



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center VoIP Inbound – Issue 1.0

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) IP Toll Free VoIP Inbound Service. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP Trunk Service offers. These Application Notes illustrate IP Toll Free VoIP Inbound. This service provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Avaya Aura® Communication Manager. The Network Call Redirection (NCR) and SIP User-to-User Information (UII) features can be utilized together to transmit UII within SIP signaling messages to alternate destinations via the Verizon network. These Application Notes update previously published Application Notes with newer versions of Avaya Aura® Communication Manager and Avaya Aura® Session Manager, and present an example configuration for the Avaya Session Border Controller for Enterprise.

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 in the Avaya Solution & Interoperability Test Lab, utilizing a Verizon Business Dedicated Internet Access (IDA) circuit connection to the production Verizon Business IPCC Services.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	6
2.3.	Support.....	7
2.3.1	Avaya	7
2.3.2	Verizon.....	7
3.	Reference Configuration	8
3.1.	History Info and Diversion Headers	9
4.	Equipment and Software Validated	10
5.	Configure Communication Manager Release 5.2.1	10
5.1.	Verify Licensed Features	11
5.2.	System Features	13
5.3.	Node Names.....	14
5.4.	IP Interface for procr.....	15
5.5.	IP Codec Sets	15
5.6.	IP Network Region	16
5.7.	Signaling Group	18
5.8.	SIP Trunk Groups	19
5.9.	Contact Center Configuration	22
5.9.1	Announcements.....	23
5.9.2	Post-Answer Redirection to a PSTN Destination	23
5.9.3	Post-Answer Redirection With UUI to a SIP Destination	24
5.10.	Inbound Routing	25
5.11.	Calling Party Information	25
5.12.	Outbound Routing.....	26
5.13.	Saving Communication Manager Configuration Changes	28
6.	Avaya Aura ® Session Manager Configuration for SIP Trunking.....	29
6.2.	Specify SIP Domain.....	31
6.2.	Add Location	32
6.3.	Adaptations	34
6.4.	SIP Entities.....	35
6.5.	Entity Links.....	38
6.6.	Routing Policies	39
6.7.	Dial Patterns.....	40
7.	Avaya Session Border Controller for Enterprise	42
7.1.	Access the Management Interface	42
7.2.	Device Specific Settings	44
7.2.1	Define Network Information.....	44
7.2.2	Signaling Interfaces	45
7.2.3	Media Interfaces.....	46
7.3.	Global Profiles	46
7.3.1	Routing Profile.....	46
7.3.2	Topology Hiding Profile	47
7.3.3	Server Interworking	49

7.3.4	Signaling Manipulation.....	51
7.3.5	Server Configuration.....	53
7.3.6	Server Configuration for Verizon IPCC	55
7.4.	Domain Policies – Media Rules.....	57
7.5.	Domain Policies – Signaling Rules.....	59
7.6.	Domain Policies – End Point Policy Groups	60
7.7.	Device Specific Settings – End Point Flows.....	61
8.	Verizon Business IPCC Services Suite Configuration	65
9.	Verification Steps.....	65
9.1.	Communication Manager and Wireshark Trace Call Verifications	65
9.1.1	Wireshark Example of Incoming Call from PSTN via Verizon IPCC	65
9.1.2	Example Incoming Call Referred with UUI to Alternate SIP Destination	66
9.2.	System Manager and Session Manager Verifications	69
9.2.1	Call Routing Test	69
9.3.	Troubleshooting	71
10.	Conclusion	73
11.	Additional References.....	73
11.1.	Avaya	Error! Bookmark not defined.
Appendix A	74

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP Trunk Service offers. Access to these Verizon features may use Internet Dedicated Access (IDA) or Private IP (PIP). These Application Notes cover IP Toll Free VoIP Inbound using IDA access.

Verizon IP Toll Free VoIP Inbound Service provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Avaya Aura® Communication Manager. The Network Call Redirection (NCR) and SIP User-to-User Information (UUI) features can be utilized together to transmit UUI within SIP signaling messages to alternate destinations via the Verizon network.

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.

In the sample configuration, an Avaya Session Border Controller for Enterprise (SBCE) is used as an edge device between the Avaya Customer Premise Equipment (CPE) and Verizon Business. The Avaya SBCE performs SIP header manipulation and provides topology hiding. Avaya Aura® Session Manager is used as the Avaya SIP trunking “hub” connecting to Avaya Aura® Communication Manager, the Avaya SBCE, and other applications.

