



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Orange Business Services BTIP/BT SIP Trunking Service with Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.3 – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, and Avaya Session Border Controller for Enterprise 6.3 to inter-operate with the Orange Business Services BTIP/BT SIP Trunking Service via an on-premise Cisco 1841 Router provisioned by Orange Business Services. Orange Business Services is a member of the Avaya DevConnect Service Provider program.

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	4
2.2.	Test Results.....	5
2.3.	Support.....	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	11
5.	Configure Avaya Aura® Communication Manager	12
5.1.	Licensing and Capacity.....	12
5.2.	System Features	13
5.3.	IP Node Names	14
5.4.	Codecs.....	14
5.5.	IP Network Region	15
5.6.	Signaling Group.....	16
5.7.	Trunk Group.....	18
5.8.	Calling Party Information	23
5.9.	Outbound Routing.....	24
5.10.	EC500 Station Mapping.....	26
6.	Configure Avaya Aura® Session Manager	27
6.1.	Avaya Aura® System Manager Login and Navigation	28
6.2.	Specify SIP Domain.....	30
6.3.	Add Location	31
6.4.	Add Adaptation Module	32
6.5.	Add SIP Entities.....	34
6.6.	Add Entity Links.....	38
6.7.	Add Routing Policies	40
6.8.	Add Dial Patterns.....	42
6.9.	Add/View Avaya Aura® Session Manager.....	45
7.	Configure Avaya Session Border Controller for Enterprise	47
7.1.	Access the Management Interface	47
7.2.	Verify Network Configuration and Enable Interfaces	48
7.3.	Signaling Interface	51
7.4.	Media Interface	52
7.5.	Server Interworking	53
7.5.1.	Server Interworking – Session Manager.....	54
7.5.2.	Server Interworking – Orange Business Services.....	56
7.6.	Signaling Manipulation.....	57
7.7.	Server Configuration.....	59
7.7.1.	Server Configuration – Session Manager	60
7.7.2.	Server Configuration – Orange Business Services	61
7.8.	Application Rules.....	62
7.9.	Media Rules	63
7.10.	Signaling Rules	65
7.10.1.	Signaling Rules – Session Manager.....	66
7.10.2.	Signaling Rules – Orange Business Services.....	68

7.11.	Endpoint Policy Groups	69
7.11.1.	Endpoint Policy Group – Session Manager	70
7.11.2.	Endpoint Policy Group – Orange Business Services	70
7.12.	Routing.....	71
7.12.1.	Routing – Session Manager	72
7.12.2.	Routing – Orange Business Services	73
7.13.	Topology Hiding.....	74
7.13.1.	Topology Hiding – Session Manager	75
7.13.2.	Topology Hiding – Orange Business Services	76
7.14.	End Point Flows.....	77
7.14.1.	End Point Flow – Session Manager	78
7.14.2.	End Point Flow – Orange Business Services	80
8.	Orange SIP Trunking Service Configuration.....	82
9.	Verification Steps.....	82
10.	Conclusion	85
11.	References	85

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the Orange Business Services BTIP/BT (Business Talk IP / Business Talk) SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of an Avaya Aura® Session Manager 6.3, an Avaya Aura® Communication Manager Evolution Server 6.3, an Avaya Session Border Controller for Enterprise 6.3 (Avaya SBCE) and various Avaya endpoints listed in **Section 4**. In addition an Avaya Aura® System Manager 6.3 is used to configure the Avaya Aura® Session Manager. This Avaya solution connects to the Orange Business Services BTIP/BT SIP Trunking Service via an on-site Cisco 1841 Router managed by Orange Business Services as the demarcation point for the service.

Customers using this Avaya SIP-enabled enterprise solution with the Orange Business Services BTIP/BT SIP Trunking Service are able to place and receive PSTN calls via a broadband WAN connection using SIP. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

For simplicity, Orange Business Services could be referred to as “Orange”, and its BTIP/BT SIP Trunking Service as “SIP Trunking Service” in the remainder of this document.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Orange SIP Trunking Service and exercise the features and functionality listed in **Section 2.1**. It should be noted that the connection between the enterprise site and Orange Business Services is via an Orange-managed network IP connection which includes the on-premise Cisco 1841 Router connected to the public Internet. The simulated enterprise site was comprised of a Communication Manager, a Session Manager and an Avaya Session Border Controller for Enterprise.

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 trunking interoperability, the following features and functionality were covered during the compliance test.

- Sending SIP OPTIONS queries to and receiving responses from the service provider.
- Incoming calls from the PSTN to H.323 and SIP telephones at the enterprise. All inbound calls from the PSTN were routed from the service provider across the SIP trunk to the enterprise.

- Outgoing calls to the PSTN from H.323 and SIP telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft client. 1XC can place calls from the local computer or control a remote phone. Both of these modes were tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Each protocol version of 1XC was also tested.
- Inbound and outbound calls to Flare Experience for Windows (SIP soft client).
- Outbound calls to local, long distance, and international destinations.
- G.711A and G.729 codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and mobility (extension to cellular – EC500).
- Voicemail navigation for inbound and outbound calls, and voicemail Message Waiting Indicator (MWI).
- Inbound and outbound long-duration and long hold time call stability.
- T.38 fax.
- Response to incomplete call attempts and trunk errors.

2.2. Test Results

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

- **Stability:** On outbound calls, it sometimes happened that the outbound INVITE to the first Orange SIP server would receive a "500 Internal Server Error" response, but the failover outbound INVITE from the Avaya SBCE to the 2nd Orange SIP server would succeed. In some instances, both Orange SIP Servers would respond with the 500 error message, and the outbound call would fail. When this happened, usually after a time span of 30 seconds or more, the re-dialed outbound call would succeed. This problem could be specific to the Orange lab environment set up for the compliance test. Orange SIP Trunking support has been investigating.
- **Call Termination:** When an outbound call was directed to the Orange POP-C SIP Server (by using dial prefix "0066") and the connected call was terminated at the enterprise end, the call appearance would stay on the PSTN phone even though Orange responded to the BYE message from the enterprise with "200 OK". The PSTN phone would receive fast busy tones for about 15-20 seconds before the call appearance would disappear. This problem did not exist with the Orange POP-B SIP Server (when outbound calls were dialed using "0096" prefix). Orange SIP Trunking support has been investigating.

- Packet Fragmentation:** The IPsec Tunnel configured on the Orange-provisioned on-premise Cisco Router for dedicated connection to the Orange lab environment does not support packet fragmentation. During compliance testing, signaling rules were configured on the Avaya SBCE to remove certain headers in SIP messages from Avaya to Orange to help reduce the overall message size for preventing packet fragmentation (see **Sections 7.10.1** and **7.10.2**). The headers concerned were not used by Orange and therefore could be safely removed.
- Calling Number Format:** The inbound call INVITE from Orange contained a "+" followed by 11 digits in the From header for the calling number. The **EC500 Mobility** features on Communication Manager did not work properly with this number format since the EC500 mobile number configured on Communication Manager (in **off-pbx-telephone station-mapping** form) is not allowed to contain non-digits like "+" to match the number in the inbound INVITE From header. To resolve this incompatibility, a signaling manipulation script was configured on the Avaya SBCE (see **Section 7.6**) to normalize the calling number in the From header to 9 digits without the "+" and the 2-digit country code. This manipulation was similarly applied to the Contact and PAI headers for normalization of calling number format. If the "+" sign was not removed, and the call was from the EC500 mobile phone (associated with an enterprise host station on the Communication Manager **off-pbx-telephone station-mapping** form in **Section 5.10**) to another enterprise station, the receiving station's display would not display the caller as the EC500 host station, and the EC500 host station would not be able to bridge onto the call. Note that such manipulation might also be done using Adaptations configured on Session Manager, but this option was not used and verified in the compliance test.
- Remote-Address Header:** During testing it was found that the Avaya SBCE was including a Remote-Address header in INVITE request and "200 OK" response messages leaving the Avaya SBCE towards the Orange network. The Avaya SBCE was configured to remove this header (see **Section 7.10.2**) to reduce overall packet size (see item above for packet fragmentation). Though this header was properly removed in the outbound INVITE, similar signaling rule configuration on the Avaya SBCE failed to remove this header in the response messages to Orange. The Avaya SBCE support/development team is investigating. No issues were caused by the inclusion of this header in the "200 OK" response messages.
- Codec Preference:** When Communication Manager was configured to use the G.729A and G.711A codecs in that particular preference order, Orange would answer an outbound call sometimes using G.729A, and sometimes using G.711A, depending on specific gateways the call was routed through. When G.711A was configured as the preferred codec on Communication Manager, Orange answered outbound calls always using G.711A. This codec behavior had no user impact, and was simply listed here as an observation.

- **PSTN Numbering Plan:** Certain special types of calls in the PSTN numbering plan, like Operator, Operator-Assisted, outbound toll-free, directory assistance, or local emergency calls, were not tested since the Orange lab environment was not set up for routing these special PSTN numbers.
- **Remote Worker:** Remote Worker (phones connected directly to the public Internet function as enterprise local extensions) is not supported by the combined Avaya/Orange solution as documented in these Application Notes since its setup requires Avaya SBCE be directly connected to the public Internet via its public interface, whereas in the tested solution Avaya SBCE was connected to the on-premise Cisco Router via a network internal to the enterprise. Conceptually, Remote Worker can be implemented using a second and dedicated Avaya SBCE connected directly to the public Internet, but this setup was beyond the scope of this compliance test.

Items not supported by the Orange SIP Trunking Service included the following:

- **REFER** – The Orange SIP Trunking Service does not support use of the SIP REFER message for call redirection (transfer). During compliance testing, the SIP INVITE message was used for testing call transfers.
- **Session Timer** – Session timer based on RFC 4028 is not supported by Orange network. Instead, Orange issues periodic in-dialog OPTIONS messages towards the enterprise to refresh active call sessions (at about 15-20 minute intervals). During compliance testing, the enterprise sent session refresh UPDATE messages towards Orange with the configured session timer on Communication Manager.

In addition, the Orange Business Services SIP Trunking Service requires the following behavior in SIP messaging:

- The calling party number contained in the outbound SIP message From header must be in the form of a National Number (NSN) “0NSN” or “+CCNSN” or “00CCNSN” where CC is the Country Code. For simplicity, the compliance test used the “0NSN” format. See **Section 5.8** for the relevant configuration.

2.3. Support

For support on the Orange SIP Trunking Service, please contact Orange Business Services via the following:

- BTIP offer: <http://www.orange-business.com/fr/produits/business-talk-ip>
- Business Talk offer: <http://www.orange-business.com/en/products/business-talk>

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to the Orange SIP Trunking Service. This is the configuration used for the compliance test.

The components used to create the simulated enterprise site included:

- System Manager
- Session Manager
- Communication Manager
- Avaya G450 Media Gateway
- Avaya SBCE
- Avaya 1600-Series IP telephones (H.323)
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 1100/1200-Series IP telephones (SIP)
- Avaya A175 Desktop Video Device (SIP)
- One-X Communicator softphone (H.323 and SIP)
- Flare Experience for Windows softphone (SIP)

For the compliance test, Orange deployed a Cisco 1841 Router at the enterprise site serving as the demarcation point for the Orange SIP Trunking Service. This Cisco 1841 Router was configured by Orange to establish secured access to the Orange network through IPsec Tunnel (see Note below). The public side of the Avaya SBCE connects to the Cisco 1841 Router and the private side connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

Note: In production environment of the Orange SIP Trunking Service, the standard connection of the enterprise site to the Orange network is through the Orange Business VPN (Orange MPLS-based IPVPN) offer.

