



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Trunk SIP IDA 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 6.2 with the Verizon Business Internet Direct Access (IDA) IP Trunk service. The Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Avaya Session Border Controllers for Enterprise.

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 Internet Direct Access (IDA) circuit connection to the production Verizon Business IP Trunking service.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	5
2.3.	History Info and Diversion Headers	6
2.4.	Support.....	7
2.4.1	Avaya	7
2.4.2	Verizon.....	7
2.5.	Known Limitations	7
3.	Reference Configuration	8
3.1.	The SIP Trunk Redundant (2-CPE) Architecture Option	9
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Communication Manager	11
5.1.	Verify Licensed Features	11
5.2.	Dial Plan.....	13
5.3.	Node Names.....	13
5.4.	Processor Ethernet Configuration	14
5.5.	Network Regions for Gateway, Telephones	14
5.6.	IP Codec Sets	17
5.7.	SIP Signaling Groups.....	18
5.8.	SIP Trunk Groups	19
5.9.	Route Pattern Directing Outbound Calls to Verizon	21
5.10.	Public Numbering	22
5.11.	ARS Routing For Outbound Calls	22
5.12.	EC500 Configuration for Diversion Header Testing	23
5.13.	Saving Communication Manager Configuration Changes	23
6.	Configure Avaya Aura® Session Manager	24
6.1.	Domains	26
6.2.	Locations.....	27
6.3.	Adaptations	30
6.4.	SIP Entities.....	32
6.5.	Entity Links.....	37
6.6.	Routing Policies	38
6.7.	Dial Patterns.....	42
6.7.1	Inbound Call Dial Pattern	42
6.7.2	Outbound Call Dial Pattern.....	43
7.	Configure Avaya Session Border Controller for Enterprise	44
7.1.	Access the Management Interface	44
7.2.	Device Specific Settings	46
7.2.1	Define Network Information.....	46
7.2.2	Signaling Interfaces	47
7.2.3	Media Interfaces.....	47
7.3.	Global Profiles	48
7.3.1	Routing Profile.....	48
7.3.2	Topology Hiding Profile	49
7.3.3	Server Interworking Profile	51
7.3.4	Signaling Manipulation.....	54

7.3.5	Server Configuration for Session Manager.....	56
7.3.6	Server Configuration for Verizon IPT	57
7.4.	Domain Policies – Media Rules.....	59
7.5.	Domain Policies – Signaling Rules.....	61
7.6.	Domain Policies – End Point Policy Groups	62
7.7.	Device Specific Settings – End Point Flows.....	63
8.	Verification Steps.....	66
8.1.	Illustration of OPTIONS Handling	66
8.2.	Avaya Aura® Communication Manager Verifications	66
8.2.1	Example Incoming Call from PSTN via Verizon SIP Trunk	66
8.3.	Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications.....	68
8.3.1	Verify SIP Entity Link Status	68
8.3.2	Call Routing Test	70
8.4.	Avaya Session Border Controller for Enterprise Verification	72
8.4.1	Welcome Screen	72
8.4.2	Alarms	73
8.4.3	Incidents	73
8.4.4	Tracing	74
9.	Conclusion	75
10.	Additional References.....	75
10.1.	Avaya	75
10.2.	Verizon Business	76
Appendix A: Unscreened ANI Testing and Configuration.....		77
Verification		78
Appendix B: Avaya Session Border Control for Enterprise – Sigma Script “EXAMPLE 2”.....		80

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.2 and Avaya Aura® Communication Manager Release 6.2 with the Verizon Business Internet Direct Access (IDA) 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 Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Avaya Session Border Controllers for Enterprise (ASBCE). The Verizon Business SIP Trunk redundant (2-CPE) architecture provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the customer premises equipment (CPE).

Dual ASBCEs are used as edge devices between the Avaya CPE and the Verizon Business network, and provide for Verizon Business 2-CPE redundancy. In addition, the ASBCEs provide Network Address Translation (NAT) functionality to convert the addresses used within the enterprise to the Verizon routable addresses.

Note - The Verizon Business SIP Trunk Redundant (2-CPE) architecture is a service option and its use is not a requirement of the Verizon Business IP Trunk service offer.

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically re-routed to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two ASBCEs. One ASBCE is designated as Primary and one as Secondary although a Round-Robin configuration was also tested.

Avaya Aura® Session Manager is provisioned for fail-over of outbound calls from one ASBCE to the other if there is a failure (e.g., timeout, or error response) associated with the first choice. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary ASBCE, if there is a failure (e.g., timeout, or error response) then the call will be sent to the Secondary ASBCE.

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.

2. General Test Approach and Test Results

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

The equipment used in this testing scenario was in a shared lab environment. This has necessitated header adaptations that may not be applicable to customer deployments.

2.1. 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 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.
- Initial IP-IP Direct communications
- 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)
- 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
- Long hold time calls
- Automatic fail-over testing associated with the 2-CPE redundancy (i.e., calls automatically re-routed around component outages).
- Round-robin of inbound calls with the 2-CPE redundancy
- Domestic and EMEA configurations were tested

2.2. Test Results

- **SIP PHONE REFRESH:** When using an Avaya SIP phone with G.711 as the preferred codec and a call is established as G.711, when a re-invite is issued by Communication

Manager for a shuffle, Verizon sends an ACK with just G.729 listed, so the SIP Phone will switch codecs to G.729. The user experience will not be affected and the calls stays connected.

- **CALL-ID ON CALL TRANSFERS:** When a PSTN caller is transferred off-net (to another PSTN user) the 2nd PSTN phone will see the Caller-ID of the CPE phone. The user experience will not be affected and this is mentioned as an observation.
- **2 – CPE TESTING:** Although the Sipera will proxy OPTIONS messages from inside the network to outside, sourcing of OPTIONS must be turned on if a 2-CPE configuration is used or failover will not occur in an expedient manner.
- **DIRECT MEDIA:** When the **Convert 180 to 183 for Early Media** field on the Communication Manager trunk group form page 4 is set to “y” and the **Initial IP-IP Direct Media** field on the Communication Manager signaling group form page 1 is set to “y”, an H323 endpoint may send a 183 without SDP which is undesirable to Verizon. Therefore, the recommendation in **Section 5.7** is to leave the **Initial IP-IP Direct Media** field to “n”. Internal tracking issue defsw122017 has been created.
- **P-ASSERTED-IDENTITY:** The ASBCE does not hide the internal domain in the P-Asserted Identity Header. A sigma script is used (Detailed in Appendix B as a work around and internal tracking issue AURORA-421 has been created.
- **DSCP CODE POINTS:** The ASBCE does not mark locally sourced messages with the correct QoS. (e.g. 100 Trying). Internal tracking issue AURORA-202 has been created.
- **CONTACT HEADER:** When performing a transfer to the PSTN and a local extension is being translated by the public or private unknown numbering table to a DID, the SIP Header “Contact” may contain the local extension instead of the DID. A sigma script is used (Detailed in Appendix B) as a work around and internal tracking issue defsw121215 has been created.
- **ASBCE SIGMA SCRIPT:** If using a Sigma Script and the Sigma Script is edited or a warm restart is performed, the Sigma Script may stop working. The work around is to delete the Sigma Script and reinstall it. Internal tracking issue AURORA-254 has been created for this issue.

2.3. 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. Communication Manager SIP trunk group form provides options for specifying whether History Info Headers or Diversion Headers are sent.

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

The Communication Manager Call Forwarding or Extension to Cellular (EC500) features may be used for the call scenarios testing Diversion Header.

2.4. Support

2.4.1 Avaya

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

2.4.2 Verizon

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

2.5. Known Limitations

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

- Emergency 911/E911 Services Limitations and Restrictions - Although Verizon provides 911/E911 calling capabilities and 911 capabilities were tested, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.
- Verizon Business IP Trunking service does not support G.711a codec for domestic service (EMEA only).
- Verizon Business IP Trunking service does not support G.729B codec.
- Verizon Business only supports T.38 for fax domestically not in EMEA.

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.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the testing. The Avaya CPE location simulates a customer site.

The ASBCEs receives traffic from the Verizon Business IP Trunk service on port 5060 and sends traffic to the Verizon Business IP trunk service on port 5208 (domestic) and 5234(EMEA), using UDP protocol for network transport (required by the Verizon Business IP Trunk service). The Verizon Business IP Trunk service provided 10 digits Direct Inward Dial (DID) numbers for domestic and 11 digits DID numbers for EMEA testing. These DID numbers can be mapped by Session Manager or Communication Manager to Avaya telephone extensions.

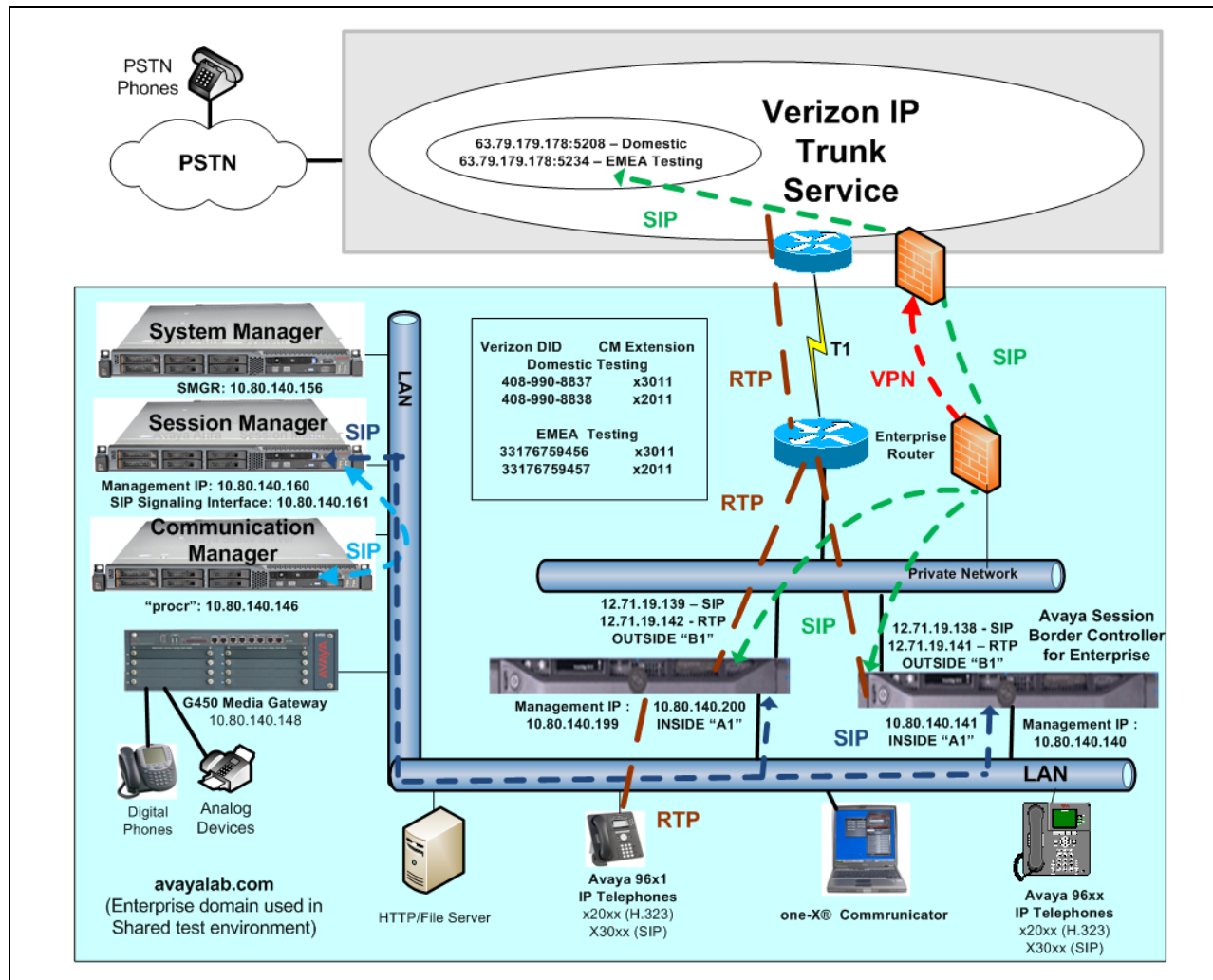


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon Business IP Trunk can use an IP Address or a domain name. The Avaya CPE environment was known to Verizon Business IP Trunk service as FQDN, *icrcn1n0002.customer08.tsengr.com* for domestic testing and *icrcn1n0002.customer34.tsengr.com* for EMEA testing. The Avaya CPE environment used the domain "avayalab.com" at the

enterprise. As such, the ASBCEs 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 IP Address
 - 63.79.179.178:5208 - *domestic*
 - 63.79.179.178:5234 - *EMEA*
- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
 - *icrcn1n0002.customer08.tsengr.com* – *domestic*
 - *icrcn1n0002.customer34.tsengr.com* - *EMEA*
- Primary and Secondary Avaya Session Border Controllers for Enterprise Release 4.0.5
- Avaya Aura® Communication Manager Release 6.2
- Avaya Aura® Session Manager Release 6.2
- Avaya 96X1 Series IP telephones using the SIP and H.323 software bundle.
- Avaya 9600 Series IP telephones using the SIP and H.323 software bundle.
- Avaya Digital Phones
- Avaya Analog Phones

3.1. The SIP Trunk Redundant (2-CPE) Architecture Option

Verizon Business and Avaya developed the SIP Trunk Redundant (2-CPE) architecture to ensure that SIP trunk calls can be automatically rerouted to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two Avaya Session Border Controllers for Enterprise. One ASBCE is designated as Primary and one as Secondary. The ASBCEs reside at the edge of the customer network.