The Verizon Business IP Toll Free VoIP Inbound Service provides inbound toll-free service via standards-based SIP trunks. Using SIP Network Call Redirection (NCR), trunk-to-trunk connections of certain inbound calls at Avaya Aura® Communication Manager can be avoided by requesting that the Verizon network transfer the inbound caller to an alternate destination. In addition, the SIP User-to-User Information (UUI) feature can be utilized with the SIP NCR feature to transmit UUI within SIP signaling messages to alternate destinations. This capability allows the service to transmit a limited amount of call-related data between call centers to enhance customer service and increase call center efficiency. Examples of UUI data might include a customer account number obtained during a database query or the best service routing data exchanged between sites.

For more information on the Verizon Business IP Contact Center service, visit <http://www.verizonbusiness.com/Products/communications/contact-center/>

2. General Test Approach and Test Results

The Avaya equipment depicted in **Figure 1** demonstrates connectivity to the commercially available Verizon Business IPCC IP Toll Free VoIP Inbound Service. This allows PSTN users to dial toll-free numbers assigned by Verizon. The toll-free numbers were configured to be routed within the enterprise to Avaya Aura® Communication Manager endpoints including Vector Directory Numbers (VDNs). The VDNs are associated with vectors configured to exercise the ACD functionality of Communication Manager as well as Verizon IPCC Services including NCR to PSTN Destinations and NCR with UUI.

The test approach was manual testing of inbound and referred calls using the Verizon IPCC Services on a production Verizon IDA Access Circuit, as shown in **Figure 1**.

The main objectives were to verify the following features and functionality:

- Inbound Verizon toll-free calls to Communication Manager endpoints and VDNs/Vectors
- Inbound private toll-free calls (e.g., PSTN caller uses *67 followed by the toll-free number)
- Inbound Verizon toll-free calls redirected using Communication Manager SIP NCR (via SIP REFER/Refer-To) to PSTN alternate destinations
- Inbound Verizon IP toll-free calls redirected using Communication Manager SIP NCR with UUI (via SIP REFER/Refer-To with UUI) to a SIP-connected destination
- Inbound toll-free voice calls can use G.711MU or G.729A codecs.
- Inbound toll-free voice calls can use DTMF transmission using RFC 2833
- Inbound toll-free voice calls via the Verizon IP-IVR
- Inbound toll-free voice calls received via the Verizon IP-IVR and redirected using a vector

Testing was successful. Test observations or limitations are described in **Section 2.2**.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the execution of test cases from the Verizon-authored interoperability test plan [VZ-Test-Plan].

- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya location. Configuration was varied such that these incoming toll-free calls were directed to Communication Manager Telephone extensions and Communication Manager VDNs containing call routing logic to exercise SIP NCR.
- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a toll free call before the call has been answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a toll-free number directed to a busy user or resource when no redirection on busy conditions are configured (which would be unusual in a contact center).

- Proper termination of an inbound IP Toll Free call left in a ringing state for a relatively long duration, which again would be unusual in a contact center. In the sample configuration, Verizon sent a SIP CANCEL to cancel the call after three minutes of ring no answer conditions, returning busy tone to the PSTN caller.
- Privacy requests for inbound toll-free calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67 from a mobile phone), the inbound toll-free call can be successfully completed while withholding presentation of the PSTN caller ID to user displays. (When the caller requests privacy, Verizon IP Toll Free sends the caller ID in the P-Asserted-Identity header and includes “Privacy: id” which is honored by Communication Manager).
- Inbound toll-free call with long holding time call stability. Communication Manager sends a re-INVITE with SDP to refresh the session at the configured session refresh interval specified on the Communication Manager Trunk group handling the call. In the sample configuration, the session refresh re-INVITE was sent after 900 seconds (15 minutes). This interval is configured for the trunk group as described in **Section 5.8**. The call continued with proper talk path.
- Telephony features such as hold and resume. When a Communication Manager user holds a call in the sample configuration, Communication Manager will send a re-INVITE to Verizon with a media attribute “sendonly”. The SIP 200 OK response to the re-INVITE from Verizon will include media attribute “recvonly”. While the call remains on hold, RTP will flow from the Avaya CPE to Verizon, but no RTP will flow from Verizon to the Avaya CPE (i.e., as intended). When the user resumes the call from hold, bi-directional media path resumes. Although it would be unexpected in a contact center, calls on hold for longer than the session refresh interval were tested, and such calls could be resumed after the session refresh.
- Transfer of toll-free calls between Communication Manager Users.
- Incoming voice calls using the G.729A and G.711 ULAW codecs and proper protocol procedures related to media.
- DTMF transmission using RFC2833. For inbound toll-free calls, PSTN users dialing post-answer DTMF digits are recognized properly by the Avaya CPE.
- Proper DiffServ markings for SIP signaling and RTP media flowing from the Avaya CPE to Verizon.
- Inbound toll-free calls from the Verizon IP-IVR answered at a station or a vector.
- Inbound toll-free calls from the Verizon IP-IVR answered at a station or a vector and then transferred using a SIP REFER message.