For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses in these Application Notes.

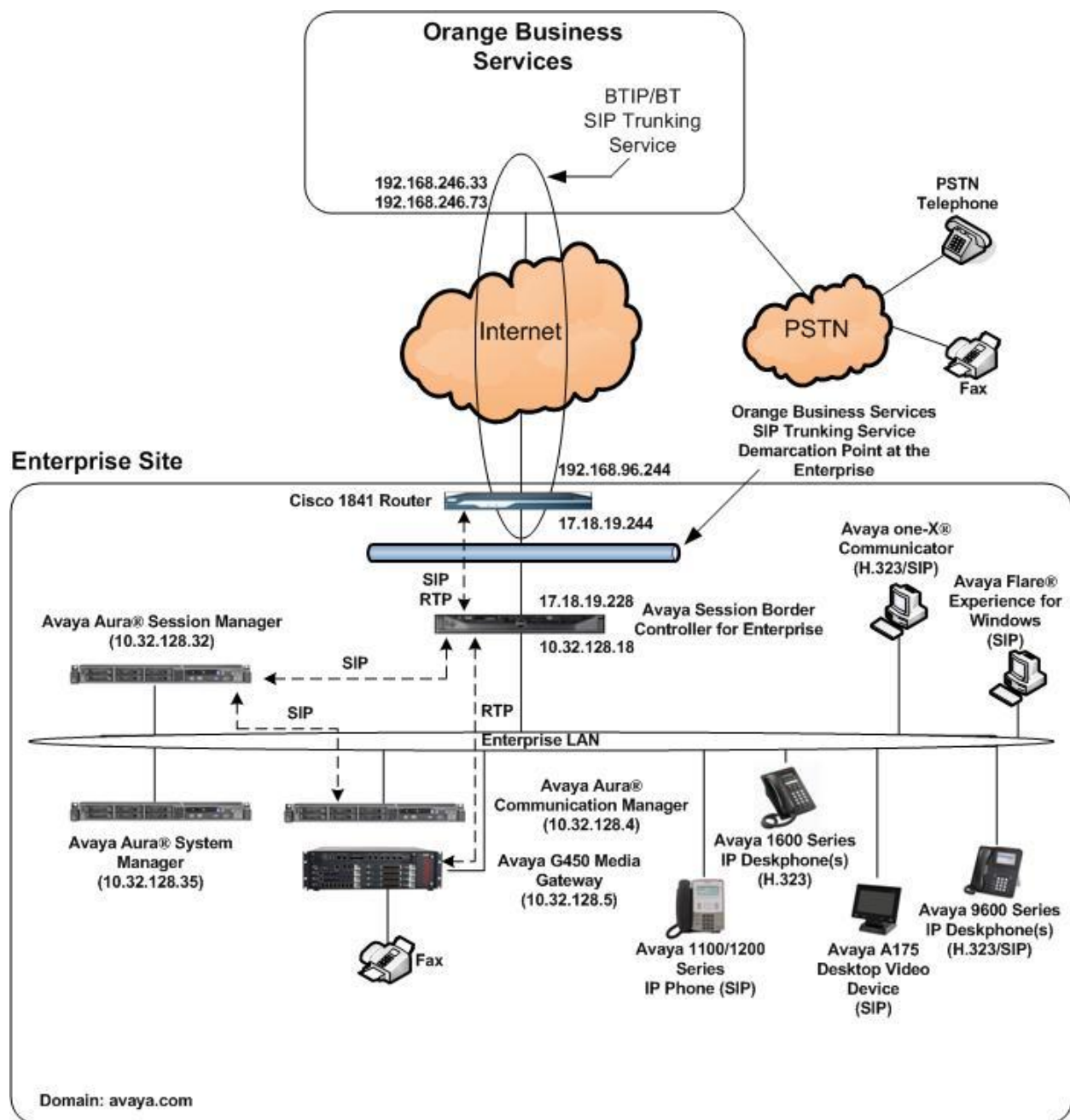


Figure 1: Avaya IP Telephony Network with the Orange SIP Trunking Service

A dedicated trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls from the PSTN, the calls flow from the service provider to the Avaya SBCE then to Session Manager. Session Manager uses 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 arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound feature treatment such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the Avaya SBCE. From the Avaya SBCE, the call is sent to the Orange SIP Trunking Service.

The Orange SIP Trunking Service used two SIP servers to handle inbound and outbound calls. For inbound calls, distinct sets of DID numbers were provisioned; outbound calls were routed to a specific SIP server based on dial prefixes (“0066” or “0096”).

Important: Note that both the Orange on-premise Cisco Router and the Avaya SBCE are connected to the same internal network at the Orange Business Services SIP Trunking Service Demarcation Point at the Enterprise (see **Figure 1**). The route configuration for that internal network must be administered to direct any traffic from the Avaya SBCE to the Orange network (192.168.246.33 and 192.168.246.73 in **Figure 1**) to the LAN interface of the Cisco Router (17.18.19.244 in **Figure 1**). This internal network route configuration is not included / described in these Application Notes.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® System Manager running on HP® DL360 Server	6.3.11 (Build No. 6.3.0.8.5682-6.3.8.4751) (Software Update Revision 6.3.11.8.2933) System Platform 6.3.5.01003.0
Avaya Aura® Session Manager running on HP® DL360 Server	6.3.11.0.631103
Avaya Aura® Communication Manager running on Avaya S8300 Server	6.3.9.0-SP9 (R016x.03.0.124.0-21971) System Platform 6.3.5.01003.0
Avaya G450 Media Gateway	34.5.1 /1
Avaya Session Border Controller for Enterprise running on Dell R210 V2 server	6.3.1-22-4653
Avaya 1616 IP Deskphone (H.323) running Avaya one-X® Deskphone Value Edition	1.3 SP4
Avaya 9611G IP Deskphone (H.323) running Avaya one-X® Deskphone Edition	6.3.1
Avaya 9621G IP Deskphone (SIP) running Avaya one-X® Deskphone SIP Edition	6.3.1
Avaya 1140E IP Telephone (SIP)	4.04.14.00s
Avaya A175 Desktop Video Device with Avaya Flare® Experience	SIP Version 1.1.3 (SIP_A175_1_1_3_021913)
Avaya one-X® Communicator (H.323 or SIP)	6.2.4.07-FP4
Avaya Flare® Experience for Windows	1.1.4.23
Orange Business Services SIP Trunking Service Solution Components	
Equipment/Software	Release/Version
On-Premise Cisco 1841 Router	IOS c1841-adventerprisek9-mz.151-4.M5
OBS network side Cisco 1841 Router	IOS c1841-adventerprisek9-mz.124-8b
Acme Packet Net-Net SBC	SCX6.3.0 MR-5 Patch 4 (Build 644)
Session Router running on HP® DL360 G8 Server	Acme Packet Net-Net OS SE SCZ7.1.2 MR-3 GA (Build 359)
ATOS Application Server	Lot 5.2
POP B Call Server	5x Phase 3
POP B Audiocode M8K MGW	6.0.47
POP C Call Server	5x Phase 2
POP C Huawei MGW	R009C05 SPC125

Table 1: Equipment and Software Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Orange SIP Trunking Service. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from Orange. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager 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. Note that the public IP addresses shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements are not revealed.

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 the service provider. The example shows that **4000** SIP trunks are available and **80** 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 to add additional capacity.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
	Maximum Administered H.323 Trunks: 4000	36	
	Maximum Concurrently Registered IP Stations: 2400	2	
	Maximum Administered Remote Office Trunks: 4000	0	
	Maximum Concurrently Registered Remote Office Stations: 2400	0	
	Maximum Concurrently Registered IP eCons: 68	0	
	Max Concur Registered Unauthenticated H.323 Stations: 100	0	
	Maximum Video Capable Stations: 2400	1	
	Maximum Video Capable IP Softphones: 2400	4	
	Maximum Administered SIP Trunks: 4000	80	
	Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0	
	Maximum Number of DS1 Boards with Echo Cancellation: 80	0	
	Maximum TN2501 VAL Boards: 10	0	
	Maximum Media Gateway VAL Sources: 50	0	
	Maximum TN2602 Boards with 80 VoIP Channels: 128	0	
	Maximum TN2602 Boards with 320 VoIP Channels: 128	0	
	Maximum Number of Expanded Meet-me Conference Ports: 300	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 be transferred back to the PSTN then leave the field set to **none**.

```
change system-parameters features                               Page 1 of 20
      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
```

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 **anonymous** for both.

```
change system-parameters features                               Page 9 of 20
      FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

      SCCAN PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager (**procr**) and for Session Manager (**sessionMgr**). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
cmm	10.32.128.4	
default	0.0.0.0	
procr	10.32.128.4	
procr6	::	
sessionMgr	10.32.128.32	

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. The list should include the codecs and preferred order defined by the service provider. For the compliance test, **G.711A** and **G.729A** were configured using ip-codec-set 5. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

change ip-codec-set 5		Page 1 of 2
IP Codec Set		
Codec Set: 5		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.711A	n	2
2: G.729A	n	2
3:		

On **Page 2**, set the **Fax Mode** to **t.38-standard** for T.38 fax calls.

change ip-codec-set 5		Page 2 of 2
IP CODEC SET		
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
Modem	t.38-standard	0
TDD/TTY	off	0
H.323 Clear-channel	US	3
SIP 64K Data	n	0
		ECM: y
		Packet Size (ms)
		20

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. 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 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 with the following parameters:

- Set **Authoritative Domain** to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set **Codec Set** to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 5                                     Page 1 of 20

                                IP NETWORK REGION

Region: 5
Location:                Authoritative Domain: avaya.com
                        Name: A SP Region                Stub Network Region: n
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
                        Codec Set: 5                    Inter-region IP-IP Direct Audio: yes
                        UDP Port Min: 2048                IP Audio Hairpinning? n
                        UDP Port Max: 3329
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 5 and region 1. 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 example below shows the settings used for the compliance test. It indicates that codec set 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 5 will automatically create a complementary table entry on the IP network region 1 form for destination region 5. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** (not shown).

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

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 5 was used for this purpose and was configured using the parameters highlighted below.

- Set **Group Type** to **sip**.
- Set **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between Communication Manager and Session Manager. If TLS is used here, it must also be used on the Session Manager entity link defined in **Section 6.6**.
- Set **IMS Enabled** to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set **Peer Detection Enabled** 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 as a Session Manager.
- Set **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 **Far-end Node Name** to **sessionMgr**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set **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 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been

established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to and from the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5068**.

- Set **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set **Far-end Domain** to the domain of the enterprise.
- Set **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 SIP trunk and the enterprise endpoint.
- Set **Alternate Route Timer** to **15**. This defines the number of seconds that Communication Manager will wait for a response (other than “100 Trying”) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

add signaling-group 5		Page 1 of 2	
SIGNALING GROUP			
Group Number: 5	Group Type: sip		
IMS Enabled? n	Transport Method: tcp		
Q-SIP? n			
IP Video? n	Enforce SIPS URI for SRTP? y		
Peer Detection Enabled? y	Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y			
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n			
Alert Incoming SIP Crisis Calls? n			
Near-end Node Name: procr	Far-end Node Name: sessionMgr		
Near-end Listen Port: 5068	Far-end Listen Port: 5068		
	Far-end Network Region: 5		
Far-end Domain: avaya.com			
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n		
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n		
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y		
Enable Layer 3 Test? n	IP Audio Hairpinning? n		
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n		
	Alternate Route Timer(sec): 15		

Note: For the compliance test, **IP-IP Direct Media** and **H.323 Station Outgoing Direct Media** were left at the default setting (disabled). These 2 parameters can be turned on to reduce media shuffling reINVITE messages from Communication Manager after the call has been established, as long as the customer has validated all supported call scenarios including off-net call redirections.

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 5 was configured using the parameters highlighted below.

- Set **Group Type** to **sip**.
- Enter a descriptive name for **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set **Service Type** to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set **Signaling Group** to the signaling group defined in **Section 5.6**.
- Set **Number of Members** 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.

add trunk-group 5		Page 1 of 21	
TRUNK GROUP			
Group Number: 5	Group Type: sip	CDR Reports: y	
Group Name: A-SP-Trunk	COR: 1	TN: 1	TAC: 1005
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 5		
	Number of Members: 10		

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than “100 Trying”) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** setting on the signaling group form described in **Section 5.6**.

Verify that **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITE messages must be sent to keep the active session alive. For the compliance test, the value of **300** seconds was used.

add trunk-group 5	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 15000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 300	
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 **Numbering Format** to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. To remove the + sign, the **Numbering Format** was set to **private** and the **Numbering Format** in the route pattern was set to **unk-unk** (see **Section 5.9**).

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

add trunk-group 5		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
	UI Treatment: service-provider	
	Replace Restricted Numbers? y	
	Replace Unavailable Numbers? y	
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		
DSN Term? n	SIP ANAT Supported? N	

On **Page 4**, set **Mark Users as Phone** to **y** so that the URI host part will contain the parameter “user=phone” in the outbound INVITE Request-URI. Since the Orange SIP Trunking Service does not support the SIP REFER message the **Network Call Redirection** field must be set to **n**. Set **Send Diversion Header** to **y** and **Support Request History** to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set **Telephone Event Payload Type** to **101**, the value used by the Orange SIP Trunking Service.

Set **Always Use re-INVITE for Display Updates** to **n**. This setting directs Communication Manager to use UPDATE (if supported by the remote end) instead of re-INVITE for phone display update in off-net call re-directions (forward and transfer).

add trunk-group 5	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Shuffling with SDP? n	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	

To ensure interoperability with Avaya SIP endpoints, the **Mark Users as Phone** field must also be set to **y** on the SIP trunk used by the SIP endpoints to register and communicate with the Session Manager. In most cases, this will be the trunk created during the initial installation of the Session Manager. In the case of the compliance test, this was trunk-group 1.

