perform header manipulations.
- 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.

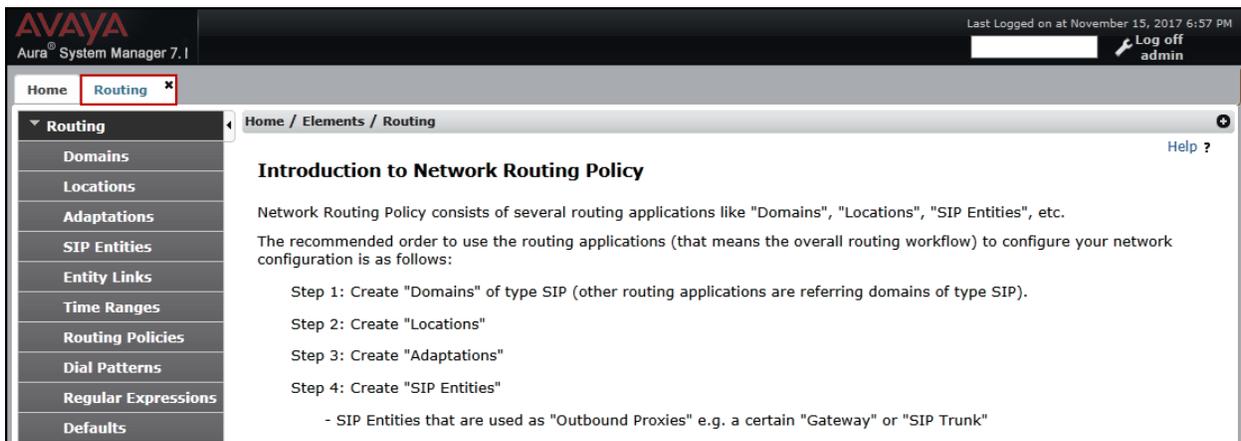
The following sections assume that the initial configuration of Session Manager and System Manager has already been completed, and that network connectivity exists between System Manager and Session Manager.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.



6.2. SIP Domain

Create an entry for each SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this was the enterprise domain, *avaya.lab.com*. Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save.

The screen below shows the entry for the enterprise domain.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and a "Log off admin" button. The left-hand navigation pane is expanded to show "Routing" and "Domains". The main content area is titled "Domain Management" and contains a table with one entry. The table has columns for "Name", "Type", and "Notes". The entry is "avaya.lab.com", "sip", and "HG V-Domain".

Name	Type	Notes
avaya.lab.com	sip	HG V-Domain

6.3. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).
- Click **Commit** to save.

The following screen shows the location details for the location named *Session Manager*. Later, this location will be assigned to the SIP Entity corresponding to Session Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a 'Log off admin' button. The breadcrumb trail is 'Home / Elements / Routing / Locations'. The left sidebar menu is expanded to 'Routing', with 'Locations' selected. The main content area is titled 'Location Details' and contains the following fields:

- General**
 - * Name: Session Manager
 - Notes: VMware Session Manager
- Dial Plan Transparency in Survivable Mode**
 - Enabled:
 - Listed Directory Number:
 - Associated CM SIP Entity:

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

The following screen shows the location details for the location named *Communication Manager*. Later, this location will be assigned to the SIP Entity corresponding to Communication Manager. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a 'Log off' button. The breadcrumb trail is 'Home / Elements / Routing / Locations'. The left sidebar menu is expanded to 'Routing', with 'Locations' selected. The main content area is titled 'Location Details' and contains the following fields:

- General**
 - * Name: Communication Manager
 - Notes: VMware Communication Manager
- Dial Plan Transparency in Survivable Mode**
 - Enabled:
 - Listed Directory Number:
 - Associated CM SIP Entity:

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

The following screen shows the location details for the location named *Avaya SBCE*. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and a user session summary: "Last Logged on at November 15, 2017 6:57 PM" with a "Log off admin" button. Below the navigation bar, there are tabs for "Home" and "Routing". The "Routing" tab is active, and a sub-menu on the left lists various routing-related options: "Routing", "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The "Locations" option is highlighted. The main content area shows the breadcrumb "Home / Elements / Routing / Locations" and a "Help ?" link. The title of the page is "Location Details", with "Commit" and "Cancel" buttons to its right. Under the "General" section, the "* Name:" field is filled with "Avaya SBCE" and is highlighted with a red box. The "Notes:" field contains "VMware Avaya SBCE". Below this, the "Dial Plan Transparency in Survivable Mode" section includes an "Enabled:" checkbox (which is unchecked), a "Listed Directory Number:" field, and an "Associated CM SIP Entity:" field.

6.4. Adaptations

In order to improve interoperability with third party elements, Session Manager 7.1 incorporates the ability to use Adaptation modules to remove specific headers that are either Avaya proprietary or deemed excessive/unnecessary for non-Avaya elements.

For the compliance test, an Adaptation named *CM_Outbound_Header_Removal* was created to block the following headers from outbound messages, before they were forwarded to the Avaya SBCE: AV-Global-Session-ID, AV-Correlation-ID, Alert-Info, Endpoint-View, P-AV-Message-ID, P-Charging-Vector and P-Location. These headers contain private information from the enterprise, which should not be propagated outside of the enterprise boundaries. They also add unnecessary size to outbound messages, while they have no significance to the service provider.

Navigate to **Routing** → **Adaptations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Adaptation Name:** Enter an appropriate name.
- **Module Name:** Select the *DigitConversionAdapter* option.
- **Module Parameter Type:** Select *Name-Value Parameter*.

Click **Add** to add the name and value parameters, as follows:

- **Name:** Enter *eRHdrs*. This parameter will remove the specified headers from messages in the egress direction.
- **Value:** Enter “*Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-Id, P-Location, Endpoint-View*”
- Click **Commit** to save.

The screen below shows the adaptation created for the compliance test. This adaptation will later be applied to the SIP Entity corresponding to the Avaya SBCE. All other fields were left at their default values.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and a user session indicator "Last Logged on at November 15, 2017 6:57 PM" with a "Log off admin" button. The main content area is titled "Adaptation Details" and includes "Commit" and "Cancel" buttons. A left-hand navigation menu lists various routing-related items, with "Adaptations" highlighted. The "General" section contains the following fields:

- * Adaptation Name:** CM_Outbound_Header_Removal
- * Module Name:** DigitConversionAdapter
- Module Parameter Type:** Name-Value Parameter

Below these fields is a table for defining parameters:

Add		Remove	
<input type="checkbox"/>	Name		Value
<input type="checkbox"/>	leRHdrs		"Alert-Info, P-Charging-Vector, AV-Global-Session-ID, AV-Correlation-ID, P-AV-Message-id, P-

At the bottom of the table, it says "Select : All, None".

6.5. 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 the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling (see **Figure 1**).
- **Type:** Select *Session Manager* for Session Manager, *CM* for Communication Manager and *SIP Trunk* (or *Other*) for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If Adaptations were to be created, here is where they would be applied to the entity.
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.
- Click **Commit** to save.

The following screen shows the addition of the *Session Manager* SIP Entity for Session Manager. The IP address of the Session Manager Security Module is entered in the **FQDN or IP Address** field.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar shows 'Home' and 'Routing' (selected). The left sidebar contains a tree view with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' section. The form fields are as follows:

- Name:** Session Manager
- FQDN or IP Address:** 10.64.101.249
- Type:** Session Manager (dropdown)
- Notes:** VMware Session Manager
- Location:** Session Manager (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/New_York (dropdown)
- Minimum TLS Version:** Use Global Setting (dropdown)

Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area. The user is logged in as 'admin' and the session expires on November 15, 2017 at 6:57 PM.

The following screen shows the addition of the *Communication Manager Trunk 2* SIP Entity for Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, the creation of a separate SIP entity for Communication Manager is required. This SIP Entity should be different than the one created during the Session Manager installation, used by all other enterprise SIP traffic. The **FQDN or IP Address** field is set to the IP address of the “**procr**” interface in Communication Manager, as seen in **Section 5.3**. Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user session summary showing 'Last Logged on at November 15, 2017 6:57 PM' and a 'Log off admin' button. The main content area is titled 'SIP Entity Details' and is divided into a left-hand navigation menu and a central form. The navigation menu lists various configuration options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted with a red box), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The central form, under the 'General' tab, contains the following fields: '* Name' (text input: 'Communication Manager Trunk 2', highlighted with a red box), '* FQDN or IP Address' (text input: '10.64.101.241', highlighted with a red box), 'Type' (dropdown menu: 'CM'), 'Notes' (text input: 'Used for SP Testing'), 'Adaptation' (dropdown menu), 'Location' (dropdown menu: 'Communication Manager', highlighted with a red box), and 'Time Zone' (dropdown menu: 'America/New_York', highlighted with a red box). At the top right of the form area, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The breadcrumb navigation at the top of the form area reads 'Home / Elements / Routing / SIP Entities'.

The following screen shows the addition of the *Avaya SBCE* SIP Entity for the Avaya SBCE:

- The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**).
- On the **Adaptation** field, the adaptation module *CM_Outbound_Header_Removal* previously defined in **Section 6.4** was selected.
- Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.