Session Manager is provisioned to attempt outbound calls to the Primary ASBCE first. If that attempt fails, the Secondary ASBCE is used. Similarly, the Verizon Business Private IP Trunk service node will send inbound calls to the Primary ASBCE. If there is no response then the call will be sent to the Secondary ASBCE.

4. Equipment and Software Validated

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

Equipment:	Software:
HP ProLiant DL360 G7	Avaya Aura® Communication Manager Release 6.2 SP2.1
HP ProLiant DL360 G7	Avaya Aura® System Manager 6.2 SP2

HP ProLiant DL360 G7	Avaya Aura® Session Manager 6.2 SP2
G450 Gateway	3.1.20.1
DELL 210 RII	Avaya Session Border Controller for Enterprise Version 4.0.5Q09
Avaya 9600-Series Telephones (H.323)	96xx-IPT-H323-R3_1_3-112211
Avaya 9600-Series Telephones (SIP)	96xx-IPT-SIP-R2_6_6_0-102111
Avaya 96X1- Series Telephones (SIP)	96x1-IPT-SIP-R6_0_3-120511
Avaya 96X1- Series Telephones (H323)	96x1-IPT-H323-R6_0_5-091911
Avaya One-X Communicator (H.323)	6.1.3.08_SP3-Patch2-35791
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
Okidata Analog Fax	N/A

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager

This section illustrates an example configuration allowing SIP signaling via the “Processor Ethernet” of the Avaya Server to Session Manager. In configurations that use an Avaya G650 Media Gateway, it is also possible to use a C-LAN card in the Avaya G650 Media Gateway for SIP signaling to Session Manager.

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.

5.1. 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** is 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. Each call from a SIP endpoint to the Verizon Business IP Trunk service uses two SIP trunks 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:		12000	0	
Maximum Concurrently Registered IP Stations:		18000	3	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		18000	0	
Maximum Video Capable IP Softphones:		18000	0	
Maximum Administered SIP Trunks:		24000	40	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		128	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	

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	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? n	DCS Call Coverage? y	
ASAI Link Plus Capabilities? n	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? 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	IP Stations? y	
Enable 'dadmin' Login? y	ISDN Feature Plus? n	
Enhanced Conferencing? y	ISDN/SIP Network Call Redirection? y	
Enhanced EC500? y	ISDN-BRI Trunks? y	
Enterprise Survivable Server? n	ISDN-PRI? y	
Enterprise Wide Licensing? n	Local Survivable Processor? n	
ESS Administration? y	Malicious Call Trace? y	
Extended Cvg/Fwd Admin? y	Media Encryption Over IP? n	
External Device Alarm Admin? y	Mode Code for Centralized Voice Mail? n	
Five Port Networks Max Per MCC? n	Multifrequency Signaling? y	
Flexible Billing? n	Multimedia Call Handling (Basic)? y	
Forced Entry of Account Codes? y	Multimedia Call Handling (Enhanced)? y	
Global Call Classification? y	Multimedia IP SIP Trunking? y	
Hospitality (Basic)? y		
Hospitality (G3V3 Enhancements)? y		
IP Trunks? y		
IP Attendant Consoles? y		

On **Page 5** of the *display system-parameters customer-options* form, verify that the **Processor Ethernet** feature is 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? n		
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	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

5.2. Dial Plan

In the reference configuration the Avaya CPE environment uses four digit local extensions, such as 2xxx, 3xxx or 4xxx. Trunk Access Codes (TAC) are 3 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: 1
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	3	fac							
2	4	ext							
3	4	ext							
4	4	ext							
8	1	fac							
9	1	fac							
*	3	fac							
*1	4	dac							
#	3	fac							

5.3. 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 “**ASM6-2**” with IP address **10.80.140.160**. The node name and IP address for the Processor Ethernet “**procr**” is **10.80.140.146**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
ASM6-2	10.80.140.160	
Gateway1	10.80.140.1	
default	0.0.0.0	
procr	10.80.140.146	
procr6	::	

5.4. Processor Ethernet Configuration

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 procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		
Target socket load: 19660		
Enable Interface? y	Allow H.323 Endpoints? y	
	Allow H.248 Gateways? y	
Network Region: 1	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.80.140.146	

5.5. 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. To provide testing flexibility, network region 4 was associated with other components used specifically for the Verizon testing.

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 1** is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the address of the Processor Ethernet (10.80.140.146), and that the gateway IP address is 10.80.140.148. These fields are not configured in this screen, but just display the current information for the Media Gateway.

change media-gateway 1

MEDIA GATEWAY 1

Page 1 of 2

Type: g450

Name: G450

Serial No: 08IS35173859

Encrypt Link? y

Enable CF? n

Network Region: 1

Location: 1

Site Data:

Recovery Rule: none

Registered? y

FW Version/HW Vintage: 31 .20 .1 /1

MGP IPV4 Address: 10.80.140.148

MGP IPV6 Address:

Controller IP Address: 10.80.140.146

MAC Address: 00:1b:4f:03:42:d8

The following screen shows **Page 2** for **Media Gateway 1**. The gateway has an **S8300** in slot V1 (unused), a **MM712** media module supporting Avaya digital phones in slot V2, a **MM710** T1 board in V3(unused), a **MM711** supporting analog devices in slot V4, another **MM710** T1 board in V8 (unused), and the capability to provide announcements and music on hold via “gateway-announcements” in logical slot V9.

change media-gateway 1

MEDIA GATEWAY 1

Page 2 of 2

Type: g450

Slot	Module Type	Name	DSP Type	FW/HW version
V1:	S8300	ICC MM	MP80	68 3
V2:	MM712	DCP MM		
V3:	MM710	DS1 MM		
V4:	MM711	ANA MM		
V5:				
V6:				
V7:				
V8:	MM710	DS1 MM		
V9:	gateway-announcements	ANN VMM		

Max Survivable IP Ext: 8

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 10.80.140.29 would be mapped to network region 1, based on the configuration in bold 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: 10.80.140.0	/24	1	n		
TO: 10.80.140.255					

The following screen shows IP Network Region 4 configuration. In the shared test environment, network region 4 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 4 will be used for calls within region 4. The shared Avaya Interoperability Lab test environment uses the domain “avayalab.com” (i.e., for network region 1 including the region of the Processor Ethernet “procr”). The domain is set to the shared lab domain of “avayalab.com”. Session Manager or the ASBCE can adapt “avayalab.com” to either “icrcn1n0002.customer08.tsengr.com” (domestic) or “icrcn1n0002.customer34.tsengr.com” (EMEA). In this configuration, the ASBCE is adapting the domains.

change ip-network-region 4		Page 1 of 20
IP NETWORK REGION		
Region: 4		
Location:	Authoritative Domain: avayalab.com	
Name: Verizon testing		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 4	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 3029		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

The following screen shows the inter-network region connection configuration for region 4. The first bold row shows that network region 4 is directly connected to network region 1, and that codec set 4 will also be used for any connections between region 4 and region 1. For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the **codec set** column for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, Page 4 will also show codec set 4 for region 4 to region 1 connectivity.

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

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the Codec Set parameter on **Page 1**, but codec set 4 will be used for connections between region 1 and region 4 as noted previously. In the shared test environment, network region 1 was in place prior to adding the Verizon test environment and already used **Authoritative Domain** “avayalab.com”. Where necessary, Session Manager or the ASBCE will adapt the domain from “avayalab.com” to the appropriate domain.

change ip-network-region 1										Page	1	of	20
IP NETWORK REGION													
Region: 1													
Location: 1 Authoritative Domain: avayalab.com													
Name: Enterprise													
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													
Call Control PHB Value: 46													
Audio PHB Value: 46													
Video PHB Value: 26													
802.1P/Q PARAMETERS													
Call Control 802.1p Priority: 6													
Audio 802.1p Priority: 6													
Video 802.1p Priority: 5													
H.323 IP ENDPOINTS										AUDIO RESOURCE RESERVATION PARAMETERS			
										RSVP Enabled? n			
H.323 Link Bounce Recovery? y													
Idle Traffic Interval (sec): 20													
Keep-Alive Interval (sec): 5													
Keep-Alive Count: 5													

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 4, and that codec set 4 will be used for any connections between region 4 and region 1.

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

5.6. IP Codec Sets

The following screen shows the configuration for codec set 4, the codec set configured to be used for calls within region 4 and for calls between region 1 and region 4. 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.729A, since G.729A 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 4, 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 4, 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 ASBCE. Include G.711MU in the ip-codec-set if fax will be used.

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

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 4				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				

The following screen shows the configuration for codec set 1. This default configuration for codec set 1, using G.711MU, is used for Avaya Modular Messaging and other connections within region 1.

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: 1.722-64K		2	20			
2: G.711MU	n	2	20			
3: G.729A	n	2	20			
4:						

5.7. 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 “ASM6-

2”. 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. **Direct IP-IP Audio Connections** allows for shuffling from the media gateway directly to an IP endpoint. The **Initial IP-IP Direct Media** will allow calls to be set up directly to IP endpoints, removing the media gateway and the need to shuffle a call, however it can result in a 183 without SDP which Verizon does not recommend, therefore it is recommended that this be left off. See **Section 2.2** for more details.

The following screen shows signaling group 68. Signaling group 68 will be used for processing PSTN calls to / from Verizon via Session Manager. The **Far-end Network Region** is configured to region 4. Port 5062 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 5062. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. In the sample configuration, the **Peer Detection Enabled** field was set to “n”. Other parameters may be left at default values. Note that the **Alternate Route Timer** that defaults to 6 seconds has been changed to 12 seconds, this timer impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead Routing (LAR) can be triggered, after the expiration of the Alternate Route Timer.

change signaling-group 68		Page 1 of 2
SIGNALING GROUP		
Group Number: 68	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? n Peer Server: Others		
Near-end Node Name: procr	Far-end Node Name: ASM6-2	
Near-end Listen Port: 5062	Far-end Listen Port: 5062	
	Far-end Network Region: 4	
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	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 12	

5.8. SIP Trunk Groups

This section illustrates the configuration of the SIP Trunks Groups corresponding to the SIP signaling groups from the previous section.

The following shows **Page 1** for trunk group 68, 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 68		Page 1 of 21	
TRUNK GROUP			
Group Number: 68	Group Type: sip	CDR Reports: y	
Group Name: To-ASM-Verizon	COR: 1	TN: 1	TAC: *168
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 68	
		Number of Members: 255	

The following screen shows **Page 2** for trunk group 68. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

change trunk-group 68		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): 900			
Delay Call Setup When Accessed Via IGAR? n			

The following screen shows **Page 3** for trunk group 68. All parameters except those in bold are default values. The **Numbering Format** will use “public” numbering, meaning that the public 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 68		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: public			
		UII Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Show ANSWERED BY on Display? Y			

The following screen shows **Page 4** for trunk group 68. 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. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field was a new field in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to “y” for the trunk group handling inbound calls from Verizon produces this result. 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 68	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? y Send Diversion Header? y Support Request History? n Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? y Always Use re-INVITE for Display Updates? n Identity for Calling Party Display: P-Asserted-Identity Block Sending Calling Party Location in INVITE? n Enable Q-SIP? n	

5.9. Route Pattern Directing Outbound Calls to Verizon

Route pattern 68 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.

If desired, one or more alternate Communication Manager trunks can be listed in the route pattern so that the Look-Ahead Routing (**LAR**) “next” setting can route-advance to attempt to complete the call using alternate trunks should there be no response or an error response from the far-end.

change route-pattern 68										Page 1 of 3		
Pattern Number: 68 Pattern Name: To-VZ-IP-Trunk												
SCCAN? n Secure SIP? n												
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits			QSIG		
										Intw		
1:	68	0								n	user	
2:											n	user
3:											n	user
4:											n	user
5:											n	user
6:											n	user
		BCC	VALUE	TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	No. Numbering	
		0	1	2	M	4	W	Request		Dgts Format		
										Subaddress		
1:	y	y	y	y	y	n	n	rest		unk-unk	next	
2:	y	y	y	y	y	n	n	rest		none		
3:	y	y	y	y	y	n	n	rest		none		
4:	y	y	y	y	y	n	n	rest		none		
5:	y	y	y	y	y	n	n	rest		none		
6:	y	y	y	y	y	n	n	rest		none		

5.10. Public Numbering

The *change public-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 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 (x2011) is mapped to a DID number that is known to Verizon for this SIP Trunk connection (408-990-8837), when the call uses trunk group 68. 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 public-unknown-numbering trunk-group 68 0					Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT						
				Total		
Ext	Ext	Trk	CPN	CPN		
Len	Code	Grp(s)	Prefix	Len		
4	2011	68	4089908837	10	Total Administered: 6	
4	3011	68	33176759456	11	Maximum Entries: 9999	
4	3013	68	33176759456	11	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.	
4	4011	68	4089908838	10		

5.11. 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. Various example scenarios for a multi-location network with failover routing are provided in reference [PE]. In these Application Notes, the ARS “all locations” table directs ARS calls to specific SIP Trunks to Session Manager.