```
change trunk-group 1                                     Page 4 of 21
                                                         PROTOCOL VARIATIONS

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

            Send Diversion Header? n
            Support Request History? y
            Telephone Event Payload Type:
                Shuffling with SDP? n

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

Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
```

5.8. Calling Party Information

The calling party number is sent in the SIP From, Contact and PAI headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. These numbers (plus a prefix “0”) were assigned to the five extensions 40000, 41012, 41016, 41018 and 41024. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions. See the bullet item on the calling party number in **Section 2.2** for more details.

change private-numbering 5					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5 4				5	Total Administered: 41
5	40000	5	0296086900	10	Maximum Entries: 540
5	41012	5	0296086902	10	
5	41016	5	0296086906	10	
5	41018	5	0296086908	10	
5	41024	3	0296086904	10	

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 8 will send the calling party number as the **Private Prefix** plus the extension number.

change private-numbering 5					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5 8				5	Total Administered: 36
5	8	5	02960	10	Maximum Entries: 540

5.9. 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: 4			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	dac							
3	5	ext							
4	5	ext							
8	1	fac							
9	1	fac							
*	3	fac							
#	3	fac							

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

change feature-access-codes			FEATURE ACCESS CODE (FAC)						Page 1 of 11
Abbreviated Dialing List1 Access Code:									
Abbreviated Dialing List2 Access Code:									
Abbreviated Dialing List3 Access Code:									
Abbreviated Dial - Prgm Group List Access Code:									
Announcement Access Code:									
Answer Back Access Code:									
Attendant Access Code:									
Auto Alternate Routing (AAR) Access Code: 8									
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:						
Automatic Callback Activation:			Deactivation:						
Call Forwarding Activation Busy/DA: *01 All: *02			Deactivation: *03						
Call Forwarding Enhanced Status: Act:			Deactivation:						

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows dialed strings tested in the compliance test. All dialed strings are mapped to route pattern **55** which contains the SIP trunk to the service provider (as defined next). The prefix “0066” or “0096” plus a national number of 9 digits were dialed to call destinations on the French PSTN. The additional Country Code “001” was used for calls to reach 10-digit destination numbers in the US.

change ars analysis 00							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
0066	13	13	55	intl		n	
0066001	17	17	55	intl		n	
0096	13	13	55	intl		n	
0096001	17	17	55	intl		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 route pattern in the following manner. The example below shows the values used for route pattern 55 configured for the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **5** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** Set this field 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 55														Page 1 of 3	
Pattern Number: 4														Pattern Name: A-SP Route	
SCCAN? n														Secure SIP? n	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC							
No			Mrk	Lmt	List	Del	Digits	QSIG							
							Dgts	Intw							
1:	5	0	1					n	user						
2:								n	user						
3:								n	user						
4:								n	user						
		BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature		PARM	No.	Numbering	LAR	
		0	1	2	M	4	W	Request				Dgts	Format		
														Subaddress	
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		

5.10. EC500 Station Mapping

Use the **change off-pbx-telephone station-mapping x** command to configure an EC500 mobile or PSTN destination number for the EC500 host station **x**. The screen below demonstrates this configuration for the EC500 host station **41016**. When a call reaches station **41016**, Communication Manager will make an outbound call to **140948052** with prefix **0066** via Automatic Route Selection (**ars**).

- **Station Extension:** Enter the extension for the EC500 host station.
- **Application:** Enter **EC500**.
- **Dial Prefix:** Enter the dial prefix when Communication Manager is calling out to the EC500 destination number when receiving a call at the EC500 host station.
- **Phone Number:** Enter the EC500 mobile or PSTN destination number. See the bullet item **Calling Number Format** in **Section 2.2** for more details about setting this field.
- **Trunk Selection:** Enter **ars**.

change off-pbx-telephone station-mapping 41016							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
41016	EC500	0066	-	140948052	ars	1	

6. Configure Avaya Aura® Session Manager

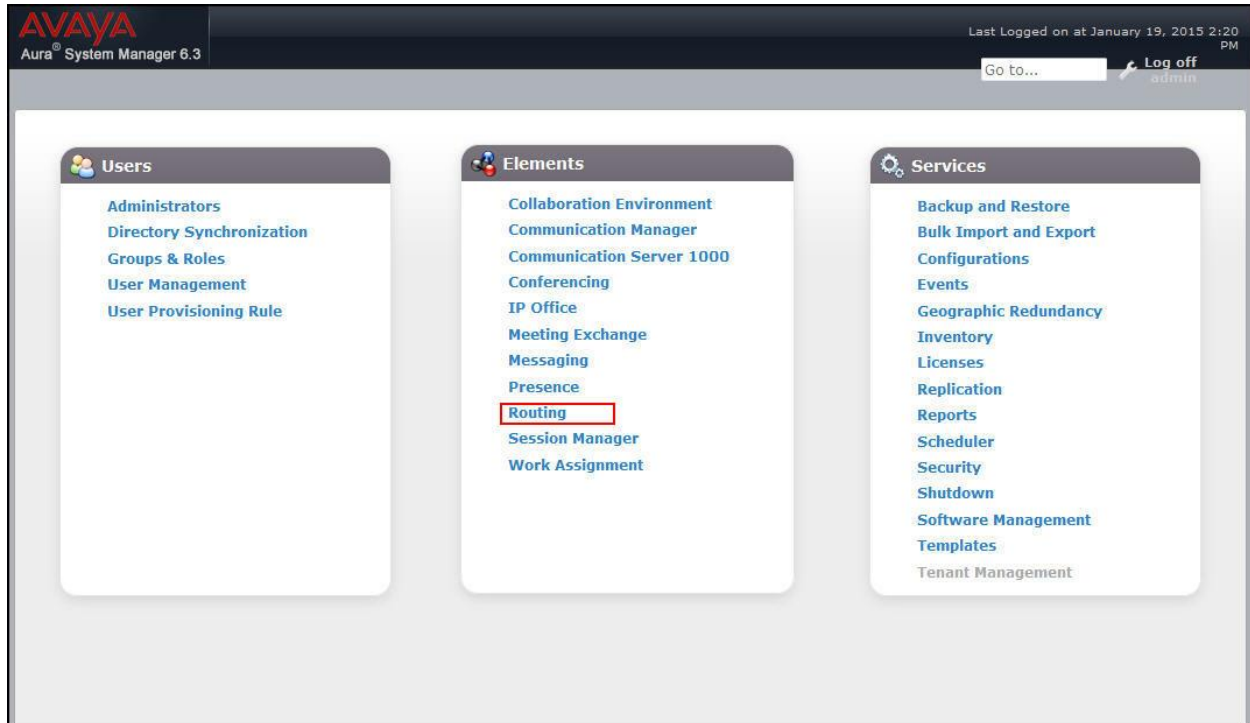
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the Avaya SBCE and Session Manager.
- 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 define dialed digit strings and govern which Routing Policy is used to service a call.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

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

6.1. Avaya Aura® 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. The **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements** → **Routing** link highlighted below.



Clicking the **Elements** → **Routing** link displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

AVAYA
Aura® System Manager 6.3

Last Logged on at January 19, 2015 2:20 PM
Go to... Log off

Home Routing x

Home / Elements / Routing

Routing

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 7: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 - (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 8: Create "Dial Patterns"
 - Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"
- Step 9: Create "Regular Expressions"
 - Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

- Step 7: "Routing Policies" are defined
- Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avaya.com**).

Navigate to **Routing → Domains** in the left-hand navigation pane (see **Section 6.1**) 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 screenshot shows the 'Domain Management' form in the Session Manager interface. The breadcrumb trail is 'Home / Elements / Routing / Domains'. The form has a 'Commit' button and a 'Cancel' button. Below the buttons is a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The 'Name' column contains '* avaya.com', the 'Type' column contains 'sip', and the 'Notes' column contains 'Enterprise Domain'. There is a 'Filter: Enable' link on the right side of the table. At the bottom of the form, there are 'Commit' and 'Cancel' buttons.

Name	Type	Notes
* avaya.com	sip	Enterprise Domain

The screen below shows the configured entry for the enterprise domain.

The screenshot shows the 'Domain Management' list view in the Session Manager interface. The breadcrumb trail is 'Home / Elements / Routing / Domains'. The list view has a 'Help ?' link. Below the link are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below the buttons is a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The 'Name' column contains 'avaya.com', the 'Type' column contains 'sip', and the 'Notes' column contains 'Enterprise Domain'. There is a 'Filter: Enable' link on the right side of the table. At the bottom of the table, there is a 'Select : All, None' link.

Name	Type	Notes
avaya.com	sip	Enterprise Domain

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named **VNJ Lab**, which includes all equipment on the enterprise including Communication Manager, Session Manager and the Avaya SBCE.

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane (see **Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

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

Home / Elements / Routing / Locations

Location Details

Commit Cancel Help ?

General

* Name: VNJ Lab

Notes: Enterprise Site for SP Testing

Scroll down to the **Location Pattern** section. Click **Add** and enter the following values. Use default values for all remaining fields.

- **IP Address Pattern:** Add all IP address patterns used to identify the location.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.

Location Pattern

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
10.32.128.	CPE

Select : All, None

Commit Cancel

6.4. Add Adaptation Module

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic module, and can modify other headers to permit interoperability with third party SIP products.

For the compliance test, one adaptation was created for Communication Manager. The adaptation mapped inbound DID numbers from Orange to local Communication Manager extensions.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane (see **Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter or select **DigitConversionAdapter**.
- **Notes:** Enter a description (optional).

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel Help ?

General

* Adaptation Name: PRT-CM-Trk5-Adapt

Module Name: DigitConversionAdapter

Module Parameter Type:

Egress URI Parameters:

Notes: Map SP DID's to CM extensions

To map inbound DID numbers from Orange Business Services to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **destination** since this digit conversion only applies to the destination number.

Click **Commit** to save.

The screenshot shows the 'Digit Conversion for Outgoing Calls from SM' window with 5 items listed. The table below represents the data shown in the window:

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+33296086900	*12	*12		*12	40000	destination		
<input type="checkbox"/>	*+33296086902	*12	*12		*12	41012	destination		
<input type="checkbox"/>	*+33296086904	*12	*12		*12	41024	destination		
<input type="checkbox"/>	*+33296086906	*12	*12		*12	41016	destination		
<input type="checkbox"/>	*+33296086908	*12	*12		*12	41018	destination		

At the bottom of the window, there are 'Commit' and 'Cancel' buttons.

In a real customer environment, often the DID number is comprised of the local extension plus a prefix. If this is true, then a single digit conversion entry can be created for all extensions. In the example below, a 5 digit prefix is deleted from each incoming DID number (sample DID pattern shown in the screen) leaving a 5 digit extension to be routed by Session Manager.

The screenshot shows the 'Digit Conversion for Outgoing Calls from SM' window with 1 item listed. The table below represents the data shown in the window:

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*70366	*10	*10		*5		destination		

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (see **Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in the location **VNJ Lab**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows the 'SIP Entity Details' form in the Avaya Aura Management Console. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The form is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields:

- Name:** Pkway-SM
- FQDN or IP Address:** 10.32.128.32
- Type:** Session Manager (dropdown menu)
- Notes:** Parkway
- Location:** VNJ Lab (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/New_York (dropdown menu)
- Credential name:** (empty text field)

Below the 'General' tab is the 'SIP Link Monitoring' section, which contains a dropdown menu set to 'Use Session Manager Configuration'.

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

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

For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5068 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.

Port

TCP Failover port:

TLS Failover port:

4 Items Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input type="text"/>
<input type="checkbox"/>	5060	UDP	avaya.com	<input type="text"/>
<input type="checkbox"/>	5061	TLS	avaya.com	<input type="text"/>
<input type="checkbox"/>	5068	TCP	avaya.com	<input type="text"/>

Select : All, None

The following screen shows the addition of the Communication Manager SIP entity. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager other than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for digit manipulation in **Section 6.4**. The **Location** field is set to **VNJ Lab** which is the location defined for the subnet where Communication Manager resides.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The main title is 'SIP Entity Details', with 'Commit' and 'Cancel' buttons to its right. A 'Help ?' link is in the top right corner. The 'General' section contains the following fields: 'Name' (PRT-CM-Trk5), 'FQDN or IP Address' (10.32.128.4), 'Type' (CM), 'Notes' (Princeton CM Trunk 5), 'Adaptation' (PRT-CM-Trk5-Adapt), 'Location' (VNJ Lab), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), and 'Call Detail Recording' (none). The 'Loop Detection' section has 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section has 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

Home / Elements / Routing / SIP Entities

SIP Entity Details [Commit](#) [Cancel](#) [Help ?](#)

General

* Name: PRT-CM-Trk5

* FQDN or IP Address: 10.32.128.4

Type: CM

Notes: Princeton CM Trunk 5

Adaptation: PRT-CM-Trk5-Adapt

Location: VNJ Lab

Time Zone: America/New_York

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE SIP entity. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). The **Location** field is set to **VNJ Lab** which is the location defined for the subnet where the Avaya SBCE resides.

The screenshot shows a web interface for configuring SIP entities. The breadcrumb navigation at the top reads "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". In the top right corner, there are "Commit" and "Cancel" buttons, and a "Help ?" link. The "General" tab is selected. The form contains the following fields:

- Name:** VNJ-SBCE1
- * FQDN or IP Address:** 10.32.128.18
- Type:** SIP Trunk (dropdown menu)
- Notes:** A-SBCE for Avaya Aura Platform
- Adaptation:** (empty dropdown menu)
- Location:** VNJ Lab (dropdown menu)
- Time Zone:** America/New_York (dropdown menu)
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** egress (dropdown menu)

Below the "General" section, there are two more sections:

- Loop Detection:** Loop Detection Mode: Off (dropdown menu)
- SIP Link Monitoring:** SIP Link Monitoring: Use Session Manager Configuration (dropdown menu)

6.6. Add 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 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-hand navigation pane (see **Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in **Section 5.6**.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager entity link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager entity link, select the Communication Manager SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted** from pull-down menu.

Click **Commit** to save.

The following screen illustrates 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**. For the compliance test, the TCP protocol was used (for ease in troubleshooting traces) but the recommended configuration is to use TLS.

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* PRT-Trk5-Link	* Pkway-SM	TCP	* 5068	* PRT-CM-Trk5	<input type="checkbox"/>	* 5068	trusted	<input type="checkbox"/>	

Select : All, None

The following screen illustrates the Entity Link to the Avaya SBCE.

Home / Elements / Routing / Entity Links Help ?

Entity Links Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* VNJ-SBCE1-Link	* Pkway-SM	TCP	* 5060	* VNJ-SBCE1	<input type="checkbox"/>	* 5060	trusted	<input type="checkbox"/>	

Select : All, None

6.7. Add 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 must be added: one for Communication Manager and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (see **Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies (i.e., the route destination) 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 screen shows the routing policy for Communication Manager.

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit Cancel [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
PRT-CM-Trk5	10.32.128.4	CM	Princeton CM Trunk 5

The following screen shows the routing policy for the Avaya SBCE.

Home / Elements / Routing / Routing Policies

Help ?

Routing Policy Details

CommitCancel

General

* Name:

VNJ-SBCE1-RP

Disabled:

☐

* Retries:

0

Notes:

Outbound to A-SBCE

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
VNJ-SBCE1	10.32.128.18	SIP Trunk	A-SBCE for Avaya Aura Platform