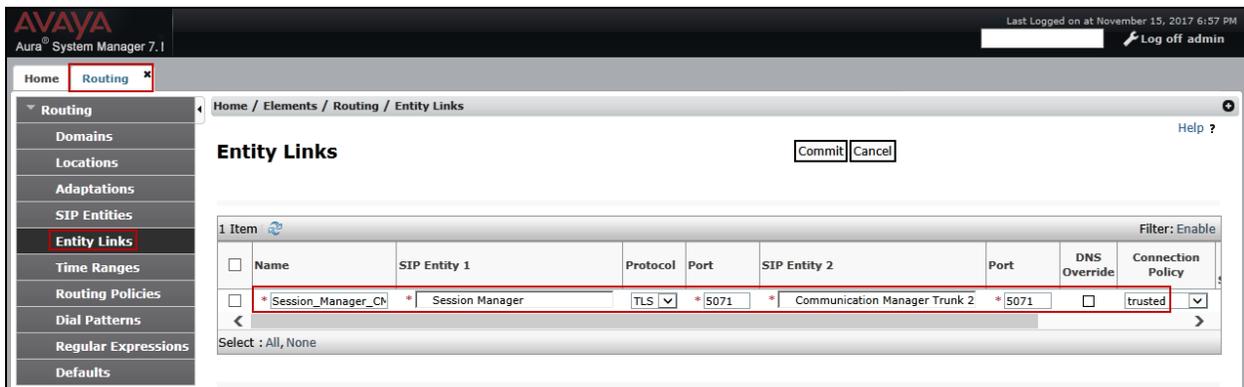
The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', and a user session summary: 'Last Logged on at November 15, 2017 6:57 PM' with a 'Log off admin' button. The main content area is titled 'SIP Entity Details' and is divided into a left-hand navigation menu and a central form. The navigation menu lists 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted with a red box), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The central form, under the 'General' tab, contains the following fields: '* Name: Avaya SBCE', '* FQDN or IP Address: 10.64.101.243', 'Type: SIP Trunk', 'Notes: VMware Avaya SBCE', 'Adaptation: CM_Outbound_Header_Removal', 'Location: Avaya SBCE', and 'Time Zone: America/New_York'. The 'FQDN or IP Address', 'Adaptation', 'Location', and 'Time Zone' fields are highlighted with red boxes. At the top right of the form area, there are 'Commit' and 'Cancel' buttons and a 'Help ?' link.

6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Communication Manager for use only by service provider traffic and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left navigation pane and click on 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 from the drop-down menu (**Section 6.5**).
- **Protocol:** Select the transport protocol used for this link (**Section 5.6**).
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end (**Section 5.6**).
- **SIP Entity 2:** Select the name of the other system from the drop-down menu (**Section 6.5**).
- **Port:** Port number on which the other system receives SIP requests from Session Manager (**Section 5.6**).
- **Connection Policy:** Select **Trusted** to allow calls from the associated SIP Entity.
- Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**. *TLS* transport and port *5071* were used.



The screenshot shows the Avaya Aura System Manager 7.1 interface. The left navigation pane is expanded to 'Routing' and 'Entity Links' is selected. The main content area shows the 'Entity Links' configuration page with a table containing one row of data. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The values in the row are: Name: Session_Manager_CK, SIP Entity 1: Session Manager, Protocol: TLS, Port: 5071, SIP Entity 2: Communication Manager Trunk 2, Port: 5071, DNS Override: unchecked, and Connection Policy: trusted. There are 'Commit' and 'Cancel' buttons at the top right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
* Session_Manager_CK *	Session Manager	TLS	* 5071 *	* Communication Manager Trunk 2 *	* 5071 *	<input type="checkbox"/>	trusted

The Entity Link to the Avaya SBCE is shown below; *TLS* transport and port *5061* were used.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and a user login status "Last Logged on at: November 15, 2017 6:57 PM" with a "Log off admin" link. A notification banner indicates "1 New important message(s). Click to view details." The left sidebar contains a menu with "Routing" selected, and sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Entity Links" and includes "Commit" and "Cancel" buttons. Below the title, it shows "1 Item" and a "Filter: Enable" option. A table lists the configuration details for the selected item:

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
<input type="checkbox"/>	*Session_Manager_AS*	Session Manager	TLS	*5061*	Avaya SBCE	*5061*	<input type="checkbox"/>	trusted

Below the table, there is a "Select : All, None" option.

6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added: an incoming policy with Communication Manager as the destination, and an outbound policy to the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed:

- In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose the appropriate SIP entity to which this routing policy applies (**Section 6.5**) and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below.
- Use default values for remaining fields.
- Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and the Avaya SBCE.

AVAYA
Aura System Manager 7.1

Last Logged on at November 15, 2017 6:57 PM

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: To CM Trunk 2

Disabled:

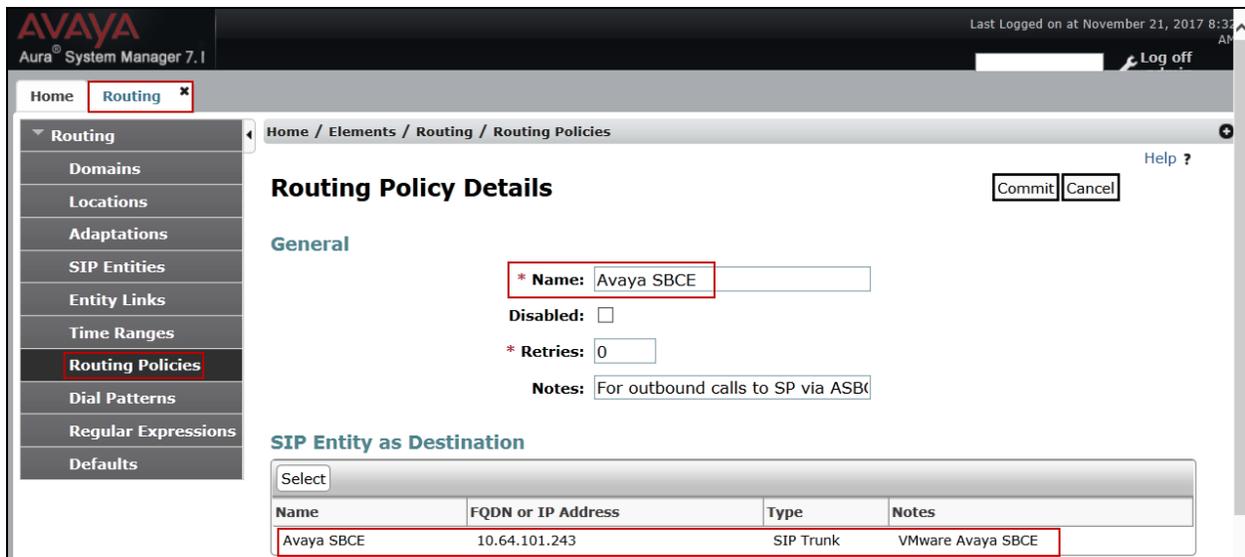
* Retries: 0

Notes: For inbound calls to CM via Trunk

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Communication Manager Trunk 2	10.64.101.241	CM	Used for SP Testing



6.8. Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to the service provider and vice versa. Dial Patterns define which route 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 on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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, or select “**ALL**” to route incoming calls to all SIP domains.
- **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 (**Section 6.3**).
- Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria (**Section 6.7**). Click **Select** (not shown).
- Click **Commit** to save.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with **552881**, arriving from location **Avaya SBCE**, used route policy **Communication Manager Trunk 2** to Communication Manager.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The breadcrumb trail is Home / Elements / Routing / Dial Patterns. The 'Dial Pattern Details' form is displayed with the following fields:

- * Pattern: 552881
- * Min: 10
- * Max: 10
- Emergency Call:
- Emergency Priority: 1
- Emergency Type:
- SIP Domain: avaya.lab.com
- Notes:

Below the form is the 'Originating Locations and Routing Policies' section, which contains a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> Avaya SBCE	VMware Avaya SBCE	To CM Trunk 2	0	<input type="checkbox"/>	Communication Manager Trunk 2	For inbound calls to CM via Trunk 2

Repeat this procedure as needed to define additional dial patterns for other range of numbers assigned by the service provider to the enterprise, to be routed to Communication Manager.

The example in this screen shows the 13 digit dialed numbers for outbound international calls, beginning with **001**, arriving from the **Communication Manager** location, will use route policy **Avaya SBCE**, which sends the call out to the PSTN via Avaya SBCE and the service provider SIP Trunk. The SIP Domain was set to **avaya.lab.com**.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home' and 'Routing' (highlighted with a red box). The breadcrumb path is 'Home / Elements / Routing / Dial Patterns'. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the following fields are visible:

- * Pattern: 001 (highlighted with a red box)
- * Min: 13 (highlighted with a red box)
- * Max: 13 (highlighted with a red box)
- Emergency Call:
- Emergency Priority: 1
- Emergency Type: [empty field]
- SIP Domain: avaya.lab.com (highlighted with a red box)
- Notes: [empty field]

 Below this is the 'Originating Locations and Routing Policies' section, which contains a table with one item. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The single row is highlighted with a red border.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Communication Manager	VMware Communication Manager	Avaya SBCE	0	<input type="checkbox"/>	Avaya SBCE	For outbound calls to SP via ASBCE

Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the service provider’s network via the Avaya SBCE.

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

Note - The configuration tasks required to support TLS transport for signaling and SRTP for media inside of the enterprise (private network side) and outside of the enterprise (public network side) are beyond the scope of these Application Notes; hence they are not discussed in this document.

7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The screenshot shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in a large, stylized red font. Below it, the text "Session Border Controller for Enterprise" is written in a bold, black font. On the right, the "Log In" section features a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Underneath the button, there is a "WELCOME TO AVAYA SBC" message, followed by a warning: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Below this warning is a paragraph of legal disclaimer text: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom of the page, the copyright notice "© 2011 - 2017 Avaya Inc. All rights reserved." is visible.