The following screen shows a specific ARS configuration as an example. If a user dials the ARS access code followed by 13035387024, the call will select route pattern 68. Of course, matching of the dialed string need not be this specific. The ARS configuration shown here is not intended to be prescriptive.

change ars analysis 13035387022						Page	1 of	2
ARS DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 1		
Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Reqd		
13035387024	11	11	68	hnpa		n		

The *list ars route-chosen* command can be used on a target dialed number to check whether routing will behave as intended. An example is shown below.

list ars route-chosen 13035387022						
ARS ROUTE CHOSEN REPORT						
Location: 1		Partitioned Group Number: 1				
Dialed	Total		Route	Call	Node	Location
String	Min	Max	Pattern	Type	Number	
13035387022	11	11	68	hnpa		all
Actual Outpulsed Digits by Preference (leading 35 of maximum 42 digit)						
1: 13035387022						

5.12. 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 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 2010. Use the command *change off-pbx-telephone station mapping x* where *x* is Communication Manager station (e.g. 2010).

- **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., 3035387024)
- **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 2010								Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode			
2010	EC500	-		3035387024	ars	1				

5.13. Saving Communication Manager Configuration Changes

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

6. Configure Avaya Aura® Session Manager

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.

10.80.140.156 https://10.80.140.156/network-login/ Google

AVAYA 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.

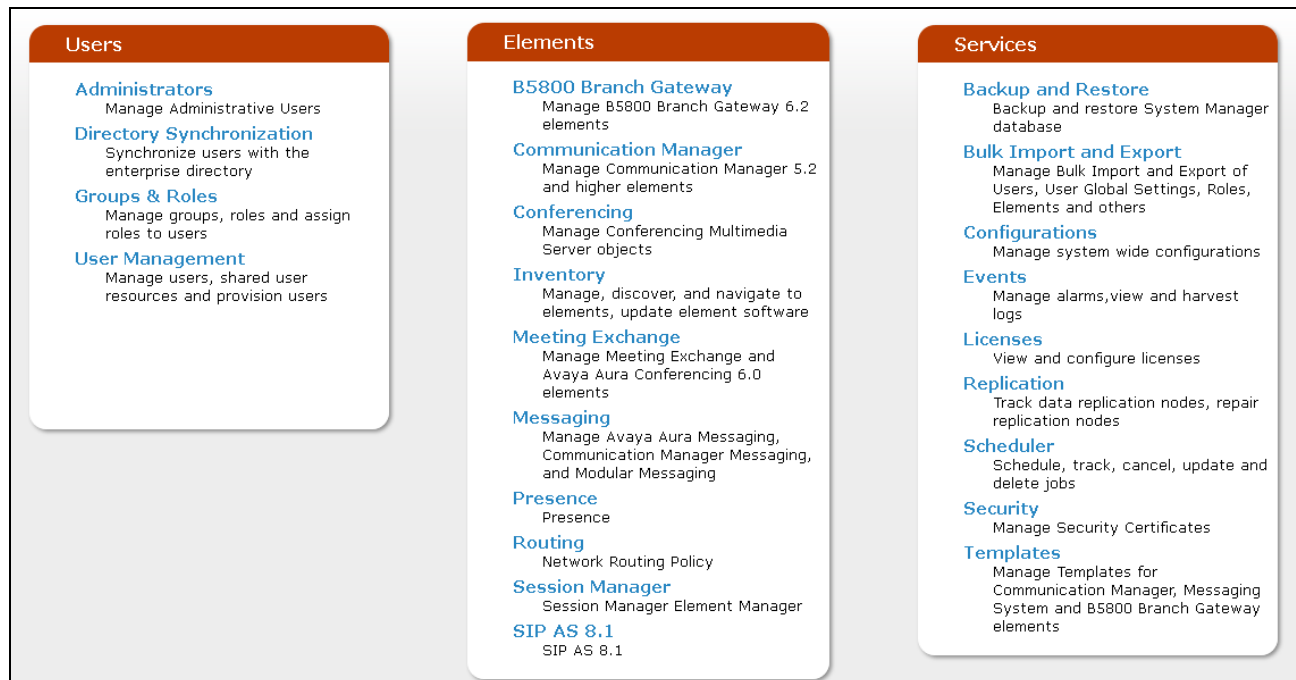
User ID:

Password:

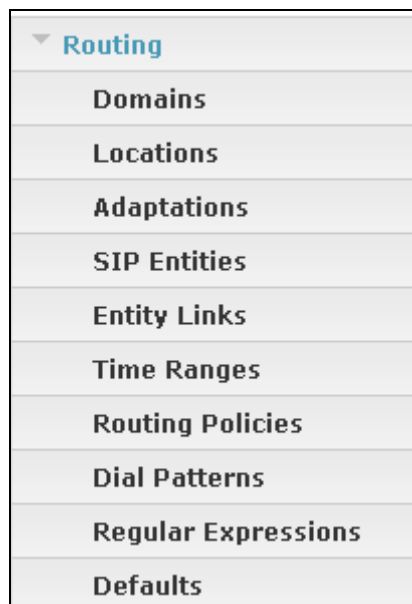
Log On **Cancel**

[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)

6.1. 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. The ASBCE will adapt the domain in **Section 7.3.2**.

Home / Elements / Routing / Domains				
Domain Management				
<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 Refresh				
<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avaya.globalipcom.com	sip	<input type="checkbox"/>	CPE domain known to Verizon
<input type="checkbox"/>	avayalab.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon IPT Network Domain

Domain Management			
Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset lo			
1 Item Refresh			
Name	Type	Default	Notes
* <input type="text" value="avayalab.com"/>	<input type="text" value="sip"/>	<input type="checkbox"/>	<input type="text"/>

6.2. 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. There were two ASBCEs used for the 2-CPE configuration, but configurations are identical except for IP Addresses.

Home / Elements / Routing / Locations		
Location		
<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 Refresh		
<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Avaya-SBCE-1	Avaya SBCE-1
<input type="checkbox"/>	Avaya-SBCE-2	Avaya-SBCE-2
<input type="checkbox"/>	Location_140	Subnet 140

The following image shows the details for the location named “Avaya-SBCE-1”, corresponding to the ASBCE relevant to these Application Notes. Later, the location with name “Avaya-SBCE-1” will be assigned to the corresponding SIP Entity. Note that no IP Address is used in the **Location Pattern** section.

Home / Elements / Routing / Locations

Location Details

General

* Name: Avaya-SBCE-1

Notes: Avaya SBCE-1

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items Refresh

	IP Address Pattern	Notes
* Input Required		

The following image shows the location details for the location named “Avaya-ASBCE-2”. In the sample configuration, other location parameters retained default values.

Location Details

General

* Name: Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Total Bandwidth: Multimedia Bandwidth: Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): Kbit/SecMaximum Multimedia Bandwidth (Inter-Location): Kbit/Sec* Minimum Multimedia Bandwidth: Kbit/Sec* Default Audio Bandwidth:

Alarm Threshold

Overall Alarm Threshold: %Multimedia Alarm Threshold: %* Latency before Overall Alarm Trigger: Minutes* Latency before Multimedia Alarm Trigger: Minutes

Location Pattern

0 Items [Refresh](#)

<input type="checkbox"/>	IP Address Pattern	Notes
--------------------------	--------------------	-------

* Input Required

The following image shows the location details for the location named “Location_140”. In the sample configuration, other location parameters retained default values. This location will be used to identify Communication Manager.

Home / Elements / Routing / Locations

Location Details

General

* Name: Location_140

Notes: Subnet 140

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items Refresh

	IP Address Pattern	Notes
<input type="checkbox"/>		

* Input Required

6.3. 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 (not shown).

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			
Adaptations			
<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"/>			
9 Items <input type="button" value="Refresh"/>			
<input type="checkbox"/>	Name	Module name	Egress URI Parameters
<input type="checkbox"/>	CM-ES-VZ	DigitConversionAdapter	
<input type="checkbox"/>	CM-ES-VZ-IPCC	DigitConversionAdapter odstd=avayalab.com fromto=true	
<input type="checkbox"/>	History Diversion IPT	VerizonAdapter osrcd=advec.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true	
<input type="checkbox"/>	IPCC Verizon Interop Lab	VerizonAdapter	
<input type="checkbox"/>	MM to 4digits	DigitConversionAdapter fromto=true	
<input type="checkbox"/>	SBC-VzB-IPCC	DigitConversionAdapter osrcd=advec.avaya.globalipcom.com	
<input type="checkbox"/>	To VZ	VerizonAdapter odstd=172.30.209.21 fromto=true	
<input type="checkbox"/>	Verizon Test	VerizonAdapter	
<input type="checkbox"/>	Verizon Unscreened ANI	VerizonAdapter osrcd=advec.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.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 ASBCE, specifying that all communication from the Session Manager to the ASBCE will use this adapter. This adaptation uses the “VerizonAdapter” and adds a Diversion Header with **9727289417** to test Verizon’s Unscreened ANI feature (**Appendix A** explains this in more detail).

Adaptation Details										<input type="button" value="Commit"/>	<input type="button" value="Cancel"/>
General											
* Adaptation name:		<input type="text" value="Verizon_Test"/>									
Module name:		<input type="text" value="VerizonAdapter"/>									
Module parameter:		<input type="text"/>									
Egress URI Parameters:		<input type="text"/>									
Notes:		<input type="text"/>									
Digit Conversion for Incoming Calls to SM											
<input type="button" value="Add"/>		<input type="button" value="Remove"/>									
0 Items <input type="button" value="Refresh"/>										Filter: <input type="button" value="Enable"/>	
<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes		
Digit Conversion for Outgoing Calls from SM											
<input type="button" value="Add"/>		<input type="button" value="Remove"/>									
2 Items <input type="button" value="Refresh"/>										Filter: <input type="button" value="Enable"/>	
<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes		
<input type="checkbox"/>	* 4089908837	* 11	* 11		* 0		origination	9727289417			
<input type="checkbox"/>	* 4089908838	* 11	* 11		* 0		origination	9727289417			

The following screen shows the adaptation details for the adapter named “CM-ES-VZ” that will be assigned to the SIP Entity for Communication Manager. The “DigitConversionAdapter” is used and incoming digits are translated from DID numbers to local extensions for calls going out from Session Manager to Communication Manager. Alternatively, this could be done in Communication Manager in the *incoming-call-handling treatment* form for the trunk group.

Home / Elements / Routing / Adaptations
[Help ?](#)

Adaptation Details
Commit Cancel

General

* Adaptation name: CM-ES-VZ
Module name: DigitConversionAdapter
Module parameter:
Egress URI Parameters:
Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 4089908837	* 10	* 10		* 10	3011	both		
<input type="checkbox"/>	* 4089908838	* 10	* 10		* 10	2011	both		

Select : All, None

* Input Required
Commit Cancel

6.4. 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-1”, “Avaya-SBCE-2”, “ASM-62”, and “CM-Evolution-procr-5062” are relevant to these Application Notes.

SIP Entities				
<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"/>				
6 Items Refresh			Filter: Enable	
<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	ASM-62	10.80.140.160	Session Manager	
<input type="checkbox"/>	Avaya-SBCE-1	10.80.140.141	Other	Sipera-SBC-1 Outside 2.2.2.2
<input type="checkbox"/>	Avaya-SBCE-2	10.80.140.200	Other	Sipera-SBC-2 Outside 1.1.1.2
<input type="checkbox"/>	CM6.2	10.80.140.146	CM	
<input type="checkbox"/>	CM-Evolution-procr-5062	10.80.140.146	CM	CM-ES procr IP, different port
<input type="checkbox"/>	CM-Evolution-procr-5063	10.80.140.146	CM	CM-ES procr IP, different port
Select : All, None				

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.

SIP Entity Details		<input type="button" value="Commit"/> <input type="button" value="Cancel"/>
General		
* Name:	<input type="text" value="ASM-62"/>	
* FQDN or IP Address:	<input type="text" value="10.80.140.160"/>	
Type:	<input type="text" value="Session Manager"/>	
Notes:	<input type="text"/>	
Location:	<input type="text" value="Location_140"/>	
Outbound Proxy:	<input type="text"/>	
Time Zone:	<input type="text" value="America/Denver"/>	
Credential name:	<input type="text"/>	
SIP Link Monitoring		
SIP Link Monitoring:	<input type="text" value="Use Session Manager Configuration"/>	

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						
<input type="button" value="Add"/> <input type="button" value="Remove"/>						
5 Items Refresh						
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	ASM-62	TCP	* 5060	CM6.2	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5062	CM-Evolution-procr-5062	* 5062	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5063	CM-Evolution-procr-5063	* 5063	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	Avaya-SBCE-1	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	Avaya-SBCE-2	* 5060	Trusted

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”. To enable calls with Verizon IP Trunk to be distinguished from other types of SIP calls using the same Session Manager, TCP port 5062 was added, with **Default Domain** “avayalab.com”. Click the **Add** button to configure a new port. TCP was used in the sample configuration for improved visibility during testing.