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Orange Business Services and vice versa. Dial patterns define which routing policy should 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-hand navigation pane (see **Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

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

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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example is for outbound calls and shows that numbers that begin with **0066** and have a destination domain of **avaya.com** from **ALL** locations use the routing policy **VNJ-SBCE1-RP**.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		VNJ-SBCE1-RP	0	<input type="checkbox"/>	VNJ-SBCE1	Outbound to A-SBCE

Select : All, None

A similar routing policy was defined during compliance testing for routing outbound calls dialed with the prefix “0096”.

The second example is for inbound calls and shows that 12- digit numbers that start with **+33296** to domain **avaya.com** and originating from **ALL** locations use route policy **PRT-CM-Trk5-RP**. These are the numbers contained in the INVITE messages to the enterprise from Orange Business Services.

Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

Commit Cancel

General

* Pattern: +33296

* Min: 12

* Max: 12

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes: Orange DID

Originating Locations and Routing Policies

Add Remove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		PRT-CM-Trk5-RP	0	<input type="checkbox"/>	PRT-CM-Trk5	Inbound to CM

Select : All, None

6.9. Add/View Avaya Aura® Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, from the **Home** page, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (see **Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, select the appropriate Session Manager and click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the host name or IP address of the Session Manager management interface.

The screen below shows the Session Manager values used for the compliance test.

The screenshot shows the 'View Session Manager' configuration page. The breadcrumb navigation at the top is 'Home / Elements / Session Manager / Session Manager Administration'. There is a 'Return' button and a 'Help ?' link. Below the title, there is a list of tabs: 'General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |'. Below the tabs, there is a 'General' section with a dropdown arrow. The configuration fields are as follows:

SIP Entity Name	Pkway-SM
Description	
Management Access Point Host Name/IP	10.32.128.31
Direct Routing to Endpoints	Enable
VMware Virtual Machine	<input type="checkbox"/>

In the **Security Module** section, enter/verify the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save**, (not shown), to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.

Security Module

SIP Entity IP Address 10.32.128.32

Network Mask 255.255.255.0

Default Gateway 10.32.128.254

Call Control PHB 46

QOS Priority 6

Speed & Duplex Auto

VLAN ID -

*SIP Firewall Configuration Pkwy-SM Rule Set

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 has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the Avaya SBCE private or public network interfaces (i.e., A1 and B1). If the management interface has not been configured on a separate subnet, then contact your Avaya representative for guidance in correcting the configuration.

On all screens described in this section, it is to be assumed that parameters are left at their default values unless specified otherwise.

7.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The Avaya SBCE login page will appear as shown below. Log in with the appropriate credentials.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there are three paragraphs of legal disclaimer text and a copyright notice at the bottom.

AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

After logging in, the Dashboard screen will appear as shown below. Verify that **License State** is **OK** as highlighted. The Avaya SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license if necessary.

All configuration screens of the Avaya SBCE are accessed by navigating the menu tree in the left pane.

The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left sidebar contains a menu tree with Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Dashboard' and contains several sections: Information, Installed Devices, Alarms (past 24 hours), Incidents (past 24 hours), and Notes. The Information section is expanded, showing System Time (08:15:11 AM GMT-06:00), Version (6.3.1-22-4653), Build Date (Fri Nov 21 17:35:09 EST 2014), License State (OK), Aggregate Licensing Overages (0), and Peak Licensing Overage Count (0). The License State is highlighted with a red box. The Installed Devices section shows EMS and sp-ucsec1. The Alarms and Incidents sections are empty. The Notes section shows 'No notes found.'

7.2. Verify Network Configuration and Enable Interfaces

To view the network information provided during installation, navigate to **System Management**. In the right pane, click **View** highlighted below.

The screenshot shows the Avaya Session Border Controller for Enterprise System Management page. The top navigation bar is the same as the dashboard. The left sidebar is the same as the dashboard. The main content area is titled 'System Management' and contains a tabbed interface with Devices, Updates, SSL VPN, and Licensing. The Devices tab is selected, showing a table with columns: Device Name, Management IP, Version, Status, Reboot, Shutdown, Restart Application, View, Edit, and Uninstall. The table contains one row for sp-ucsec1 with Management IP 10.32.101.10, Version 6.3.1-22-4653, and Status Commissioned. The View button is highlighted with a red box.

A System Information page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**sp-ucsec1**). This name will be referenced in other configuration screens. The two **Network Configuration** entries highlighted below are directly related to the SIP trunking solution described in these Application Notes. Interfaces **A1** and **B1** represent the private and public interfaces of the Avaya SBCE. Each of these interfaces must be enabled after installation.

System Information: sp-ucsec1
X

General Configuration

Appliance Name sp-ucsec1

Box Type SIP

Deployment Mode Proxy

Device Configuration

HA Mode No

Two Bypass Mode No

License Allocation

Standard Sessions 0
Requested: 0

Advanced Sessions 0
Requested: 0

Scopia Video Sessions 0
Requested: 0

Encryption ☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.32.128.18	10.32.128.18	255.255.255.0	10.32.128.254	A1
17.18.19.228	17.18.19.228	255.255.255.0	17.18.19.250	B1
192.168.1.254	192.168.1.254	255.255.255.0	192.168.1.254	E1
192.168.1.254	192.168.1.254	255.255.255.0	192.168.1.254	E1
192.168.1.254	192.168.1.254	255.255.255.0	192.168.1.254	E1

DNS Configuration

Primary DNS 10.32.128.200

Secondary DNS

DNS Location DMZ

DNS Client IP 10.32.128.18

Management IP(s)

IP 10.32.101.10

To enable the interfaces, first navigate to **Device Specific Settings** → **Network Management** in the left pane and select the device being managed in the center pane. In the right pane, in the **Interfaces** tab verify that **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click on **Disabled** and confirm in the pop-up confirmation window to toggle to **Enabled**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, the **Network Management** option is highlighted with a red box. The main content area is titled "Network Management: sp-ucsec1". It features two tabs: "Interfaces" (selected) and "Networks". Below the tabs is a table with the following data:

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

An "Add VLAN" button is located in the top right corner of the table area. The status of interfaces A1 and B1 is "Enabled", while A2 and B2 are "Disabled".

7.3. Signaling Interface

A signaling interface defines an IP address, protocols and listen ports that the Avaya SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings** → **Signaling Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, signaling interface **Int_Sig_Intf** was created for the Avaya SBCE internal interface and signaling interface **Ext_Sig_Intf** was created for the Avaya SBCE external interface. Both are highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set **Signaling IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set **Signaling IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- In the **UDP Port**, **TCP Port** and **TLS Port** fields, enter the port the Avaya SBCE will listen on for each transport protocol. For the internal interface, the Avaya SBCE was configured to listen for TCP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP or TCP on port 5060. Since Orange SIP Trunking Services uses UDP on port 5060, it would have been sufficient to simply configure the Avaya SBCE for UDP.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, **Signaling Interface** (highlighted), End Point Flows, Session Flows, DMZ Services, and TURN/STUN Service. The main content area is titled "Signaling Interface: sp-ucsec1". Below this title, there is a "Devices" tab with "sp-ucsec1" selected. A warning message states: "Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below the warning is a table of signaling interfaces. The table has columns: Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. Two interfaces are listed: Int_Sig_Intf and Ext_Sig_Intf, both highlighted with a red border. The table also includes "Edit" and "Delete" links for each interface. Below the table, there are two more interfaces listed: Int_Ext_Sig and Ext_Ext_Sig, but they are not highlighted.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Int_Sig_Intf	10.32.128.18	5060	---	---	None	Edit	Delete
Ext_Sig_Intf	17.18.19.228	5060	5060	---	None	Edit	Delete
Int_Ext_Sig	17.18.19.228	5060	---	5061	AvayaSBCS1 (Server)	Edit	Delete
Ext_Ext_Sig	17.18.19.228	5060	---	5061	AvayaSBCS1 (Server)	Edit	Delete

7.4. Media Interface

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the Avaya SBCE.

To create a new interface, navigate to **Device Specific Settings** → **Media Interface** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new interface, followed by a series of pop-up windows in which the interface parameters can be configured. Once complete, the settings are shown in the far right pane.

For the compliance test, media interface **Int_Media_Intf** was created for the Avaya SBCE internal interface and media interface **Ext_Media_Intf** was created for the Avaya SBCE external interface. Both are highlighted below. When configuring the interfaces, configure the parameters as follows:

- Set **Name** to a descriptive name.
- For the internal interface, set **Media IP** to the IP address associated with the private interface (A1) defined in **Section 7.2**. For the external interface, set **Media IP** to the IP address associated with the public interface (B1) defined in **Section 7.2**.
- Set **Port Range** to a range of ports acceptable to both the Avaya SBCE and the far-end. For the compliance test, the default port range was used for both interfaces.

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
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 DMZ Services
 TURN/STUN Service

Media Interface: sp-ucsec1

Devices
sp-ucsec1

Media Interface

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

[Add](#)

Name	Media IP	Port Range	Edit	Delete
Int_Media_Intf	10.32.128.18	35000 - 40000	Edit	Delete
Ext_Media_Intf	17.18.19.228	35000 - 40000	Edit	Delete
SIP_Media_Interface_200	17.18.19.228	35000 - 40000	Edit	Delete
SIP_Media_Interface_10	10.32.128.18	35000 - 40000	Edit	Delete

7.5. Server Interworking

A server interworking profile defines a set of parameters that aid in interworking between the Avaya SBCE and a connected server. Create separate server interworking profiles for Session Manager and the service provider SIP server. These profiles will be applied to the appropriate server in **Section 7.7.1** and **7.7.2**.

To create a new profile, navigate to **Global Profiles → Server Interworking** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. Alternatively, a new profile may be created by selecting an existing profile in the center pane and clicking the **Clone** button in the right pane. This will create a copy of the selected profile which can then be edited as needed. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before the server interworking profiles were added for the compliance test.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation pane lists various system management options, with 'Server Interworking' highlighted under the 'Global Profiles' section. The main content area is titled 'Interworking Profiles: cs2100' and features an 'Add' button. Below this, a list of existing profiles is shown, including 'cs2100', 'avaya-ru', 'OCS-Edge-Ser...', 'cisco-ccm', 'cups', and 'OCS-FrontEnd...'. To the right, a 'Clone' button is visible. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' The 'General' tab is selected, displaying a table of parameters for the 'cs2100' profile.

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No

7.5.1. Server Interworking – Session Manager

For the compliance test, server interworking profile **PkwySM** was created for Session Manager by cloning the existing profile **avaya-ru**. The **General** tab parameters are shown below. When creating the profile, the default values were used for all parameters except the setting of **Yes** for **T.38 Support**, since T.38 fax was tested during compliance testing.

General	Timers	URI Manipulation	Header Manipulation	Advanced
General				
Hold Support	NONE			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
URI Group	None			
Send Hold	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
Re-Invite Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
Privacy				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
DTMF				
DTMF Support	None			

The **Timers**, **URI Manipulation** and **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **Yes**.

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				No
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				Yes
OCS Extensions				No
AVAYA Extensions				Yes
NORTEL Extensions				No
Diversion Manipulation				No
Metaswitch Extensions				No
Reset on Talk Spurt				No
Reset SRTP Context on Session Refresh				No
Has Remote SBC				Yes
Route Response on Via Port				No
Cisco Extensions				No
Lync Extensions				No

[Edit](#)

7.5.2. Server Interworking – Orange Business Services

For the compliance test, server interworking profile **SP-General-T38** was created for the Orange Business Services SIP server. When creating the profile, the default values were used for all parameters except the setting of **Yes** for **T.38 Support** since T.38 was tested during compliance testing. The **General** tab parameters are shown below.

General	Timers	URI Manipulation	Header Manipulation	Advanced
General				
Hold Support	NONE			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
URI Group	None			
Send Hold	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
Re-Invite Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
Privacy				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
DTMF				
DTMF Support	None			

The **Timers**, **URI Manipulation**, **Header Manipulation** tabs have no entries.

The **Advanced** tab parameters are shown below. Note that **AVAYA Extensions** is set to **No**.

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				Yes
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				No
OCS Extensions				No
AVAYA Extensions				No
NORTEL Extensions				No
Diversion Manipulation				No
Metaswitch Extensions				No
Reset on Talk Spurt				No
Reset SRTP Context on Session Refresh				No
Has Remote SBC				Yes
Route Response on Via Port				No
Cisco Extensions				No
Lync Extensions				No

7.6. Signaling Manipulation

Signaling manipulation scripts provides for the manipulation of SIP messages which cannot be achieved by other configuration within the Avaya SBCE.

The compliance test used a signaling manipulation script to remove the prefix “+33” from the URI in the **From**, **To**, and **PAI** (P-Asserted-Identity) headers in request messages to Session Manager and response messages from Session Manager.

To create a signaling manipulation script, navigate to **Global Profiles → Signaling Manipulation** (see 2nd screen below). Click on **Add** in the center pane. In the pop-up **Signaling Manipulation Editor** window, type in a script title and enter the script statements/commands.

Save the script by clicking on **Save**. For the compliance test, a script named **RemoveOrangePrefix** was created as shown below.

Signaling Manipulation Editor

AVAYA

Title Save