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

The screenshot displays the Avaya Session Border Controller for Enterprise dashboard. At the top, there is a navigation bar with links for 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-hand navigation pane is highlighted, showing options like Administration, Backup/Restore, System Management, and Device Specific Settings. The main content area is titled "Dashboard" and features a prominent red warning banner: "This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic." Below this, a section lists expired certificates, including "Rapid_SSL_Cert.crt (Certificate)". The dashboard is divided into several panels: "Information" (System Time, Version, Build Date, License State: OK, Aggregate Licensing Overages: 0, Peak Licensing Overage Count: 0, Last Logged in at, Failed Login Attempts), "Installed Devices" (EMS, Avaya_SBCE), "Active Alarms (past 24 hours)" (None found), and "Incidents (past 24 hours)" (Avaya_SBCE : No Subscriber Flow Matched).

7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named *Avaya_SBCE* is shown. The management IP address that was configured during installation is blurred out for security reasons, the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is *Commissioned*, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

The screenshot shows the Avaya Session Border Controller for Enterprise System Management interface. The navigation menu on the left includes: Dashboard, Administration, Backup/Restore, System Management (highlighted), Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'System Management' and contains tabs for Devices, Updates, SSL VPN, Licensing, and Key Bundles. The 'Devices' tab is active, displaying a table with the following data:

Device Name	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Uninstall
Avaya_SBCE	[Blurred]	7.2.0.0-18-13712	Commissioned						

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.

System Information: Avaya_SBCE X

<p>General Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Appliance Name</td><td>Avaya_SBCE</td></tr> <tr><td>Box Type</td><td>SIP</td></tr> <tr><td>Deployment Mode</td><td>Proxy</td></tr> </table>	Appliance Name	Avaya_SBCE	Box Type	SIP	Deployment Mode	Proxy	<p>Device Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">HA Mode</td><td>No</td></tr> <tr><td>Two Bypass Mode</td><td>No</td></tr> </table>	HA Mode	No	Two Bypass Mode	No	<p>License Allocation</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Standard Sessions <small>Requested: 2000</small></td><td>2000</td></tr> <tr><td>Advanced Sessions <small>Requested: 2000</small></td><td>2000</td></tr> <tr><td>Scopia Video Sessions <small>Requested: 500</small></td><td>500</td></tr> <tr><td>CES Sessions <small>Requested: 0</small></td><td>0</td></tr> <tr><td>Transcoding Sessions <small>Requested: 0</small></td><td>0</td></tr> <tr><td>Encryption</td><td><input checked="" type="checkbox"/></td></tr> </table>	Standard Sessions <small>Requested: 2000</small>	2000	Advanced Sessions <small>Requested: 2000</small>	2000	Scopia Video Sessions <small>Requested: 500</small>	500	CES Sessions <small>Requested: 0</small>	0	Transcoding Sessions <small>Requested: 0</small>	0	Encryption	<input checked="" type="checkbox"/>
Appliance Name	Avaya_SBCE																							
Box Type	SIP																							
Deployment Mode	Proxy																							
HA Mode	No																							
Two Bypass Mode	No																							
Standard Sessions <small>Requested: 2000</small>	2000																							
Advanced Sessions <small>Requested: 2000</small>	2000																							
Scopia Video Sessions <small>Requested: 500</small>	500																							
CES Sessions <small>Requested: 0</small>	0																							
Transcoding Sessions <small>Requested: 0</small>	0																							
Encryption	<input checked="" type="checkbox"/>																							

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.64.101.243	10.64.101.243	255.255.255.0	10.64.101.1	A1
				A1
				A1
				B1
				B1
10.10.80.51	10.10.80.51	255.255.255.128	10.10.80.1	B1

<p>DNS Configuration</p> <table style="width: 100%; border-collapse: collapse;"> <tr style="border: 2px solid red;"><td style="width: 30%;">Primary DNS</td><td>8.8.8.8</td></tr> <tr><td>Secondary DNS</td><td>7.7.7.7</td></tr> <tr><td>DNS Location</td><td>DMZ</td></tr> <tr style="border: 2px solid red;"><td>DNS Client IP</td><td>10.10.80.51</td></tr> </table>	Primary DNS	8.8.8.8	Secondary DNS	7.7.7.7	DNS Location	DMZ	DNS Client IP	10.10.80.51	<p>Management IP(s)</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>IP #1 (IPv4)</td><td> </td></tr> </table>	IP #1 (IPv4)	
Primary DNS	8.8.8.8										
Secondary DNS	7.7.7.7										
DNS Location	DMZ										
DNS Client IP	10.10.80.51										
IP #1 (IPv4)											

The highlighted IP addresses in the **System Information** screen are the ones used for the SIP trunk to Clearcom, and are the ones relevant to these Application Notes. Other IP addresses assigned to the Avaya SBCE **A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked in this document.

In the reference configuration, the private interface of the Avaya SBCE (10.64.101.243) was used to connect to the enterprise network, while its public interface (10.10.80.51) was used to connect to the public network. See **Figure 1**.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

DNS server configuration can be entered or modified as needed, by clicking **Edit** on the **System Management/Devices** tab shown on the previous page. Under **DNS Settings**, enter the IP addresses of the **Primary** and **Secondary** DNS servers. During the compliance test, public DNS servers were used, and the IP address corresponding to the public interface of the Avaya SBCE was selected from the **DNS Client IP** scroll down menu, as shown on the screen below. Click **Finish** (not shown) when done.

Edit Device: Avaya_SBCE
X

Address and interface changes must be made in Network Management.

Any changes to the management network on this device will reboot the device.

General Settings

Appliance Name

Device Settings

High Availability (HA)

DNS Settings

Primary <small>Ex: 202.201.192.1</small>	<input style="width: 90%;" type="text" value="8.8.8.8"/>	
Secondary <small>Optional, Ex: 202.201.192.1</small>	<input style="width: 90%;" type="text" value="7.7.7.7"/>	
DNS Client IP	<input style="width: 90%;" type="text" value="10.10.80.51"/>	<input type="button" value="v"/>

IPv4 Network Settings

Management IP <small>Ex: 192.168.150.8</small>	<input style="width: 90%;" type="text" value="10.10.80.51"/>
Network Prefix or Subnet Mask <small>Ex: 24 or 255.255.255.0</small>	<input style="width: 90%;" type="text" value="255.255.255.0"/>
Gateway <small>Ex: 192.168.150.1</small>	<input style="width: 90%;" type="text" value="10.64.101.1"/>

Licensing Settings

Standard Sessions <small>Available: 100</small>	<input style="width: 90%;" type="text" value="2000"/>
Advanced Sessions <small>Available: 100</small>	<input style="width: 90%;" type="text" value="2000"/>
Scopia Video Sessions <small>Available: 100</small>	<input style="width: 90%;" type="text" value="500"/>
CES Sessions <small>Available: 100</small>	<input style="width: 90%;" type="text" value="0"/>
Transcoding Sessions <small>Available: 100</small>	<input style="width: 90%;" type="text" value="0"/>
Encryption <small>Available: Yes</small>	<input checked="" type="checkbox"/>

7.3. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

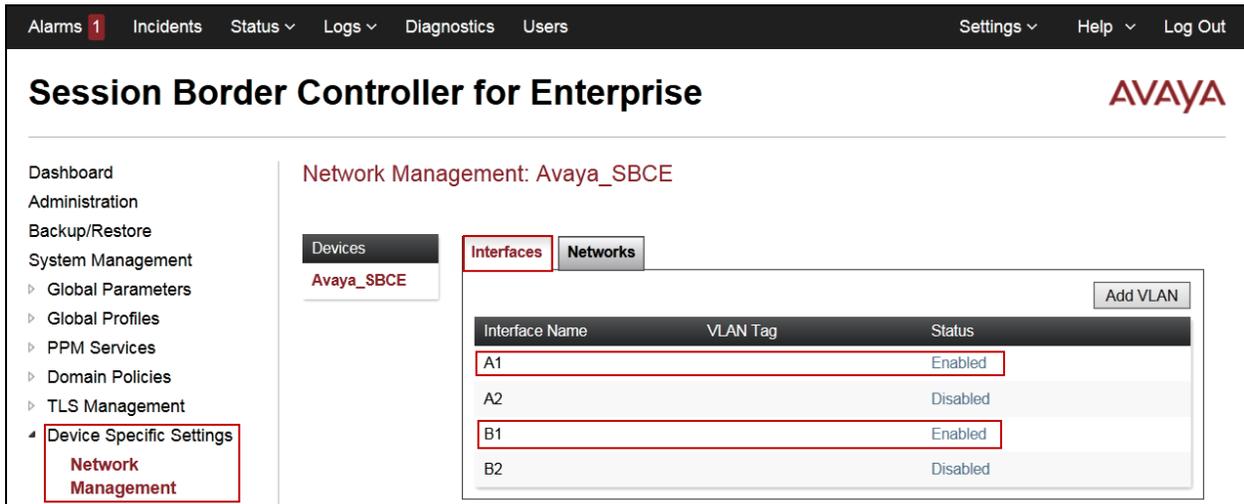
Select **Network Management** from **Device Specific Settings** on the left-side menu. Under **Devices** in the center pane, select the device being managed, *Avaya_SBCE* in the sample configuration. On the **Networks** tab, verify or enter the network information as needed.

Note that in the configuration used during the compliance test, the IP addresses assigned to the private (*10.64.101.243*) and public (*10.10.80.51*) sides of the Avaya SBCE are the ones relevant to these Application Notes.

The screenshot shows the Avaya SBCE web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo. The left sidebar contains a menu with 'Device Specific Settings' expanded to show 'Network Management'. The main content area is titled 'Network Management: Avaya_SBCE' and has two tabs: 'Interfaces' and 'Networks'. The 'Networks' tab is active and shows a table with the following data:

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Network_A1	10.64.101.1	255.255.255.0	A1	10.64.101.243	Edit	Delete
Network_B1	10.10.80.1	255.255.255.128	B1	10.10.80.51	Edit	Delete

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** and **B1** interfaces. Click the buttons under the **Status** column if necessary to enable the interfaces.