Port

TCP Failover port: 5060

TLS Failover port: 5061

3 Items | [Refresh](#)
Filter: Enable

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

Select : All, None

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “Avaya-SBCE-1”. The **FQDN or IP Address** field is configured with the ASBCE inside IP Address (10.80.140.141). “Other” is selected from the **Type** drop-down menu for ASBCE SIP Entities. This ASBCE has been assigned to **Location** “Avaya-SBCE-1”, the “Verizon_Test” adapter is applied, and **SIP Link Monitoring** is enabled (to ensure expeditious failover in the 2-CPE testing) with both **Proactive Monitoring Interval** and **Reactive Monitoring Interval** set to 300 seconds. Other parameters (not shown) retain default values.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: Avaya-SBCE-1

* FQDN or IP Address: 10.80.140.141

Type: Other

Notes:

Adaptation: Verizon_Test

Location: Avaya-SBCE-1

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 300

* Reactive Monitoring Interval (in seconds): 300

* Number of Retries: 1

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “Avaya-SBCE-2”. The **FQDN or IP Address** field is configured with the ASBCE inside IP Address (10.80.140.200). “Other” is selected from the **Type** drop-down menu for ASBCE SIP Entities. This ASBCE has been assigned to **Location** “Avaya-SBCE-2”, the “Verizon_Test” adapter is applied, and **SIP Link Monitoring** has been enabled at 300 seconds. Other parameters retain default values.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: Avaya-SBCE-2

* FQDN or IP Address: 10.80.140.200

Type: Other

Notes:

Adaptation: Verizon_Test

Location: Avaya-SBCE-2

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 300

* Reactive Monitoring Interval (in seconds): 300

* Number of Retries: 1

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named “CM-Evolution-procr-5062”. The **FQDN or IP Address** field contains the IP Address of the “processor Ethernet” (10.80.140.146). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used, instead of, or in addition to, the “processor Ethernet”. “CM” is selected from the **Type** drop-down menu and the “CM-ES-VZ” Adaptation is selected.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: CM-Evolution-procr-5062

* FQDN or IP Address: 10.80.140.146

Type: CM

Notes: CM-ES procr IP, different port

Adaptation: CM-ES-VZ

Location:

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

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

6.5. 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 Communication Manager SIP trunk configuration), TCP was selected as the transport protocol for the 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 highlighted in yellow, named “Link_ASBCE-1”, “Link_ASBCE-2” and “Link_CM-ES-VZ-5062” 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 “Avaya-SBCE-1”, 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, the entity link named “ASM_Link_to_CM” uses TCP and port 5060 and the entity link used by Verizon IP Trunk named “Link_CM-ES-VZ-5062” uses TCP and port 5062.

Home / Elements / Routing / Entity Links								
Entity Links Help ?								
<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"/>								
9 Items Refresh Filter: Enable								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
<input type="checkbox"/>	ASM-62_CM521_tg3_5061_TLS	ASM-62	TLS	5061	CM521_tg3	5061	Trusted	
<input type="checkbox"/>	ASM-62_ModularMessaging_5060_TCP	ASM-62	TCP	5060	ModularMessaging	5060	Trusted	
<input type="checkbox"/>	ASM-CM521_tg1	ASM-62	TCP	5060	CM521_tg1	5060	Trusted	
<input type="checkbox"/>	ASM_Link_to_CM	ASM-62	TCP	5060	CM6.2	5060	Trusted	
<input type="checkbox"/>	CM-ES-VZ-5063	ASM-62	TCP	5063	CM-Evolution-procr-5063	5063	Trusted	VZ IPCC
<input type="checkbox"/>	Link_ASBCE-1	ASM-62	TCP	5060	Avaya-SBCE-1	5060	Trusted	SBC-Outside-222
<input type="checkbox"/>	Link_ASBCE-2	ASM-62	TCP	5060	Avaya-SBCE-2	5060	Trusted	SBC-Outside-111
<input type="checkbox"/>	Link_CM-ES-VZ-5062	ASM-62	TCP	5062	CM-Evolution-procr-5062	5062	Trusted	
<input type="checkbox"/>	Sipera-SBC-3	ASM-62	TCP	5060	Avaya-SBCE-3	5060	Trusted	SBC outside 1112

The link named “ASM_Link_to_CM” links Session Manager “ASM-62” with Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Verizon IP Trunk related configuration. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager.

The link named “Link_CM-ES-VZ-5062” also links Session Manager “ASM-62” with Communication Manager processor Ethernet. However, this link uses port 5062 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon IP Trunk from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

6.6. 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 (not shown).

The following screen shows the **Routing Policy Details** for the policy named “CM-ES-VZ_IPT_RPolicy” associated with DID calls from Verizon IP Trunk to Communication Manager as well as outbound calls from Communication Manager to Verizon. Observe the **SIP Entity as**

Destination is the entity named “CM-Evolution-procr-5062” which uses Communication Manager processor Ethernet IP Address (10.80.140.146).

Home / Elements / Routing / Routing Policies

Routing Policy Details Commit

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM-Evolution-procr-5062	10.80.140.146	CM	CM-ES procr IP, different port

The following screen shows the **Routing Policy Details** for the policy named “ASBCE-1-to-Vz_RPolicy” associated with outgoing calls from Communication Manager to the PSTN via Verizon through the ASBCE. Observe the **SIP Entity as Destination** as the entity named “Avaya-SBCE-1” that was created in **Section 6.4**.

Home / Elements / Routing / Routing Policies

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya-SBCE-1	10.80.140.141	Other	Sipera-SBC-1 Outside 2.2.2.2

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<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

The following screen shows the **Routing Policy Details** for the policy named “ASBCE-2-to-Vz_RPolicy” associated with outgoing calls from Communication Manager to the PSTN via

Verizon through the ASBCE. Observe the **SIP Entity as Destination** is the entity named “Avaya-SBCE-2”. In the **Time of Day** area, note that a **Ranking** can be configured. To allow the “Avaya-SBCE-2” to receive calls from Session Manager even when the “Avaya-SBCE-1” is operational, the default rank of 0 (also assigned to “Avaya-SBCE-1”) can be retained.

Home / Elements / Routing / Routing Policies

Routing Policy Details

[Help ?](#)

General

* Name: ASBCE-2-to-Vz-RPolicy

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya-SBCE-2	10.80.140.200	Other	Sipera-SBC-2 Outside 1.1.1.2

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<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

If it is intended that “Avaya-SBCE-1” should always be tried by Session Manager before “Avaya-SBCE-2”, the rank of “Avaya-SBCE-2” can be changed to 1 as shown below. Both the “load sharing” approach where “Avaya-SBCE-1” and “Avaya-SBCE-2” use the same rank, and the strict rank order priority of “Avaya-SBCE-1” over “Avaya-SBCE-2” were successfully tested in the sample configuration.

Routing Policy Details

Commit

Cancel

General

* Name: ASBCE-2-to-Vz-RPolicy

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya-SBCE-2	10.80.140.200	Other	Sipera-SBC-2 Outside 1.1.1.2

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	1		24/7		<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

6.7. 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.

6.7.1 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 408-990-8837, Verizon delivers the number to the enterprise, and the ASBCE sends the call to Session Manager. The pattern below matches on 408-990-XXXX. Dial patterns can alternatively match on ranges of numbers (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named “CM-ES-VZ_IPT_RPolicy” is selected, which sends the call to Communication Manager using port 5062 as described previously. In the Avaya Interoperability Lab configuration, calls to this number from any of the two originating locations, including the one with **Originating Location Name** “Avaya-SBCE-1”, are routed to Communication Manager.

Dial Pattern Details

Commit

Cancel

General

* Pattern: 408990

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add

Remove

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"/>	Avaya-SBCE-1	Avaya SBCE-1	CM-ES-VZ_IPT_RPolicy	0	<input type="checkbox"/>	CM-Evolution-procr-5062	Inbound VZ to unique CM port
<input type="checkbox"/>	Avaya-SBCE-2	Avaya-SBCE-2	CM-ES-VZ_IPT_RPolicy	0	<input type="checkbox"/>	CM-Evolution-procr-5062	Inbound VZ to unique CM port

6.7.2 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 9-1-303-XXX-XXX, 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-1” or the “Avaya-SBCE-2” via the **Routing Policy Name** “Avaya-SBCE-1-to-Verizon” and “Avaya-SBCE-2-to-Verizon”. The routing policy associated with the “Avaya-SBCE-2” for the pattern below has a rank of 1. With this configuration, all calls will use “Avaya-SBCE-1” first, and only try “Avaya-SBCE-2” if the call attempt through “Avaya-SBCE-1” is unsuccessful. Session Manager can be configured to distribute the calls among the ASBCEs (same rank) or prefer one ASBCE over another (different ranks).

Dial Pattern Details

Commit

Cancel

General

* Pattern: 1303

* Min: 11

* Max: 13

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add

Remove

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"/>	Location_140	Subnet 140	ASBCE-1-to-Vz_RPolicy	0	<input type="checkbox"/>	Avaya-SBCE-1	Outbound to Verizon via Siperia-1
<input type="checkbox"/>	Location_140	Subnet 140	ASBCE-2-to-Vz-RPolicy	1	<input type="checkbox"/>	Avaya-SBCE-2	

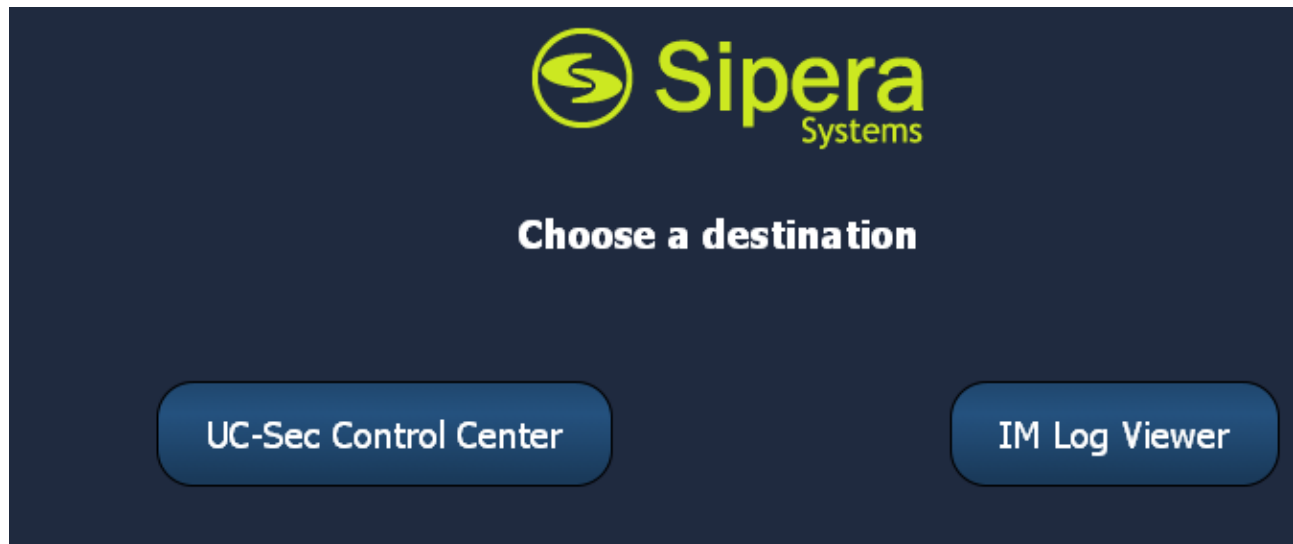
7. Configure Avaya Session Border Controller for Enterprise

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 SBC and the assignment of a management IP Address have already been completed.

7.1. Access the Management Interface

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**.

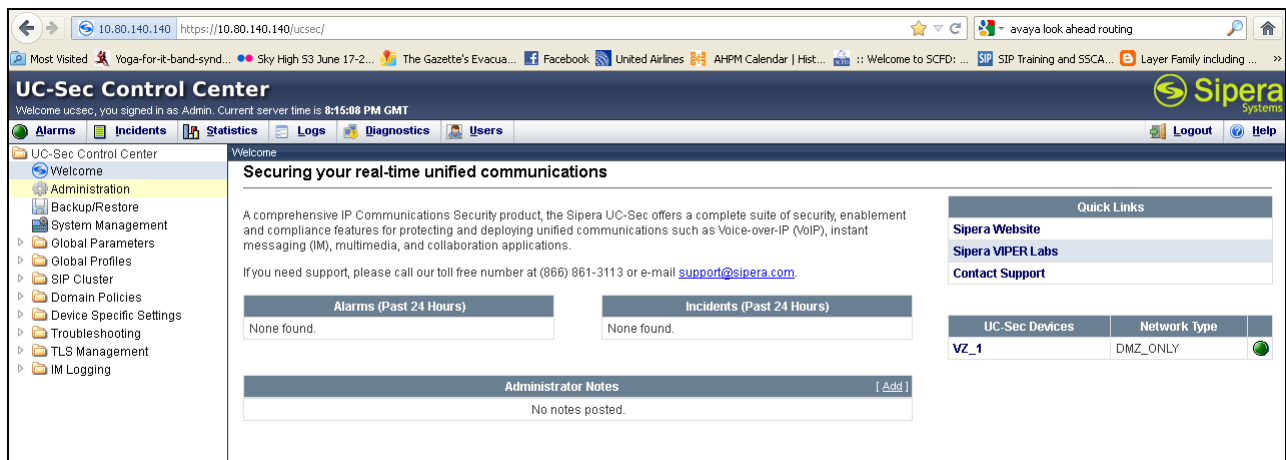


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

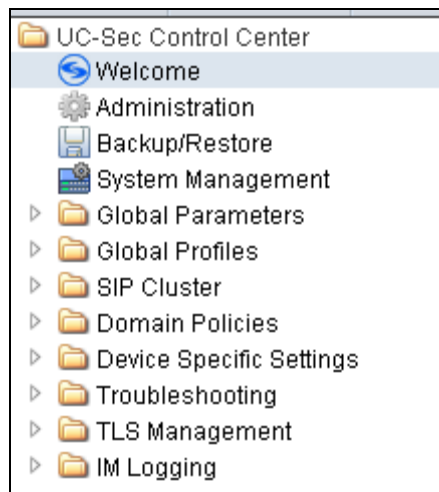
[Visit the Sipera Systems website to learn more.](#)

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.

