



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

## Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Release 5.2.1 with the Verizon Business Private IP (PIP) IP Trunk service.

The Verizon Business IP Trunk service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

**The configuration and software versions described in these Application Notes have not yet been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.**

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., utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

# Table of Contents

1.	Introduction.....	4
1.1.	Interoperability Compliance Testing .....	4
1.2.	Support.....	4
1.2.1	Avaya .....	4
1.2.2	Verizon.....	4
1.3.	Known Limitations .....	5
2.	Reference Configuration .....	6
2.1.	History Info and Diversion Headers .....	7
3.	Equipment and Software Validated .....	8
4.	Configure Avaya Aura® Communication Manager Release 5.2.1 .....	9
4.1.	Verify Licensed Features .....	9
4.2.	Processor Ethernet Configuration on Common Server.....	11
4.3.	Dial Plan.....	12
4.4.	Node Names.....	13
4.5.	Network Regions for Gateway, Telephones .....	13
4.6.	IP Codec Sets .....	15
4.7.	SIP Signaling Groups.....	15
4.8.	SIP Trunk Groups .....	17
4.9.	Route Pattern Directing Outbound Calls to Verizon .....	20
4.10.	Route Pattern for Internal Calls via Session Manager .....	20
4.11.	Private Numbering.....	21
4.12.	ARS Routing for Outbound Calls .....	22
4.13.	Incoming Call Handling Treatment for Incoming Calls .....	22
4.14.	EC500 Configuration for Diversion Header Testing.....	23
4.15.	Saving Communication Manager Configuration Changes .....	23
5.	Configure Avaya Aura® Session Manager Release 6.2 .....	24
5.1.	Domains .....	27
5.2.	Locations.....	28
5.3.	Adaptations .....	29
5.4.	SIP Entities.....	32
5.5.	Entity Links.....	36
5.6.	Time Ranges .....	37
5.7.	Routing Policies .....	38
5.8.	Dial Patterns.....	39
5.8.1	Inbound Call Dial Pattern .....	39
5.8.2	Outbound Call Dial Pattern.....	40
6.	Avaya Session Border Controller for Enterprise .....	41
6.1.	Access the Management Interface .....	41
6.2.	Global Profiles – Server Interworking.....	43
6.2.1	Server Interworking - Avaya .....	43
6.2.2	Server Interworking – Verizon IP Trunk .....	46
6.3.	Global Profiles – Routing .....	48
6.3.1	Routing Configuration for Session Manager .....	49
6.3.2	Routing Configuration for Verizon IP Trunk .....	49
6.3.3	Topology Hiding for Session Manager.....	50

6.3.4	Topology Hiding for Verizon IP Trunk .....	51
6.3.5	Signaling Manipulation.....	53
6.4.	Global Profiles – Server Configuration .....	54
6.4.1	Server Configuration for Session Manager.....	55
6.4.2	Server Configuration for Verizon IP Trunk.....	57
6.5.	Domain Policies – Application Rule.....	61
6.6.	Domain Policy – Media Rules .....	62
6.7.	Domain Policies – Signaling Rules.....	64
6.8.	Domain Policies – End Point Policy Groups .....	65
6.9.	Device Specific Settings - Network Management .....	67
6.10.	Device Specific Settings – Media Interface.....	68
6.11.	Device Specific Settings – Signaling Interface.....	70
6.12.	Device Specific Settings – End Point Flows.....	72
7.	Verizon Business IP Trunk Services Suite Configuration.....	75
7.1.	Service Access Information .....	75
8.	Verification Steps.....	76
8.1.	Illustration of OPTIONS Handling.....	76
8.2.	Avaya Aura® Communication Manager Verifications .....	77
8.2.1	Example Incoming Call from PSTN via Verizon SIP Trunk .....	77
8.2.2	Example Outgoing Calls to PSTN via Verizon IP Trunk .....	79
8.3.	Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications.....	81
8.3.1	Verify SIP Entity Link Status .....	81
8.3.2	Call Routing Test .....	83
8.4.	Avaya Session Border Controller for Enterprise Verification.....	84
8.4.1	Welcome Screen .....	84
8.4.2	Alarms .....	84
8.4.3	Incidents .....	85
8.4.4	Tracing .....	86
9.	Conclusion .....	87
10.	Additional References.....	88
10.1.	Avaya .....	88
10.2.	Verizon Business .....	88
Appendix A: Unscreened ANI Testing and Configuration.....		89
Verification .....		91

# 1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Release 5.2.1 with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

**The configuration and software versions described in these Application Notes have not yet been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon labs independent certification.**

## 1.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Avaya Aura® Communication Manager and the PSTN can be made using G.711MU or G.729A codecs.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF using RFC 2833
  - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)
  - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Avaya Modular Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g., International, operator assist, 411, 711)
- Hold / Retrieve with music on hold
- Call transfer using two approaches
  - REFER approach (Communication Manager Network Call Redirection flag on trunk group form set to “y”)
  - INVITE approach (Communication Manager Network Call Redirection flag on trunk group form set to “n”)
- Conference calls
- SIP Diversion Header for call redirection
  - Call Forwarding
  - EC500

## 1.2. Support

### 1.2.1 Avaya

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>

### 1.2.2 Verizon

For technical support on Verizon Business IP Trunk service offer, visit online support at <http://www.verizonbusiness.com/us/customer/>

### 1.3. Known Limitations

The following limitations are noted for the sample configuration described in these Application Notes:

- Avaya Aura® Communication Manager 5.2.1 does not support the use of SIP phones and the H.323 IP phones simultaneously in the sample configuration; therefore, the configuration of SIP phones is not covered by these Application Notes.
- Emergency 911/E911 Services Limitations and Restrictions- Although Verizon provides 911/E911 calling capabilities, 911 capabilities were not tested, therefore it is the Customer's responsibility to ensure proper operation with its equipment/software vendor.
- If calls requiring in-band DTMF (rather than RFC 2833 signaling) will be required, the "DTMF over IP" parameter on the Avaya Aura® Communication Manager SIP signaling group carrying such calls can be set to "in-band" rather than "rtp-payload". If the Communication Manager SIP signaling group is set to "rtp-payload", and a call is established using RFC 2833, Communication Manager will not subsequently switch to using "in-band" procedures to signal DTMF. Avaya is considering an enhancement for a future release of Communication Manager that would allow a call initially established with RFC 2833 to switch to using in-band DTMF based on subsequent SIP SDP exchanges.
- Verizon Business IP Trunking service does not support G.729B codec.
- Verizon has recently begun to offer T.38 as a fax option for SIP trunks. This native T.38 implementation from Verizon has some restrictions for robust interoperability with Avaya products. There are both short-term and longer-term solution choices available.

#### Short-Term:

Use an approved SIP gateway to provide full T.38, and optionally, support Verizon's specialized G.711 offer for fax transport. One example is AudioCodes' MP-114 SIP gateway running version 6.20A.035.001 or higher with Communication Manager 5.2.1 SP-12, 6.0.1 SP-6 or higher. Other short-term options include using Verizon's TDM services or special TDM routing between locations.

#### Longer-Term:

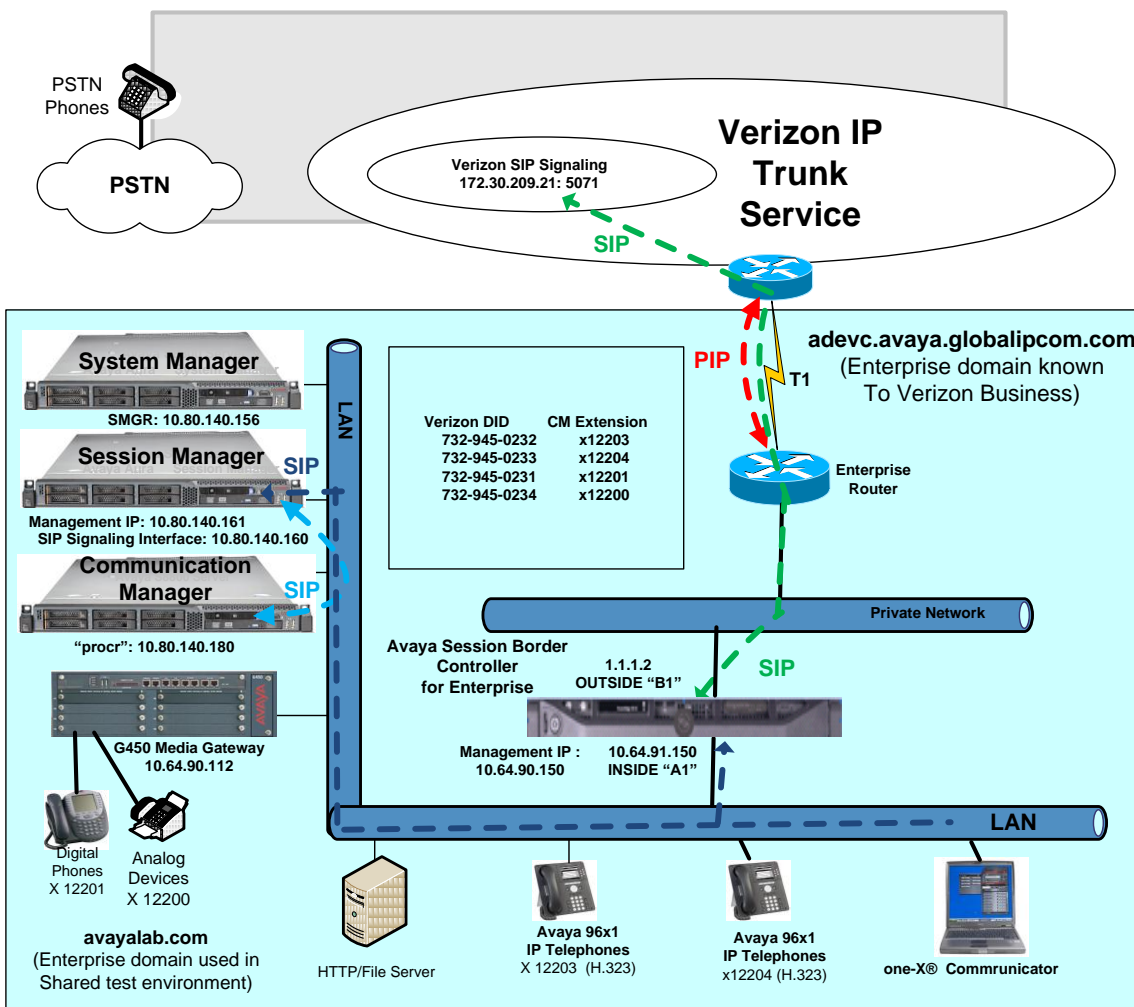
By mid-2013, Avaya should have software options to fully interoperate with both Verizon fax offers of T.38 and their specialized G.711 service. More information is available in GRIP-4852. With GRIP-4852 functionality, there is no need to have a front-end SIP gateway.

**Note** – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

## 2. Reference Configuration

**Figure 1** illustrates the sample configuration used for the testing. The Avaya CPE location simulates a customer site. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon service node.

The Avaya SBCE receive traffic from the Verizon Business IP Trunk service on port 5060 and send traffic to the Verizon Business IP trunk service on port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunk service). The Verizon Business IP Trunk service provided Direct Inward Dial (DID) 10 digit numbers. These DID numbers were mapped by Avaya Aura® Session Manager or Avaya Aura® Communication Manager to Avaya telephone extensions.



**Figure 1: Avaya Interoperability Test Lab Configuration**

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk service as FQDN *adevc.avaya.globalipcom.com*. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, Session Manager or the SBCE are used to adapt the “avayalab.com” domain to the domain known to Verizon. These Application Notes indicate a configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to the Verizon Business IP Trunk service.

**Note** – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use their own FQDNs and IP addressing as required.

In summary, the following components were used in the reference configuration.

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
  - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
  - *adevc.avaya.globalipcom.com*
- Session Border Controllers for Enterprise
- Avaya Aura® Communication Manager Release 5.2.1, SP 13
- Avaya Aura® Session Manager Release 6.2
- Avaya 96X1 Series IP telephones using the H.323 software bundle
- Avaya 9600 Series IP telephones using the H.323 software bundle
- Avaya Digital Phones
- Avaya Analog Phones

## 2.1. History Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History Info Headers. Instead, the Verizon Business IP Trunk service requires that SIP Diversion Header be sent for redirected calls. The Avaya Aura® Communication Manager SIP trunk group form provides options for specifying whether History Info Headers or Diversion Headers are sent.

If Avaya Aura® Communication Manager sends the History Info Header, Avaya Aura® Session Manager can convert the History Info header into the Diversion Header. This is performed by specifying the “*Verizon Adapter*” adaptation in Avaya Aura® Session Manager.

Communication Manager call forwarding or Extension to Cellular (EC500) features may be used for the call scenarios involving Diversion Header.

### 3. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

<b>Equipment:</b>	<b>Software:</b>
Avaya Aura® Communication Manager	Release 5.2.1 load 016.4 SP 13
Avaya Aura® System Manager	6.2
Avaya Aura® Session Manager	6.2
G450 Gateway	3.1.20.1
Avaya Session Border Controller for Enterprise	4.0.5Q09
Avaya 9600-Series Telephones (H.323)	96xx-IPT-H323-R3_1_3-112211
Avaya 96X1- Series Telephones (H323)	96x1-IPT-H323-R6_0_5-091911
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
Okidata Analog Fax	N/A
Avaya One-X Communicator (H.323)	6.1.3.08_SP3-Patch2-35791

**Table 1: Equipment and Software Used in the Sample Configuration**



## 4. Configure Avaya Aura® Communication Manager Release 5.2.1

This section describes the procedure for configuring Avaya Aura® Communication Manager for SIP Trunk service. A SIP trunk is established between Communication Manager and Avaya Aura® Session Manager for use by signaling traffic to and from Verizon.

**Note** - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

### 4.1. Verify Licensed Features

The Communication Manager License file controls customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

On **Page 2** of the *display system-parameters customer-options* form, verify that the **Maximum Administered SIP Trunks** are sufficient for the combination of trunks to the Verizon Business IP Trunk service offer and any other SIP applications. Each call from a non-SIP endpoint to the Verizon Business IP Trunk service uses one SIP trunk for the duration of the call.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		8000	0
Maximum Concurrently Registered IP Stations:		18000	2
Maximum Administered Remote Office Trunks:		0	0
Maximum Concurrently Registered Remote Office Stations:		0	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Registered Unauthenticated H.323 Stations:		18000	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
<b>Maximum Administered SIP Trunks:</b>		<b>5000</b>	<b>283</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		8000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		10	0
Maximum Media Gateway VAL Sources:		250	1
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.)			

On **Page 3** of the *display system-parameters customer-options* form, verify that **ARS** is enabled.

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
<b>ARS? y</b>	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? y		
Async. Transfer Mode (ATM) Trunking? y	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		

On **Page 4** of the *display system-parameters customer-options* form, verify that the **Enhanced EC500**, **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		<b>IP Stations? y</b>
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? y
<b>Enhanced EC500? y</b>	<b>ISDN/SIP Network Call Redirection? y</b>	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		<b>ISDN-PRI? y</b>
ESS Administration? n	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? n	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? n	Multifrequency Signaling? y	
Global Call Classification? n	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? n	Multimedia IP SIP Trunking? y	
<b>IP Trunks? y</b>		
IP Attendant Consoles? y		

On **Page 5** of the *display system-parameters customer-options* form, verify that the **Private Networking** and **Processor Ethernet** features are enabled.

display system-parameters customer-options		Page 5 of 11
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? y		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
<b>Private Networking? y</b>	TN2501 VAL Maximum Capacity? y	
Processor and System MSP? y	Uniform Dialing Plan? y	
<b>Processor Ethernet? y</b>	Usage Allocation Enhancements? y	
Remote Office? n	Wideband Switching? n	
Restrict Call Forward Off Net? y	Wireless? n	
Secondary Data Module? y		

## 4.2. Processor Ethernet Configuration on Common Server

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the reference configuration.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** Fields are set to **Y**.
- Assign a network region (e.g. **1**).
- Use default values for the remaining parameters.

change ip-interface pro		Page 1 of 1
IP INTERFACES		
Type: PROC	Target socket load: 1700	
<b>Enable Interface? y</b>	<b>Allow H.323 Endpoints? y</b>	
	<b>Allow H.248 Gateways? y</b>	
Network Region: 1	Gatekeeper Priority: 5	

### 4.3. Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, such as 12xxx . Trunk Access Codes (TAC) are 4 digits in length and begin with \*. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

The dial plan is modified with the ***change dialplan analysis*** command as shown below.