7.4. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the Trunk Server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.

A Media Interface facing the public side was similarly created with the name *Public_med*, as shown below.

- Under **IP Address**, the network and IP address to be associated with this interface was selected.
- The **Port Range** was left at the default values.
- Click **Finish**.

The screenshot shows a configuration window titled "Add Media Interface". The window contains the following fields and values:

Field	Value
Name	Public_med
IP Address	Network_B1 (B1, VLAN 0) / 10.10.80.51
Port Range	35000 - 40000
TLS Profile	None

A "Finish" button is located at the bottom of the window.

7.5. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the device being managed and click the **Add** button (not shown).

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.6**.
- Select a **TLS Profile**.
- Click **Finish**.

The screenshot shows the 'Add Signaling Interface' configuration window. The form is titled 'Add Signaling Interface' and has a close button 'X' in the top right corner. The form contains the following fields and values:

- Name:** Private_sig
- IP Address:** Network_A1 (A1, VLAN 0) (dropdown), 10.64.101.243 (dropdown)
- TCP Port:** (text box), Leave blank to disable
- UDP Port:** (text box), Leave blank to disable
- TLS Port:** 5061 (text box), Leave blank to disable
- TLS Profile:** New_ServiceProvider_Server_TLS (dropdown)
- Enable Shared Control:**
- Shared Control Port:** (text box)

A 'Finish' button is located at the bottom center of the form.

A second Signaling Interface with the name **Public_sig** was similarly created in the service provider's direction.

- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.
- Select a **TLS Profile**.
- Click **Finish**.

The screenshot shows a configuration window titled "Add Signaling Interface". The form includes the following fields and values:

- Name:** Public_sig
- IP Address:** Network_B1 (B1. VLAN 0) (dropdown), 10.10.80.51 (dropdown)
- TCP Port:** (text box), Leave blank to disable
- UDP Port:** (text box), Leave blank to disable
- TLS Port:** 5061, Leave blank to disable
- TLS Profile:** Clearcom_Cert (dropdown)
- Enable Shared Control:**
- Shared Control Port:** (text box)

A "Finish" button is located at the bottom of the form.

7.6. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.6.1. Server Interworking Profile – Enterprise

Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Global Profiles** → **Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select *avaya-ru* from the list of pre-defined profiles. Click **Clone**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the AVAYA logo. The left navigation pane is expanded to "Global Profiles" > "Server Interworking". The main content area is titled "Interworking Profiles: avaya-ru" and features an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, there are tabs for "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of configuration parameters:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No

- Enter a descriptive name for the cloned profile.
- Click **Finish**.

The "Clone Profile" dialog box is shown with the following fields:

- Profile Name: avaya-ru
- Clone Name: Avaya-SM (highlighted with a red box)

A "Finish" button is located at the bottom of the dialog.

The **Timers**, **Privacy**, **URI Manipulation** and **Header Manipulation** tabs contain no entries. The **Advanced** tab settings are shown on the screen below:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'Domain DoS', 'Media Forking', 'Routing', 'Server Configuration', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', and 'PPM Services'. The 'Global Profiles' section is expanded, and 'Avaya-SM' is selected.

The main content area is titled 'Interworking Profiles: Avaya-SM'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A blue bar prompts the user to 'Click here to add a description.' Below this are tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'Advanced' tab is active, showing a table of settings:

Setting	Value
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No

Below the table is a 'DTMF' section with a table:

Setting	Value
DTMF Support	None

An 'Edit' button is located at the bottom right of the settings area.

7.6.2. Server Interworking Profile – Service Provider

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Global Profiles** → **Server Interworking** on the left navigation pane and click **Add** (not shown).

- Enter a descriptive name for the new profile.
- Click **Next**, then click **Finish** on the last tab leaving remaining fields with default values (not shown).



7.7. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform granular header manipulations on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [8] in the **References** section for more information on this topic.

Sigma scripts were created during the compliance test to correct the following interoperability issues (refer to **Section 2.2**):

- Include the SIP trunk credential's username in the "From" header of all outbound calls.
- Copy the destination DID number present in the "To" header of incoming calls to the "Request-URI" header.
- Remove the "gsid" and "epv" parameters from outbound "Contact" headers.

The script will later be applied to the Server Configuration profile corresponding to the service provider in **Section 7.8.2**.

On the left navigation pane, select **Global Profiles** → **Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

- For **Title** enter a name, the name *Clearcom_Script* was chosen in this example.
- Copy the complete script from **Appendix A**.
- Click **Save**.

The following screen capture shows the **Clearcom_Script** script after it was added.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The main header is 'Session Border Controller for Enterprise'. The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Parameters', 'Global Profiles', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', 'RADIUS', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The 'Signaling Manipulation' category is highlighted. The main content area is titled 'Signaling Manipulation Scripts: Clearcom_Script' and features 'Upload' and 'Add' buttons. Below the title, it indicates 'Showing page 1 of 2.' and a link to 'Click here to add a description.'. A list of scripts is shown on the right, including 'Remove Remote Ad...', 'Remove_Replace H...', 'Remove_Unwanted...', 'otg', 'CenturyLink', 'Remove Remote Ad...', 'Add Supported_repl...', 'Remove Privacy: id', 'Change_Diversion', 'GSID_EPV', 'Change_Diversion_1', 'Remove_UPDATE', 'Remove_UPDATE_...', 'Change Max-Forward', and 'Remove_Sendonly'. The 'Signaling Manipulation' script is selected, and its configuration is displayed in a code editor. The script content is as follows:

```
//Replace Username in "REQUEST-LINE" with "TO" number on Inbound
within session "ALL"
{
act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{
%HEADERS["Request_Line"][1].URI.USER = %HEADERS["To"][1].URI.USER;
}
}

//Insert Username in the FROM header on Outbound
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%fromuser = %HEADERS["From"][1].URI.USER;
%HEADERS["From"][1].URI.USER = "avayasbc1";
}
}

//Remove gsid and epv parameters in outbound Contact header
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
}
}
```

An 'Edit' button is located at the bottom right of the code editor.

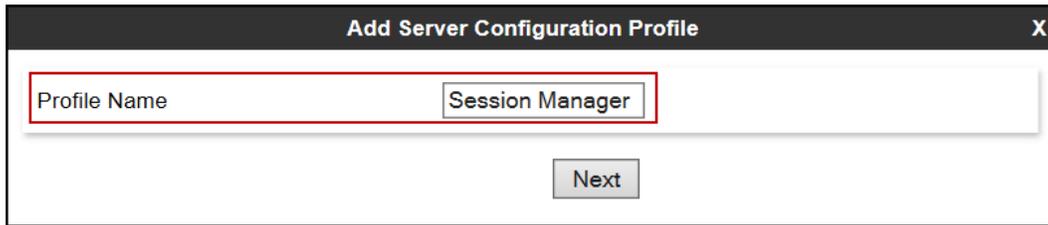
7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and Clearcom SIP Proxy (Trunk Server).

7.8.1. Server Configuration Profile – Enterprise

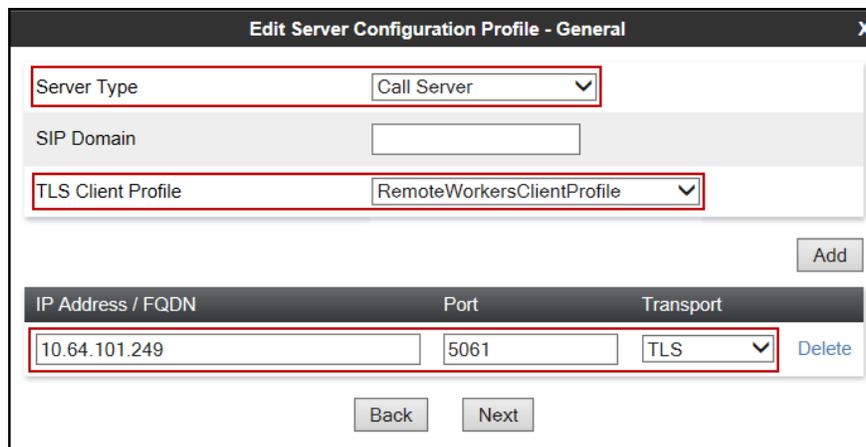
From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server.

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



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

- On the **Edit Server Configuration Profile – General** tab select *Call Server* from the drop down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 6.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.6**.
- Select a **TLS Client Profile**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and buttons:

- Server Type**: A dropdown menu set to "Call Server".
- SIP Domain**: An empty text input field.
- TLS Client Profile**: A dropdown menu set to "RemoteWorkersClientProfile".
- Add**: A button located to the right of the TLS Client Profile dropdown.
- IP Address / FQDN**: A table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "10.64.101.249", "5061", and "TLS".
- Delete**: A button located to the right of the table.
- Back** and **Next**: Buttons located at the bottom of the dialog.

- Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown).
- Select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Click **Finish**.