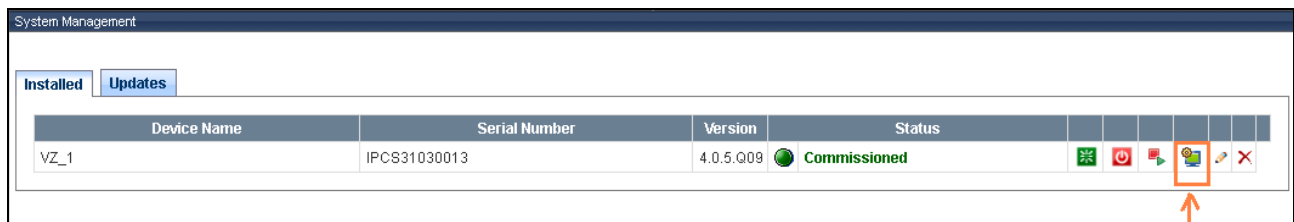
The main page of the UC-Sec Control Center will appear.



The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.



To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **Vz_1** is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).



The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: VZ_1

Network Configuration

General Settings

Appliance Name	VZ_1
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.80.140.141	10.80.140.141	255.255.255.0	10.80.140.1	A1
12.71.19.138	12.71.19.138	255.255.255.0	12.71.19.137	B1
12.71.19.141	12.71.19.141	255.255.255.0	12.71.19.129	B1

DNS Configuration

Primary DNS	
Secondary DNS	
DNS Location	DMZ
DNS Client IP	12.71.19.138

Management IP(s)

IP	10.80.140.140
----	---------------

7.2. Device Specific Settings

7.2.1 Define Network Information

Network information is required on the ASBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the ASBCE can have only one interface assigned. One internal interface addresses and two external interface addresses were required for the Verizon testing. To define the network information, navigate to **Device Specific Settings** → **Network Management** in the **UC-Sec Control Center** menu on the left hand side and click **Add IP**. A new line appears that can be configured.

- **IP Address:** Enter the IP Address for the internal interface
- **Gateway:** Enter the appropriate gateway IP Address
- **Interface:** Select the desired hardware interface (**A1**)

Click **Save Changes**.

Repeat the process for external interfaces using **B1**.

Note: Multiple IP addresses defined on a single interface must be in the same subnet.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 10:57:21 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

Device Specific Settings > Network Management: VZ_1

UC-Sec Devices

VZ_1

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
10.80.140.141		10.80.140.1	A1
12.71.19.138		12.71.19.137	B1
12.71.19.141		12.71.19.129	B1

Select the **Interface Configuration** tab and click on **Toggle State** to enable the A1 and B1 interfaces.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 10:57:57 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - SNMP
 - End Point Flows

Device Specific Settings > Network Management: VZ_1

UC-Sec Devices

VZ_1

Network Configuration Interface Configuration

Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

7.2.2 Signaling Interfaces

- To define the signaling interfaces on the ASBCE, navigate to **Device Specific Settings** → **Signaling Interface** in the **UC-Sec Control Center** menu on the left hand side and Select **Add Signaling Interface**.

Define a signaling interface for Verizon:

- Name** Enter a descriptive name for the external signaling interface for the Verizon network
- IP Address:** Choose the external address for the signaling
- TCP/UDP/TLS Port:** Enter the port for the desired protocol

Click **Finish** (not shown).

Repeat the process for the internal Avaya network.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 11:17:31 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface

Device Specific Settings > Signaling Interface: VZ_1

UC-Sec Devices

VZ_1

Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Inside_to_CPE	10.80.140.141	5060	5060	---	None	✎ ✕
Sig_Outside_to_Vz	12.71.19.138	---	5060	---	None	✎ ✕

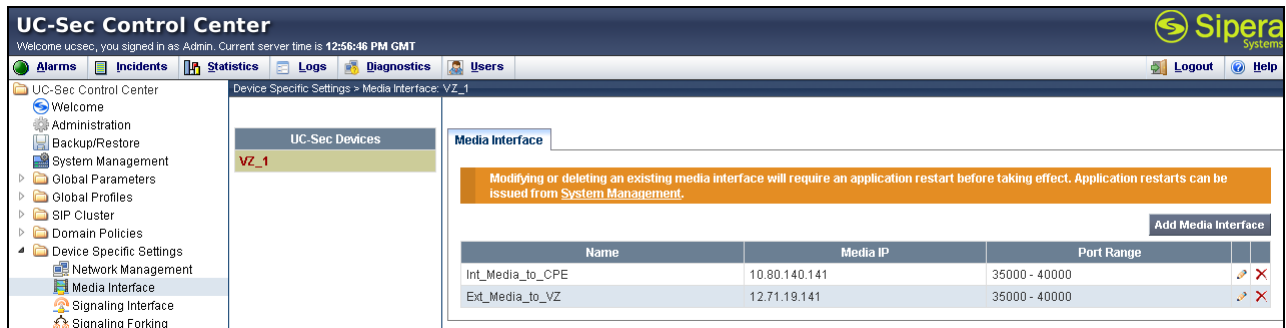
7.2.3 Media Interfaces

To define the media interfaces on the ASBCE, navigate to **Device Specific Settings** → **Media Interface** in the **UC-Sec Control Center** menu on the left hand side and select **Add Media Interface**. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signaling or can be different.

Define a media interface for Verizon:

- **Name** Enter a descriptive name for the external media interface for the Verizon network
- **IP Address:** Choose the external address for the media
- **Port Range:** Enter port ranges for the media path

Repeat the process for the internal Avaya network.



7.3. Global Profiles

Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.3.1 Routing Profile

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Create a Routing Profile for Session Manager and Verizon SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the primary Next Hop Server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop Server.
- **Next Hop Priority:** Check the checkbox.
- **Next Hop in Dialog:** (Optional) Check only if information in the Via Header is to be used instead of received port and IP.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish** (not shown).

The following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module. The **Outgoing Transport** must match the ASBCE Entity Link created on Session Manager in **Section 6.5**.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:39:32 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Route to SM6.2

Add Profile

Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

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

The following screen shows the Routing Profile to Verizon. In the **Next Hop Server 1** field enter the IP address with a colon and then the port number used for the Verizon IP Trunk. Check the **Next Hop Priority** option and enter **UDP** for the **Outgoing Transport** field.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:19:02 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Vz_IPT

Add Profile

Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profile

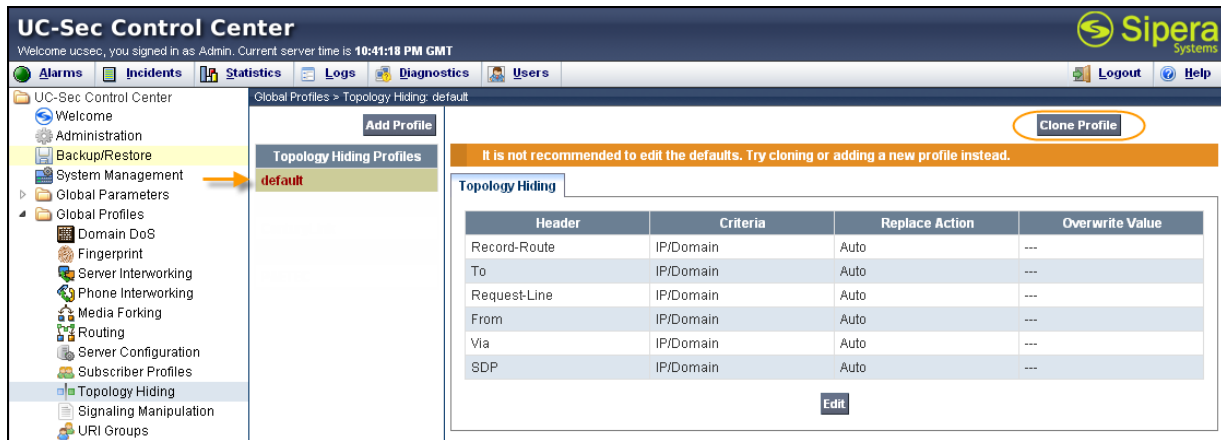
Add Routing Rule

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	+	63.79.179.178:5208	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

7.3.2 Topology Hiding Profile

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.

Create a Topology Hiding Profile for the enterprise and SIP Trunk. In the sample configuration, the **Enterprise** and **SIP Trunk** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center → Global Profiles → Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown below.



Enter a descriptive name for the new profile and click **Finish** (“Avaya” for the Enterprise profile and “Verizon_IPT” for the SIP Trunk profile).

Profile Name	default
Clone Name	Avaya

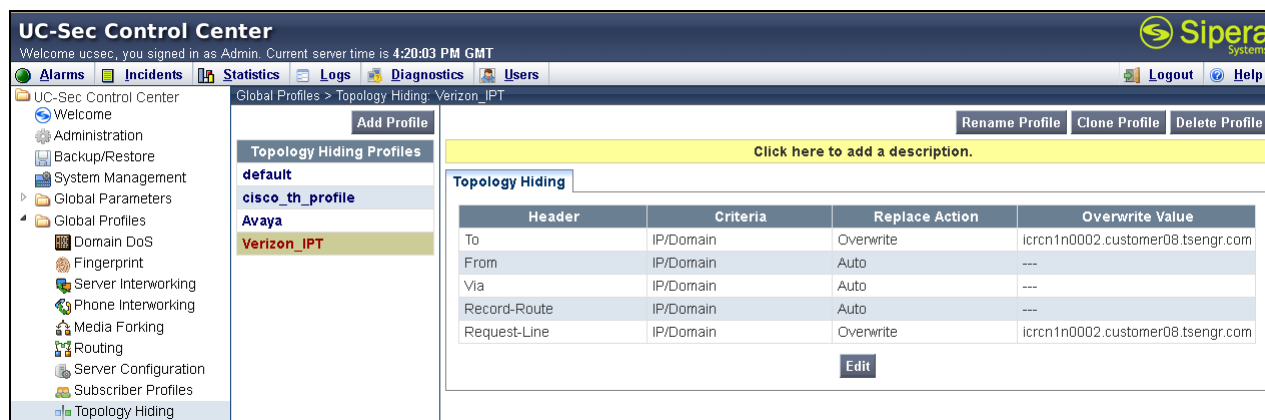
Finish

Edit the **Avaya** profile to overwrite the **To**, **Request-Line** and **From** headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.1**) and the Communication Manager signaling group Far-end Domain (**Section 5.7**). Click **Finish** to save the changes.

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

Finish

It is not necessary to modify the **Verizon_IPT** profile from the default values if IP addresses are used. Shown here is the domain for domestic circuits “icrcn1n0002.customer08.tsengr.com” set to overwrite the **To** and the **Request-Line**. The following screen shows the Topology Hiding Profile **Verizon_IPT** created for Verizon:



7.3.3 Server Interworking Profile

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

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

Interworking Profile ✕

Profile Name

Verizon_IPT

Next

In the new window that appears, default values can be used. Click **Next** to continue.

Editing Profile: Verizon-IPCC

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 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

Next

Default values can also be used for the next two windows that appear. Click **Next** to continue.