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

## 4.4. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following ***change node-names ip*** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is “SM” with IP address 10.80.140.160. The node name and IP address for the Processor Ethernet “procr” is 10.80.140.180.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
MM	205.3.3.55	
<b>SM</b>	<b>10.80.140.160</b>	
default	0.0.0.0	
<b>procr</b>	<b>10.80.140.180</b>	

## 4.5. Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that media gateway 3 is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (10.80.140.180), and that the gateway IP address is 10.64.90.112. These fields are not configured in this screen, but rather simply display the current information for the gateway.

change media-gateway 3		Page 1 of 1	
MEDIA GATEWAY			
Number: 3	Registered? y		
Type: g450	FW Version/HW Vintage: 31 .22 .0 /1		
Name: G450-1	MGP IP Address: 10 .64 .90 .112		
Serial No: 11N510735839	Controller IP Address: 10 .80 .140.180		
Encrypt Link? y	MAC Address: b4:b0:17:90:82:50		
Network Region: 1	Location: 1	Enable CF? n	
		Site Data:	
Recovery Rule: 1			
Slot	Module Type	Name	DSP Type FW/HW version
V1:			MP80 69 6
V2:			MP80 69 6
V3:			MP80 69 6
V4:			MP80 69 6
V5:			
V6:			
V7:	MM712	DCP MM	
V8:	MM711	ANA MM	Max Survivable IP Ext: 8
V9:	gateway-announcements	ANN VMM	

The bottom of the screen shows the gateway has a MM712 media module supporting Avaya digital phones in slot v7, a MM711 supporting analog devices in slot v8, and the capability to provide announcements and music on hold via “gateway-announcements” in logical slot v9.

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the “gatekeeper” (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 10.80.150.101 would be mapped to network region 2, based on the bold configuration below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map			Page 1 of 63		
IP ADDRESS MAPPING					
IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
-----	-----	-----	-----	-----	-----
FROM: 10.80.150.100	/	2	n		
TO: 10.80.150.199					
FROM:	/		n		
TO:					

The following screen shows IP Network Region 2 configuration. In the shared test environment, network region 2 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 1 will be used for calls within region 2. The shared test environment uses the domain “avayalab.com” (i.e., for network region 2 including the region of the Processor Ethernet “procr”).

change ip-network-region 2		Page 1 of 19
IP NETWORK REGION		
Region: 2		
Location: 1		Authoritative Domain: avayalab.com
Name: IP Phones		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? n
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? y
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		

## 4.6. IP Codec Sets

The following screen shows the configuration for codec set 1, the codec set configured to be used for calls within region 1 and for calls within region 2. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls to and from the PSTN via the SIP trunks would use G.711MU, since G.711MU is preferred by both Verizon and the Avaya ip-codec-set. Any calls using this same codec set that are between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722. Note that if G.711MU is omitted from the list of allowed codecs in ip-codec-set 1, calls from Verizon that are answered by Avaya Modular Messaging will use G450 VoIP resources to convert from G.729a (facing Verizon) to G.711MU (facing Modular Messaging). If G.711MU is included in ip-codec-set 1, then calls from Verizon that are answered by Modular Messaging will not use G450 VoIP resources, but rather be “ip-direct” using G.711MU from Modular Messaging to the inside of the SBCE. Include G.711MU in the ip-codec-set if fax will be used.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames		Packet		
Codec	Suppression	Per	Pkt	Size (ms)		
1: G.722-64K		2		20		
2: G.711MU	n	2		20		
3: G.729	n	2		20		
4:						

On **Page 2** of the form:

- Configure the Fax **Mode** field to “t.38-standard”, T.38 is newly supported by Verizon and was tested successfully in this test configuration.
- Configure the Fax **Redundancy** field to “0”.

change ip-codec-set 1				Page	2 of	2
IP Codec Set						
Allow Direct-IP Multimedia? n						
	Mode	Redundancy				
FAX	t.38-standard	0				
Modem	off	0				
TDD/TTY	US	3				
Clear-channel	n	0				

## 4.7. SIP Signaling Groups

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM”. In the example screens, the **Transport Method** for all signaling groups is “tcp”. In production, TLS transport between Communication Manager and Session Manager can be used. The **Enable**

**Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 1. Signaling group 1 will be used for processing PSTN calls to / from Verizon via Session Manager. The **Far-end Network Region** is configured to region 10. Port 5060 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Verizon DID numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5060. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. Other parameters may be left at default values.

change signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 10	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	



## 4.8. SIP Trunk Groups

This section illustrates the configuration of the SIP Trunk Group corresponding to the SIP signaling group from the previous section.

The following shows **Page 1** for trunk group 1, which will be used for incoming and outgoing PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to “public-ntwrk” for the trunks that will handle calls with Verizon. The **Direction** has been configured to “two-way” to allow incoming and outgoing calls in the sample configuration.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SIP Trunk to SP	COR: 1	TN: 1	TAC: *101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 1	
		Number of Members: 10	

The following shows **Page 2** for trunk group 1; all parameters shown are default values.

change trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 600			
Disconnect Supervision - In? y Out? y			

The following shows **Page 3** for trunk group 1. All parameters except those in bold are default values. The **Numbering Format** will use “private” numbering, meaning that the private numbering table would be consulted for any mappings of Communication Manager extensions to alternate numbers to be sent to Session Manager. Optionally, replacement text strings can be configured using the “system-parameters features” screen, such that incoming “private” (anonymous) or “restricted” calls can display an Avaya-configured text string on called party telephones.

change trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
<b>Numbering Format: private</b>		
UI Treatment: service-provider		
<b>Replace Restricted Numbers? y</b>		
<b>Replace Unavailable Numbers? y</b>		
Show ANSWERED BY on Display? y		

The following shows **Page 4** for trunk group 1. The **PROTOCOL VARIATIONS** page is one reason why it can be advantageous to configure incoming calls from Verizon to arrive on specific signaling groups and trunk groups. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to “y” enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal “send-only” media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor “send-only” media signaling is required, this field may be left at the default “n” value. In the testing associated with these Application Notes, transfer testing using REFER was successfully completed with the **Network Call Redirection** flag set to “y”, and transfer testing using INVITE was successfully completed with the **Network Call Redirection** flag set to “n”.

For redirected calls, Verizon supports the Diversion header, but not the History-Info header. Communication Manager can send the Diversion header by marking **Send Diversion Header** to “y”. Alternatively, Communication can send the History-Info header by setting **Support Request History** to “y”, and Session Manager can adapt the History-Info header to the Diversion header using the “VerizonAdapter”. In the testing associated with these Application Notes, call redirection testing with Communication Manager sending Diversion Header was completed successfully. Communication Manager configuration was then changed, and call redirection testing with Communication Manager sending History-Info and Session Manager adapting to Diversion Header was completed successfully.

change trunk-group 1	Page	4 of	21
<p>PROTOCOL VARIATIONS</p> <p>Mark Users as Phone? n</p> <p>Prepend '+' to Calling Number? n</p> <p>Send Transferring Party Information? n</p> <p>Network Call Redirection? y</p> <p>Send Diversion Header? y</p> <p>Support Request History? n</p> <p>Telephone Event Payload Type: 101</p>			

## 4.9. Route Pattern Directing Outbound Calls to Verizon

Route pattern 1 will be used for calls destined for the PSTN via the Verizon IP Trunk service. Digit manipulation can be performed on the called number, if needed, using the **No. Del Dgts** and **Inserted Digits** parameters. Digit manipulation can also be performed by Session Manager.

change route-pattern 1															Page 1 of 3	
Pattern Number: 1 Pattern Name: To SIP SP																
SCCAN? n Secure SIP? n																
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted									DCS/ IXC
No			Mrk	Lmt	List	Del	Digits									QSIG
															Intw	
															</	

## 4.11. Private Numbering

The *change private-unknown-numbering* command may be used to define the format of numbers sent to Verizon in SIP headers such as the “From” and “PAI” headers. In general, the mappings of internal extensions to Verizon DID numbers may be done in Session Manager (via Digit Conversion in adaptations) or in Communication Manager (via public-unknown-numbering, and incoming call handling treatment for the inbound trunk group).

In the bolded row shown in the example abridged output below, a specific Communication Manager extension (12201) is mapped to a DID number that is known to Verizon for this SIP Trunk connection (7329450231), when the call uses trunk group 1. Alternatively, Communication Manager can send the five digit extension to Session Manager, and Session Manager can adapt the number to the Verizon DID. Both methods were tested successfully.

change private-numbering 0				Page 1 of 2
NUMBERING - PRIVATE FORMAT				
Ext	Ext	Trk	Private	Total
Len	Code	Grp(s)	Prefix	Len
5	12		5	Total Administered: 3
5	122	99	5	Maximum Entries: 540
5	12201	1	7329450231	10
5	12203	1	7329450232	10
5	12204	1	7329450233	10

## 4.12. ARS Routing for Outbound Calls

Although not illustrated in these Application Notes, location-based routing may be configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns. In these Application Notes, the ARS “all locations” table directs ARS calls to specific SIP Trunks to Session Manager.

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subnet of the dialed strings tested as part of the testing. All dialed strings are mapped to route pattern 1 which contains SIP trunk to Session Manager.

change ars analysis 303							Page 1 of 2	
ARS DIGIT ANALYSIS TABLE								
Location: all				Percent Full:			0	
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
303		10	10	1	hnpa		n	
311		3	3	1	svcl		n	
411		3	3	1	svcl		n	
501		10	10	1	hnpa		n	
511		3	3	1	svcl		n	
611		3	3	1	svcl		n	
711		3	3	1	svcl		n	
720		10	10	1	hnpa		n	
732		10	10	1	hnpa		n	

## 4.13. Incoming Call Handling Treatment for Incoming Calls

In general, the “incoming call handling treatment” for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Avaya Aura® Session Manager is present, Session Manager can also be used to perform digit conversion, and digit manipulation and the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Verizon is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of DID number 7329450231-34 to extension 12200-12204 respectively.

change inc-call-handling-trmt trunk-group 1				Page	1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del Insert		
Feature	Len	Digits			
public-ntwrk	11	17329450233	all	12204	
public-ntwrk	10	7329450231	all	12201	
public-ntwrk	10	7329450232	all	12203	
public-ntwrk	10	7329450233	all	12204	
public-ntwrk	10	7329450234	all	12200	
public-ntwrk					

#### 4.14. EC500 Configuration for Diversion Header Testing

When EC500 is enabled for a Communication Manager station, a call to that station will generate a new outbound call from Avaya Aura® Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 12203. Use the command *change off-pbx-telephone station mapping x* where *x* is the Communication Manager station (e.g. 12203).

- **Station Extension** – This field will automatically populate.
- **Application** – Enter “EC500”.
- **Dial Prefix** – Enter a prefix (e.g., 1) if required by the routing configuration.
- **Phone Number** – Enter the phone that will also be called (e.g., 3035380023).
- **Trunk Selection** – Enter “ars”. This means ARS will be used to determine how Communication Manager will route to the **Phone Number** destination.
- **Config Set** – Enter “1”.
- Other parameters can retain default values.

change off-pbx-telephone station-mapping 12203							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode		
12203	EC500	-		3035380023	ars	1			
		-							
		-							

#### 4.15. Saving Communication Manager Configuration Changes

The command *save translation all* can be used to save the configuration.

## 5. Configure Avaya Aura® Session Manager Release 6.2

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

**Note** – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between System Manager and Session Manager.

Session Manager is managed via System Manager. Using a web browser, access “https://<ip-addr of System Manager>/SMGR”. In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button as shown in the example System Manager 6.2 **Log On** screen below.

Avaya Aura® System Manager 6.2

Home / Log On

### Log On

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification 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.

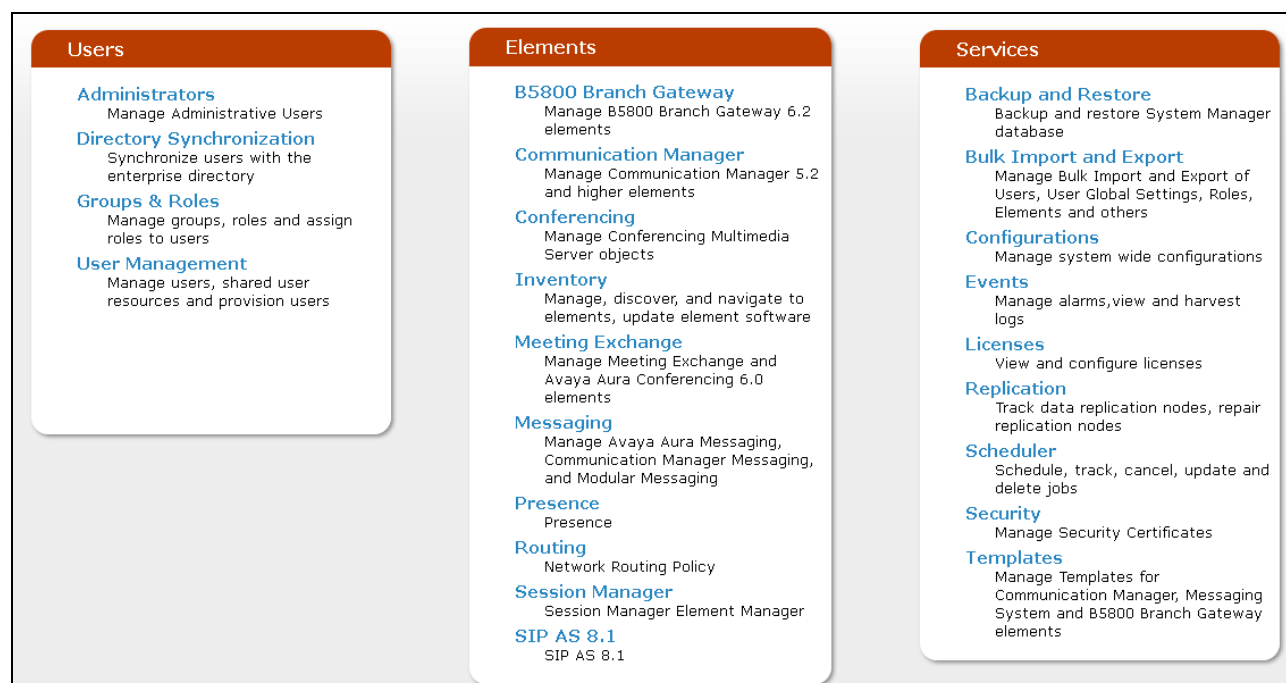
User ID:

Password:

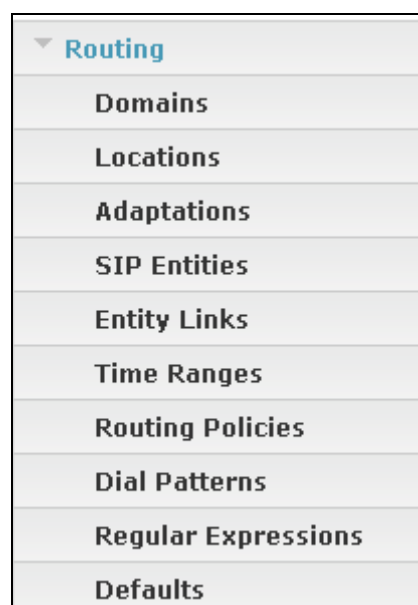
[Change Password](#)



Once logged in, a **Home Screen** is displayed. An abridged **Home Screen** is shown below.



Under the heading “Elements” in the center, select **Routing**. The screen shown below shows the various sub-headings available on the left hand side menu.



The right side of the screen, illustrated below, outlines a series of steps. The sub-sections that follow are in the same order as the steps outlined under **Introduction to Network Routing Policy** in the abridged screen shown below.

### 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"

Scroll down to review additional information as shown below. In these Application Notes, all steps are illustrated with the exception of Step 9, since “Regular Expressions” were not used.

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)

Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

## 5.1. Domains

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button after changes are completed.

The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among other Avaya interoperability test efforts. The domain “avayalab.com” was used for communication with Avaya SIP Telephones and other Avaya systems and applications. The domain “avayalab.com” is not known to the Verizon production service.

Home / Elements / Routing / Domains				
<b>Domain Management</b>				
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>				
3 Items   <a href="#">Refresh</a>				
<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	<a href="#">adevc.avaya.globalipcom.com</a>	sip	<input type="checkbox"/>	CPE domain known to Verizon
<input type="checkbox"/>	<a href="#">avayalab.com</a>	sip	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">pcelban0001.avayalincroft.globalipcom.com</a>	sip	<input type="checkbox"/>	Verizon IPT Network Domain

The domain “adevc.avaya.globalipcom.com” is the domain known to Verizon as the enterprise SIP domain. In the sample configuration, Verizon included this domain as the host portion of the Request-URI for inbound DID calls.

1 Item   <a href="#">Refresh</a>			
Name	Type	Default	Notes
* <input type="text" value="adevc.avaya.globalipcom.com"/>	<input type="text" value="sip"/>	<input type="checkbox"/>	<input type="text" value="CPE domain known to Verizon"/>

The domain “pcelban0001.avayalincroft.globalipcom.com” is associated with the Verizon network in the sample configuration. For example, for calls from the enterprise site to Verizon, this domain can appear in the Request-URI in the INVITE message sent to Verizon. The following screen shows the relevant configuration.