Add Server Configuration Profile - Advanced X

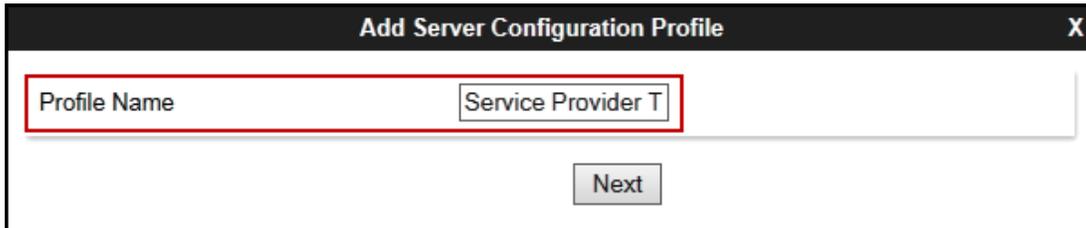
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-SM ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>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

Back Finish

7.8.2. Server Configuration Profile – Service Provider

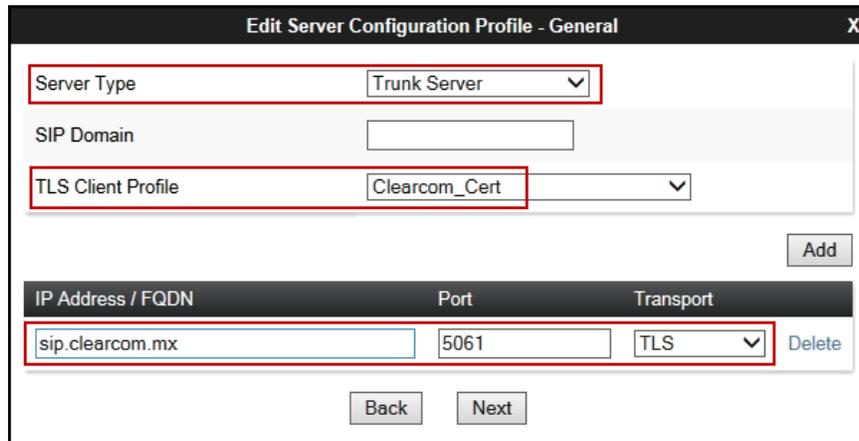
Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- Enter an appropriate **Profile Name** similar to the screen below.
- Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. The main area contains a text input field labeled "Profile Name" with the text "Service Provider T" entered. Below the input field is a "Next" button.

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, *sip.clearcom.mx* (the Fully Qualified Domain Name of the service provider SIP proxy server. This information was provided by Clearcom).
- Enter **5061** under **Port**, and select **TLS** for **Transport**.
- Select a **TLS Client Profile**.
- Click **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General". It has a close button (X) in the top right corner. The main area contains several fields: "Server Type" (dropdown menu set to "Trunk Server"), "SIP Domain" (empty text field), "TLS Client Profile" (dropdown menu set to "Clearcom_Cert"), and an "Add" button. Below these fields is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The table contains one row with the values "sip.clearcom.mx", "5061", and "TLS". There is a "Delete" button next to the row. At the bottom of the dialog are "Back" and "Next" buttons.

On the **Add Server Configuration Profile - Authentication** window:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential provided by the service provider for SIP trunk registration.
- Enter the **Realm** credential provided by the service provider for SIP trunk registration. Note that the Service Provider's Domain Name was used (Must be entered, currently cannot be detected automatically from the challenge).
- Enter **Password** credential provided by the service provider for SIP trunk registration. Click **Next**.

The screenshot shows a window titled "Add Server Configuration Profile - Authentication". The window contains a form with the following fields and values:

Enable Authentication	<input checked="" type="checkbox"/>
User Name	User123
Realm (Leave blank to detect from server challenge)	clearcom.mx
Password	••••••
Confirm Password	••••••

At the bottom of the form, there are two buttons: "Back" and "Next".

On the **Add Server Configuration Profile - Heartbeat** window:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, **120** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: Use the **User Name** entered above in the **Authentication** screen (**User123**) and the Service Provider's domain name (**clearcom.mx**), as shown on the screen below.
 - **To URI**: Use the **User Name** entered above in the **Authentication** screen (**User123**) and the Service Provider's domain name (**clearcom.mx**), as shown on the screen below.
- Click **Next** until the **Add Server Configuration Profile - Advanced** window is reached.

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER ▾
Frequency	120 seconds
From URI	Jser123@clearcom.mx
To URI	Jser123@clearcom.mx

Back Next

On the **Add Server Configuration Profile - Advanced** window:

- Select **SP-General** from the **Interworking Profile** drop down menu.
- Select the **Clearcom_Script** from the **Signaling Manipulation Script** drop down menu (**Section 7.7**).
- Click **Finish**.

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

Back Finish

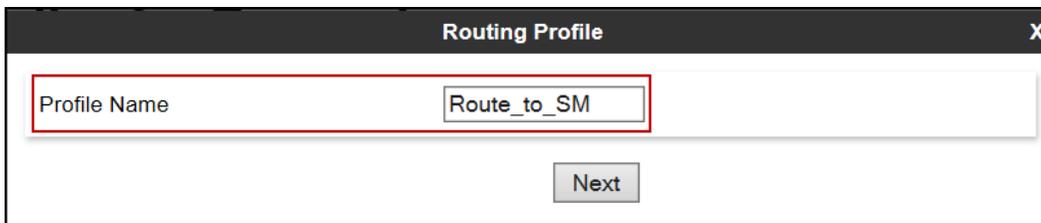
7.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the service provider SIP trunk.

7.9.1. Routing Profile – Enterprise

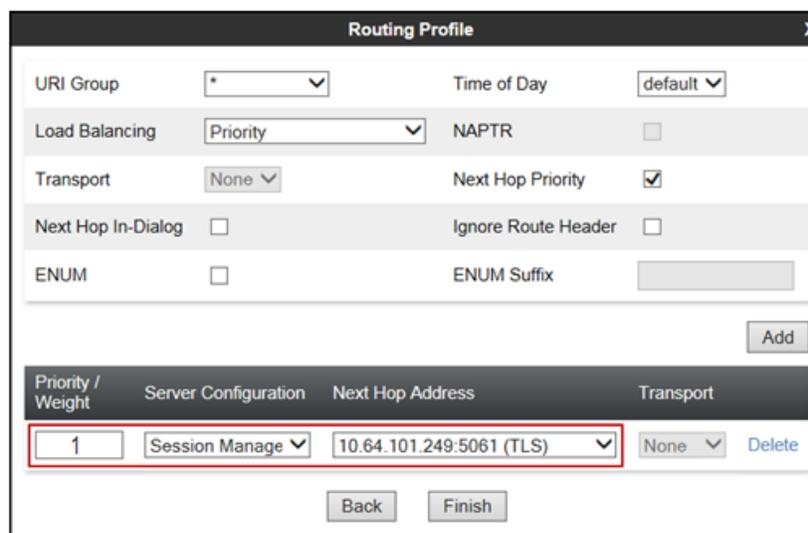
To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown).

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" which contains the text "Route_to_SM". A red rectangular box highlights this field. Below the input field, there is a "Next" button.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **Server Configuration**, select **Session Manager**. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the Session Manager Server Configuration Profile in **Section 7.8.1**.
- Defaults were used for all other parameters.
- Click **Finish**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. The dialog contains several configuration options:

- URI Group: *
- Time of Day: default
- Load Balancing: Priority
- NAPTR:
- Transport: None
- Next Hop Priority:
- Next Hop In-Dialog:
- Ignore Route Header:
- ENUM:
- ENUM Suffix: (empty field)

Below these options is an "Add" button. At the bottom of the dialog, there is a table with the following data:

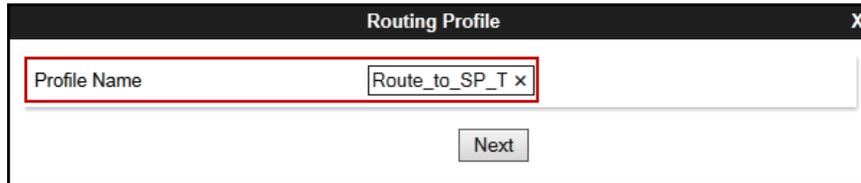
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manager	10.64.101.249:5061 (TLS)	None

Buttons for "Back" and "Finish" are located at the bottom of the dialog.

7.9.2. Routing Profile – Service Provider

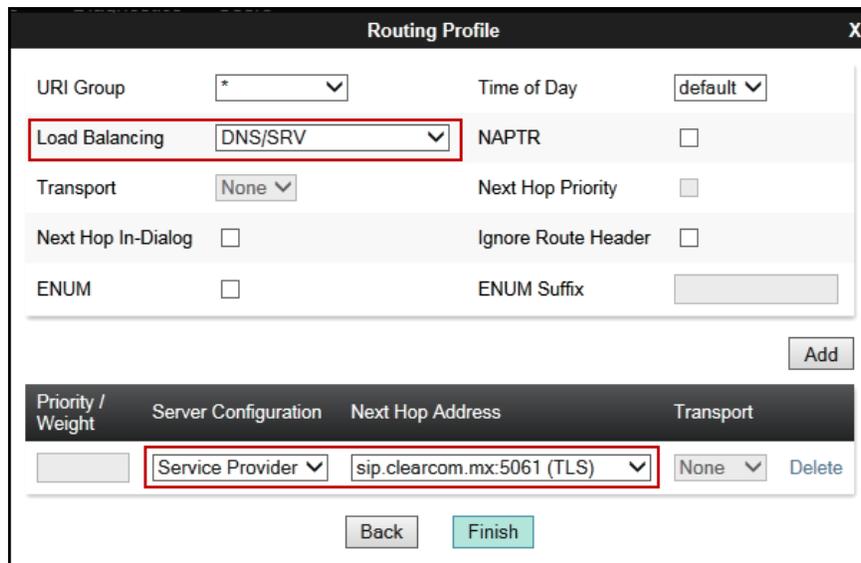
Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route.