```
1 // Remove plus sign and country code in Response
2
3 within session "ALL"
4 {
5   act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6   {
7     %HEADERS["From"][1].regex_replace("\\+33", "");
8     %HEADERS["To"][1].regex_replace("\\+33", "");
9     %HEADERS["P-Asserted-Identity"][1].regex_replace("\\+33", "");
10  }
11 }
12
13 // Remove plus sign and country code in Request
14
15 within session "ALL"
16 {
17   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
18   {
19     %HEADERS["From"][1].regex_replace("\\+33", "");
20     %HEADERS["To"][1].regex_replace("\\+33", "");
21     %HEADERS["P-Asserted-Identity"][1].regex_replace("\\+33", "");
22  }
23 }
```

The screen below shows the saved script listed on the Avaya SBCE.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

- Domain DoS
- Fingerprint
- Server Interworking
- Phone Interworking
- Media Forking
- Routing
- Server Configuration
- Topology Hiding
- Signaling Manipulation**
- URI Groups

PPM Services

Domain Policies

TLS Management

Device Specific Settings

Signaling Manipulation Scripts: RemoveOrangePrefix

Upload Add Download Clone Delete

Click here to add a description.

Signaling Manipulation

```
// Remove plus sign and country code in Response

within session "ALL"
{
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %HEADERS["From"][1].regex_replace("\\+33", "");
    %HEADERS["To"][1].regex_replace("\\+33", "");
    %HEADERS["P-Asserted-Identity"][1].regex_replace("\\+33", "");
  }
}