1 Item Refresh		Filter: Enable	
Name	Type	Default	Notes
* pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon IPT Network Domain

## 5.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.

Home / Elements / Routing / Locations

[Help ?](#)

### Location

5 Items Refresh		Filter: Enable
<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	<a href="#">Avaya-SBCE-1</a>	Avaya SBCE-1
<input type="checkbox"/>	<a href="#">Avaya-SBCE-2</a>	Avaya-SBCE-2
<input type="checkbox"/>	<a href="#">Avaya-SBCE-3</a>	Avaya SBCE-3
<input type="checkbox"/>	<a href="#">CM521</a>	CM 5.2.1
<input type="checkbox"/>	<a href="#">Location 140</a>	Subnet 140
Select : All, None		

The following image shows the top portion of the screen for the location details for the location named “Avaya-SBCE 3”, corresponding to the Avaya SBC for Enterprise relevant to these Application Notes. Later, the location with name “Avaya-SBCE-3” will be assigned to the corresponding SIP Entity.

The screenshot displays the 'Location Details' configuration window for a location named 'Avaya-SBCE-3'. On the left is a sidebar menu with options: Locations (selected), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons at the top right. The 'General' section contains fields for 'Name' (Avaya-SBCE-3) and 'Notes' (Avaya SBCE-3). The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (Kbit/sec), 'Total Bandwidth', 'Multimedia Bandwidth', and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', '\* Minimum Multimedia Bandwidth', and '\* Default Audio Bandwidth'. The 'Alarm Threshold' section includes fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', '\* Latency before Overall Alarm Trigger', and '\* Latency before Multimedia Alarm Trigger'. At the bottom, the 'Location Pattern' section has 'Add' and 'Remove' buttons.

### 5.3. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

The following screen shows a portion of the list of adaptations that were available in the sample configuration, not all of which are applicable to these Application Notes.

Home / Elements / Routing / Adaptations

Help ?

### Adaptations

9 Items	<a href="#">Refresh</a>	Filter: <a href="#">Enable</a>		
<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	<a href="#">CM-ES-VZ</a>	DigitConversionAdapter		
<input type="checkbox"/>	<a href="#">CM-ES-VZ-IPCC</a>	DigitConversionAdapter odstd=avayalab.com fromto=true		Verizon IPCC to CM Numbers
<input type="checkbox"/>	<a href="#">History Diversion IPT</a>	VerizonAdapter osrcd=advec.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true		Verizon adaptation
<input type="checkbox"/>	<a href="#">IPCC Verizon Interop Lab</a>	VerizonAdapter		
<input type="checkbox"/>	<a href="#">MM to 4digits</a>	DigitConversionAdapter fromto=true		converting 5 to 4 digits VM
<input type="checkbox"/>	<a href="#">SBC-VzB-IPCC</a>	DigitConversionAdapter osrcd=advec.avaya.globalipcom.com		
<input type="checkbox"/>	<a href="#">To VZ</a>	VerizonAdapter odstd=172.30.209.21 fromto=true		
<input type="checkbox"/>	<a href="#">Verizon Test</a>	VerizonAdapter		
<input type="checkbox"/>	<a href="#">Verizon Unscreened ANI</a>	VerizonAdapter osrcd=advec.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcpm.com fromto=true		

Select : [All](#), [None](#)

The following screen shows the adaptation details. The adapter named “Verizon\_Test” will later be assigned to the SIP Entity for the Avaya SBCE-3, specifying that all communication from the Session Manager to the Avaya SBCE- 3 will use this adapter. This adaptation uses the “Verizon Adapter” and specifies three parameters that are used to adapt the FQDN to the domains expected by the Verizon network in the sample configuration. Again, this may not be required in all networks, but is used here to adapt the avayalab.com domain that is used in the shared test environment among other Avaya interoperability test efforts.

Home / Elements / Routing / Adaptations

Adaptation Details

[Help ?](#)

General

\* Adaptation name:
Verizon\_Test

Module name:
VerizonAdapter

Module parameter:
osrcd=adefc.avaya.globalipcom.cc

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

0 Items
Refresh

☐

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Filter: Enable

Digit Conversion for Outgoing Calls from SM

2 Items
Refresh

☐

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
...	...	...	...	...	...	...	...	...

Filter: Enable

The “**Module parameter:**” line contains the following line:

**osrcd=adefc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true**

- `overrideDestinationDomain : “osrcd=adefc.avaya.globalipcom.com”`. This configuration enables the source domain to be overwritten with “adefc.avaya.globalipcom.com”. For example, for outbound PSTN calls from the Avaya CPE to Verizon, the PAI header will contain “adefc.avaya.globalipcom.com” as expected by Verizon.
- `overrideDestinationDomain : “odstd=pcelban0001.avayalincroft.globalipcom.com”` This configuration enables the destination domain to be overwritten with “pcelban0001.avayalincroft.globalipcom.com”. For example, for outbound PSTN calls from the Avaya CPE to Verizon, the Request-URI header will contain “pcelban0001.avayalincroft.globalipcom.com” as expected by Verizon.

- **Fromto:** The parameter “**fromto=true**” enables Session to modify From and To headers of the message. If omitted or set to any other value, From and To headers will not be modified.

The ”History\_Diversion\_IPT” Module Parameter statement above is overriding avayalab.com with the FQDNs know by Verizon towards the Avaya SBCE. It is also necessary to override the FQDNs known to Verizon back to avayalab.com towards the Communication Manager. This could be done on the next Adaptation “CM-ES-VZ” with the same parameters odstcd and osrccd or here in the ”History\_Diversion\_IPT” adapter with the statements:

- `ingressOverrideDestinationDomain: “iodstd=avayalab.com”`
- `ingressOverrideDestinationDomain: “iosrccd=avayalab.com”`

## 5.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed. The following screen shows a portion of the list of configured SIP entities. In this screen, the SIP Entities named “Avaya-SBCE 3”, “ASM-62”, and “CM521\_tg1” & “CM521\_tg3” are relevant to these Application Notes.

Home / Elements / Routing / SIP Entities				
				<a href="#">Help ?</a>
<b>SIP Entities</b>				
<input type="button" value="Edit"/> <input type="button" value="New"/> <input type="button" value="Duplicate"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/>				
10 Items <a href="#">Refresh</a> <span style="float: right;">Filter: <a href="#">Enable</a></span>				
<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	<a href="#">ASM-62</a>	10.80.140.160	Session Manager	
<input type="checkbox"/>	<a href="#">Avaya-SBCE-1</a>	10.80.140.141	Other	Sipera-SBC-1 Outside 2.2.2.2
<input type="checkbox"/>	<a href="#">Avaya-SBCE-2</a>	10.80.140.200	Other	Sipera-SBC-2 Outside 1.1.1.2
<input type="checkbox"/>	<a href="#">Avaya-SBCE-3</a>	10.64.91.150	SIP Trunk	Sipera-SBC-3 outside 1.1.1.2 using adaptation
<input type="checkbox"/>	<a href="#">CM521_tg1</a>	10.80.140.180	CM	
<input type="checkbox"/>	<a href="#">CM521_tg3</a>	10.80.140.180	CM	SIP Phones
<input type="checkbox"/>	<a href="#">CM6.2</a>	10.80.140.146	CM	
<input type="checkbox"/>	<a href="#">CM-Evolution-procr-5062</a>	10.80.140.146	CM	CM-ES procr IP, different port
<input type="checkbox"/>	<a href="#">CM-Evolution-procr-5063</a>	10.80.140.146	CM	CM-ES procr IP, different port
<input type="checkbox"/>	<a href="#">ModularMessaging</a>	205.3.3.56	Modular Messaging	
Select : <a href="#">All</a> , <a href="#">None</a>				

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “ASM-62”. The **FQDN or IP Address** field for “ASM-62” is the Session Manager Security Module IP Address (10.80.140.160), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is “Session Manager”. Select an appropriate location for the Session



Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location “Location\_140”. The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.

[Help](#)

### SIP Entity Details

#### General

\* Name:

\* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

#### SIP Link Monitoring

SIP Link Monitoring:

Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for “ASM-62”. The links relevant to these Application Notes are described in the subsequent section.

### Entity Links

9 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	ASM-62	TLS	* 5061	CM521_tg3	* 5061	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	ModularMessaging	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	CM521_tg1	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	CM6.2	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5062	CM-Evolution-procr-5062	* 5062	Trusted

Select : [All](#), [None](#) < Previous | Page  of 2 | Next >

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, illustrating the configured ports for “ASM-62”. In the sample configuration, TCP port 5060 was already in place for the shared test environment, using **Default Domain** “avayalab.com”. Click the **Add** button to configure a new port.

Port

TCP Failover port:

TLS Failover port:

Add Remove

3 Items Refresh
Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	avayalab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5062"/>	TCP	adevc.avaya.globalipcom.com	Verizon IPT testing
<input type="checkbox"/>	<input type="text" value="5063"/>	TCP	adevc.avaya.globalipcom.com	Verizon IPCC testing

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Refresh
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

\* Input Required

Commit Cancel

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “Avaya-SBCE 3”. The **FQDN or IP Address** field is configured with the Avaya SBC inside IP Address (10.64.91.150). “SIP Trunk” is selected from the **Type** drop-down menu for SBC SIP Entities. This SBCE has been assigned to **Location** “Avaya-SBCE3”, and the “Verizon\_Test” adapter is applied. Other parameters (not shown) retain default values.

SIP Entity Details

Help ?  
Commit Cancel

General

\* Name: Avaya-SBCE-3

\* FQDN or IP Address: 10.64.91.150

Type: SIP Trunk

Notes: Sipera-SBC-3 outside 1.1.1.2 using

Adaptation: Verizon\_Test

Location: Avaya-SBCE-3

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

\* Proactive Monitoring Interval (in seconds): 900

\* Reactive Monitoring Interval (in seconds): 120

The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named “CM521\_tg1”. This is the SIP Entity that was added in the shared environment, after adding the Verizon IP Trunk configurations. The **FQDN or IP Address** field contains the IP Address of the “processor Ethernet” (10.80.140.180). In systems with Avaya G450 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the “processor Ethernet”. “CM” is selected from the **Type** drop-down menu.

Home / Elements / Routing / SIP Entities

SIP Entity Details

[Help ?](#)

Commit

Cancel

General

\* Name:

CM521\_tg1

\* FQDN or IP Address:

10.80.140.180

Type:

CM

Notes:

Adaptation:

Location:

CM521

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

none

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

## 5.5. Entity Links

To view or change Entity Links, select **Routing → Entity Links**. Click on the checkbox corresponding to the name of a link and **Edit** to edit an existing link, or the **New** button to add a link. Click the **Commit** button after changes are completed.

**Note** – In the Entity Link configurations below (and in the Communication Manager SIP trunk configuration), TCP was selected as the transport protocol for the Avaya CPE in the sample configuration. TCP was used to facilitate trace analysis during network verification. TLS may be used between Communication Manager and Session Manager in customer deployments.

The following screen shows a list of configured links. In the screen below, the links named “Sipera-SBCE-3” and “ASM-CM521\_tg1” are most relevant to these Application Notes. Each

link uses the entity named “ASM-62” as **SIP Entity 1**, and the appropriate entity, such as “CM521\_tg1” for **SIP Entity 2**. Note that there are multiple SIP Entity Links, using different TCP ports, linking the same “ASM-62” with the Processor Ethernet of Communication Manager. For example, for one link, named “ASM\_to\_CM”, both entities use TCP and port 5060. For the entity link used by Verizon IP Trunk named “CM-ES-VZ-5062”, both entities use TCP and port 5062.

Entity Links Help ?

Edit New Duplicate Delete More Actions ▾

9 Items	Refresh										Filter: Enable
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes			
<input type="checkbox"/>	<a href="#">ASM-62_CM521_tg3_5061_TLS</a>	ASM-62	TLS	5061	CM521_tg3	5061	Trusted				
<input type="checkbox"/>	<a href="#">ASM-62_ModularMessaging_5060_TCP</a>	ASM-62	TCP	5060	ModularMessaging	5060	Trusted				
<input type="checkbox"/>	<a href="#">ASM-CM521_tg1</a>	ASM-62	TCP	5060	CM521_tg1	5060	Trusted				
<input type="checkbox"/>	<a href="#">ASM_to_CM</a>	ASM-62	TCP	5060	CM6.2	5060	Trusted				
<input type="checkbox"/>	<a href="#">CM-ES-VZ-5062</a>	ASM-62	TCP	5062	CM-Evolution-proc-5062	5062	Trusted				
<input type="checkbox"/>	<a href="#">CM-ES-VZ-5063</a>	ASM-62	TCP	5063	CM-Evolution-proc-5063	5063	Trusted				VZ IPCC
<input type="checkbox"/>	<a href="#">Sipera-SBC-1</a>	ASM-62	TCP	5060	Avaya-SBCE-1	5060	Trusted				SBC-Outside-2222
<input type="checkbox"/>	<a href="#">Sipera-SBC-2</a>	ASM-62	TCP	5060	Avaya-SBCE-2	5060	Trusted				SBC-Outside-1112
<input type="checkbox"/>	<a href="#">Sipera-SBC-3</a>	ASM-62	TCP	5060	Avaya-SBCE-3	5060	Trusted				SBC outside 1112

Select : All, None

## 5.6. Time Ranges

To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the “24/7” range since time-based routing was not the focus of these Application Notes. Click the **Commit** button after changes are completed.

Home / Elements / Routing / Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions ▾

2 Items	Refresh										Filter
<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	<a href="#">24/7</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7
<input type="checkbox"/>	<a href="#">Anytime</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	24/7

## 5.7. Routing Policies

To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click the **Commit** button after changes are completed.

The following screen shows the **Routing Policy Details** for the policy named “ASM to CM521” associated with incoming calls from Verizon IP Trunk to Communication Manager. Observe the **SIP Entity as Destination** is the entity named “CM521\_tg1” which uses the Communication Manager processor Ethernet IP Address (10.80.140.180).

Routing Policy Details

Commit

Cancel

General

\* Name:

ASM to CM521

Disabled:

☐

\* Retries:

0

Notes:

inbound VZ to CM521

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM521_tg1	10.80.140.180	CM	

The following screen shows the **Routing Policy Details** for the policy named “Avaya-SBCE-3-to-Verizon” associated with outgoing calls from Communication Manager to the PSTN via Verizon through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named “Avaya-SBCE-3”.

Routing Policy Details

Commit

Cancel

General

\* Name:

Avaya-SBCE-3-to Verizon

Disabled:

☐

\* Retries:

0

Notes:

outbound to verizon via Sipera-3

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya-SBCE-3	10.64.91.150	SIP Trunk	Sipera-SBC-3 outside 1.1.1.2 using adaptation

## 5.8. Dial Patterns

To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

### 5.8.1 Inbound Call Dial Pattern

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Verizon IP Trunk service, such as 732-945-0233, Verizon delivers the number to the enterprise, and the Avaya SBCE sends the call to Session Manager. The pattern below matches on 732-945-023. Dial patterns can alternatively match on ranges of numbers (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named “ASM to CM521” is selected, which sends the call to Communication Manager using port 5062 as described previously. In the configuration, calls to this number from **Originating Location Name** “Avaya-SBCE-3”, are routed to Communication Manager.

[Home](#) / [Elements](#) / [Routing](#) / [Dial Patterns](#)

Dial Pattern Details

[Help ?](#)

Commit

Cancel

General

\* Pattern:

732945023

\* Min:

10

\* Max:

10

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Avaya-SBCE-3	Avaya SBCE-3	ASM to CM521	0	<input type="checkbox"/>	CM521_tg1	inbound VZ to CM521

## 5.8.2 Outbound Call Dial Pattern

The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 9-1-XXX-XXX-XXXX, Communication Manager sends the call to Session Manager. Session Manager will match the dial pattern shown below and send the call to the Avaya SBCE-3 via the **Routing Policy Name** “Avaya-SBCE-3-to-Verizon”.