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
Back	Next

Interworking Profile	
Configuration is not required. All fields are optional.	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
Transport Timers	
TCP Connection Inactive Timer	<input type="text"/> seconds, [600 - 3600]
Back	Next

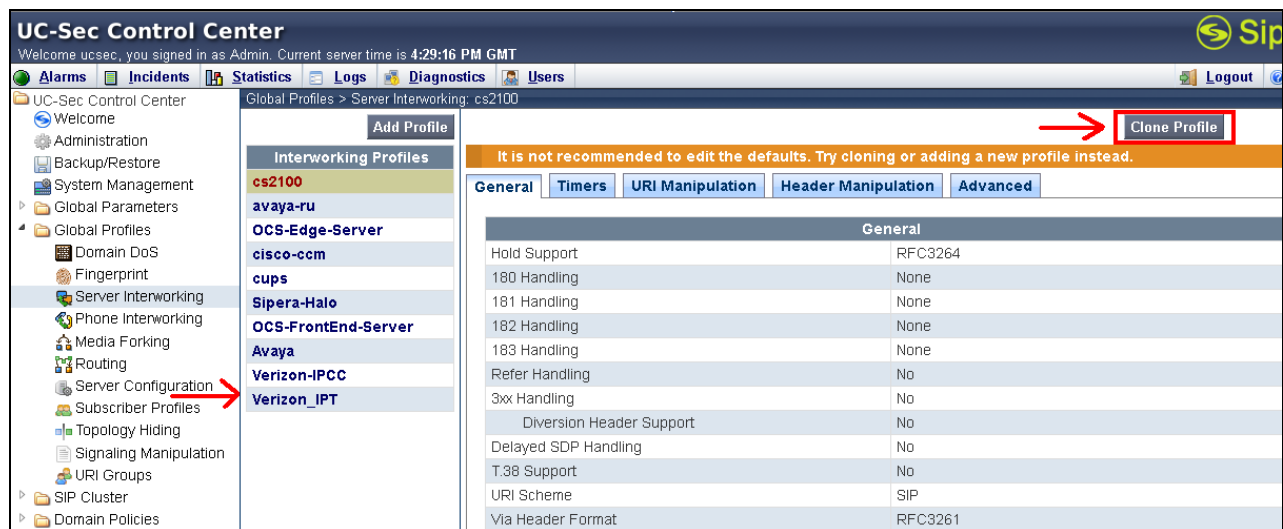
On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

Click **Finish** to save changes.

Interworking Profile	
Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLIC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>
Back	Finish

The **Avaya** profile (for the enterprise) will be created by cloning the **Verizon_IPT** profile created in the previous section. To clone a Server Interworking Profile, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on the previously created **Verizon_IPT** profile, then click on **Clone Profile** as shown below.



Enter a descriptive name for the new profile and click **Finish** to save the profile.

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

Profile Name	Verizon_IPT
Clone Name	Avaya

A red box highlights the 'Avaya' text in the 'Clone Name' field. A 'Finish' button is located at the bottom right of the dialog.

7.3.4 Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the ASBCE. Using this language, a script can be written and tied to a given flow through the web management interface. The ASBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and to remove unwanted headers in the SIP messages to and from Verizon. To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown).

A new blank SigMa Editor window will pop up. The script will act on all outbound traffic to Verizon after the SIP message has been routed through the ASBCE. The script is further broken down as follows:

- **within session “ALL”** Transformations applied to all SIP sessions.
- **act on message** Actions to be taken to any SIP message.
- **%DIRECTION=“OUTBOUND”** Applied to a message leaving the Avaya SBCE.
- **%ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has been routed through the Avaya SBCE.
- **Remove(%HEADERS[“Alert-Info”][1]);** Used to remove an entire header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message.
- **%HEADERS[“Contact”][1];** Used to replace a value in the header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message. **See Section 2.2. CONTACT HEADER.**
- **%HEADERS[“P-Asserted-Identity”][1];** Used to replace a value in the header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message. **See Section 2.2 P-ASSERTED-IDENTITY.**

With this script, the Endpoint-View, Alert-Info, User-Agent, Server, and P-Location headers will be removed. The Contact Header and P-Asserted Identity Headers that match on the first value will be replaced with the second value.

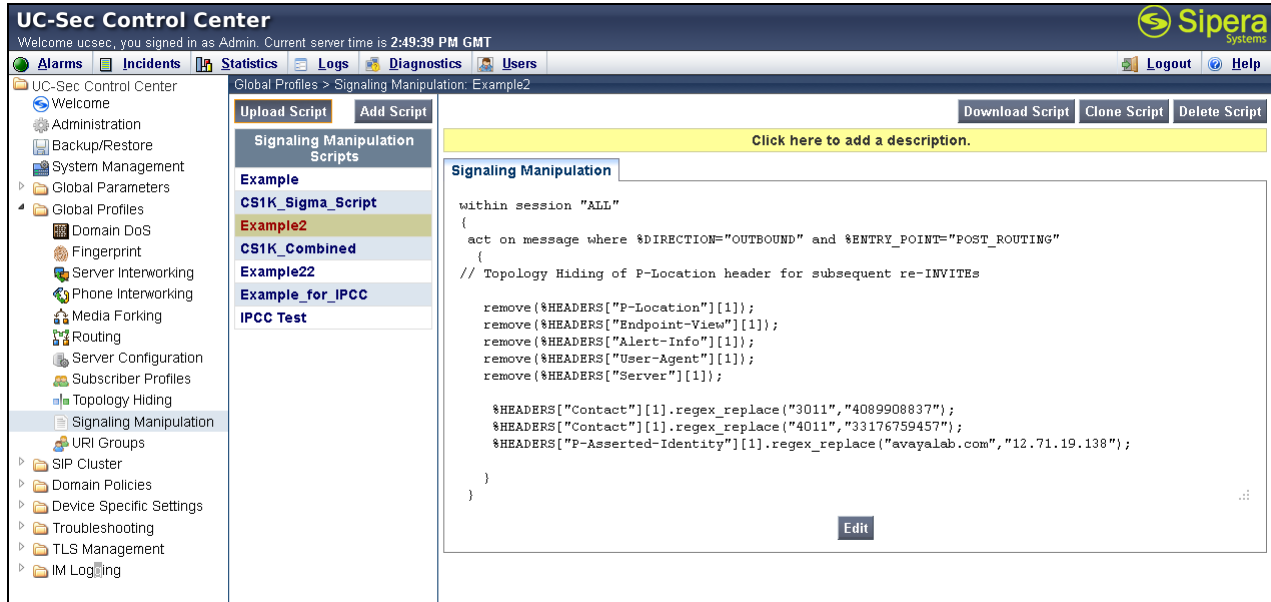
```

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     remove(%HEADERS["P-Location"][1]);
8     remove(%HEADERS["Endpoint-View"][1]);
9     remove(%HEADERS["Alert-Info"][1]);
10    remove(%HEADERS["User-Agent"][1]);
11    remove(%HEADERS["Server"][1]);
12
13    %HEADERS["Contact"][1].regex_replace("3011", "4089908837");
14    %HEADERS["Contact"][1].regex_replace("4011", "33176759457");
15    %HEADERS["P-Asserted-Identity"][1].regex_replace("avayalab.com", "12.71.19.138");
16
17  }
18 }
19

```

Click **Save**.

The following screen shows the finished Signaling Manipulation Script **Example2**. This script will later be applied to the Verizon Server Configuration in **Section 7.3.5**. The details of these script elements can be found in **Appendix B**.



7.3.5 Server Configuration for Session Manager

Servers are defined for each server connected to the ASBCE. In this case, Verizon is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager Server, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the pop-up menu.

The screenshot shows a dialog box titled 'Add Server Configuration Profile'. It has a close button (X) in the top right corner. The 'Profile Name' field contains the text 'Avaya_SM6.2'. Below the field is a 'Next' button.

In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module
- **Supported Transports:** Select **TCP**. This is the transport protocol used in the ASBCE Entity Link on Session Manager **Section 6.5**

- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the ASBCE Entity Link on Session Manager in **Section 6.5**.

Click **Next** to continue.

Verify **Enable Authentication** is unchecked as Session Manager does not require authentication. Click **Next** to continue.

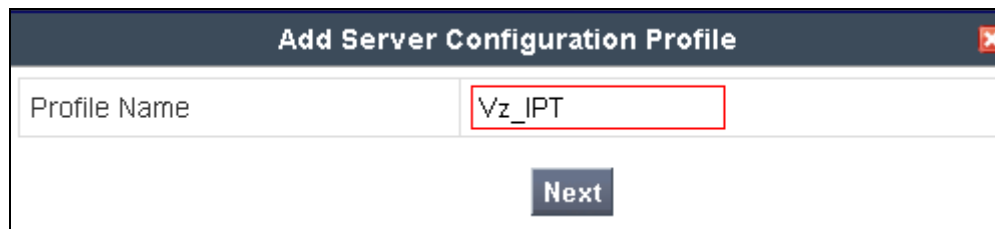
Click **Next** to continue.

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.3.3**, in **Signaling Manipulation Script** select a script if desired. Use default values for all remaining fields. Click **Finish** to save the configuration.

7.3.6 Server Configuration for Verizon IPT

In the Routing Profile created in **Section 7.3.1**, there were two IP addresses configured for one routing profile. In the Server Configuration section both of these addresses will be configured.

To define the Verizon IP Trunk navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and repeat the instructions above with the displayed values.

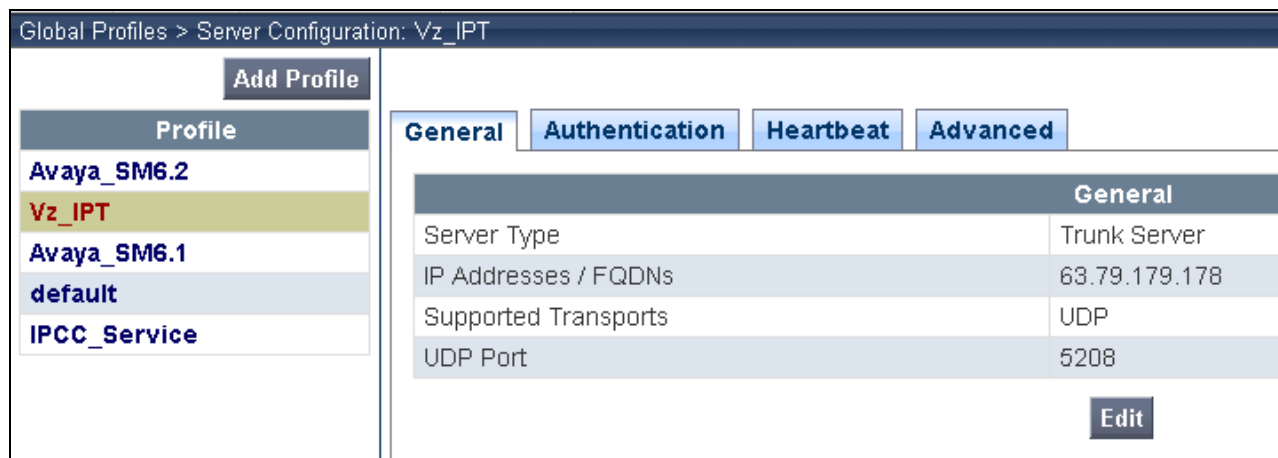


Add Server Configuration Profile

Profile Name: Vz_IPT

Next

General tab: select **Trunk Server** as the **Server Type** and specify **IP Addresses**, Supported Transport, and UDP Port .



Global Profiles > Server Configuration: Vz_IPT

Add Profile

Profile

- Avaya_SM6.2
- Vz_IPT**
- Avaya_SM6.1
- default
- IPCC_Service

General | **Authentication** | **Heartbeat** | **Advanced**

General	
Server Type	Trunk Server
IP Addresses / FQDNs	63.79.179.178
Supported Transports	UDP
UDP Port	5208

Edit

Authentication and **Heartbeat** tabs (notice that external OPTIONS are enabled in this configuration):

In the new window that appears, OPTIONS were only configured for the Verizon side. Enter the following values. Use default values for all remaining fields:

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing **60** seconds was chosen for the Verizon side only.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Add Server Configuration Profile - Authentication

Enable Authentication ☐

User Name

Realm

Password

Confirm Password

Back **Next**

Edit Server Configuration Profile - Heartbeat

Enable Heartbeat ☒

Method OPTIONS

Frequency seconds

From URI

To URI

TCP Probe ☐

TCP Probe Frequency seconds

Finish

Advanced tab: select **Vz_IPT** for **Interworking Profile** and **Example2** as the **Signaling Manipulation Script**.

Global Profiles > Server Configuration: Vz_IPT

Add Profile

Profile
Avaya_SM6.2
Vz_IPT
Avaya_SM6.1
default
IPCC_Service

General Authentication Heartbeat **Advanced**

Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Verizon_IPT
Signaling Manipulation Script	Example2
UDP Connection Type	SUBID

Edit

Click **Finish** to save changes (not shown).

7.4. Domain Policies – Media Rules

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

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.

UC-Sec Control Center

Alarms Incidents Statistics Logs Diagnostics Users

UC-Sec Control Center

Domain Policies > Media Rules: default-low-med

Add Rule

Filter By Device...

Clone Rule

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 Turing Test

Media NAT Learn Media IP dynamically

Edit

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

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

Add Rule Filter By Device... **Rename Rule** **Clone Rule** **Delete Rule**

Click here to add a description.

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

Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

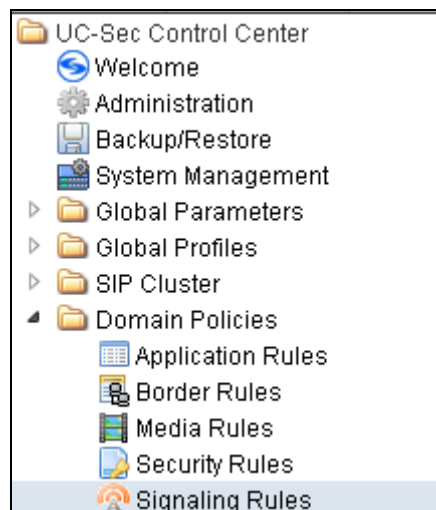
Audio DSCP EF

Video QoS

Video DSCP EF

7.5. 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

Next

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			
Add Rule	Filter By Device...	Rename Rule Clone Rule Delete Rule	
Click here to add a description.			
Signaling Rules default No-Content-Type-Checks HideP-Loc signal-QoS Block_Hdr_Remark	General Requests Responses Request Headers Response Headers Signaling QoS		
Signaling QoS <input checked="" type="checkbox"/>			
QoS Type DSCP			
DSCP AF32			

7.6. 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.