- Enter an appropriate **Profile Name** similar to the example below.
- Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route_to_SP_T". Below the input field is a "Next" button.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- **Load Balancing:** Select *DNS/SRV*.
- Click on the **Add** button to add a **Next-Hop Address**.
- **Server Configuration:** Select *Service Provider TLS*.
- The **Next Hop Address** is populated automatically with *sip.clearcom.mx:5061 (TLS)* Service Provider FQDN, Port and Transport, Server Configuration Profile defined in **Section 7.8.2**
- Click **Finish**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. The dialog contains several configuration options:

- URI Group: *
- Time of Day: default
- Load Balancing: DNS/SRV (highlighted with a red box)
- NAPTR:
- Transport: None
- Next Hop Priority:
- Next Hop In-Dialog:
- Ignore Route Header:
- ENUM:
- ENUM Suffix: (empty text field)

Below these options is an "Add" button. At the bottom of the dialog, there is a table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, Transport, and Delete.

Priority / Weight	Server Configuration	Next Hop Address	Transport	Delete
	Service Provider (highlighted with a red box)	sip.clearcom.mx:5061 (TLS) (highlighted with a red box)	None	Delete

At the bottom of the dialog are "Back" and "Finish" buttons.

7.10. Topology Hiding

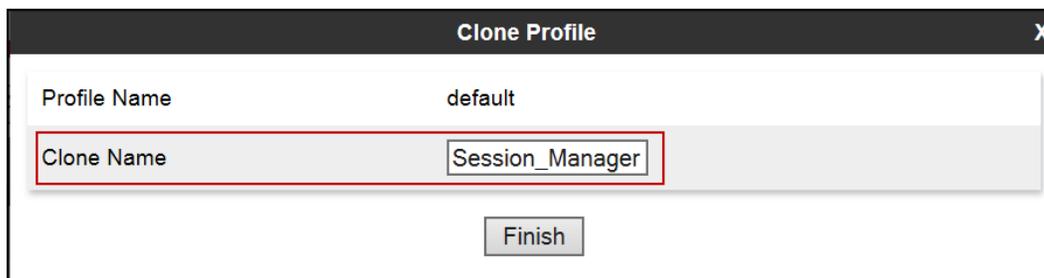
Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select *default* from the list of pre-defined profiles and click the **Clone** button (not shown).

- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The screenshot shows a dialog box titled "Clone Profile" with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first field is labeled "Profile Name" and contains the text "default". The second field is labeled "Clone Name" and contains the text "Session_Manager"; this field is highlighted with a red rectangular border. Below the input fields is a button labeled "Finish".

On the newly cloned *Session_Manager* profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select *Overwrite* in the **Replace Action** column and enter the enterprise SIP domain *avaya.lab.com*, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.2**.
- Default values were used for all other fields.
- Click **Finish**.

The screenshot shows a window titled "Edit Topology Hiding Profile" with a close button (X) in the top right corner. Below the title bar is a table with the following columns: Header, Criteria, Replace Action, and Overwrite Value. Each row also has a "Delete" button on the right. The rows are: SDP, To, From, Refer-To, Via, Record-Route, Request-Line, and Referred-By. The "To", "From", and "Request-Line" rows are highlighted with red boxes. The "Request-Line" row is also highlighted with a red box around the "Overwrite" action and "avaya.lab.com" value.

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

Finish

7.10.2. Topology Hiding Profile – Service Provider

To add the Topology Hiding Profile in the service provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side, select *default* from the list of pre-defined profiles and click the **Clone** button (not shown).

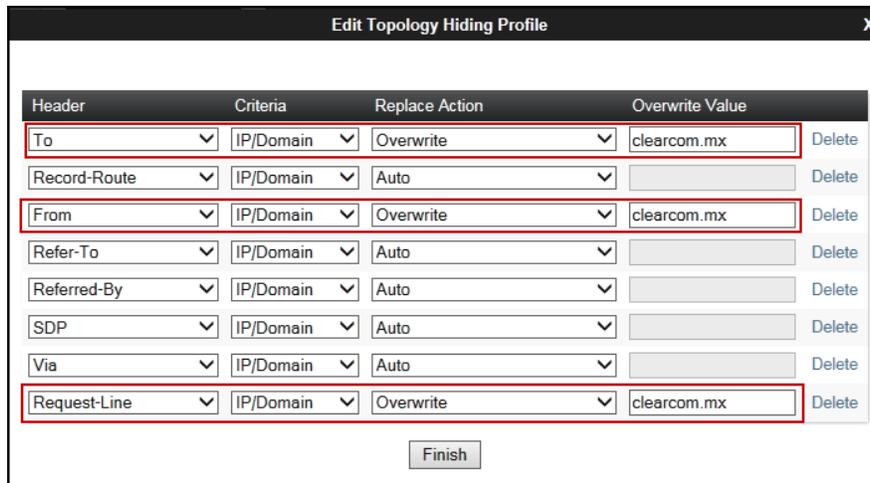
- Enter a **Clone Name** such as the one shown below.
- Click **Finish**.



The screenshot shows a dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two input fields: "Profile Name" with the value "default" and "Clone Name" with the value "Service_Provider". A "Finish" button is located at the bottom center of the dialog.

On the newly cloned *Service_Provider* profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select *Override* in the **Replace Action** column and enter the enterprise SIP domain *clearcom.mx*, in the **Override Value** column of these headers, as shown below. This is the service provider's domain name.
- Default values were used for all other fields.
- Click **Finish**.



The screenshot shows a dialog box titled "Edit Topology Hiding Profile" with a close button (X) in the top right corner. It contains a table with the following columns: Header, Criteria, Replace Action, Overwrite Value, and a Delete button. The table is as follows:

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

A "Finish" button is located at the bottom center of the dialog.

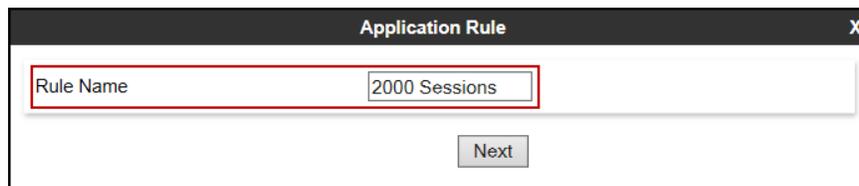
7.11. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

7.11.1. Application Rules

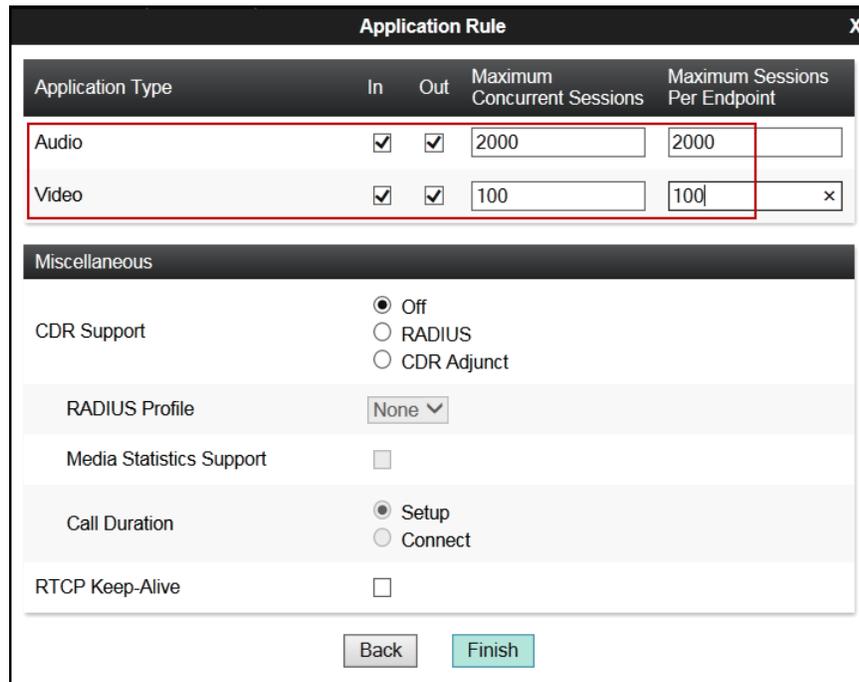
Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**, Click on the **Add** button to add a new rule.

- Under **Rule Name** enter the name of the profile, e.g., **2000 Sessions**.
- Click **Next**.



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. Below the title bar is a text input field labeled "Rule Name" containing the text "2000 Sessions". Below the input field is a "Next" button.

- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the values of **2000** for Audio and **100** for Video were used in the sample configuration.
- Click **Finish**.



The screenshot shows a window titled "Application Rule" with a close button (X) in the top right corner. Below the title bar is a table with the following columns: "Application Type", "In", "Out", "Maximum Concurrent Sessions", and "Maximum Sessions Per Endpoint". The table has two rows: "Audio" and "Video". The "Audio" row has "In" and "Out" checked, "Maximum Concurrent Sessions" set to "2000", and "Maximum Sessions Per Endpoint" set to "2000". The "Video" row has "In" and "Out" checked, "Maximum Concurrent Sessions" set to "100", and "Maximum Sessions Per Endpoint" set to "100". Below the table is a "Miscellaneous" section with the following options: "CDR Support" (radio buttons for Off, RADIUS, CDR Adjunct), "RADIUS Profile" (dropdown menu set to "None"), "Media Statistics Support" (checkbox), "Call Duration" (radio buttons for Setup, Connect), and "RTCP Keep-Alive" (checkbox). At the bottom of the window are "Back" and "Finish" buttons.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100

7.11.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, two media rules (shown below) were used; one toward Session Manager and one toward the Service Provider.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter *SM_SRTP*.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select *SRTP_AES_CM_128_HMAC_SHA1_80*.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck *Encrypted RTCP*.
- Under Audio Encryption, check *Interworking*.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that *Capability Negotiation* is checked.
- Click **Next**.