**General**

\* Pattern:

1

\* Min:

11

\* Max:

11

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

**Originating Locations and Routing Policies**

AddRemove

2 Items Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CM521	CM 5.2.1	Avaya-SBCE-3 -to Verizon	0	<input type="checkbox"/>	Avaya-SBCE-3	outbound to verizon via Sipera -3



## 6. Avaya Session Border Controller for Enterprise

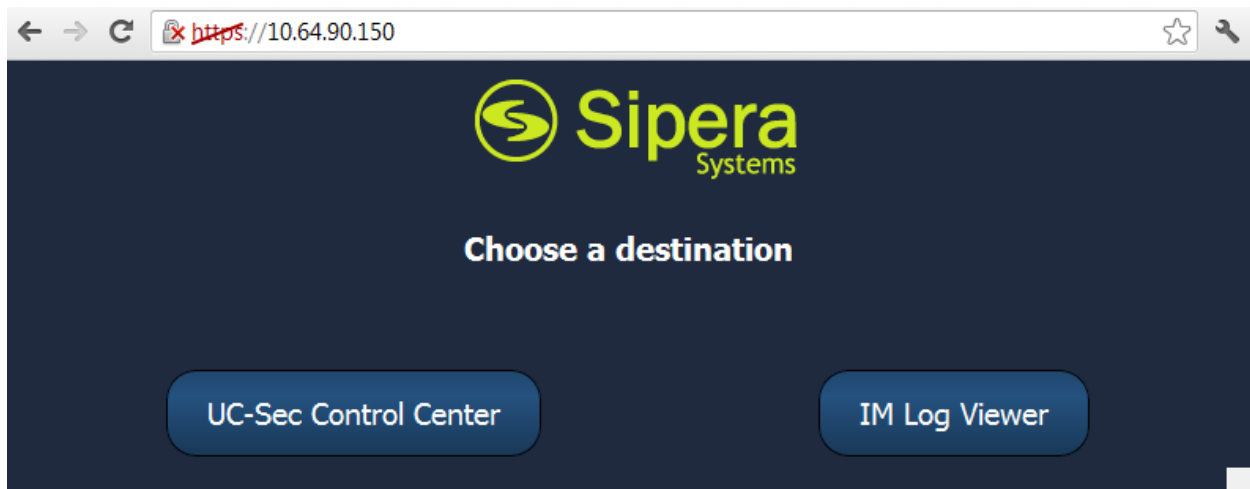
In the sample configuration, an Avaya Session Border Controller for Enterprise is used as the edge device between the Avaya CPE and Verizon Business.

These Application Notes assume that the installation of the SBCE and the assignment of a management IP Address have already been completed.

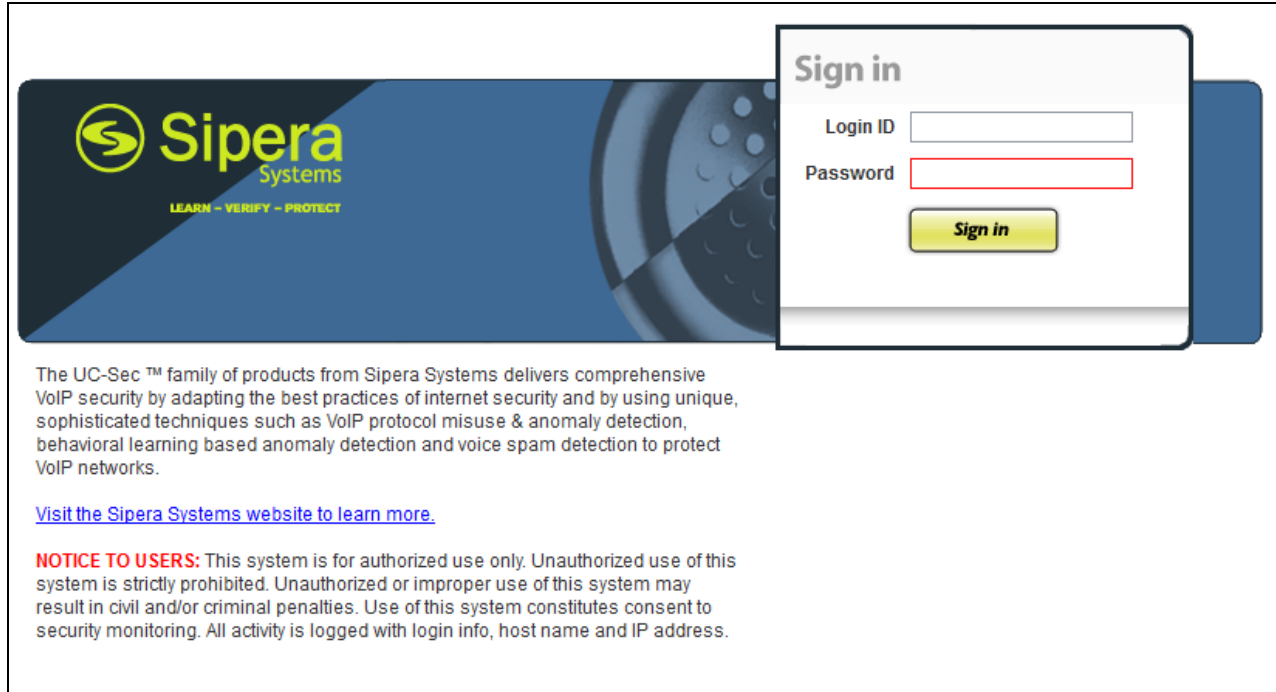
**Note** – The following Sections describe the provisioning of the Primary SBCE. The configuration of the Secondary SBCE is identical unless otherwise noted (e.g. IP addressing).

### 6.1. Access the Management Interface

In the sample configuration, the management IP is 10.64.90.150. Access the web management interface by entering <https://<ip-address>> where <ip-address> is the management IP address assigned during installation. Select **UC-Sec Control Center**.



A log in screen is presented. Enter an appropriate **Login ID** and **Password**.



The login screen features the Sipera Systems logo on the left, which includes a green circular icon with a stylized 'S' and the text 'Sipera Systems' and 'LEARN - VERIFY - PROTECT'. On the right is a 'Sign in' form with fields for 'Login ID' and 'Password', and a yellow 'Sign in' button. Below the form, there is a paragraph of text about the UC-Sec family of products, a link to the Sipera Systems website, and a 'NOTICE TO USERS' section.

**Sign in**

Login ID

Password

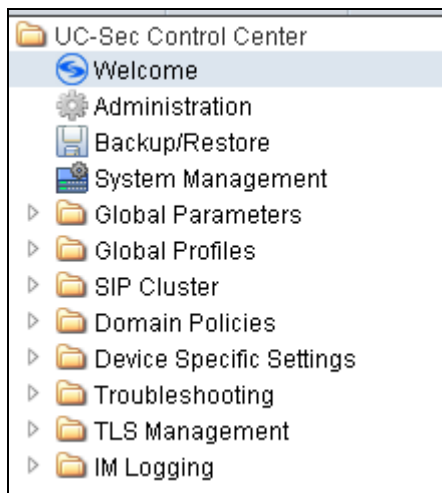
**Sign in**

The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Sipera Systems website to learn more.](#)

**NOTICE TO USERS:** This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

Once logged in, a UC-Sec Control Center screen will be presented. The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.



## 6.2. Global Profiles – Server Interworking

Select **Global Profiles** → **Server Interworking** from the left-side menu as shown below.



### 6.2.1 Server Interworking - Avaya

Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “Avaya” shown below. Click **Next**.



The following screens illustrate the “General” parameters used in the sample configuration for the Interworking Profile named “Avaya”. Most parameters retain default values. In the sample configuration, **T.38 support** was checked (optional), and **Hold Support** was set for None.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<div>Back Next</div>	

Click **Next** (not shown) to advance to configure Privacy and DTMF General parameters, which can retain default values. The following screen shows the complete **General** tab used in the sample configuration for interworking profile named “Avaya.”

		Rename Profile	Clone Profile	Delete Profile
Click here to add a description.				
<div> <div>General</div> <div>Timers</div> <div>URI Manipulation</div> <div>Header Manipulation</div> <div>Advanced</div> </div>				
<b>General</b>				
Hold Support	RFC3264			
180 Handling	None			
181 Handling	None			
182 Handling	None			
183 Handling	None			
Refer Handling	No			
3xx Handling	No			
Diversion Header Support	No			
Delayed SDP Handling	No			
T.38 Support	Yes			
URI Scheme	SIP			
Via Header Format	RFC3261			
<b>Privacy</b>				
Privacy Enabled	No			
User Name				
P-Asserted-Identity	No			
P-Preferred-Identity	No			
Privacy Header				
<b>DTMF</b>				
DTMF Support	None			

The following screen illustrates the **Advanced Settings** configuration. The “Topology Hiding: Change Call-ID” defaults to Yes, but was changed in the test configuration to allow for easier correlation of data. This setting in this field is at the discretion of the user. Both settings were tested. All other parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

General	Timers	URI Manipulation	Header Manipulation	Advanced
<b>Advanced Settings</b>				
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	
SLiC 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	
<b>Edit</b>				

## 6.2.2 Server Interworking – Verizon IP Trunk

Click the **Add Profile** button (not shown) to add a new profile or select an existing interworking profile. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as “Verizon” shown below. Click **Next**.

Interworking Profile	
Profile Name	Verizon
<b>Next</b>	

The following screens illustrate the “General” parameters used in the sample configuration for the Interworking Profile named “Verizon”. Most parameters retain default values. In the sample

configuration, **T.38 support** was set to “Yes”, **Hold Support** was set for RFC3264, all other fields retained default values.

General	Timers	URI Manipulation	Header Manipulation	Advanced
<b>General</b>				
Hold Support		RFC3264		
180 Handling		None		
181 Handling		None		
182 Handling		None		
183 Handling		None		
Refer Handling		No		
3xx Handling		No		
Diversion Header Support		No		
Delayed SDP Handling		No		
T.38 Support		Yes		
URI Scheme		SIP		
Via Header Format		RFC3261		
<b>Privacy</b>				
Privacy Enabled		No		
User Name				
P-Asserted-Identity		No		
P-Preferred-Identity		No		
Privacy Header				
<b>DTMF</b>				
DTMF Support		None		
<a href="#">Edit</a>				

The following screen illustrates the **Advanced Settings** configuration. All parameters shown are default values. Note that the default configuration will result in Record-Route headers in SIP messages.

General	Timers	URI Manipulation	Header Manipulation	Advanced
<b>Advanced Settings</b>				
Record Routes				BOTH
Topology Hiding: Change Call-ID				Yes
Call-Info NAT				Yes
Change Max Forwards				Yes
Include End Point IP for Context Lookup				No
OCS Extensions				No
AVAYA Extensions				No
NORTEL Extensions				No
SLiC 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
<a href="#">Edit</a>				

## 6.3. Global Profiles – Routing

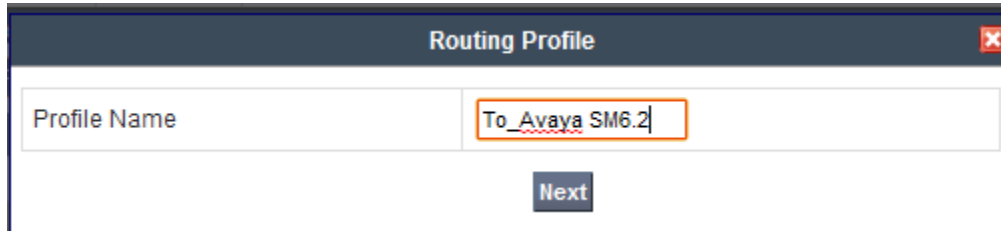
Select **Global Profiles** → **Server Configuration** from the left-side menu as shown below.





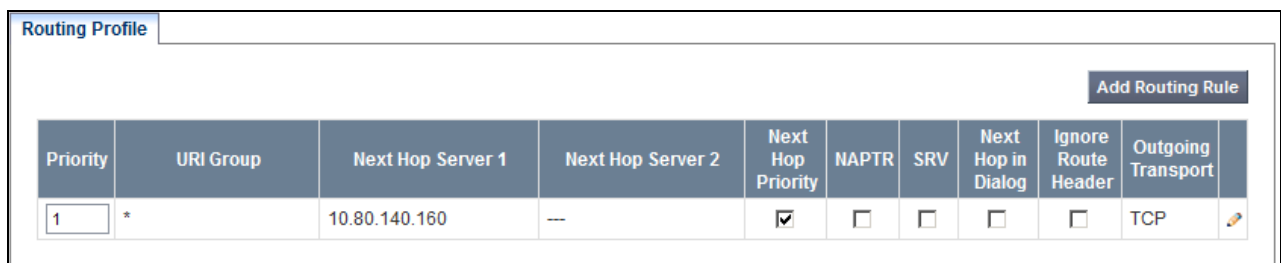
### 6.3.1 Routing Configuration for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as “To\_Avaya\_SM6.2” shown below. Click **Next**.




The screenshot shows a 'Routing Profile' window with a title bar containing a close button. Inside, there is a 'Profile Name' label followed by a text input field containing 'To\_Avaya SM6.2'. Below the input field is a 'Next' button.

For the **Next Hop Routing**, enter the IP Address of the Session Manager SIP signaling interface as **Next Hop Server 1**, as shown below. Check **Next Hop Priority**. Choose **TCP** for **Outgoing Transport**.

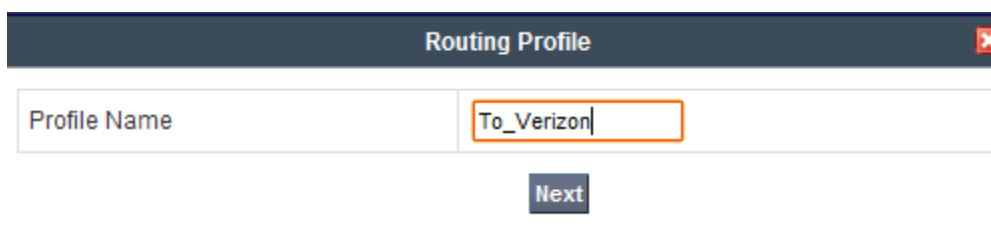


The screenshot shows a 'Routing Profile' window with a title bar containing a close button. Below the title bar is a tab labeled 'Routing Profile'. To the right of the tab is an 'Add Routing Rule' button. Below this is a table with the following columns: Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, Outgoing Transport, and an edit icon. The first row of the table contains the following values: 1, \*, 10.80.140.160, ---, ☒, ☐, ☐, ☐, ☐, TCP, and an edit icon.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	10.80.140.160	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP	

### 6.3.2 Routing Configuration for Verizon IP Trunk

Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as “To\_Verizon” shown below. Click **Next**.



The screenshot shows a 'Routing Profile' window with a title bar containing a close button. Inside, there is a 'Profile Name' label followed by a text input field containing 'To\_Verizon'. Below the input field is a 'Next' button.

For the **Next Hop Routing**, enter the IP Address of the Verizon SIP signaling interface as **Next Hop Server 1**, as shown below. Check **Next Hop Priority**. Choose **UDP** for **Outgoing Transport**.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	172.30.209.21:5071	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

### 6.3.3 Topology Hiding for Session Manager

The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

Click the **Add Profile** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as “Avaya” shown below. Click **Next**.

Topology Hiding Profile	
Profile Name	Avaya
Next	

In the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

If it is desired to ensure that the domain received by Session Manager from the SBCE is the expected enterprise domain, select “Overwrite” as the **Replace Action** for the To, From, and Request-Line headers. Enter the enterprise domain in the **Overwrite Value** column as shown below. In the example below, the domain received by Session Manager is changed by the SBCE to “avayalab.com”. Click **Finish**.

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

**Finish**

After configuration is completed, the Topology Hiding for profile “Avaya” will appear as follows.

Topology Hiding				
Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Overwrite	avayalab.com	
Via	IP/Domain	Auto	---	
From	IP/Domain	Overwrite	avayalab.com	
Request-Line	IP/Domain	Overwrite	avayalab.com	
SDP	IP/Domain	Auto	---	
Record-Route	IP/Domain	Auto	---	

### 6.3.4 Topology Hiding for Verizon IP Trunk

Click the **Add Profile** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as “Verizon” shown below. Click **Next**.

**Topology Hiding Profile**

Profile Name:

**Next**

Again, in the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers. The default “Auto” behaviors are sufficient. Click **Finish**.

Edit Topology Hiding Profile ✕

Add Header

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

Finish

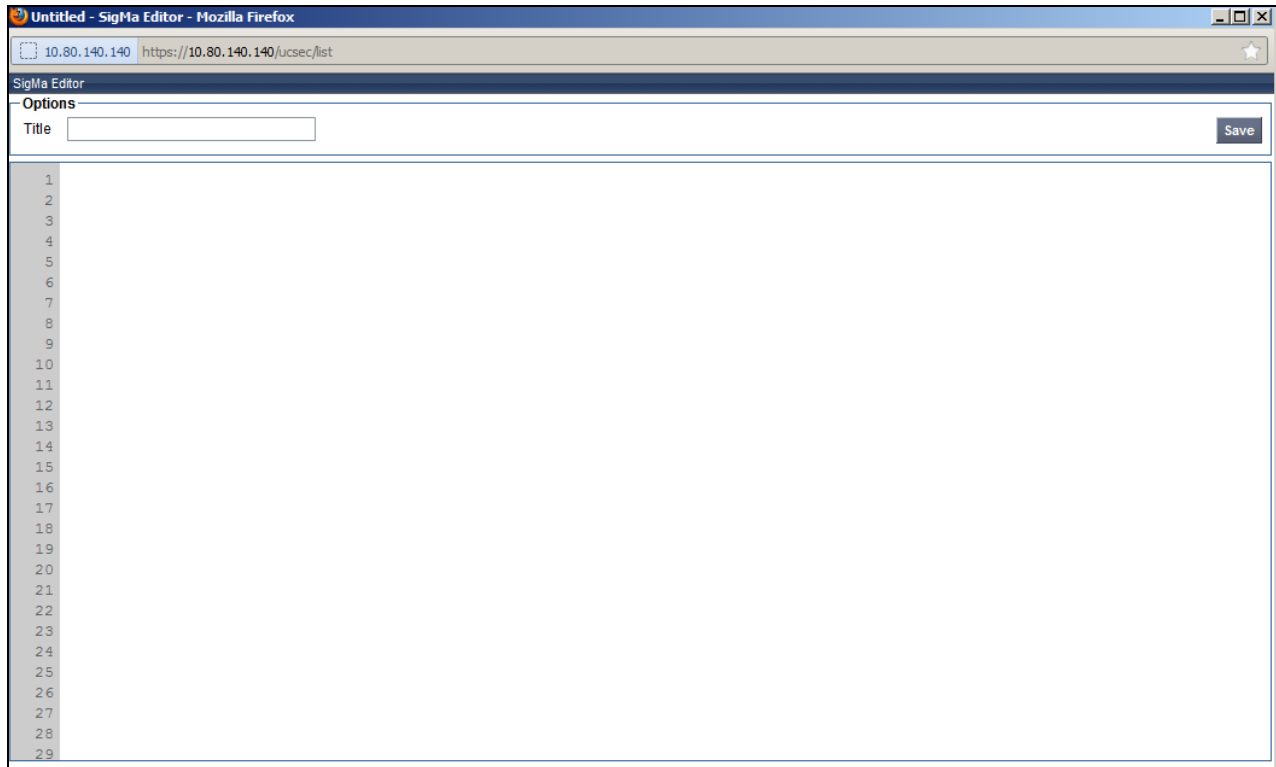
After configuration is completed, the **Topology Hiding** for profile “Verizon” will appear as follows.