// Remove plus sign and country code in Request

within session "ALL"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["From"][1].regex_replace("\\+33", "");
    %HEADERS["To"][1].regex_replace("\\+33", "");
    %HEADERS["P-Asserted-Identity"][1].regex_replace("\\+33", "");
  }
}
```

Edit

RemoveOrangePrefix

AMC; Reviewed:
SPOC 2/17/2015

Solution & Interoperability Test Lab Application Notes
©2015 Avaya Inc. All Rights Reserved.

58 of 87
OBSAura63SBCE63

The **RemoveOrangePrefix** script is tied to the **Pkwy-SM** server in Server Configuration (Section 7.7.1).

Note that use of Signaling Manipulation scripts demands higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should be used with care and only in cases where the use of Signaling Rules (Section 7.10) does not meet the desired result. Refer to [18] for information on the Avaya SBCE scripting language.

7.7. Server Configuration

A server configuration profile defines the attributes of the physical server. Create separate server configuration profiles for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Server Configuration** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before the servers profiles were added for the compliance test.



7.7.1. Server Configuration – Session Manager

For the compliance test, server configuration profile **Pkwy-SM** was created for Session Manager. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Call Server**.
- Set **IP Addresses / FQDNs** to the IP address of the Session Manager signaling interface.
- Select the appropriate **Transport** protocol used for SIP signaling between Session Manager and the Avaya SBCE. In the compliance test, **TCP** was tested.
- Set **Port** to the standard SIP port of **5060**. This is the port Session Manager will listen on for SIP messages from the Avaya SBCE.

Dialog box titled "Edit Server Configuration Profile - General".

Server Type: Call Server

Add

IP Address / FQDN	Port	Transport
10.32.128.32	5060	TCP

Delete

Finish

On the **Advanced** tab, check **Enable Grooming**, select the **Interworking Profile** for Session Manager defined in **Section 7.5.1**, and select the **Signaling Manipulation Script** created in **Section 7.6**.

Dialog box titled "Edit Server Configuration Profile - Advanced".

Enable DoS Protection: ☐

Enable Grooming: ☒

Interworking Profile: PkwySM

Signaling Manipulation Script: RemoveOrangePrefix

Connection Type: SUBID

Finish

7.7.2. Server Configuration – Orange Business Services

For the compliance test, server configuration profile **SP-Orange** was created for Orange Business Services. When creating the profile, configure the **General** tab parameters as follows:

- Set **Server Type** to **Trunk Server**.
- Set **IP Addresses / FQDNs** to the IP address of the Orange SIP server (2 Orange SIP servers were set up for the compliance test as shown in **Figure 1**).
- Select the appropriate **Transport** protocol used for SIP signaling between Orange and the Avaya SBCE. In the compliance test, **UDP** was tested.
- Set **Port** to the standard SIP port of **5060**. This is the port the Orange SIP server will listen on for SIP messages from the Avaya SBCE.

Edit Server Configuration Profile - General

Server Type: Trunk Server

Add

IP Address / FQDN	Port	Transport	
192.168.246.33	5060	UDP	Delete
192.168.246.73	5060	UDP	Delete

Finish

On the **Advanced** tab, select the **Interworking Profile** for Orange Business Services defined in **Section 7.5.2**.

Edit Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile: SP-General-T38

Signaling Manipulation Script: None

Connection Type: SUBID

Finish

7.8. Application Rules

An application rule defines the allowable SIP applications and associated parameters. An application rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-trunk** application rule (shown below) was used for both Session Manager and the Orange Business Services SIP server.

To view an existing rule, navigate to **Domain Policies** → **Application Rules** in the left pane. In the center pane, select the rule (e.g., **default-trunk**) to be viewed.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the hierarchy: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, and Application Rules (highlighted). The main content area is titled 'Application Rules: default-trunk' and includes 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.' The 'Application Rule' section contains a table with the following data:

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

Below the table is a 'Miscellaneous' section with the following settings:

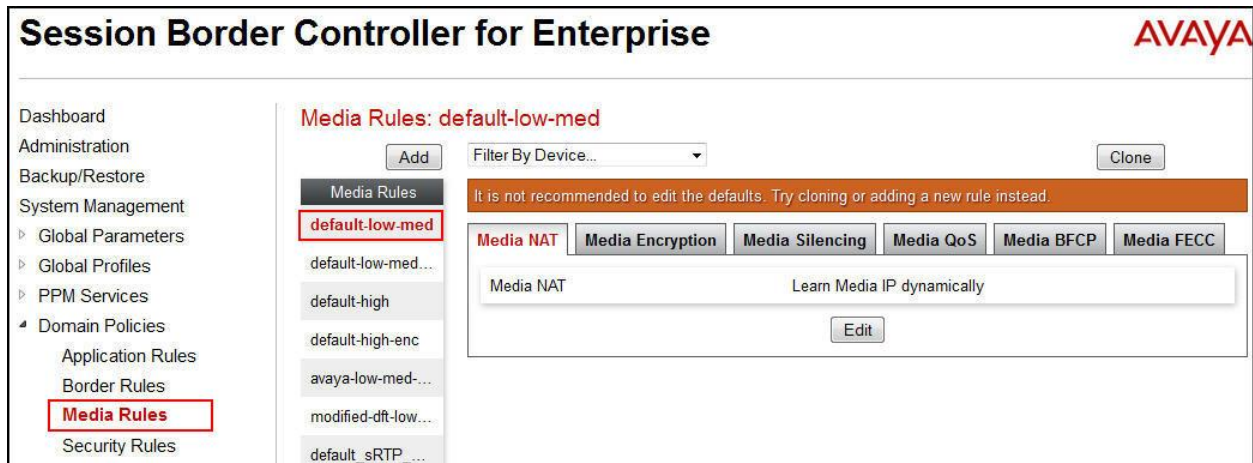
Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

An 'Edit' button is located at the bottom of the 'Miscellaneous' section.

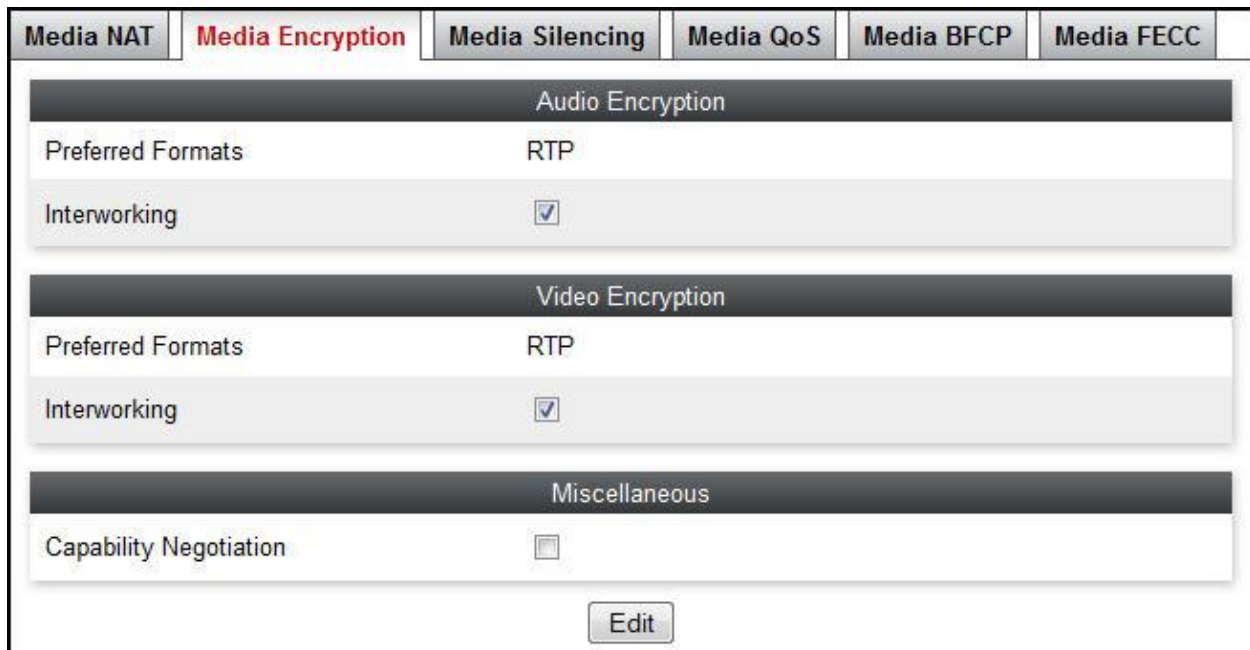
7.9. Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.11**. For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Session Manager and the Orange Business Services SIP server.

To view an existing rule, navigate to **Domain Policies → Media Rules** in the left pane. In the center pane, select the rule (e.g., **default-low-med**) to be viewed.



Each of the tabs of the **default-low-med** media rule is shown below (the **Media NAT** tab is shown above). The **Media Encryption** tab indicates that no encryption was used.



The **Media Silencing** tab shows Media Silencing was disabled.

Media NAT	Media Encryption	Media Silencing	Media QoS	Media BFCP	Media FECC
<div>Media Silencing <input type="checkbox"/></div> <div>Edit</div>					

The settings in the **Media QoS** tab are shown below.

Media NAT	Media Encryption	Media Silencing	Media QoS	Media BFCP	Media FECC
<div>Media QoS Reporting</div> <div>RTCP Enabled <input type="checkbox"/></div> <div>Media QoS Marking</div> <div>Enabled <input type="checkbox"/></div> <div>Edit</div>					

The **Media BFCP** tab is shown below.

Media NAT	Media Encryption	Media Silencing	Media QoS	Media BFCP	Media FECC
<div>Binary Floor Control Protocol</div> <div>BFCP Enabled <input type="checkbox"/></div> <div>Edit</div>					

The **Media FECC** tab is shown below.

Media NAT	Media Encryption	Media Silencing	Media QoS	Media BFCP	Media FECC
<div>Far End Camera Control</div> <div>FECC Enabled <input type="checkbox"/></div> <div>Edit</div>					

7.10. Signaling Rules

A signaling rule defines the processing to be applied to the selected signaling traffic. A signaling rule is one component of the larger endpoint policy group defined in **Section 7.11**. A specific signaling rule was created for Session Manager. The Orange Business Services SIP server used the **default** rule.

To create a new rule, navigate to **Domain Policies → Signaling Rules** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new rule, followed by a series of pop-up windows in which the rule parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing rule, select the rule from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Signaling Rules' highlighted. The main content area is titled 'Signaling Rules: default' and includes an 'Add' button, a 'Filter By Device...' dropdown, and a 'Clone' button. A warning banner 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', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing settings for 'Inbound' and 'Outbound' traffic. The 'Content-Type Policy' section is also visible, with a table for actions and an 'Exception List'.

Content-Type Policy			
Enable Content-Type Checks <input checked="" type="checkbox"/>			
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

7.10.1. Signaling Rules – Session Manager

For the compliance test, signaling rule **SessMgr_SigRules** was created for Session Manager to prevent certain proprietary headers in the SIP messages sent from the Session Manager from being propagated to Orange Business Services. These headers may contain internal addresses or other information about the internal network. Other message headers were removed to reduce overall message size for preventing packet fragmentation (see the item **Packet Fragmentation** in **Section 2.2** for more details).

Select the **SessMgr_SigRules** rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on request messages such as the initial INVITE message.

An entry is created by clicking the **Add In Header Control** or **Add Out Header Control** button depending on the direction (relative to the Avaya SBCE) of the message to be modified.

Header manipulation on request messages from Session Manager can be created by clicking the **Add In Header Control** button in the **Request Headers** tab as shown below. Entries were created to perform the following actions:

1. Removes the **AV-Correlation-ID** header from **INVITE** messages in the **IN** direction (on request messages in from Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from **ALL** messages in the **IN** direction.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID		
				Add In Header Control		Add Out Header Control		
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Similarly, header manipulation can be performed on SIP response messages from Session Manager. This can be created by clicking the **Add In Header Control** button in the **Response Headers** tab as shown below. Entries were created in the same manner as was done on the **Request Headers** tab. The entries shown perform the following actions:

1. Removes the **Av-Global-Session-ID** header from the **200** response to **INVITE** messages in the **IN** direction (on response messages in from Session Manager to Avaya SBCE).
2. Removes the **Endpoint-View** header from any **2XX** response to **ALL** message in the **IN** direction.
3. Removes the **Endpoint-View** header from any **1XX** response to **INVITE** messages in the **IN** direction.
4. Removes the **P-AV-Message-Id** header from any **200** response to **INVITE** messages in the **IN** direction.
5. Removes the **P-Location** header from any **2XX** response to **ALL** messages in the **IN** direction.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID			
				<div>Add In Header Control</div>	<div>Add Out Header Control</div>				
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Av-Global-Session-ID	200	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	200	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.10.2. Signaling Rules – Orange Business Services

For the compliance test, signaling rule **Orange_SigRules** was created to remove certain headers in the SIP request messages sent from the Avaya SBCE to Orange Business Services. These headers were removed to reduce overall message size for preventing packet fragmentation (see the item **Packet Fragmentation** in **Section 2.2** for more details). Follow the same procedures outlined in **Section 7.10.1** to configure for removing these headers in **Orange_SigRules**.

The screen below shows the configuration entries for removing headers in request messages sent by the Avaya SBCE out to the Orange Business Services. Note that all the entries were configured for the **OUT** direction (through **Add Out Header Control**).

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID		
				Add In Header Control		Add Out Header Control		
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	INVITE	Forbidden	Remove Header	No	OUT	Edit	Delete
2	Av-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	OUT	Edit	Delete