Media Encryption X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	RTP
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

Capability Negotiation	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

Finish

- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown).

To add a media rule in the Service Provider direction, from the menu on the left-hand side, select **Domain Policies → Media Rules**.

- Click on the **Add** button to add a new media rule (not shown).
- Under **Rule Name** enter *ServiceProvider_SRTP* (not shown).
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select *SRTP_AES_CM_128_HMAC_SHA1_80*.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck *Encrypted RTCP*.
- Under Audio Encryption, check *Interworking*.
- Repeat the above steps under Video Encryption.
- Under Miscellaneous verify that *Capability Negotiation* is checked.
- Click **Next**.

Media Encryption X

Audio Encryption

Preferred Format #1 SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2 RTP

Preferred Format #3 NONE

Encrypted RTCP

MKI

Lifetime
Leave blank to match any value. 2^

Interworking

Video Encryption

Preferred Format #1 SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2 RTP

Preferred Format #3 NONE

Encrypted RTCP

MKI

Lifetime
Leave blank to match any value. 2^

Interworking

Miscellaneous

Capability Negotiation

Finish

Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish** (not shown)

7.11.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left sidebar menu lists various configuration categories, with 'Domain Policies' expanded to show 'Signaling Rules' highlighted in red. The main content area is titled 'Signaling Rules: default' and features an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'General' tab is active, showing a 'UCID' field and three sections: 'Inbound', 'Outbound', and 'Content-Type Policy'. The 'Inbound' and 'Outbound' sections each contain a table with columns for 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers', all set to 'Allow'. The 'Content-Type Policy' section includes a checked 'Enable Content-Type Checks' checkbox, an 'Action' set to 'Allow', a 'Multipart Action' set to 'Allow', and an 'Exception List' field. An 'Edit' button is located at the bottom of the configuration area.

7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

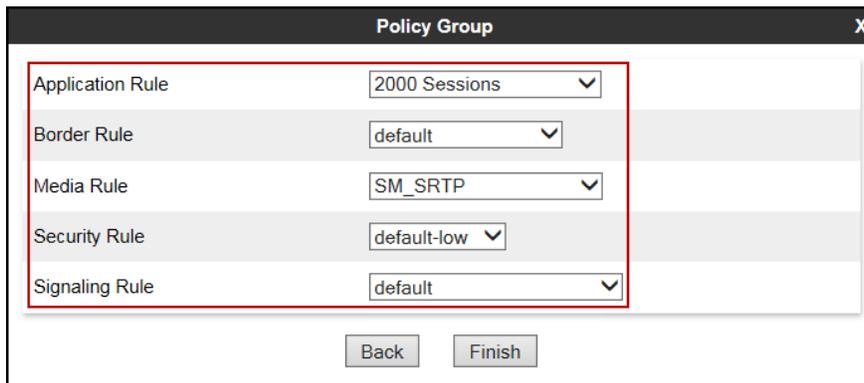
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Enterprise". A red rectangular box highlights the "Group Name" field. Below the input field, there is a "Next" button.

Under the **Policy Group** tab enter the following:

- **Application Rule:** *2000 Sessions* (Section 7.11.1).
- **Border Rule:** *default*.
- **Media Rule:** *SM_SRTP* (Section 7.11.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.11.3).
- Click **Finish**.

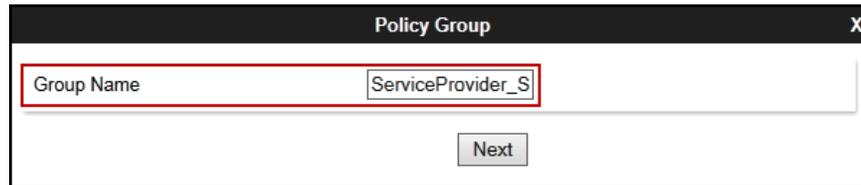


The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. The dialog contains a list of rules with dropdown menus for each. A red rectangular box highlights the rule selection area. The rules and their selected values are: Application Rule (2000 Sessions), Border Rule (default), Media Rule (SM_SRTP), Security Rule (default-low), and Signaling Rule (default). Below the rule list, there are "Back" and "Finish" buttons.

7.12.2. End Point Policy Group – Service Provider

To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add** (not shown).

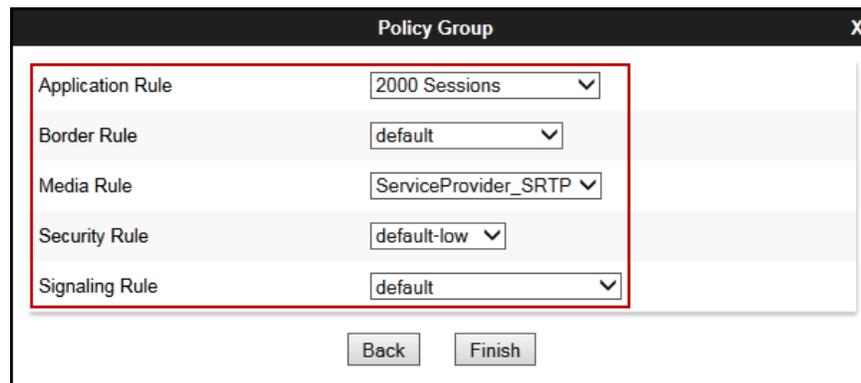
- Enter an appropriate name in the **Group Name** field.
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Below the title bar, there is a text input field labeled "Group Name" containing the text "ServiceProvider_S". A red rectangular box highlights the "Group Name" label and the input field. Below the input field, there is a "Next" button.

Under the **Policy Group** tab enter the following:

- **Application Rule:** *2000 Sessions* (Section 7.11.1).
- **Border Rule:** *default*.
- **Media Rule:** *ServiceProvider_SRTP* (Section 7.11.2).
- **Security Rule:** *default-low*.
- **Signaling Rule:** *default* (Section 7.11.3).
- Click **Finish**.



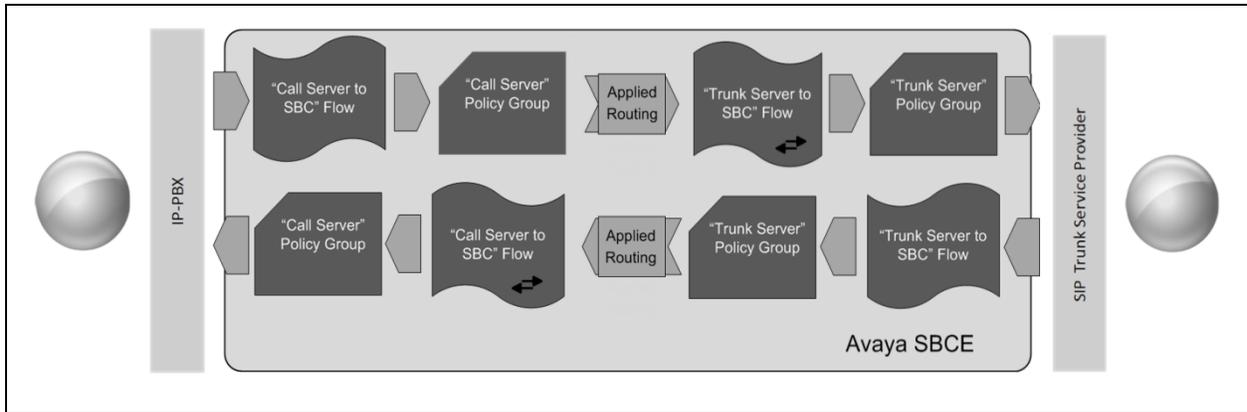
The screenshot shows the "Policy Group" dialog box with the following configuration:

Rule Type	Selected Value
Application Rule	2000 Sessions
Border Rule	default
Media Rule	ServiceProvider_SRTP
Security Rule	default-low
Signaling Rule	default

At the bottom of the dialog box, there are two buttons: "Back" and "Finish". A red rectangular box highlights the rule configuration area.

7.13. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named *Session_Manager_Flow* created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for the Service Provider in **Section 7.9.2**, which is the reverse route of the flow. Click **Finish**.

Field	Value
Flow Name	Session_Manager_Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
Secondary Media Interface	None
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP_TLS
Topology Hiding Profile	Session_Manager
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

7.13.2. End Point Flow – Service Provider

A second Server Flow with the name *SIP_Trunk_Flow_TLS* was similarly created in the Service Provider direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.1**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish**.

Edit Flow: SIP_Trunk_Flow_TLS	
Flow Name	SIP_Trunk_Flow_TLS
Server Configuration	Service Provider TLS
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
Secondary Media Interface	None
End Point Policy Group	ServiceProvider_SRTP
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

8. Clearcom SIP Trunk Service Configuration

To use Clearcom SIP Trunk Service, a customer must request the service from Clearcom using the established sales processes. The process can be started by contacting Clearcom via the corporate web site at: <http://www.clearcom.mx/>

During the signup process, Clearcom and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Clearcom's network.

Clearcom will provide the following information:

- SIP Trunk registration credentials (user name, password, SIP domain).
- Fully Qualified Domain Name of the Clearcom SIP proxy server.
- DID numbers.
- Public DNS IP addresses.
- Supported codecs and order of preference.
- Any IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices (firewall).

9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of commands that can be used to troubleshoot the solution.

9.1. General Verification Steps

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Communication Manager Verification

The following commands can be entered in the Communication Manager SAT terminal to verify the SIP trunk functionality:

- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group number>
Displays trunk group service state.

- **status station** <extension number>
Displays signaling and media information for an active call on a specific station.

9.3. Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring**. Click the Session Manager instance (*Session Manager* in the example below).