<b>Topology Hiding</b>				
Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Auto	---	
Via	IP/Domain	Auto	---	
From	IP/Domain	Auto	---	
Request-Line	IP/Domain	Auto	---	
Record-Route	IP/Domain	Auto	---	

### 6.3.5 Signaling Manipulation

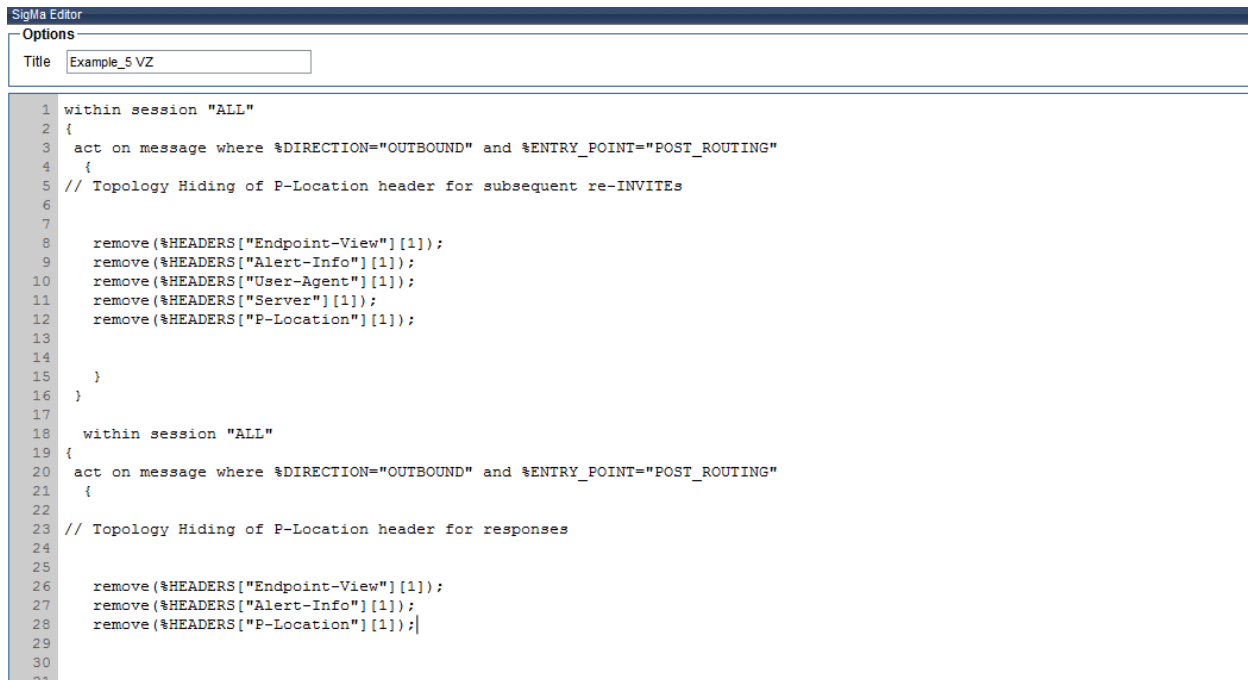
This feature adds the ability to add, change and delete any of the headers and other information in a SIP message. The feature will add the ability to configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language.

Click the **Add Script** button (not shown) to add a new script, or select an existing script to edit. If adding a script, a screen such as the following is displayed. Enter a title in the upper left and then enter the text to manipulate headers and click **Save**.



The screenshot shows a web browser window titled "Untitled - SigMa Editor - Mozilla Firefox". The address bar displays "10.80.140.140" and "https://10.80.140.140/ucsec/ist". The application interface includes a "SigMa Editor" header, an "Options" section with a "Title" input field and a "Save" button, and a large text area for scripting. The text area is numbered from 1 to 29 on the left side.

In 6.2, there are two proprietary headers (P-Location and Endpoint View) and one standard header (Alert-Info) that contain internal information and that are not applicable to a service provider that need to be stripped. These headers were stripped with a Sigma script and applied in the server configuration section. The script “Example\_5 VZ” is shown here. This script will be applied in the next section, ‘Server Configuration’.



The screenshot shows the Sigma Editor window with a title bar 'Sigma Editor'. Below the title bar is a tab labeled 'Options'. Under 'Options', there is a 'Title' field containing 'Example\_5 VZ'. The main area of the editor displays a script with line numbers 1 through 31. The script is divided into two sections, each starting with 'within session "ALL"'. The first section (lines 1-16) is for 'OUTBOUND' messages and removes headers 'Endpoint-View', 'Alert-Info', 'User-Agent', 'Server', and 'P-Location'. The second section (lines 18-29) is also for 'OUTBOUND' messages and removes headers 'Endpoint-View', 'Alert-Info', and 'P-Location'.

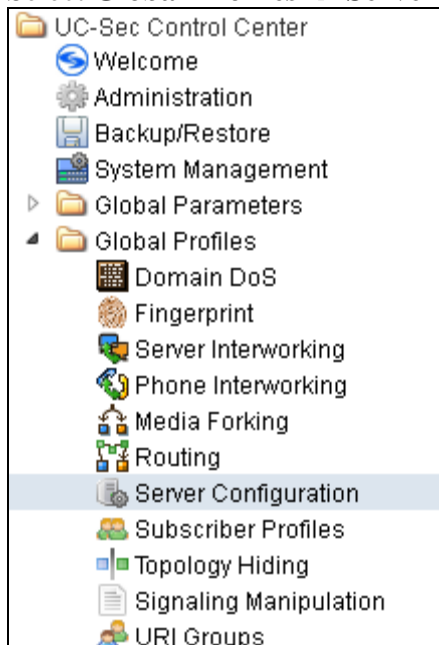
```

1  within session "ALL"
2  {
3    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4    {
5      // Topology Hiding of P-Location header for subsequent re-INVITES
6
7
8      remove(%HEADERS["Endpoint-View"][1]);
9      remove(%HEADERS["Alert-Info"][1]);
10     remove(%HEADERS["User-Agent"][1]);
11     remove(%HEADERS["Server"][1]);
12     remove(%HEADERS["P-Location"][1]);
13
14
15   }
16 }
17
18 within session "ALL"
19 {
20   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
21   {
22
23     // Topology Hiding of P-Location header for responses
24
25
26     remove(%HEADERS["Endpoint-View"][1]);
27     remove(%HEADERS["Alert-Info"][1]);
28     remove(%HEADERS["P-Location"][1]);
29
30
31

```

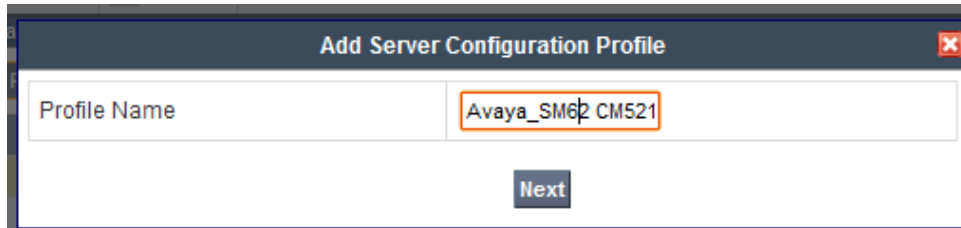
## 6.4. Global Profiles – Server Configuration

Select **Global Profiles** → **Server Configuration** from the left-side menu as shown below.



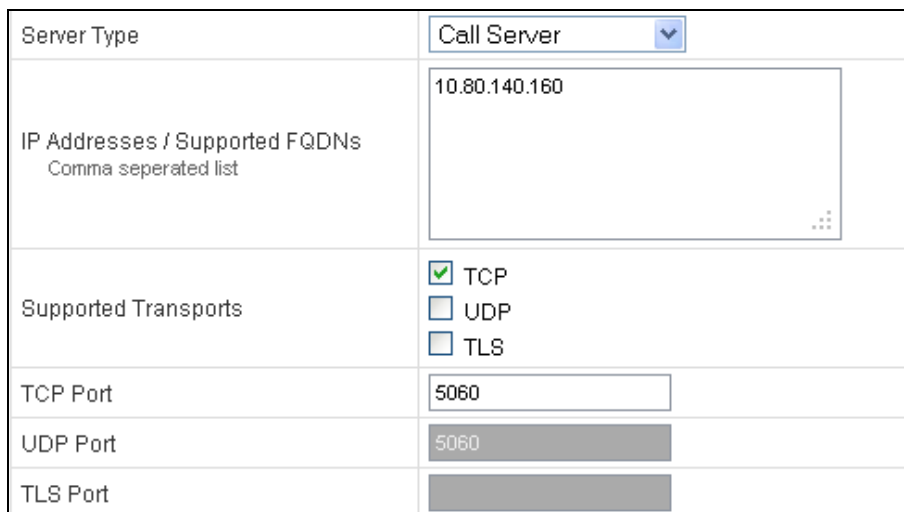
### 6.4.1 Server Configuration for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as “Avaya\_SM62 CM521” shown below. Click **Next**.



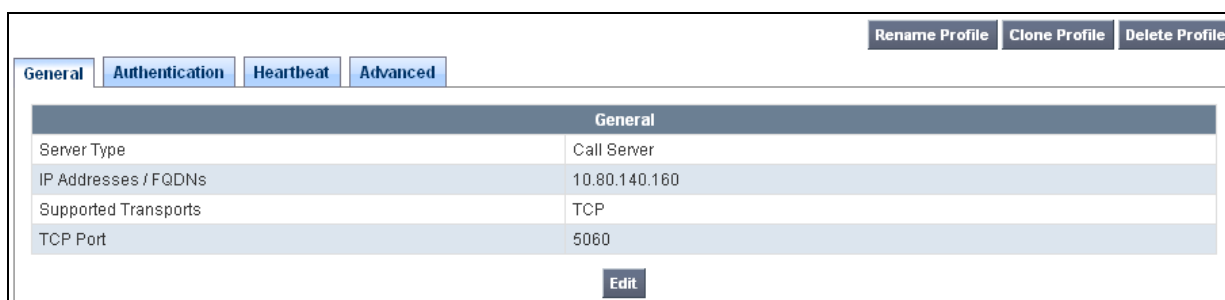
The screenshot shows a dialog box titled "Add Server Configuration Profile". It has a "Profile Name" input field containing the text "Avaya\_SM62 CM521". Below the input field is a "Next" button.

The following screens illustrate the Server Configuration with Profile name “Avaya\_SM”. In the “General” parameters, select “Call Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface in the sample configuration is entered. This IP Address is 10.80.140.160. In the **Supported Transports** area, TCP is selected, and the **TCP Port** is set to 5060. This configuration corresponds with the Session Manager entity link configuration for the entity link to the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.



The screenshot shows the "General" configuration tab for the "Avaya\_SM62 CM521" profile. The "Server Type" is set to "Call Server". The "IP Addresses / Supported FQDNs" field contains the IP address "10.80.140.160". The "Supported Transports" section shows "TCP" selected. The "TCP Port" is set to "5060".

Once configuration is completed, the **General** tab for “Avaya\_SM62 CM521” will appear as shown below.



The screenshot shows the "General" configuration tab for the "Avaya\_SM62 CM521" profile. The "Server Type" is set to "Call Server". The "IP Addresses / FQDNs" field contains the IP address "10.80.140.160". The "Supported Transports" section shows "TCP" selected. The "TCP Port" is set to "5060". An "Edit" button is visible at the bottom.

If adding the profile, click **Next** to accept default parameters for the Authentication tab, and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click edit.

The SBC can be configured to source “heartbeats” in the form of SIP OPTIONS. If SBC-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select “OPTIONS” from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC toward Session Manager. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@10.64.91.150
To URI	ping@10.80.140.160
TCP Probe	<input checked="" type="checkbox"/>
TCP Probe Frequency	10 seconds
Finish	

If SBC sourced OPTIONS are configured, the **Heartbeat** tab for “Avaya\_SM62 CM521” will appear as shown below.

Avaya_SM62 CM521	
<a href="#">Rename Profile</a> <a href="#">Clone Profile</a> <a href="#">Delete Profile</a>	
<a href="#">General</a> <a href="#">Authentication</a> <a href="#">Heartbeat</a> <a href="#">Advanced</a>	
Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@10.64.91.150
To URI	ping@10.80.140.160
TCP Probe	<input checked="" type="checkbox"/>
TCP Probe Frequency	10 seconds
Edit	



If adding a profile, click **Next** to continue to the “Advanced” settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** “Avaya” created previously. Click **Finish**.

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<input type="button" value="Finish"/>	

Once configuration is completed, the **Advanced** tab for “Avaya\_SM62 CM521” will appear as shown below.

Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
TCP Connection Type	SUBID

## 6.4.2 Server Configuration for Verizon IP Trunk

Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as “Verizon SIP Trunk” shown below. Click **Next**.

Add Server Configuration Profile	
Profile Name	Verizon SIP Trunk
<input type="button" value="Next"/>	

The following screens illustrate the Server Configuration with Profile name “Verizon SIP Trunk”. In the “General” parameters, select “Trunk Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the Verizon-provided Verizon IP Trunk IP Address is

entered. This IP Address is 172.30.209.21. In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to 5071.

Add Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	172.30.209.21
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5071
TLS Port	
<div>Back Next</div>	

If adding the profile, click **Next** to accept default parameters for the Authentication tab, and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click edit.

The SBC can be configured to source “heartbeats” in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the SBC is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends SIP OPTIONS to the inside private IP Address of the SBC, the SBC will send SIP OPTIONS to Verizon. When Verizon responds, the SBC will pass the response to Session Manager.

If SBC-sourced OPTIONS are desired, select “OPTIONS” from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.

Edit Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@1.1.1.2
To URI	ping@172.30.209.21
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
Finish	

If the optional SBC sourced OPTIONS configuration is completed, the **Heartbeat** tab for “Verizon SIP Trunk” will appear as shown below.

Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@1.1.1.2
To URI	ping@172.30.209.21
TCP Probe	<input type="checkbox"/>

Edit

If adding a profile, click **Next** to continuing to the “Advanced” settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** “Verizon” created previously, and Signaling Manipulation Script will be the script shown in the previous section titled “Example\_5VZ”. Other SBC features, such as DoS Protection and Grooming, can be configured according to customer preference. Click **Finish**.

Edit Server Configuration Profile - Advanced
✕

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Verizon ▼
Signaling Manipulation Script	Example_5 VZ ▼
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Finish

Once configuration is completed, the **Advanced** tab for “Verizon SIP Trunk” will appear as shown below.