3	History-Info	ALL	Forbidden	Remove Header	No	OUT	Edit	Delete
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	OUT	Edit	Delete
5	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	OUT	Edit	Delete
6	P-Location	ALL	Forbidden	Remove Header	Yes	OUT	Edit	Delete
7	Remote-Address	ALL	Forbidden	Remove Header	Yes	OUT	Edit	Delete
8	Remote-Party-ID	INVITE	Forbidden	Remove Header	No	OUT	Edit	Delete
9	User-Agent	INVITE	Forbidden	Remove Header	No	OUT	Edit	Delete
10	x-nt-GUID	INVITE	Forbidden	Remove Header	Yes	OUT	Edit	Delete

The screen below shows the configuration for removing the **Remote-Address** header in the 2XX response messages sent by the Avaya SBCE out to the Orange Business Services. This configuration was found during testing to be ineffective (see the item **Remote-Address Header** in **Section 2.2** for details), but was included here for completeness.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID	
				<div>Add In Header Control</div>	<div>Add Out Header Control</div>		
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction
1	Remote-Address	2XX	ALL	Forbidden	Remove Header	Yes	OUT
<div>EditDelete</div>							

7.11. Endpoint Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the Avaya SBCE and a signaling endpoint (connected server). Thus, an endpoint policy group must be created for Session Manager and the service provider SIP server. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.14**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by a series of pop-up windows in which the group parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing group, select the group from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific endpoint policy groups were added for the compliance test.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies (highlighted), Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups (highlighted), and Groups. The main content area is titled "Policy Groups: default-low" and includes an "Add" button and a "Filter By Device..." dropdown. A warning message states: "It is not recommended to edit the defaults. Try adding a new group instead." Below this is a table with a single row and a tooltip that says "Hover over a row to see its description." The "Policy Group" tab is active, showing a table with the following data:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default	default	default-low-med	default-low	default	default	Edit Clone

7.11.1. Endpoint Policy Group – Session Manager

For the compliance test, endpoint policy group **SM** was created for Session Manager as shown below. For **Application**, enter the application rule specified in **Section 7.8**. For **Media**, enter the media rule specified in **Section 7.9**. For **Signaling**, enter the signaling rule created in **Section 7.10.1**.

Policy Groups: SM

Add Rename Clone Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	SessMgr_SigRules	Edit

Summary

7.11.2. Endpoint Policy Group – Orange Business Services

For the compliance test, endpoint policy group **Orange-Policy-Grp** was created for the Orange Business Services SIP server as shown below. For **Application**, enter the application rule specified in **Section 7.8**. For **Media**, enter the media rule specified in **Section 7.9**. For **Signaling**, enter the signaling rule created in **Section 7.10.2**.

Policy Groups: Orange-Policy-Grp

Add Rename Clone Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	Orange_SigRules	Edit

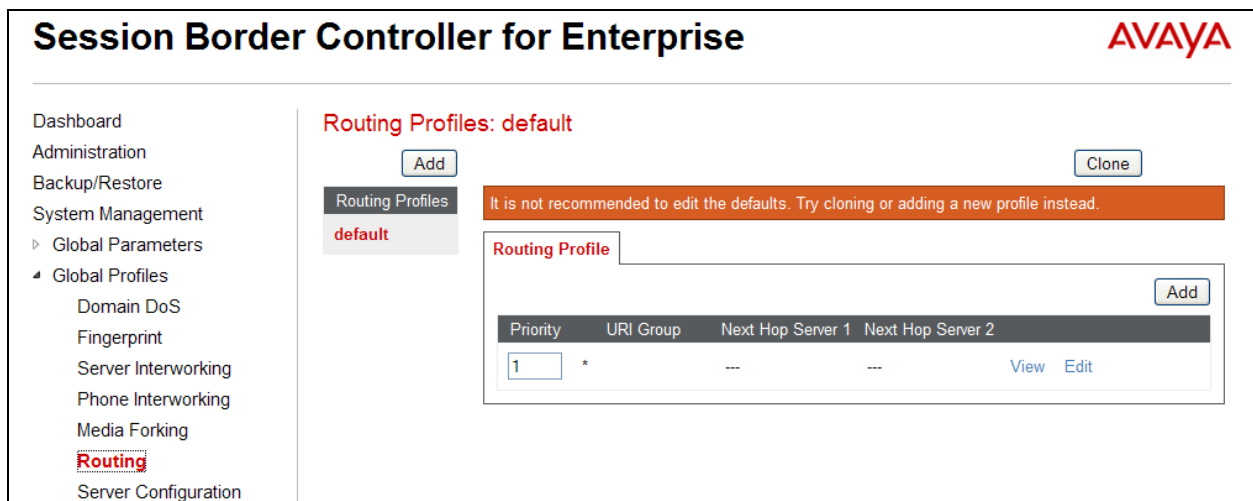
Summary

7.12. Routing

A routing profile defines where traffic will be directed based on the contents of the URI. A routing profile is applied only after the traffic has matched an endpoint server flow defined in **Section 7.14**. Create separate routing profiles for Session Manager and the service provider SIP server.

To create a new profile, navigate to **Global Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a series of pop-up windows in which the profile parameters can be configured. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile, select the profile from the center pane.

The screen below shows the GUI elements described above before specific routing profiles were added for the compliance test.



7.12.1. Routing – Session Manager

For the compliance test, routing profile **To-PkwySM** was created for routing calls to Session Manager. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card * to match on any URI.
- Set **Next Hop Address** to the IP address of Session Manager signaling interface.
- Set **Transport** to **TCP**.

The screenshot shows the 'Routing Profiles: To_PkwySM' configuration window. On the left is a sidebar with a list of routing profiles: 'default', 'To_SM', 'To_Trunks', 'To_HeadsetSM', 'To_PkwySM', 'To_PkwySM', 'To_HeadsetSM', 'To_SM_PSW', 'default_PSW', 'To_Pkwy_PSW', 'To_Head_PSW', and 'To_PkwySM'. The 'To_PkwySM' profile is selected and highlighted with a red box. The main area displays the configuration for the selected profile. At the top, there are buttons for 'Add', 'Rename', 'Clone', and 'Delete'. Below these is a blue bar with the text 'Click here to add a description.' The 'Routing Profile' section contains an 'Update Priority' button and an 'Add' button. Below this is a table with the following columns: 'Priority', 'URI Group', 'Time of Day', 'Load Balancing', 'Next Hop Address', and 'Transport'. The table contains one row with the following values: '1', '*', 'default', 'Priority', '10.32.128.32', and 'TCP'. To the right of the 'Transport' column are 'Edit' and 'Delete' links.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.32.128.32	TCP

7.12.2. Routing – Orange Business Services

For the compliance test, routing profile **To-Trunks** was created for routing calls to Orange Business Services. When creating the profile, configure the parameters as follows:

- Set **URI Group** to the wild card * to match on any URI.
- Set **Next Hop Address** to the IP addresses of the 2 Orange SIP servers.
- Set **Transport** to **UDP**.

Routing Profiles: To_Trunks

Buttons: Add, Rename, Clone, Delete

Routing Profiles list: default, To_Trunk, **To_Trunks**, To_Trunk1, To_Trunk2, To_Trunk3

Click here to add a description.

Routing Profile

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	192.168.246.33	UDP	Edit Delete
				192.168.246.73	UDP	

7.13. Topology Hiding

Topology hiding allows the host part of some SIP message headers to be modified in order to prevent private network information from being propagated to the untrusted public network. It can also be used as an interoperability tool to adapt the host portion of these same headers to meet the requirements of the connected servers. The topology hiding profile is applied as part of the endpoint flow in **Section 7.14**.

To create a new profile, navigate to **Global Profiles → Topology Hiding** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by a pop-up window in which a header can be selected and configured. Additional headers can be added in this window. Once complete, the settings are shown in the far right pane. To view the settings of an existing profile (e.g., **default**), select the profile from the center pane. The settings will appear in the right pane.

The screen below shows the GUI elements described above before specific topology hiding profiles were added for the compliance test.

Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▾ Global Profiles

Domain DoS

Fingerprint

Server Interworking

Phone Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

Topology Hiding Profiles: default

AddClone

Topology Hiding Profiles

default

cisco_th_profile

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

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---

Edit

7.13.1. Topology Hiding – Session Manager

For the compliance test, topology hiding profile **PRT-Domain** was created for Session Manager. This profile will be applied to traffic from the Avaya SBCE to Session Manager. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers except **Request-Line**, **From** and **To** which should be set to **Overwrite**.
- For those headers to be overwritten, the **Overwrite Value** is set to the enterprise domain (**avaya.com**).

Topology Hiding Profiles: PRT-Domain

Buttons: Add, Rename, Clone, Delete

Topology Hiding Profiles list: default, cisco_th_profile, SP-General, PRT-Domain (selected), SP-CLAN, SP-CLAN2

Click here to add a description.

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

Edit

7.13.2. Topology Hiding – Orange Business Services

For the compliance test, topology hiding profile **SP-General** was created for Orange Business Services. This profile will be applied to traffic from the Avaya SBCE to Orange Business Services. When creating the profile, configure the parameters as follows:

- Set **Header** to the header whose host part of the URI is to be modified.
- Set **Criteria** to **IP/Domain** to indicate that the host part should be modified if it is an IP address or a domain.
- Set **Replace Action** to **Auto** for all headers.

Topology Hiding Profiles: SP-General

Add

Topology Hiding Profiles

default

cisco_th_profile

SP-General

SP-General

PRT-Domain

SP-General

SP-General

Rename

Clone

Delete

Click here to add a description.

Topology Hiding

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

Edit

7.14. End Point Flows

End point flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source end point flow and the destination end point flow. In the case of the compliance test, the signaling endpoints are Session Manager and the service provider SIP server.

To create a new flow for a server endpoint, navigate to **Device Specific Settings → End Point Flows** in the left pane. In the center pane, select the Avaya SBCE device (**sp-ucsec1**) to be managed. In the right pane, select the **Server Flows** tab and click the **Add** button. A pop-up window (not shown) will appear requesting the name of the new flow and the flow parameters. Once complete, the configured flow is shown in the far right pane under the server name beside the **Server Configuration** heading.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface, End Point Flows (highlighted with a red box), Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, and Troubleshooting. The main content area is titled "End Point Flows: sp-ucsec1". It features a "Devices" tab with "sp-ucsec1" selected. Below this, there are two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of server configurations. The table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. There are two rows of data, each with a "View", "Clone", "Edit", and "Delete" link. The first row is for "Avaya-SBCE" and the second row is for "H323-Avaya-SBCE".

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya-SBCE	-	End_Sig_Inf	Inf_Sig_Inf	SIP	To_Termin	View Clone Edit Delete
2	H323-Avaya-SBCE	-	H323_End_Sig	H323_Inf_Sig	H323-User-SBCE	default	View Clone Edit Delete

7.14.1. End Point Flow – Session Manager

For the compliance test, end point flow **Pkwy-SM** was created for Session Manager. All traffic from Session Manager will match this flow as the source flow and use the specified **Routing Profile** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Session Manager server created in **Section 7.7.1**.
- To match all traffic, set **URI Group**, **Transport**, and **Remote Subnet** to *.
- Select the external signaling interface for **Received Interface**.