Domain Policies > End Point Policy Groups: default-low	
Add Group	Filter By Device...
Policy Groups	It is not recommended to edit the defaults. Try adding a new group instead.

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 **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**.

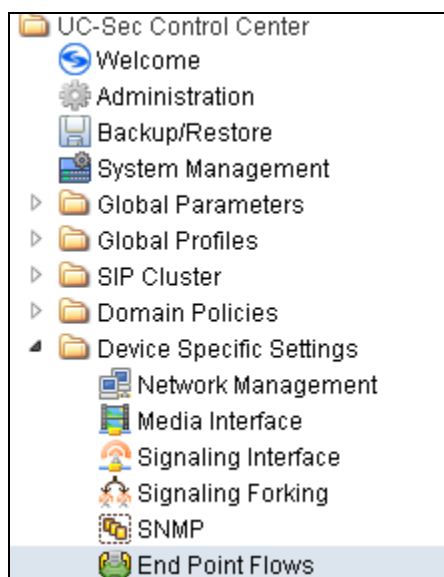
Policy Group	
Application Rule	default
Border Rule	default
Media Rule	default-low-med-QoS
Security Rule	default-low
Signaling Rule	Block_Hdr_Remark
Time of Day Rule	default
<div>Back Finish</div>	

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

ps: default-low-remark							
Filter By Device...						Rename Group Delete Group	
Click here to add a description.							
Hover over a row to see its description.							
Policy Group						View Summary Add Policy Set	
Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default	default	default-low-med-QoS	default-low	Block_Hdr_Remark	default	

7.7. Device Specific Settings – End Point Flows

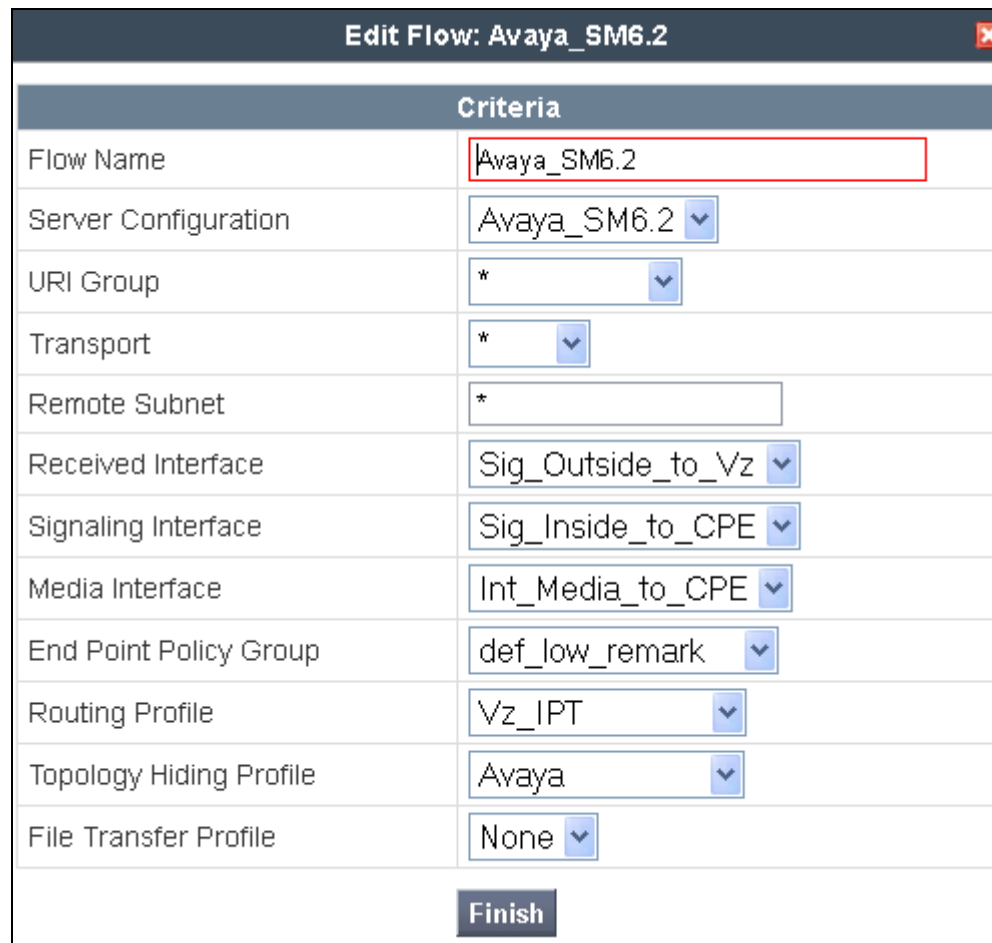
Select **Device Specific Setting** → **End Point Flows** from the left-side menu as shown below.



Under **UC-Sec Devices**, select the device being managed, which was named “Vz_1” in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.



The following screen shows the flow named “Avaya_SM6.2” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.



Criteria	
Flow Name	Avaya_SM6.2
Server Configuration	Avaya_SM6.2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_to_Vz
Signaling Interface	Sig_Inside_to_CPE
Media Interface	Int_Media_to_CPE
End Point Policy Group	def_low_remark
Routing Profile	Vz_IPT
Topology Hiding Profile	Avaya
File Transfer Profile	None
<div>Finish</div>	

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

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

Edit Flow: Verizon_IP_Trunk ✕

Criteria	
Flow Name	<input style="width: 90%;" type="text" value="Verizon_IP_Trunk"/>
Server Configuration	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Vz_IPT ▼</div>
URI Group	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">* ▼</div>
Transport	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">* ▼</div>
Remote Subnet	<input style="width: 90%;" type="text" value="*"/>
Received Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Sig_Inside_to_CPE ▼</div>
Signaling Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Sig_Outside_to_Vz ▼</div>
Media Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Ext_Media_to_VZ ▼</div>
End Point Policy Group	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">def_low_remark ▼</div>
Routing Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Route to SM6.2 ▼</div>
Topology Hiding Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">Verizon_IPT ▼</div>
File Transfer Profile	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;">None ▼</div>

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

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_SM6.2	*	*	*	Sig_Outside_to_Vz	Sig_Inside_to_CPE	Int_Media_to_CPE	def_low_remark	Vz_IPT	Avaya	None		

Server Configuration: Vz_IPT

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	Verizon_IP_Trunk	*	*	*	Sig_Inside_to_CPE	Sig_Outside_to_Vz	Ext_Media_to_VZ	def_low_remark	Route to SM6.2	Verizon_IPT	None		

8. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business IDA Trunk service.

8.1. Illustration of OPTIONS Handling

This section illustrates SIP OPTIONS monitoring of the SIP trunk from Verizon to the CPE and from the CPE to Verizon through the ASBCE.

The following screens from a filtered Wireshark trace illustrate OPTIONS sent by Verizon to the 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 ASBCE, frame 5 is highlighted and expanded to show OPTIONS sent from Verizon IP Trunk (63.79.179.178) to the ASBCE (12.71.19.138). Observe the use of UDP for transport, from source port 5208 (Verizon) to destination port 5060 (Avaya). Verizon sends the Avaya domain “12.71.19.138” in the Request-Line. Note that Max-Forwards is 70.

No.	Time	Source	Destination	Protocol	Info
5	43.898498	63.79.179.178	12.71.19.138	SIP	Request: OPTIONS sip:12.71.19.138:5060
6	43.903917	12.71.19.138	63.79.179.178	SIP	Status: 200 OK

Frame 5: 407 bytes on wire (3256 bits), 407 bytes captured (3256 bits)
Ethernet II, Src: Netscreen_3f:c8:46 (00:10:db:3f:c8:46), Dst: IntelCor_cc:23:11 (00:1b:21:cc:23:11)
Internet Protocol Version 4, Src: 63.79.179.178 (63.79.179.178), Dst: 12.71.19.138 (12.71.19.138)
User Datagram Protocol, Src Port: 5208 (5208), Dst Port: sip (5060)
Session Initiation Protocol
Request-Line: OPTIONS sip:12.71.19.138:5060 SIP/2.0
Message Header
Via: SIP/2.0/UDP 63.79.179.178:5208;branch=z9hG4bKn1f51h10201h8mot31s1
Call-ID: 14d99343e60f43fb8e0b62e5ad182dc1000uiu3@63.79.179.178
To: sip:ping@c0800000633-scs-n0002-1
From: <sip:ping@63.79.179.178>;tag=cdc02e03ddf74a68581c44eb12343cb3000uiu3
Max-Forwards: 70
CSeq: 12285 OPTIONS
Route: <sip:12.71.19.138:5060;lr>

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 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-1 (i.e., not load balanced). Session Manager sends the call to Communication Manager (after manipulating the digits) via the entity link with port 5062. On Communication Manager, the incoming call arrives via signaling group 68 and trunk group 68.

The following edited Communication Manager *list trace tac* trace output shows a call incoming on trunk group 68. The PSTN telephone dialed 408-990-8837. Session Manager can map the number received from Verizon to the extension of a Communication Manager telephone (x2011), or the incoming call handling table for trunk group 68 can do the same. In the trace below, Session

Manager had already mapped the Verizon DID to a Communication Manager extension. Extension 2011 is an IP Telephone with IP address 10.80.140.133 in Region 1. Initially, the G450 Media Gateway (10.80.140.148) 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 (10.80.140.133) to the “inside” of the ASBCE (10.80.140.141).

list trace tac *168		Page 1
LIST TRACE		
time	data	
12:56:00	TRACE STARTED 08/08/2012 CM Release String cold-02.0.823.0-19926	
12:56:14	SIP<INVITE sip:2011@avayalab.com SIP/2.0	
12:56:14	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:14	active trunk-group 68 member 1 cid 0xadf	
12:56:14	SIP>SIP/2.0 183 Session Progress	
12:56:14	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:14	dial 2011	
12:56:14	ring station 2011 cid 0xadf	
12:56:14	G711MU ss:off ps:20	
	rgn:1 [10.80.140.133]:2064	
	rgn:1 [10.80.140.148]:2054	
12:56:14	G729 ss:off ps:20	
	rgn:4 [10.80.140.141]:35034	
	rgn:1 [10.80.140.148]:2056	
12:56:14	xoip options: fax:T38 modem:off tty:US uid:0x5001f	
	xoip ip: [10.80.140.148]:2056	
12:56:16	SIP>SIP/2.0 200 OK	
12:56:16	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:16	active station 2011 cid 0xadf	
12:56:16	SIP<ACK sip:+4089908838@10.80.140.146:5062;transport=tcp SI	
12:56:16	SIP<P/2.0	
12:56:16	Call-ID: BW134449745080812-1699702071@63.79.178.210	
	///INVITE from Communication Manager for shuffling from the Gateway ///	
12:56:16	SIP>INVITE sip:7025704580@10.80.140.141:5060;transport=tcp	
12:56:16	SIP>SIP/2.0	
12:56:16	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:16	SIP<SIP/2.0 100 Trying	
12:56:16	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:16	SIP<SIP/2.0 200 OK	
12:56:16	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:16	SIP>ACK sip:7025704580@10.80.140.141:5060;transport=tcp SIP	
12:56:16	SIP>/2.0	
12:56:16	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:16	G729A ss:off ps:20	
	rgn:4 [10.80.140.141]:35034	
	rgn:1 [10.80.140.133]:2064	
12:56:16	G729 ss:off ps:20	
	rgn:1 [10.80.140.133]:2064	
	rgn:4 [10.80.140.141]:35034	
12:56:22	SIP<BYE sip:+4089908838@10.80.140.146:5062;transport=tcp SI	
12:56:22	SIP<P/2.0	
12:56:22	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:22	SIP>SIP/2.0 200 OK	
12:56:22	Call-ID: BW134449745080812-1699702071@63.79.178.210	
12:56:22	idle trunk-group 68 member 1 cid 0xadf	

The following screen shows **Page 2** of the output of the *status trunk* command pertaining to this same call. Note the signaling using port 5062 between Communication Manager and Session Manager. Note the media is “ip-direct” from the IP Telephone (10.80.140.133) to the inside IP address of ASBCE (10.80.140.141) using G.729A.

```

status trunk 68/1                                     Page 2 of 3
CALL CONTROL SIGNALING
Near-end Signaling Loc: PROCR
  Signaling   IP Address      Port
  Near-end:   10.80.140.146    : 5062
  Far-end:    10.80.140.160    : 5062
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.729A
  Audio   IP Address      Port
  Near-end: 10.80.140.133    : 2890
  Far-end:  10.80.140.141    : 35070

Video Near:
Video Far:
Video Port:
Video Near-end Codec:      Video Far-end Codec:

```

The following screen shows **Page 3** of the output of the *status trunk* command pertaining to this same call. Here it can be observed that G.729A codec is used.

```

status trunk 68/1                                     Page 3 of 3
SRC PORT TO DEST PORT TALKPATH
src port: T00031
T00031:TX:10.80.140.141:35070/g729a/20ms
S00001:RX:10.80.140.133:2890/g729a/20ms

dst port: S00001

```

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.