Rename Profile

Clone Profile

Delete Profile

General

Authentication

Heartbeat

Advanced

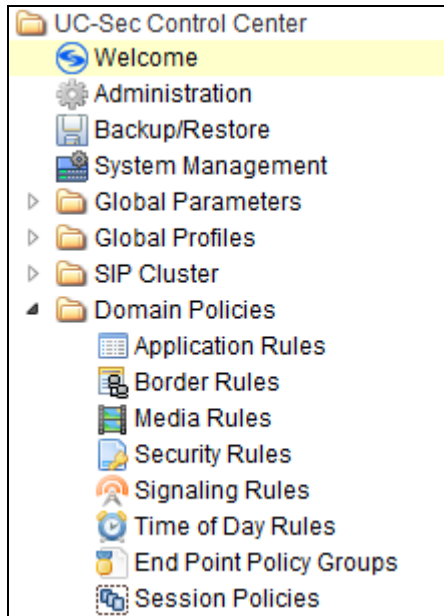
Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Verizon
Signaling Manipulation Script	Example_5 VZ
UDP Connection Type	SUBID

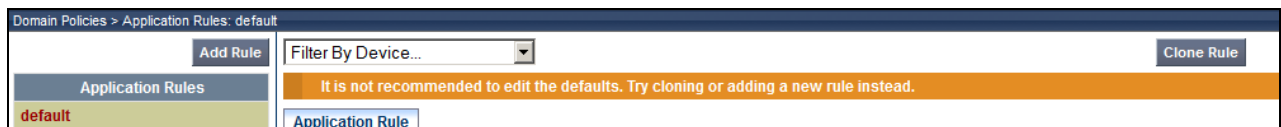
Edit

## 6.5. Domain Policies – Application Rule

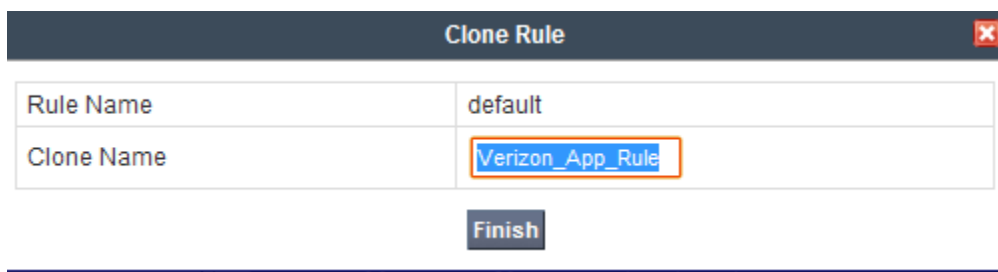
Select **Domain Policies** → **Application Rules** from the left-side menu as shown below.



In the sample configuration, a single application rule was created by cloning the default rule called “default”. Select the default rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “Verizon\_App\_Rule” as shown below. Click **Finish**.



Select the newly created rule and click the **Edit** button (not shown). In the resulting screen, change the default **Maximum Concurrent Sessions** to 2000, the **Maximum Session per Endpoint** to 2000. Click **Finish**.

Application Rule				
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		
Miscellaneous				
CDR Support	None			
IM Logging	No			
RTCP Keep-Alive	No			

## 6.6. Domain Policy – Media Rules

In the sample configuration, a single media rule was created by cloning the default rule called “default-low-med”. Select the default-low-med rule and click the **Clone Rule** button.

Domain Policies > Media Rules: default-low-med

**Add Rule**  **Clone Rule**

**Media Rules**

**default-low-med**

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

**Media NAT** **Media Encryption** **Media Anomaly** **Media Silencing** **Media QoS** **Tuning Test**

Enter a name in the **Clone Name** field, such as “default-low-med-QoS” as shown below. Click **Finish**.

Clone Rule

Rule Name

default-low-med

Clone Name

default-low-med-QoS

Finish

Select the newly created rule, select the **Media QoS** tab, and click the **Edit** button (not shown). In the resulting screen, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select “EF” for expedited forwarding as shown below. Click **Finish**.

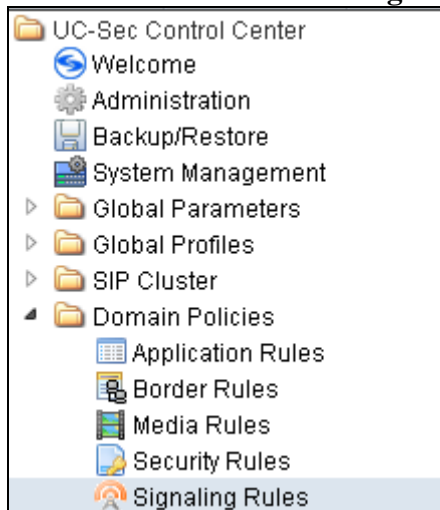
Media QoS			
<b>Media QoS Reporting</b>			
RTCP Enabled	<input type="checkbox"/>		
<b>Media QoS Marking</b>			
Enabled	<input checked="" type="checkbox"/>		
ToS			
Audio Precedence	Routine		000
Audio ToS	Minimize Delay		1000
Video Precedence	Routine		000
Video ToS	Minimize Delay		1000
DSCP			
Audio	EF		101110
Video	EF		101110
<b>Finish</b>			

When configuration is complete, the “default-low-med-QoS” media rule **Media QoS** tab appears as follows.

Domain Policies > Media Rules: default-low-med-QoS	
<div> Add Rule Filter By Device... Rename Rule Clone Rule Delete Rule </div> <div> Media Rules default-low-med default-low-med-enc default-high default-high-enc avaya-low-med-enc <b>default-low-med-QoS</b> test </div>	<div> Click here to add a description. </div> <div> Media NAT Media Encryption Media Anomaly Media Silencing <b>Media QoS</b> Turing Test </div> <div> <b>Media QoS Reporting</b> RTCP Enabled <input type="checkbox"/> </div> <div> <b>Media QoS Marking</b> Enabled <input checked="" type="checkbox"/> QoS Type DSCP </div> <div> <b>Audio QoS</b> Audio DSCP EF </div> <div> <b>Video QoS</b> Video DSCP EF </div>

## 6.7. Domain Policies – Signaling Rules

Select **Domain Policies** → **Signaling Rules** from the left-side menu as shown below.



Click the Add Rule button to add a new signaling rule. In the Rule Name field, enter an appropriate name, such as “Block\_Hdr\_Remark”.

Signaling Rule	
Rule Name	Block_Hdr_Remark
<b>Next</b>	

In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down menu. In the sample configuration, “AF32” was selected for “Assured Forwarding 32.” Click **Finish** (not shown).

Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
	Precedence	Routine	000
	ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Value	AF32	011100



After this configuration, the new “Block\_Hdr\_Remark” will appear as follows.

Domain Policies > Signaling Rules: Block\_Hdr\_Remark

Filter By Device... [v] [Rename Rule] [Clone Rule] [Delete Rule]

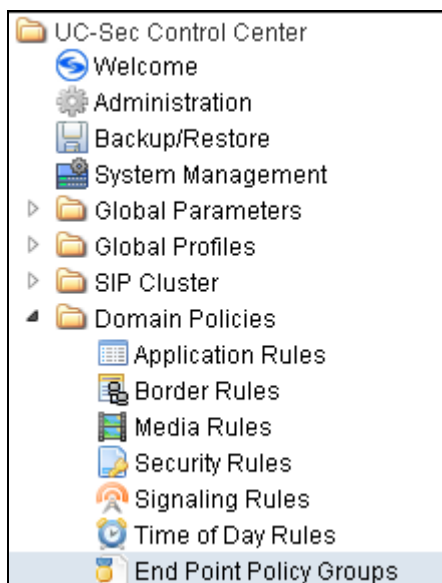
Click here to add a description.

General Requests Responses Request Headers Response Headers Signaling QoS

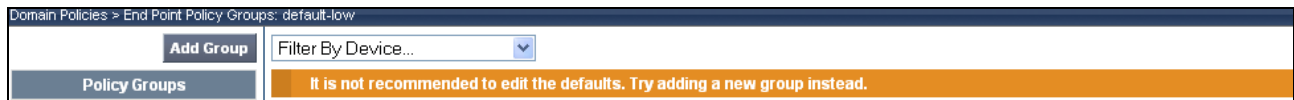
Signaling QoS	<input checked="" type="checkbox"/>
QoS Type	DSCP
DSCP	AF32

## 6.8. Domain Policies – End Point Policy Groups

Select **Domain Policies** → **End Point Policy Groups** from the left-side menu as shown below.



Select the **Add Group** button.



Enter a name in the **Group Name** field, such as “default-low-remark” as shown below. Click **Next**.

**Policy Group**

Group Name default-low-remark

Next

In the sample configuration, defaults were selected for all fields, with the exception of the **Application Rule** which was set to “Verizon\_App\_Rule”, **Media Rule** which was set to “default-low-med-QoS”, and the **Signaling Rule**, which was set to “Block\_Hdr\_Remark” as shown below. The selected non-default media rule and signaling rule chosen were created in previous sections. Click **Finish**.

**Edit Policy Set**

Application Rule	Verizon_App_Rule
Border Rule	default
Media Rule	default-low-med-QoS
Security Rule	default-low
Signaling Rule	Block_Hdr_Remark
Time of Day Rule	default

Finish

Once configuration is completed, the “default-low-remark” policy group will appear as follows.

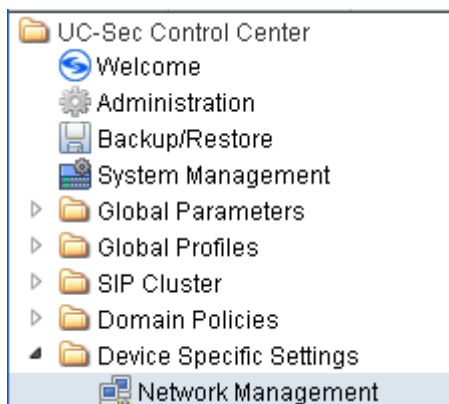
Policy Group

View Summary
Add Policy Set

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	Verizon_App_Rule	default	default-low-med-QoS	default-low	Block_Hdr_Remark	default		

## 6.9. Device Specific Settings - Network Management

Select **Device Specific Setting** → **Network Management** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named “ASBCE-3” in the sample configuration (not shown). The **Network Configuration** tab is shown below. Observe the **IP Address**, **Netmask**, **Gateway**, and **Interface** information previously assigned.

Network Configuration
Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask  
255.255.255.0

A2 Netmask

B1 Netmask  
255.255.255.0

B2 Netmask

Add IP
Save Changes
Clear Changes

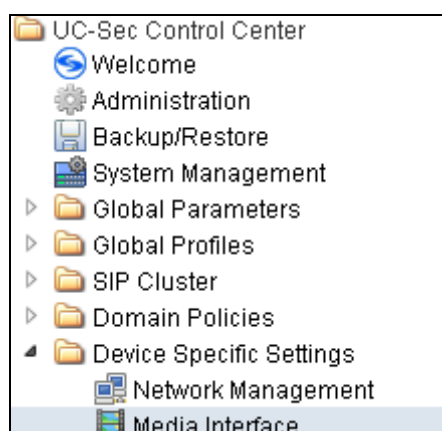
IP Address	Public IP	Gateway	Interface	
10.64.91.150		10.64.91.1	A1	✗
1.1.1.2		1.1.1.1	B1	✗

Select the **Interface Configuration** tab. The Administrative Status can be toggled between “Enabled” and “Disabled” in this screen. The following screen was captured after the interfaces had already been enabled. To enable the interface if it is disabled, click the **Toggle State** button.

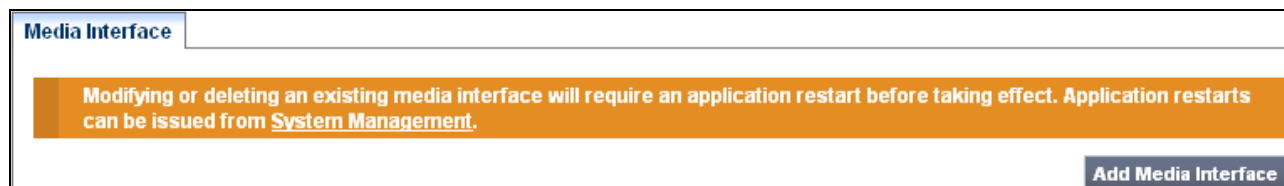
Network Configuration		Interface Configuration
Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

## 6.10. Device Specific Settings – Media Interface

Select **Device Specific Setting** → **Media Interface** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named “ASBCE-3” in the sample configuration (not shown). Select **Add Media Interface**.



Enter an appropriate **Name** for the media interface for the Avaya CPE and select the inside private IP Address from the **IP Address** drop-down menu. In the sample configuration, “Avaya\_Int\_Media” is chosen as the name, and the “inside” IP Address of the SBCE is “10.64.91.150”. For the **Port Range**, default values are shown. Click **Finish**.

Edit Media Interface	
Name	Avaya_Int_Media
IP Address	10.64.91.150
Port Range	35000 - 40000
<input type="button" value="Finish"/>	

Once again, select **Add Media Interface**. Enter an appropriate **Name** for the media interface for the public “outside” of the SBC, and select the outside public IP Address from the **IP Address** drop-down menu. In the sample configuration, “Ext\_Media\_to\_Verizon” is chosen as the name, and the “outside” public IP Address of the SBC is “1.1.1.2”. For the **Port Range**, default values are shown. Verizon IP Trunk does not require that the RTP ports be chosen within a specific range. Click **Finish**.

Edit Media Interface	
Name	Ext_Media_to_Verizon
IP Address	1.1.1.2
Port Range	35000 - 40000
<input type="button" value="Finish"/>	

The resultant Media Interface configuration used in the sample configuration is shown below.

Media Interface				
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from <a href="#">System Management</a> .				
<input type="button" value="Add Media Interface"/>				
Name	Media IP	Port Range		
Avaya_Int_Media	10.64.91.150	35000 - 40000		
Ext_Media_to_Verizon	1.1.1.2	35000 - 40000		

## 6.11. Device Specific Settings – Signaling Interface

Select **Device Specific Setting** → **Signaling Interface** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named “ASBCE-3” in the sample configuration (not shown). Select **Add Signaling Interface**.

In the Add Signaling Interface screen, enter an appropriate **Name** (e.g., “Sig\_Inside\_to\_Avaya”) for the “inside” private interface, and choose the private inside IP Address (e.g., 10.64.91.150) from the **IP Address** drop-down menu. Choose **TCP Port** “5060” since TCP and port 5060 is used between Session Manager and the ASBC in the sample configuration. Click **Finish**.

Edit Signaling Interface

Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

Name	Sig_Inside_to_Avaya
IP Address	10.64.91.150
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	
Cluster TLS <small>Only for use with Cisco SIP Clusters</small>	<input type="checkbox"/>
Enable Stun <small>Requires a UDP Port</small>	<input type="checkbox"/>

Finish

Once again, select **Add Signaling Interface**. In the Add Signaling Interface screen, enter an appropriate **Name** (e.g., “Sig\_Outside\_to\_Verizon” for the “outside” public interface, and choose the public IP Address (e.g., 1.1.1.2) from the **IP Address** drop-down menu. Choose **UDP Port** “5060”. In the sample configuration, Verizon will send SIP signaling using UDP to the CPE IP Address 1.1.1.2 and to UDP Port 5060. Click **Finish**.

Edit Signaling Interface
✕

**Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.**

Name	Sig_Outside_to_Verizon
IP Address	1.1.1.2 ▼
TCP Port <small>Leave blank to disable</small>	<input type="text"/>
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	<input type="text"/>
Cluster TLS <small>Only for use with Cisco SIP Clusters</small>	<input type="checkbox"/>
Enable Stun <small>Requires a UDP Port</small>	<input type="checkbox"/>

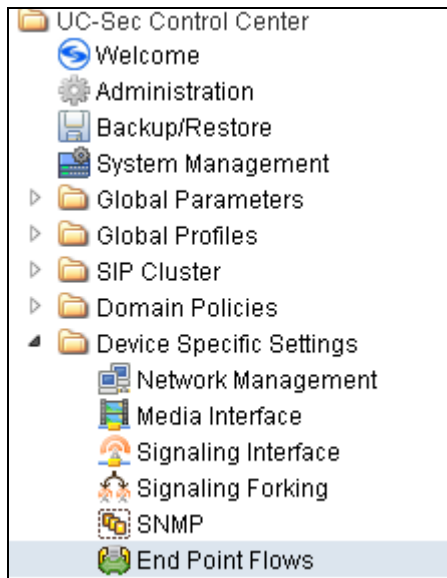
Finish

The following screen shows the signaling interfaces defined for the sample configuration.

Signaling Interface						
						Add Signaling Interface
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Inside_to_Avaya	10.64.91.150	5060	---	---	None	
Sig_Outside_to_Verizon	1.1.1.2	---	5060	---	None	

## 6.12. Device Specific Settings – End Point Flows

Select **Device Specific Setting** → **End Point Flows** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named “ASBCE-3” in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.





The following screen shows the flow named “Avaya\_SM” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: Avaya\_SM

Criteria	
Flow Name	Avaya_SM
Server Configuration	Avaya_SM6.2 CM521
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_to_Verizon
Signaling Interface	Sig_Inside_to_Avaya
Media Interface	Avaya_Int_Media
End Point Policy Group	default-low-remark
Routing Profile	To_Verizon
Topology Hiding Profile	Avaya
File Transfer Profile	None

Finish

Once again, select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named “SIP\_Trunk” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: SIP\_Trunk

Criteria	
Flow Name	SIP_Trunk
Server Configuration	Verizon SIP TRUNK
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside_to_Avaya
Signaling Interface	Sig_Outside_to_Verizon
Media Interface	Ext_Media_to_Verizon
End Point Policy Group	default-low-remark
Routing Profile	To_Avaya SM6.2
Topology Hiding Profile	Verizon
File Transfer Profile	None

Finish

The following screen summarizes the Server Flows configured in the sample configuration.