2.2. Test Results

The interoperability compliance testing of the sample configuration was completed with successful results. The following observations may be noteworthy:

- Verizon Business IPCC Services suite does not support fax.
- Verizon Business IPCC Services suite does not support History Info or Diversion Headers. The Avaya CPE will not send History-Info or Diversion header to Verizon IPCC in the sample configuration.

- Verizon Business IPCC Services suite does not support G.729 Annex b. When using G729, the Avaya CPE will always include “annexb=no” in SDP in the sample configuration.
- The presence of Avaya generated SIP headers that Verizon need not receive, such as “P-Location”, in a SIP message sent to Verizon does not cause any user-perceivable problems. Nevertheless, for consistency with previously published Application Notes, SBCE procedures are shown in **Section 7.3.4** to illustrate how headers such as P-Location that are not required by Verizon may be removed by the Avaya SBCE for Enterprise.
- **SIP REFER/TRANSFER OFF-NET:** If the public-unknown numbering table is being used to map local extensions to DIDs and a transfer to the PSTN is attempted using a SIP REFER, the Contact Header will incorrectly contain the local extension instead of the DID. This may cause the service provider to send a SIP 603 DECLINE instead of a SIP 202 ACCEPT on the REFER. This will allow the call to be transferred but will not release media resources for the transfer and the call will stay resident on the system. The recommended work-around is to use a Sigma Script detailed in **Section 7.3.4**. Internal tracking issue defsw121215 has been created for this issue.

2.3. Support

2.3.1 Avaya

For technical support, visit <http://support.avaya.com>

2.3.2 Verizon

For technical support, visit <http://www.verizonbusiness.com/us/customer/>

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the Verizon Business IPCC service node. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location is an Avaya Session Border Controller for Enterprise (ASBCE). The ASBCE receives traffic from Verizon on port 5060 and sends traffic to Verizon using destination port 5072, using UDP for transport. The PIP service defines a secure MPLS connection between the Avaya CPE T1 connection and the Verizon IPCC service node.