▼ Session Manager
Dashboard
Session Manager
Administration
Communication Profile Editor
▶ Network Configuration
▶ Device and Location Configuration
▶ Application Configuration
▼ System Status
System State
Administration
SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Run Monitor

1 Item | Refresh

<input type="checkbox"/>	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<input type="checkbox"/>	ASM-62	0/5	0	0	0

Select : All, None

All Monitored SIP Entities

Run Monitor

5 Items | Refresh | Show **ALL** ▼

Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	Avaya-SBCE-1
<input type="checkbox"/>	Avaya-SBCE-2
<input type="checkbox"/>	CM-Evolution-procr-5062
<input type="checkbox"/>	CM-Evolution-procr-5063
<input type="checkbox"/>	CM6.2

Select : All, None

From the list of monitored entities, select an entity of interest, such as “Avaya-SBCE-1”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below.

SIP Entity, Entity Link Connection Status

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-1

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	10.80.140.141	5060	TCP	Up	200 OK	Up

Return to the list of monitored entities, and select another entity of interest, such as “CM-Evolution-procr-5062”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. Note the use of port 5062.

SIP Entity, Entity Link Connection Status

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: CM-Evolution-procr-5062

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	10.80.140.146	5062	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.

▼ Session Manager
Dashboard
Session Manager
Administration
Communication Profile
Editor
▶ Network Configuration
▶ Device and Location
Configuration
▶ Application Configuration
▶ System Status
▼ System Tools
Maintenance Tests
SIP Tracer
Configuration
SIP Trace Viewer
Call Routing Test

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 <input type="text"/>	Calling Party Address <input type="text"/>
Calling Party URI <input type="text"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Wednesday"/>	Time (UTC) <input type="text" value="16:24"/>
Called Session Manager Instance <input type="text" value="ASM-62"/>	Transport Protocol <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 ASBCE on the path to Verizon. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Home / Elements / Session Manager / System Tools / Call Routing Test

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 3035387022@avayalab.com	Calling Party Address
Calling Party URI anycaller@anydomain	Session Manager Listen Port 5060
Day Of Week Wednesday	Time (UTC) 0:08
Called Session Manager Instance ASM-62	Transport Protocol TCP
Execute Test	

Routing Decisions

Route < sip:3035387022@avayalab.com > to SIP Entity Avaya-SBCE-1 (10.80.140.141). Terminating Location is Avaya-SBCE-1.

Route < sip:3035387022@avayalab.com > to SIP Entity Avaya-SBCE-2 (10.80.140.200). Terminating Location is Avaya-SBCE-2.

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.

Alarms (Past 24 Hours)

None found.

Incidents (Past 24 Hours)

VZ_1: General Method not allowed Out-Of-Dialog
VZ_1: Request Timeout
VZ_1: General Method not allowed Out-Of-Dialog
VZ_1: General Method not allowed Out-Of-Dialog
VZ_1: General Method not allowed Out-Of-Dialog

Quick Links

Sipera Website
Sipera VIPER Labs
Contact Support

UC-Sec Devices	Network Type	
VZ_1	DMZ_ONLY	

Administrator Notes

[Add]
No notes posted.

8.4.2 Alarms

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



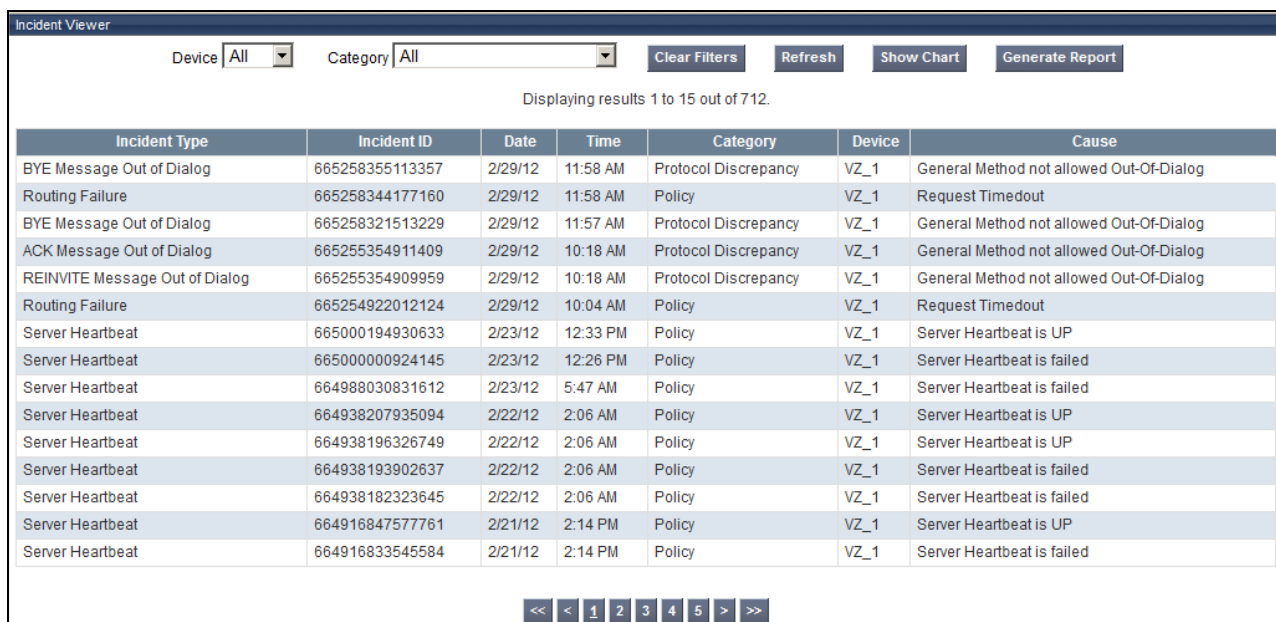
Click the Alarm button to open the Alarms Viewer.



8.4.3 Incidents

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

Click the Incidents button to open the Incident Viewer.

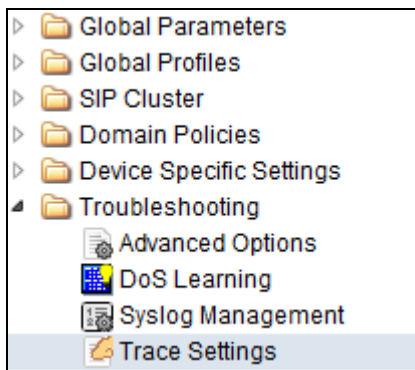


Further Information can be obtained by clicking on an incident in the incident viewer.

Incident Information				
General Information				
Incident Type	Server Heartbeat		Category	Policy
Timestamp	February 23, 2012 12:33:09 PM GMT		Device	VZ_1
Cause	Server Heartbeat is UP			
Message Data				
Response Code	200		Transport	TCP
Call ID	8d57142cb6a4bb2db3ab5301a040b218shiepaerrtab		From	sip:ping@avayalab.com
To	sip:ping@avayalab.com		Source IP	10.80.140.160
Destination IP	10.80.140.141			

8.4.4 Tracing

To take a call trace, Select **Troubleshooting** → **Trace Settings** 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
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	Test_trace.pcap		
Existing captures with the same name will be overwritten			
Start Capture		Clear	

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.

Packet Trace
Call Trace
Packet Capture
Captures

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

Packet Capture Configuration

Currently capturing	Yes
Interface	A1
Local Address (ip:port)	All :
Remote Address (*, *:port, ip, ip:port)	*
Protocol	All
Maximum Number of Packets to Capture	9999
Capture Filename Existing captures with the same name will be overwritten	Test_trace.pcap

Stop Capture

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

Packet Trace	Call Trace	Packet Capture	Captures	
				Refresh
File Name	File Size (bytes)	Last Modified		
Test_trace_20120229160214.pcap	49,152	February 29, 2012 4:02:26 PM GMT	✕	

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Trunk service, inclusive of the “2-CPE” SIP trunk redundancy architecture. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users 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 6.2
- [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>

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 the Customer passes through the Company’s network for Caller ID display purposes only. There is no charge for this feature. If a Customer selects this feature, Verizon will designate one of the 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 972-728-9417. 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 Calling Line Identification).

- Login to Session Manager as shown in **Section 6** 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** field. In the **Module parameter** field enter any domain adaptations that may be needed or alternatively they can be overwritten in the ASBCE.
- Scroll down to the **Digit Conversion for Outgoing Calls from SM** section, enter a **Matching Pattern** (e.g. 408-990-8837), with the **Min** and **Max** number of digits to match on, in the **Address to modify** field, enter **origination**, and in the **Adaptation Data** field enter the screened telephone number (e.g. 972-728-9417) provided by Verizon.
- Click **Commit**.

Home / Elements / Routing / Adaptations

Adaptation Details

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

0 Items [Refresh](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------

Digit Conversion for Outgoing Calls from SM

2 Items [Refresh](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 4089908837	* 10	* 11	<input type="text"/>	* 0	<input type="text"/>	origination	9727289417
<input type="checkbox"/>	* 4089908838	* 10	* 11	<input type="text"/>	* 0	<input type="text"/>	origination	9727289417

Select : All, None

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 **Section 6** above, and select the “Avaya-SBCE-1” entity. Under **Adaptation**, change to the newly created “Verizon_Test” adaptation.

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Verification

In the following filter Wireshark trace, it is observed that the From line contains the DID number, 408-990-8837 and in the P-Asserted-Identity header, a Diversion header has been added with the unscreened ANI (972-728-9417).

From: "4089908837"

<sip:4089908837@12.71.19.138:5060>;tag=8014d04750d7e117f2650169c5c00

Diversion: <sip: 9727289417@12.71.19.138:5060>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	12.71.19.138	63.79.179.17	SIP/SDP	Request: INVITE sip:13035387022@icrcnln0002.customer0
2	0.037845	63.79.179.178	12.71.19.138	SIP	Status: 100 Trying
3	2.159664	63.79.179.178	12.71.19.138	SIP/SDP	Status: 183 Session Progress, with session descriptio
222	4.259740	63.79.179.178	12.71.19.138	SIP/SDP	Status: 200 OK, with session description
224	4.269779	12.71.19.138	63.79.179.17	SIP	Request: ACK sip:13035387022@63.79.179.178:5208
564	7.658681	63.79.179.178	12.71.19.138	SIP	Request: BYE sip:4089908837@12.71.19.138:5060
566	7.666402	12.71.19.138	63.79.179.17	SIP	Status: 200 OK

Frame 1: 1279 bytes on wire (10232 bits), 1279 bytes captured (10232 bits)

Ethernet II, Src: IntelCor_cc:23:11 (00:1b:21:cc:23:11), Dst: Netscreen_3f:c8:46 (00:10:db:3f:c8:46)

Internet Protocol Version 4, Src: 12.71.19.138 (12.71.19.138), Dst: 63.79.179.178 (63.79.179.178)

User Datagram Protocol, Src Port: sip (5060), Dst Port: 5208 (5208)

Session Initiation Protocol

Request-Line: INVITE sip:13035387022@icrcnln0002.customer08.tsengr.com SIP/2.0

Message Header

From: "4089908837" <sip:4089908837@12.71.19.138:5060>;tag=8014d04750d7e117f2650169c5c00

To: <sip:13035387022@icrcnln0002.customer08.tsengr.com>

CSeq: 1 INVITE

Call-ID: 8014d04750d7e11802650169c5c00

Contact: "4089908837" <sip:4089908837@12.71.19.138:5060>

Record-Route: <sip:12.71.19.138:5060;ipcs-line=4494;lr;transport=udp>

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

Supported: 100rel, join, replaces, sdp-anat, timer

Max-Forwards: 67

Via: SIP/2.0/UDP 12.71.19.138:5060;branch=z9hG4bK-s1632-000847247051-1--s1632-

Accept-Language: en

P-Asserted-Identity: "4089908837" <sip:4089908837@12.71.19.138:5060>

Session-Expires: 1800;refresher=uac

Min-SE: 1800

Diversion: <sip:9727289417@12.71.19.138:5060>

Content-Type: application/sdp

P-Charging-Vector: icid-value="AAS:1340-47d014801e1d7501650267e5c9c"

Content-Length: 279

Message Body

Appendix B: Avaya Session Border Control for Enterprise – Sigma Script “EXAMPLE 2”

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and
  %ENTRY_POINT="POST_ROUTING"
  {
    // Topology Hiding of P-Location header for subsequent re-INVITEs

    remove(%HEADERS["P-Location"][1]);
    remove(%HEADERS["Endpoint-View"][1]);
    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["User-Agent"][1]);
    remove(%HEADERS["Server"][1]);

    %HEADERS["Contact"][1].regex_replace("3011","4089908837");
    %HEADERS["Contact"][1].regex_replace("4011","33176759457");
    %HEADERS["P-Asserted-Identity"][1].regex_replace("avayalab.com","12.71.19.138");

  }
}
```

©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.