- Select the internal signaling interface for **Signaling Interface**.
- Select the internal media interface for **Media Interface**.
- For **End Point Policy Group**, select the endpoint policy group defined for Session Manager in **Section 7.11.1**.
- For **Routing Profile**, select the routing profile defined in **Section 7.12.2** used to direct traffic to the Orange SIP server.
- For **Topology Hiding Profile**, select the topology hiding profile defined for Session Manager in **Section 7.13.1**.
- Leave the other fields to default settings.

Edit Flow: Pkwy-SM	
Flow Name	Pkwy-SM
Server Configuration	Pkwy-SM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf
Signaling Interface	Int_Sig_Intf
Media Interface	Int_Media_Intf
End Point Policy Group	SM
Routing Profile	To_Trunks
Topology Hiding Profile	PRT-Domain
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
<button>Finish</button>	

The screen below shows the configured **Pkwy-SM** end point flow listed with its major settings under the server name **Pkwy-SM**.

End Point Flows: **sp-ucsec1**

Devices
sp-ucsec1

Subscriber Flows

Server Flows

Server Configuration: **Pkwy-SM**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Pkwy-SM	*	Ext_Sig_Intf	Int_Sig_Intf	SM	To_Trunk	View Clone Edit Delete

Server Configuration: **Pkwy-SM**

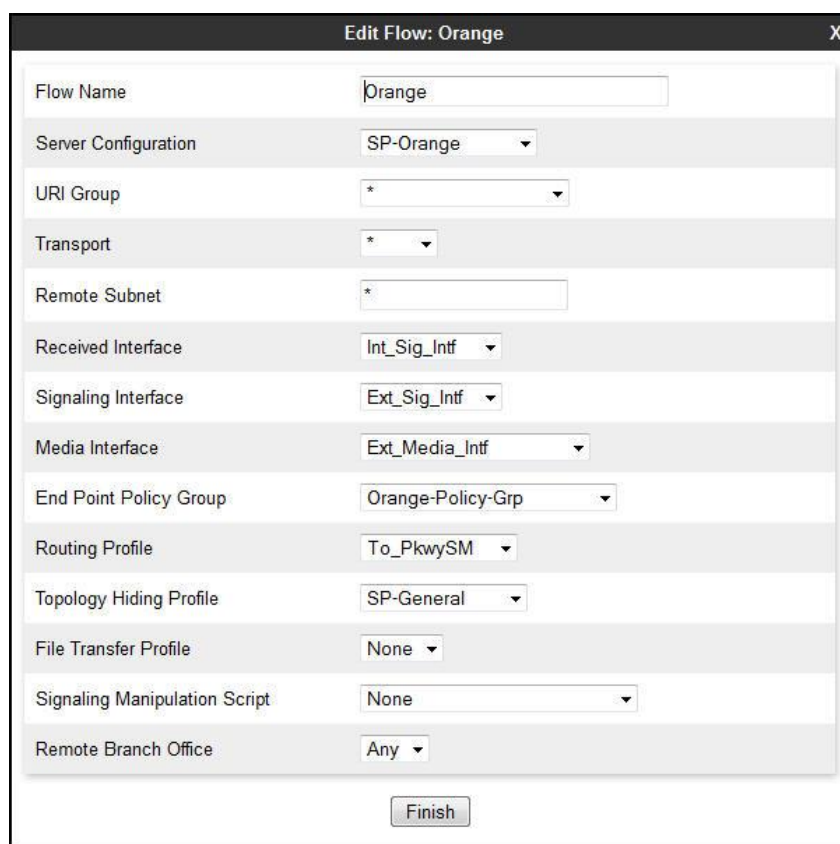
[Update](#)

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Pkwy-SM	*	Ext_Sig_Intf	Int_Sig_Intf	SM	To_Trunk	View Clone Edit Delete

7.14.2. End Point Flow – Orange Business Services

For the compliance test, end point flow **Orange** was created for the Orange SIP server. All traffic from Orange Business Services will match this flow as the source flow and use the specified **Routing Profile** to determine the destination server and corresponding destination flow. The **End Point Policy Group** and **Topology Hiding Profile** will be applied as appropriate. When creating the flow, configure the parameters as follows:

- For **Flow Name**, enter a descriptive name.
- For **Server Configuration**, select the Orange SIP server created in **Section 7.7.2**.
- To match all traffic, set **URI Group**, **Transport**, and **Remote Subnet** to *.
- Select the internal signaling interface for **Received Interface**.
- Select the external signaling interface for **Signaling Interface**.
- Select the external media interface for **Media Interface**.
- For **End Point Policy Group**, select the endpoint policy group defined for Orange Business Services in **Section 7.11.2**.
- For **Routing Profile**, select the routing profile defined in **Section 7.12.1** used to direct traffic to Session Manager.
- For **Topology Hiding Profile**, select the topology hiding profile defined for Orange Business Services in **Section 7.13.2**.
- Leave the other fields to default settings.



The screenshot shows the 'Edit Flow: Orange' configuration window. The settings are as follows:

Field	Value
Flow Name	Orange
Server Configuration	SP-Orange
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Intf
Signaling Interface	Ext_Sig_Intf
Media Interface	Ext_Media_Intf
End Point Policy Group	Orange-Policy-Grp
Routing Profile	To_PkwySM
Topology Hiding Profile	SP-General
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

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

The screen below shows the configured **Orange** end point flow listed with its major settings under the server name **SP-Orange**.

End Point Flows: sp-ucsec1

Devices
sp-ucsec1

Subscriber Flows
Server Flows

Server Configuration: SP-Land

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Land	*	Int_Sig_Intf	Ext_Sig_Intf	General-SP	To_PkwySM	View Clone Edit Delete

Server Configuration: SP-Orange

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Orange	*	Int_Sig_Intf	Ext_Sig_Intf	Orange-Policy-Grp	To_PkwySM	View Clone Edit Delete

Server Configuration: SP-Rugosa

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SP-Rugosa	*	Int_Sig_Intf	Ext_Sig_Intf	General-SP	To_PkwySM	View Clone Edit Delete

8. Orange SIP Trunking Service Configuration

Orange Business Services is responsible for the configuration of its SIP Trunking Service including the network configuration and deployment/management of the on-site Cisco 1841 Router (a Cisco 888 Router can also be used). Orange Business Services will require that the customer provide:

- The public IP address (**192.168.96.244** in **Figure 1**) and port number used to reach the on-premise Cisco Router at the edge of the enterprise.
- The internal IP address assigned to the LAN interface on the Cisco Router (**17.18.19.244** in **Figure 1**).
- The IP address (**17.18.19.228** in **Figure 1**) and port associated with the external interface of the Avaya SBCE.

Orange Business Services will provide Direct Inward Dialed (DID) numbers assigned to the enterprise and a document titled *Access SIP profile for connecting PBX to BTIP/BT SIP or FIAs2 services*. The information contained in the document (pertaining to BTIP/BT) and the DID numbers are used to complete the Communication Manager, Session Manager and the Avaya SBCE configuration discussed in the previous sections.

9. Verification Steps

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 useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

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

Troubleshooting:

1. Communication Manager:
 - **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 station** <extension number> - Displays signaling and media information for an active call on a specific station.
 - **status trunk** <trunk group number> - Displays trunk group information.
 - **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

2. Session Manager:

- **Session Manager Status** - The overall status and health summary of the administered Session Manager is shown in the **Session Manager Dashboard** by navigating to **Elements → Session Manager → Dashboard**. Verify that all the fields display proper working state as shown below.

Home / Elements / Session Manager Help ?

Session Manager Dashboard

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

Session Manager Instances

Service State Shutdown System As of 9:35 AM

1 Item Show ALL Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	Version
<input type="checkbox"/>	Pkway-SM	Core	✓	0/0/0	Up	Accept New Service	0/4	0	1/1	✓	✓	6.3.11.0.631103

Select : All, None

Clicking on the highlighted **Entity Monitoring** link (the numbers show down links vs. total links) will bring up the **Session Manager Entity Link Connection Status** window as shown below:

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: Pkway-SM

Summary View

Status Details for the selected Session Manager:

4 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	VNJ-SBCE1	10.32.128.18	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	PRT-CM-Trk1	10.32.128.4	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	PRT-CM-Trk3	10.32.128.4	5062	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	PRT-CM-Trk5	10.32.128.4	5068	TCP	FALSE	UP	200 OK	UP

- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

3. The Avaya SBCE:

The Avaya SBCE can take internal traces on specified interfaces. SIP signaling crossing both interfaces A1 and B1 can be captured for troubleshooting. In the Avaya SBCE web interface, navigate to **Device Specific Settings** → **Troubleshooting** → **Trace** to invoke this facility. In the **Packet Capture** tab, select or supply the relevant information (e.g., A1 or B1 or any interfaces, IP/port, protocol, number of packets to capture, capture file name, etc.), then press the **Start Capture** button to start the trace. The captured trace file can then be downloaded from the **Captures** tab for examination using a protocol sniffer application such as Wireshark.

The screen below shows the setup for capturing packets between the public interface of the Avaya SBCE (**B1**) and the Orange network (***:5060**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (expanded), Network Management, Media Interface, Signaling Interface, End Point Flows, Session Flows, DMZ Services, TURN/STUN Service, SNMP, Syslog Management, Advanced Options, Troubleshooting (expanded), Debugging, **Trace** (highlighted with a red box), and DoS Learning. The main content area is titled "Trace: sp-ucsec1" and features two tabs: "Packet Capture" (active) and "Captures". The "Packet Capture Configuration" form includes the following fields: Status (Ready), Interface (B1), Local Address (All : 5060), Remote Address (*:5060), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (ASBCEToFromEdgeMarc.pcap). The form also includes "Start Capture" and "Clear" buttons.

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.3, can be configured to interoperate successfully with the Orange BTIP/BT SIP Trunking Service via an on-site Cisco 1841 Router provisioned by Orange Business Services. Please refer to **Section 2.2** for any limitations, exceptions or workarounds.

11. References

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

Avaya Aura® System Platform

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3.4, Issue 2, July 2014.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3.4, Issue 2, July 2014.
- [3] *Upgrading Avaya Aura® System Manager*, Release 6.3.4, Issue 2, July 2014.

Avaya Aura® Session Manager / System Manager

- [4] *Deploying Avaya Aura® Session Manager*, Release 6.3, Issue 6, November 2014.
- [5] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014.
- [6] *Deploying Avaya Aura® System Manager on System Platform*, Release 6.3, Issue 4, June 2014.
- [7] *Administering Avaya Aura® System Manager for Release 6.3.10*, Release 6.3, Issue 6, January 2015.

Avaya Aura® Communication Manager

- [8] *Deploying Avaya Aura® Communication Manager on System Platform*, Release 6.3, Issue 6, June 2014, Document Number 18-604394.
- [9] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 10, June 2014, Document Number 03-300509.

Avaya Endpoints

- [10] *Avaya 1600 Series IP Deskphones Administrator Guide*, Release 1.3.3, Issue 4, April 2013, Document Number 16-601443.
- [11] *Administering Avaya IP Deskphone H.323 9608, 9611G, 9621G, and 9641G*, Release 6.3.1, Issue 17, January 2014, Document Number 16-300698.
- [12] *Administering Avaya one-X® Deskphone SIP for 9601, 9608, 9611G, 9621G, and 9641G*, Release 6.2.2, Issue 2, April 2013, Document Number 16-601944.
- [13] *Avaya 1140E IP Deskphone with SIP Software on Avaya Aura® User Guide*, Release 4.4, November 2013, Document Number 16-604274.
- [14] *Using the Avaya A175 Desktop Video Device with the Avaya Flare® Experience*, Document ID 16-603733, Issue 2, December 2011.
- [15] *Administering Avaya one-X® Communicator*, July 2013.
- [16] *Using Avaya Flare® Experience for Windows*, Release 1.1, Issue 2, February 2013, Document Number 18-604158.

Avaya Session Border Controller for Enterprise

- [17] *Deploying Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.
- [18] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Issue 4, October 2014.

Internet Engineering Task Force (IETF®) SIP RFC

- [19] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [20] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for the Orange BTIP/BT SIP Trunking Service is available from Orange Business Services.

©2015 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.