Subscriber Flows
Server Flows
Add Flow

Click here to add a row description.

Server Configuration: Avaya\_SM6.2 CM521

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Avaya_SM	*	*	*	Sig_Outside_to_Verizon	Sig_Inside_to_Avaya	Avaya_Int_Media	default-low-remark	To_Verizon	Avaya	None			

Server Configuration: Verizon SIP TRUNK

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	SIP_Trunk	*	*	*	Sig_Inside_to_Avaya	Sig_Outside_to_Verizon	Ext_Media_to_Verizon	default-low-remark	To_Avaya SM6.2	Verizon	None			

## 7. Verizon Business IP Trunk Services Suite Configuration

Information regarding Verizon Business IP Trunk Services suite offer can be found at <http://www.verizonbusiness.com/Products/communications/ip-telephony/> or by contacting a Verizon Business sales representative.

The reference configuration described in these Application Notes was located in the Avaya Solution and Interoperability Test Lab. Access to the Verizon Business IP Trunk Services suite was via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

### 7.1. Service Access Information

The following service access information (FQDN, IP addressing, ports, IP toll free numbers) was provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i>	<i>172.30.209.21</i>
<i>UDP port 5060</i>	<i>UDP Port 5071</i>

IP DID Numbers
732-945-0231
732-945-0232
732-945-0233
732-945-0234

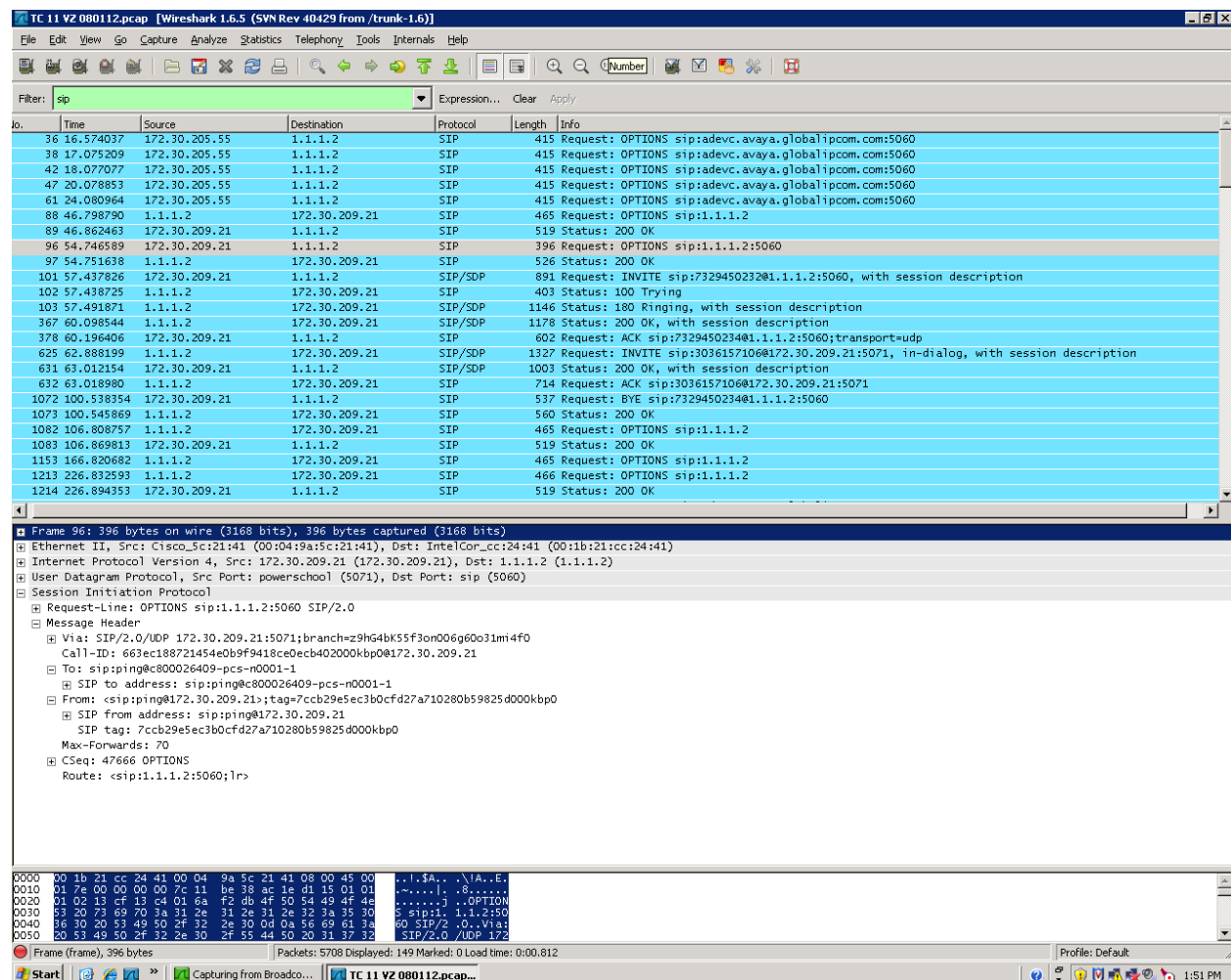
## 8. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) IP Trunk service.

### 8.1. Illustration of OPTIONS Handling

This section illustrates SIP OPTIONS monitoring of the SIP trunk from Avaya CPE to Verizon the CPE and from the CPE to Verizon through the Avaya Session Border Controller for Enterprise.

The following screens from a filtered Wireshark trace illustrate OPTIONS sent by Verizon to the Avaya CPE. Verizon IP Trunk service uses OPTIONS to determine whether the CPE is available to receive inbound calls. Therefore, proper OPTIONS response is necessary. In the trace shown below, taken from the outside public side of the SBCE, frame 96 is highlighted and expanded to show OPTIONS sent from Verizon IPC Trunk (172.30.209.21) to the SBCE (1.1.1.2). Observe the use of UDP for transport, from source port 5071 (Verizon) to destination port 5060 (Avaya). Verizon sends the Avaya domain “1.1.1.2” in the Request-Line. Note that Max-Forward is 70.



Before the SBCE replies to Verizon, the SBCE sends OPTIONS to Session Manager on the inside private interface. In the trace shown below, taken from the inside private side of the SBCE, frame 8 is highlighted and expanded to show OPTIONS sent from the inside interface of the SBCE (1.1.1.2) to Session Manager (10.80.140.160). Observe the use of UDP for transport, using port 5060. Observe that the SBCE has changed the Request-URI, From, and To headers per the previous configuration such that “avayalab.com” now appears. Note that Max-Forwards has been decremented by 1 and is now 69.

No.	Time	Source	Destination	Protocol	Length	Info
6	4.546602	172.30.205.55	1.1.1.2	SIP	415	Request: OPTIONS sip:adevc.avaya.globalipcom.com:5060
7	4.546890	1.1.1.2	172.30.205.55	SIP	376	Status: 403 Forbidden
8	4.896891	1.1.1.2	172.30.209.21	SIP	468	Request: OPTIONS sip:1.1.1.2
9	4.959934	172.30.209.21	1.1.1.2	SIP	523	Status: 200 OK
16	9.635651	1.1.1.2	172.30.209.21	SIP/SDF	1272	Request: INVITE sip:3035380026@172.30.209.21:5071, with session description
17	9.700557	172.30.209.21	1.1.1.2	SIP	334	Status: 100 Trying
23	12.191296	172.30.209.21	1.1.1.2	SIP/SDF	916	Status: 183 Session Progress, with session description
454	16.400228	172.30.209.21	1.1.1.2	SIP/SDF	941	Status: 200 OK, with session description
456	16.409092	1.1.1.2	172.30.209.21	SIP	669	Request: ACK sip:3035380026@172.30.209.21:5071
465	16.486621	1.1.1.2	172.30.209.21	SIP	997	Request: INVITE sip:3035380026@172.30.209.21:5071, in-dialog
479	16.623143	172.30.209.21	1.1.1.2	SIP/SDF	941	Status: 200 OK, with session description
481	16.630321	1.1.1.2	172.30.209.21	SIP/SDF	856	Request: ACK sip:3035380026@172.30.209.21:5071, with session description
3472	46.242160	1.1.1.2	172.30.209.21	SIP	553	Request: BYE sip:3035380026@172.30.209.21:5071
3479	46.303579	172.30.209.21	1.1.1.2	SIP	440	Status: 200 OK

Frame 8: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits)

Ethernet II, Src: IntelCor\_cc:24:41 (00:1b:21:cc:24:41), Dst: Cisco\_5c:21:41 (00:04:9a:5c:21:41)

Internet Protocol Version 4, Src: 1.1.1.2 (1.1.1.2), Dst: 172.30.209.21 (172.30.209.21)

User Datagram Protocol, Src Port: sip (5060), Dst Port: powerschool (5071)

Source port: sip (5060)

Destination port: powerschool (5071)

Length: 434

Checksum: 0x19c5 [validation disabled]

Session Initiation Protocol

Request-Line: OPTIONS sip:1.1.1.2 SIP/2.0

Message Header

From: <sip:ping@1.1.1.2:5060>;tag=2605c92cd0fb

SIP From address: sip:ping@1.1.1.2:5060

SIP tag: 2605c92cd0fb

To: <sip:ping@1.1.1.2>

SIP to address: sip:ping@1.1.1.2

Cseq: 65 OPTIONS

Call-ID: 1433245361c9ca359c0b9a2a4342cf5bshiepaertab

Contact: <sip:ping@1.1.1.2:5060;transport=udp>

Record-Route: <sip:1.1.1.2:5060;ipc-line=167;lr;transport=udp>

Max-Forwards: 69

Via: SIP/2.0/UDP 1.1.1.2:5060;branch=z9hG4bK-s1632-002089947211-1--s1632-

Accept: application/sdp

Content-Length: 0

In this same trace, frame 9 below shows Verizon responding to the OPTIONS with 200 OK. The receipt of a valid OPTIONS response from the CPE is necessary for Verizon to route inbound calls to the CPE. Since the SBCE proxies the OPTIONS received from Verizon to Session Manager, the end to end path from Verizon through to Session Manager must be in-service for OPTIONS (and ultimately calls) to be successful.

## 8.2. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

### 8.2.1 Example Incoming Call from PSTN via Verizon SIP Trunk

Incoming PSTN calls arrive from Verizon at Avaya ASBCE, which sends the call to Session Manager. In the sample configuration, when the ASBCE is in-service, Verizon sends all inbound calls to ASBCE-3. Session Manager sends the call to Communication Manager via the entity link corresponding to the Avaya Common Server using port 5062. On Communication Manager, the incoming call arrives via signaling group 1 and trunk group 1.

The following edited Communication Manager *list trace tac* trace output shows a call incoming on trunk group 1. The PSTN telephone dialed 732-945-0232. Session Manager can map the number received from Verizon to the extension of a Communication Manager telephone (x12203), or the incoming call handling table for trunk group 1 can do the same. In the trace below, Communication Manager had already mapped the Verizon DID to the Communication Manager extension. Extension 12203 is an IP Telephone with IP address 10.64.90.75 in Region 1. Initially, the G450 Media Gateway (10.64.90.112) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is “ip-direct” from the IP Telephone (10.64.90.75) to the “inside” of the Avaya SBCE (10.64.91.150).

list trace previous		Page	1
LIST TRACE			
time	data		
15:30:36	SIP<INVITE sip:7329450232@avayalab.com SIP/2.0		
15:30:36	Call-ID: d2dbca47c8812b411b41193fc677c650		
15:30:36	active trunk-group 1 member 1 cid 0x193		
15:30:36	SIP>SIP/2.0 180 Ringing		
15:30:36	Call-ID: d2dbca47c8812b411b41193fc677c650		
15:30:36	dial 12203		
15:30:36	ring station 12203 cid 0x193		
15:30:36	G711MU ss:off ps:20		
	rgn:1 [10.64.90.75]:2782		
	rgn:1 [10.64.90.112]:2056		
15:30:36	G711MU ss:off ps:20		
	rgn:10 [10.64.91.150]:35112		
	rgn:1 [10.64.90.112]:2052		
15:30:36	xoip options: fax:T38 modem:off tty:US uid:0x50112		
	xoip ip: [10.64.90.112]:2052		

The following screen shows **Page 2** of the output of the *status trunk* command pertaining to this same call. Note the signaling using port 5060 between Communication Manager and Session Manager. Note the media is “ip-direct” from the IP Telephone (10.64.90.75) to the inside IP address of SBCE (10.64.91.150) using G.711MU.

status trunk 1/1		Page 2 of 3
CALL CONTROL SIGNALING		
Near-end Signaling Loc: 01A0017		
Signaling	IP Address	Port
Near-end:	10.80.140.180	: 5060
Far-end:	10.80.140.160	: 5060
H.245 Near:		
H.245 Far:		
H.245 Signaling Loc:	H.245 Tunneled in Q.931? no	
Audio Connection Type: ip-direct		Authentication Type: None
Near-end Audio Loc:	Codec Type: G.711MU	
Audio	IP Address	Port
Near-end:	10.64.90.75	: 2782
Far-end:	10.64.91.150	: 35112
Video Near:		
Video Far:		
Video Port:		
Video Near-end Codec:		Video Far-end Codec:

## 8.2.2 Example Outgoing Calls to PSTN via Verizon IP Trunk

The following edited trace shows an outbound ARS call from IP Telephone x12204 to the PSTN number 9-303-538-0026. The call is routed to route pattern 1 and trunk group 1. The call initially uses the gateway (10.64.90.112), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (10.64.90.74) and the “inside” of the Avaya SBCE-3 (10.64.91.150).

## LIST TRACE

time	data
16:02:50	dial 93035380026 route:HNP ARS
16:02:50	route-pattern 1 preference 1 location 1/ALL cid 0x195
16:02:50	seize trunk-group 1 member 6 cid 0x195
16:02:50	Calling Number & Name 12204 IP 9641
16:02:50	SIP>INVITE sip:3035380026@avayalab.com SIP/2.0
16:02:50	Call-ID: 0c461a560f0e1175b503f896600
16:02:50	Setup digits 3035380026
16:02:50	Calling Number & Name 7329450233 IP 9641
16:02:50	SIP<SIP/2.0 100 Trying
16:02:50	Call-ID: 0c461a560f0e1175b503f896600
16:02:50	Proceed trunk-group 1 member 6 cid 0x195
16:02:53	SIP<SIP/2.0 183 Session Progress
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
16:02:53	G711MU ss:off ps:20
	rgn:10 [10.64.91.150]:35114
	rgn:1 [10.64.90.112]:2050
16:02:53	xoip options: fax:T38 modem:off tty:US uid:0x50117
	xoip ip: [10.64.90.112]:2050
16:02:53	SIP<SIP/2.0 200 OK
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
16:02:53	SIP>ACK sip:3035380026@10.64.91.150:5060;transport=tcp SIP/
16:02:53	SIP>2.0
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
16:02:53	active trunk-group 1 member 6 cid 0x195
16:02:53	SIP>INVITE sip:3035380026@10.64.91.150:5060;transport=tcp S
16:02:53	SIP>IP/2.0
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
16:02:53	SIP<SIP/2.0 100 Trying
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
16:02:53	SIP<SIP/2.0 200 OK
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
time	data
16:02:53	G711MU ss:off ps:20
	rgn:1 [10.64.90.74]:2904
	rgn:10 [10.64.91.150]:35114
16:02:53	SIP>ACK sip:3035380026@10.64.91.150:5060;transport=tcp SIP/
16:02:53	SIP>2.0
16:02:53	Call-ID: 0c461a560f0e1175b503f896600
16:02:53	G711MU ss:off ps:20
	rgn:10 [10.64.91.150]:35114
	rgn:1 [10.64.90.74]:2904
16:03:06	TRACE COMPLETE trunk-group 1 cid 0x195