The screenshot shows the Avaya Aura System Manager 7.1 interface. The breadcrumb navigation is Home / Elements / Session Manager / System Status / SIP Entity Monitoring. The page title is "SIP Entity Link Monitoring Status Summary". Below the title, there is a "Run Monitor" button and a table showing the status of monitored SIP entities. The table has columns for Session Manager, Type, Down, Partially Up, Up, Not Monitored, Deny, and Total. One row is highlighted with a red border, showing "Session Manager" of type "Core" with 1 Down, 0 Partially Up, 5 Up, 0 Not Monitored, 0 Deny, and a Total of 6.

Session Manager	Type	Monitored Entities					Total
		Down	Partially Up	Up	Not Monitored	Deny	
Session Manager	Core	1	0	5	0	0	6

Verify that the state of the Session Manager links to Communication Manager and the Avaya SBCE under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left sidebar contains a navigation menu with 'System Status' and 'SIP Entity Monitoring' highlighted. The main content area displays 'Session Manager Entity Link Connection Status'. Below this, there is a table titled 'All Entity Links for Session Manager: Session Manager'. The table has columns for SIP Entity Name, IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The 'Avaya SBCE' and 'Communication Manager Trunk 2' rows are highlighted with red boxes, indicating a 'UP' status in both the 'Conn. Status' and 'Link Status' columns.

SIP Entity Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
CS1K7.6	IPv4	172.16.5.60	5085	UDP	FALSE	DOWN	408 Request Timeout	DOWN
Avaya SBCE	IPv4	10.64.101.243	5061	TLS	FALSE	UP	200 OK	UP
Communication Manager Trunk 1	IPv4	10.64.101.241	5061	TLS	FALSE	UP	200 OK	UP
AA-Messaging	IPv4	10.64.101.250	5060	TCP	FALSE	UP	200 OK	UP
Communication Manager Trunk 2	IPv4	10.64.101.241	5071	TLS	FALSE	UP	200 OK	UP
Communication Manager Trunk 98	IPv4	10.64.101.241	5065	TLS	FALSE	UP	200 OK	UP

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test.

9.4. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: This screen provides information about the health of the SBC.

Alarms 1 Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration
Backup/Restore
System Management
▸ Global Parameters
▸ Global Profiles
▸ PPM Services
▸ Domain Policies
▸ TLS Management
▸ Device Specific Settings

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

Information	
System Time	12:27:04 PM EST Refresh
Version	7.2.0.0-18-13712
Build Date	Thu Jun 1 00:12:50 UTC 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	11/22/2017 10:47:24 EST
Failed Login Attempts	0

Installed Devices	
EMS	
Avaya_SBCE	1

Active Alarms (past 24 hours)

Avaya_SBCE : Disk utilization is more than 75% for /archive/log/ipcs

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched
Avaya_SBCE : No Subscriber Flow Matched

The following screen shows the **Alarm Viewer** page.

Help

Alarm Viewer

AVAYA

Devices

EMS 1
Avaya_SBCE

Alarms

<input checked="" type="checkbox"/>	ID	Details	State	Time	Device
No alarms found for this device.					

Clear Selected Clear All

Incidents : Provides detailed reports of anomalies, errors, policies violations, etc.

Session Border Controller for Enterprise AVAYA

Alarms **1** Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Dashboard

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

The following certificates are expired:

- Rapid_SSL_Cert.crt (Certificate)

Information	
System Time	12:27:04 PM EST Refresh
Version	7.2.0.0-18-13712
Build Date	Thu Jun 1 00:12:50 UTC 2017
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	11/22/2017 10:47:24 EST
Failed Login Attempts	0

Installed Devices
EMS
Avaya_SBCE 1

Active Alarms (past 24 hours)

Avaya_SBCE : Disk utilization is more than 75% for /archive/log/ipcs

Incidents (past 24 hours)

Avaya_SBCE : No Subscriber Flow Matched

Avaya_SBCE : No Subscriber Flow Matched

The following screen shows the Incident Viewer page.

Incident Viewer AVAYA

Device Category

Displaying results 0 to 0 out of 0.

Type	ID	Date	Time	Category	Device	Cause
No incidents found.						

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

The screenshot shows the Avaya SBCE Dashboard. At the top, there is a navigation bar with 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics' (highlighted with a red arrow), and 'Users'. The main header reads 'Session Border Controller for Enterprise' and the Avaya logo is in the top right. A left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings), and Users. The main content area is titled 'Dashboard' and features a prominent red warning banner: 'This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.' Below this, a section titled 'The following certificates are expired:' lists 'Rapid_SSL_Cert.crt (Certificate)'. There are two main panels: 'Information' and 'Installed Devices'. The 'Information' panel contains a table with system details: System Time (12:27:04 PM EST), Version (7.2.0.0-18-13712), Build Date (Thu Jun 1 00:12:50 UTC 2017), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (11/22/2017 10:47:24 EST), and Failed Login Attempts (0). The 'Installed Devices' panel shows 'EMS' and 'Avaya_SBCE' with a red '1' indicator. At the bottom, there are sections for 'Active Alarms (past 24 hours)' and 'Incidents (past 24 hours)', both showing a message: 'Avaya_SBCE : No Subscriber Flow Matched'.

The following screen shows the Diagnostics page with the results of a ping test.

The screenshot shows the Avaya SBCE Diagnostics page. At the top, there is a navigation bar with 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics' (highlighted with a red arrow), and 'Users'. The main header reads 'Session Border Controller for Enterprise' and the Avaya logo is in the top right. A left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings), and Users. The main content area is titled 'Diagnostics' and features a 'Ping Test' section. A modal window titled 'Pinging 10.64.101.249' is open, displaying the result: 'Average ping from 10.64.101.244 [A1] to 10.64.101.249 is 0.369ms.' Below the modal, there is a 'Full Diagnostic' section with a 'Ping Test' tab. The 'Ping Test' section contains a warning: 'Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.' There are input fields for 'Source Device / IP' (set to 'A1') and 'Destination IP' (set to '10.64.101.249'), and a 'Ping' button.

Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.

The screenshot displays the Avaya SBCE web interface. At the top, there is a navigation bar with 'Alarms 1', '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-hand navigation menu includes 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', 'Device Specific Settings' (highlighted with a red box), 'Network Management', 'Media Interface', 'Signaling Interface', 'End Point Flows', 'Session Flows', 'DMZ Services', 'TURN/STUN Service', 'SNMP', 'Syslog Management', 'Advanced Options', 'Troubleshooting' (highlighted with a red box), 'Debugging', 'Trace' (highlighted with a red box), and 'DoS Learning'. The main content area is titled 'Trace: Avaya_SBCE' and contains two tabs: 'Packet Capture' (highlighted with a red box) and 'Captures'. The 'Packet Capture Configuration' form includes the following fields: 'Status' (Ready), 'Interface' (Any), 'Local Address IP[Port]' (All), 'Remote Address' (with a '*' placeholder), 'Protocol' (All), 'Maximum Number of Packets to Capture' (10000), and 'Capture Filename' (Test.pcap). 'Start Capture' and 'Clear' buttons are located at the bottom of the form.

Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management), Device Specific Settings (with sub-items: Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options), Troubleshooting (with sub-items: Debugging, Trace, DoS Learning).

The main content area is titled 'Trace: Avaya_SBCE'. It features two tabs: 'Packet Capture' and 'Captures'. The 'Captures' tab is active and displays a table of captured files. A 'Refresh' button is located in the top right corner of the table area.

File Name	File Size (bytes)	Last Modified	
Test_20171122123225.pcap	176,128	November 22, 2017 12:32:47 PM EST	Delete

10. Conclusion

These Application Notes describe the procedures required to configure Avaya Aura® Communication Manager 7.1, Avaya Aura® Session Manager 7.1 and Avaya Session Border Controller for Enterprise 7.2, to connect to the Clearcom SIP Trunk service using TLS transport for signaling, as shown in **Figure 1**.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observations/limitations described in **Sections 2.1** and **2.2**.

11. 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*, Release 7.1.1, Issue 2, August 2017.
- [2] *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017.
- [3] *Administering Avaya Aura® System Manager* for Release 7.1.1, Issue 7, October 2017.
- [4] *Deploying Avaya Aura® System Manager*, Release 7.1.1, Issue 3, August 2017.
- [5] *Deploying Avaya Aura® Session Manager*, Release 7.1, Issue 1, May 2017.
- [6] *Administering Avaya Aura® Session Manager*, Release 7.1.1, Issue 2, August 2017.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.2.1, Issue 4, November 2017.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.1, Issue 4, November 2017.
- [9] *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0 - Issue 1.0*.
- [10] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.8, Issue 3, August 2017.
- [11] *Implementing and Administering Avaya Aura® Media Server*. Release 7.8, Issue 5, October 2017.
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

12. Appendix A: SigMa Script

Following is the Signaling Manipulation script that was used in the configuration of the Avaya SBCE, **Section 7.7**. When adding this script as instructed in **Section 7.8.2** enter a name for the script in the Title (e.g., **Clearcom_Script**) and copy/paste the entire script. Note that the user name shown below as “User123” will need to be changed with the correct user name provided by Clearcom for registration purpose.

Title: Clearcom_Script

```
//Replace Username in "REQUEST-LINE" with "TO" number on Inbound
within session "ALL"
{
act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
{
%HEADERS["Request_Line"][1].URI.USER = %HEADERS["To"][1].URI.USER;
}
}
//Insert Username in the FROM header on Outbound
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%fromuser = %HEADERS["From"][1].URI.USER;
%HEADERS["From"][1].URI.USER = "User123";
}
}

//Remove gsid and epv parameters in outbound Contact header
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
}
}
```

©2018 Avaya Inc. All Rights Reserved.

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

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