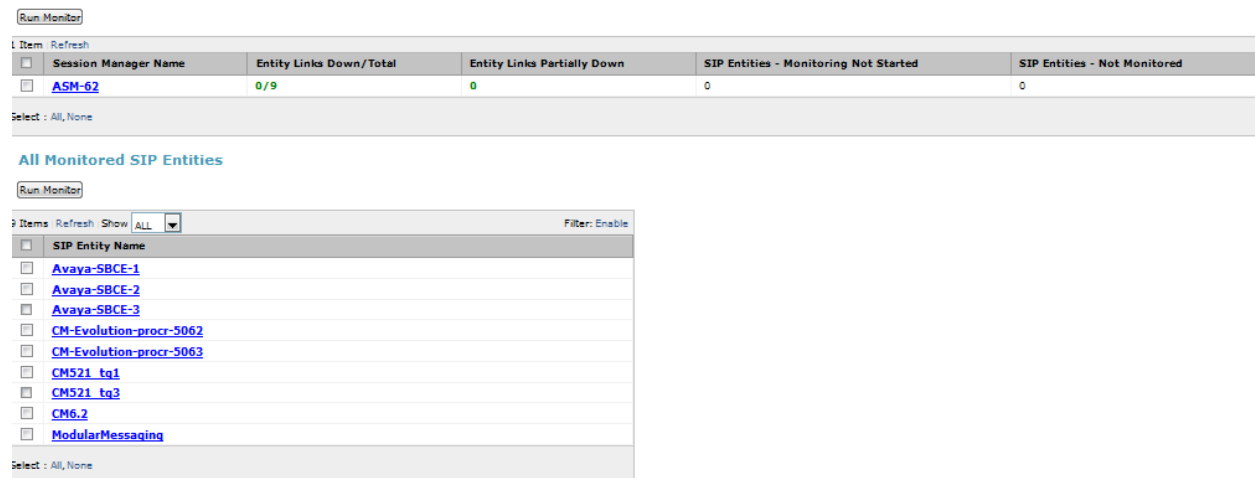
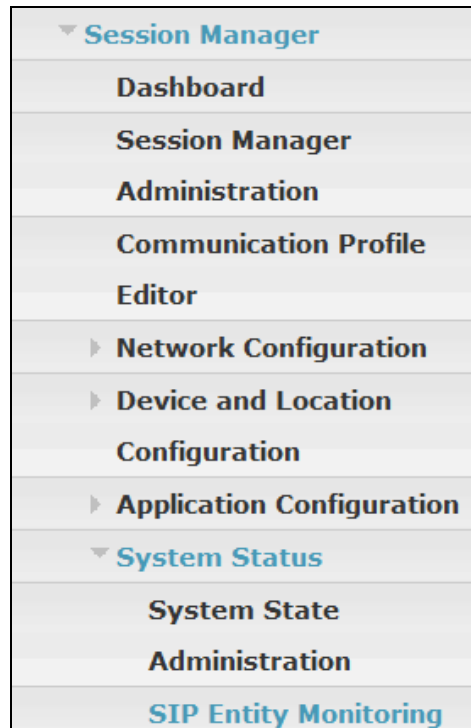


## 8.3. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager.

### 8.3.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**, as shown below.



From the list of monitored entities, select an entity of interest, such as “Avaya-SBCE-3”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring							
							Help ?
<b>SIP Entity, Entity Link Connection Status</b>							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: Avaya-SBCE-3							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	ASM-62	10.64.91.150	5060	TCP	Up	200 OK	Up

Return to the list of monitored entities, and select another entity of interest, such as “CM521-tg1”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below.

<b>SIP Entity, Entity Link Connection Status</b>							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: CM521_tg1							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	ASM-62	10.80.140.180	5060	TCP	Up	200 OK	Up

### 8.3.2 Call Routing Test

The **Call Routing Test** verifies the routing for a particular source and destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**, as shown below.



A screen such as the following is displayed.

### Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

#### SIP INVITE Parameters

Called Party URI	Calling Party Address
<input type="text"/>	<input type="text"/>
Calling Party URI	Session Manager Listen Port
<input type="text"/>	<input type="text" value="5060"/>
Day Of Week	Time (UTC)
<input type="text" value="Wednesday"/>	<input type="text" value="16:24"/>
Called Session Manager Instance	Transport Protocol
<input type="text" value="ASM-62"/>	<input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. Under **Routing Decisions**, observe that the call will route via an Avaya SBCE on the path to Verizon

Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

### Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

#### SIP INVITE Parameters

Called Party URI	Calling Party Address
<input type="text" value="3035380026@avayalab.com"/>	<input type="text" value="10.64.91.150"/>
Calling Party URI	Session Manager Listen Port
<input type="text" value="anycaller@anydomain.com"/>	<input type="text" value="5060"/>
Day Of Week	Time (UTC)
<input type="text" value="Tuesday"/>	<input type="text" value="22:53"/>
Called Session Manager Instance	Transport Protocol
<input type="text" value="ASM-62"/>	<input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

#### Routing Decisions

## 8.4. Avaya Session Border Controller for Enterprise Verification

### 8.4.1 Welcome Screen

The welcome screen shows alarms, incidents, and the status of all managed ASBCEs at a glance.

Welcome

### Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail [support@sipera.com](mailto:support@sipera.com).

Alarms (Past 24 Hours)

None found.

Incidents (Past 24 Hours)

ASBCE-3: No Subscriber Flow Matched

ASBCE-3: No Subscriber Flow Matched

ASBCE-3: No Subscriber Flow Matched

ASBCE-3: No Subscriber Flow Matched

ASBCE-3: No Subscriber Flow Matched

UC-Sec Devices

ASBCE-3

Network Type

DMZ\_ONLY

Quick Links

Sipera Website

Sipera VIPER Labs

Contact Support

Administrator Notes

[ Add ]

No notes posted.

### 8.4.2 Alarms

A list of the most recent alarms can be found under the Alarm tab on the top left bar.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:45:21 PM GMT

Alarms

Incidents

Statistics

Logs

Diagnostics

Users

## Alarms Viewer.

Alarms Viewer

UC-Sec Devices

EMS

ASBCE-3

Alarms

Alarm Details	State	Time	Device	Alarm ID
No alarms have been triggered.				

## 8.4.3 Incidents

A list of all recent incidents can be found under the incidents tab at the top left next to the Alarms.

### Incident Viewer

Incident Viewer

Device All Category All Clear Filters Refresh Show Chart Generate Report

Displaying results 1 to 15 out of 2002.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	672482739147839	8/14/12	5:31 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482709145025	8/14/12	5:30 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482679144006	8/14/12	5:29 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482649142768	8/14/12	5:28 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482619141131	8/14/12	5:27 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482589140867	8/14/12	5:26 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482559137445	8/14/12	5:25 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482529136866	8/14/12	5:24 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482499136227	8/14/12	5:23 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482469134575	8/14/12	5:22 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482439133326	8/14/12	5:21 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482409130894	8/14/12	5:20 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482379128254	8/14/12	5:19 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482349127661	8/14/12	5:18 PM	Policy	ASBCE-3	No Subscriber Flow Matched
Message Dropped	672482319124130	8/14/12	5:17 PM	Policy	ASBCE-3	No Subscriber Flow Matched

<< < 1 2 3 4 5 > >>

Further Information can be obtained by clicking on an incident in the incident viewer.

Incident Information

General Information

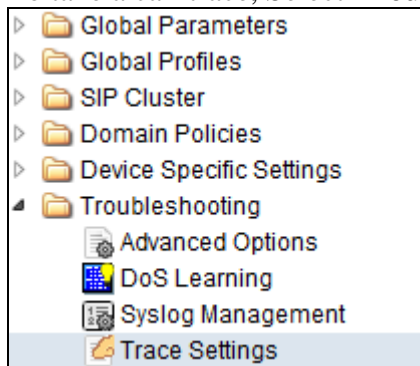
Incident Type	Message Dropped	Category	Policy
Timestamp	August 14, 2012 5:31:18 PM GMT	Device	ASBCE-3
Cause	No Subscriber Flow Matched		

Message Data

Method Name	OPTIONS		
Call ID	bb74e599df543ed63b0c7de840d382660o02f73@172.30.205.55	From	ping@172.30.205.55
To	ping@c800026409-pcs-n0001	Source IP	172.30.205.55
Destination IP	1.1.1.2		

## 8.4.4 Tracing

To take a call trace, Select **Troubleshooting** → **Tracing** from the left-side menu as shown below.



Select the Packet Capture tab and set the desired configuration for a call trace, hit **Start Capture**. Only one interface can be selected at once, so only an inside or only an outside trace is possible.

Packet Trace	Call Trace	Packet Capture	Captures
<b>Packet Capture Configuration</b>			
Currently capturing	No		
Interface	A1		
Local Address (ip:port)	All :		
Remote Address (*, *:port, ip, ip:port)	*		
Protocol	All		
Maximum Number of Packets to Capture	1000		
Capture Filename <small>Existing captures with the same name will be overwritten</small>	Test_trace.pcap		
<b>Start Capture</b> <b>Clear</b>			

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the Stop Capture button at the bottom not shown.

Packet Capture Configuration	
Currently capturing	No
Interface	A1
Local Address (ip:port)	All :
Remote Address (*, *:port, ip, ip:port)	*
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename <small>Existing captures with the same name will be overwritten</small>	Test_trace.pcap
<div>Start Capture</div> <div>Clear</div>	

Select the Captures tab at the top and your capture will be listed, you can select the File Name and choose to open it with an application like Wireshark.

Troubleshooting > Trace Settings: ASBCE-3

UC-Sec Devices

ASBCE-3

Packet Trace

Call Trace

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
<a href="#">test_trace_20120815124710.pcap</a>	212,992	August 15, 2012 12:47:26 PM GMT	X

## 9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.2, and the Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Trunk service. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager user's access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

## 10. Additional References

### 10.1. Avaya

Avaya product documentation, including the following, is available at <http://support.avaya.com>

- [1] *Installing and Configuring Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 5.2.1
- [2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509
- [3] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324
- [4] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID 03-603473
- [5] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325
- [6] *Administering Avaya Aura® System Manager*, Document Number 03-603324

Avaya Application Notes are also available at <http://support.avaya.com>

Application Notes Reference [LAR] contains additional information on Communication Manager Look-Ahead Routing.

[LAR] Sample Configuration for SIP Private Networking and SIP Look-Ahead Routing Using Avaya Communication Manager, Issue 1.0

<http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/sip-pvt-lar.pdf>

### 10.2. Verizon Business

The following documents may be obtained by contacting a Verizon Business Account Representative.

- [7] *Retail VoIP Interoperability Test Plan*
- [8] *Network Interface Specification Retail VoIP Trunk Interface (for non-registering devices)*



## Appendix A: Unscreened ANI Testing and Configuration

Unscreened ANI is a Verizon offered service (available with VoIP IP Integrated Access and VoIP IP Trunking) and is a new feature being offered with Session Manager 6.2. This service was tested successfully in this test configuration and can be implemented by following the steps here.

This feature allows Customer to send an “unscreened” ANI to the Company’s network which is then displayed to the called party as Caller ID. An “unscreened” ANI can be any telephone number that Customer passes through the Company’s network for Caller ID display purposes only. There is no charge for this feature. If Customer selects this feature, Verizon will designate one of Customer’s assigned telephone numbers as a “Screened Telephone Number” for each Customer unique location. Verizon will use the Screened Telephone Number to determine call origination for billing, call routing and E911 support. The customer is responsible for configuring its IP-PBX, PBX or other devices to accommodate and properly process the Screened Telephone Number.

The screened telephone number provided by Verizon for this test is 732-945-0821. Typically customers would have one or more screened telephone number, one for every location and a central Session Manager could be used to pass multiple screened telephone numbers to Verizon based on a Matching Pattern (i.e. a user’s CLID).

Login to Session Manager as shown above, navigate to Routing→Adaptations, and select “New”.

Create a unique name for the Adaptation, here “Verizon\_Test”. Select the “VerizonAdapter” for the **Module Name**. In module parameter enter any domain adaptations that may be needed. Here the domains known to Verizon needed to overwrite the internal lab environment name of “avayalab.com” so a **Module Parameter** of “osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true” was used.

Adaptation Details	
<b>General</b>	
* Adaptation name:	<input type="text" value="Verizon_Test"/>
Module name:	<input type="text" value="VerizonAdapter"/>
Module parameter:	<input type="text" value="osrcd=adevc.avaya.globalipcom.c"/>
Egress URI Parameters:	<input type="text"/>
Notes:	<input type="text"/>

Scroll down to the **Digit Conversion for Outgoing Calls from SM** section, enter a **Matching Pattern** (e.g. 732-945-0233), with the **Min** and **Max** number of digits to match on, in **Address to**

**modify**, select origination, and in the **Adaptation Data** enter the screened telephone number (e.g. 732-945-0821) provided by Verizon. Hit **Commit**.

**Digit Conversion for Outgoing Calls from SM**

Add Remove

3 Items Refresh Filter: Enable

	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*7329450233	*10	*10		*0		origination ▼	7329450821	

Once the Adaptation has been committed it needs to be applied to a SIP Entity. Back at the Routing screen, select SIP Entities as shown in the Session manager section above, and select the Avaya SBCE-1. Under Adaptation, change to the newly created “Verizon\_Test” adaptation.

**SIP Entity Details** Commit Cancel

**General**

\* Name: Avaya-SBCE-3

\* FQDN or IP Address: 10.64.91.150

Type: SIP Trunk ▼

Notes: Sipera-SBC-3 outside 1.1.1.2 using

Adaptation: Verizon\_Test ▼

Location: Avaya-SBCE-3 ▼

## Verification

In the following filter Wireshark trace, you can see that the From line contains the DID number, 732-945-0233 and in the p-asserted identity section, a Diversion header has been added with the screened ANI (732-945-0821).

From: "IP 9641 - SIP" <sip:7329450233@1.1.1.2:5060>;tag=80ce5662df1e11480503f896600

Diversion: sip:7329450821@1.1.1.2:5060>

No.	Time	Source	Destination	Protocol	Length	Info
12	9.927034	172.30.205.55	1.1.1.2	SIP	415	Request: OPTIONS sip:adevc.avaya.globalipcom.com:5060
13	9.927300	1.1.1.2	172.30.205.55	SIP	376	Status: 403 Forbidden
31	27.009642	1.1.1.2	172.30.209.21	SIP/SDF	1242	Request: INVITE sip:3035380026@172.30.209.21:5071, with session description
32	27.074021	172.30.209.21	1.1.1.2	SIP	316	Status: 100 Trying
37	29.460792	172.30.209.21	1.1.1.2	SIP/SDF	899	Status: 183 Session Progress, with session description
1025	39.166533	1.1.1.2	172.30.209.21	SIP	467	Request: OPTIONS sip:1.1.1.2
1033	39.228940	172.30.209.21	1.1.1.2	SIP	522	Status: 200 OK
1834	47.169008	172.30.209.21	1.1.1.2	SIP/SDF	965	Status: 200 OK, with session description
1836	47.178256	1.1.1.2	172.30.209.21	SIP	652	Request: ACK sip:3035380026@172.30.209.21:5071
1843	47.243143	1.1.1.2	172.30.209.21	SIP	972	Request: INVITE sip:3035380026@172.30.209.21:5071, in-dialog
1858	47.373381	172.30.209.21	1.1.1.2	SIP/SDF	963	Status: 200 OK, with session description
1859	47.380786	1.1.1.2	172.30.209.21	SIP/SDF	837	Request: ACK sip:3035380026@172.30.209.21:5071, with session description
4140	69.941010	172.30.205.55	1.1.1.2	SIP	415	Request: OPTIONS sip:adevc.avaya.globalipcom.com:5060
4141	69.941277	1.1.1.2	172.30.205.55	SIP	376	Status: 403 Forbidden
7098	99.178456	1.1.1.2	172.30.209.21	SIP	467	Request: OPTIONS sip:1.1.1.2

Frame 31: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits)

Ethernet II, Src: IntelCor\_cc:24:41 (00:1b:21:cc:24:41), Dst: Cisco\_5c:21:41 (00:04:9a:5c:21:41)

Internet Protocol Version 4, Src: 1.1.1.2 (1.1.1.2), Dst: 172.30.209.21 (172.30.209.21)

User Datagram Protocol, Src Port: sip (5060), Dst Port: powerschool (5071)

Session Initiation Protocol

Request-Line: INVITE sip:3035380026@172.30.209.21:5071 SIP/2.0

Message Header

From: "IP 9641" <sip:7329450233@1.1.1.2:5060>;tag=80ce5662df1e11480503f896600

To: sip:3035380026@172.30.209.21:5071

CSeq: 1 INVITE

Call-ID: e75d773997746a3439b4691768d60466

Contact: "IP 9641" <sip:7329450233@1.1.1.2:5060>

Record-Route: <sip:1.1.1.2:5060;ipcs-line=64;lr;transport=udp>

Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO, PUBLISH

Supported: timer, replaces, join, 100rel

User-Agent: Avaya CM/R015X.02.1.016.4 AVAYA-SM-6.2.2.0.622005

Max-Forwards: 66

Via: SIP/2.0/UDP 1.1.1.2:5060;branch=z9hG4bK-s1632-000001847339-1--s1632-

Accept-Language: en

Alert-Info: <cid:internal@avayalab.com>;avaya-cm-alert-type=internal

P-Asserted-Identity: "IP 9641" <sip:7329450233@1.1.1.2:5060>

Session-Expires: 1200;refresher=uac

Min-SE: 1200

Diversion: <sip:7329450821@1.1.1.2:5060>

Content-Type: application/sdp

P-Location: SM;origlocname="CM521";origsiglocname="CM521";termlocname="Avaya-SBCE-3";termsiglocname="Avaya-SBCE-3"

Content-Length: 154

Message Body

Session Description Protocol

---

**©2012 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](mailto:devconnect@avaya.com).