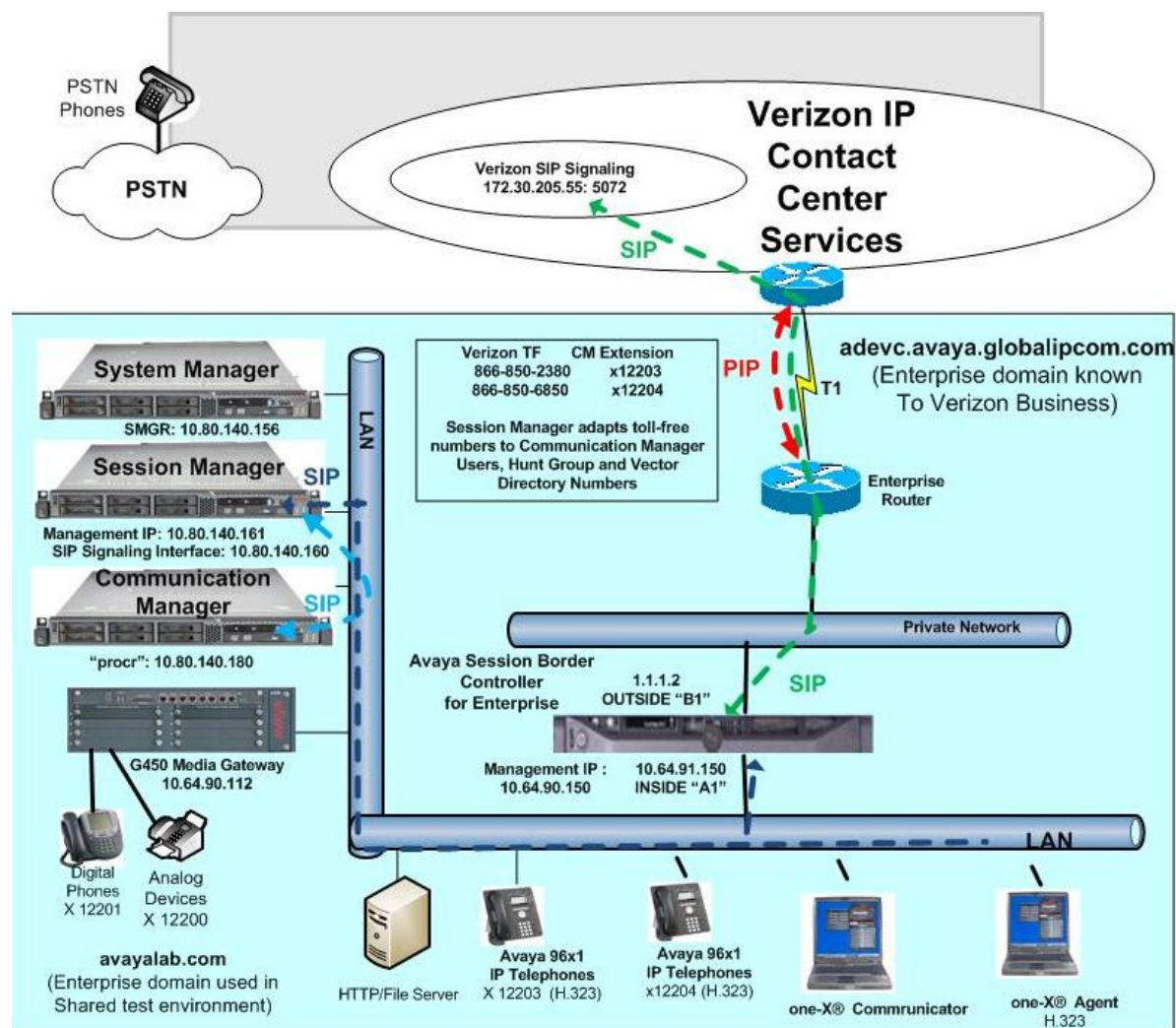


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon IP toll-free numbers were mapped by Session Manager or Communication Manager to various Communication Manager Extensions. The extension mappings were varied during the testing to allow inbound toll-free calls to terminate directly on user extensions or indirectly through hunt groups, vector directory numbers (VDNs) and vectors to user extensions and contact center agents.

For efficiency, the Avaya CPE environment utilizing Session Manager Release 6.2 and Communication Manager Release 5.2.1 was shared among other ongoing test efforts at the Avaya Solutions and Interoperability Test lab. Access to the Verizon Business IPCC services was added to a configuration that already used domain “avayalab.com” at the enterprise. As such, Session Manager or the ASBCE are used to adapt the domains as needed. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to Verizon.

The following summarizes various header contents and manipulations for IP toll-free calls in the sample configuration:

- Verizon sends the following in the initial INVITE to the CPE:
 - The CPE FQDN of *adevc.avaya.globalipcom.com* in the Request URI.
 - The Verizon gateway IP address in the from header.
 - The enterprise ASBCE outside IP address (i.e., 1.1.1.2) in the To header.
- Sends the INVITE to Avaya CPE using destination port 5060 via UDP
- Avaya Session Border Controller for Enterprise sends Session Manager:
 - The Request URI contains *avayalab.com*, to match the shared Avaya SIL test environment.
 - The host portion of the From header also contains *avayalab.com*
 - The host portion of the To header also contains *avayalab.com*
 - Sends the packet to Session Manager using destination port 5060 via TCP
- Session Manager to Communication Manager:
 - The Request URI contains *avayalab.com*, to match the shared Avaya SIL test environment.
 - Session Manager sends to Communication Manager using destination port 5060 via TCP to allow Communication Manager to distinguish Verizon IP Toll Free traffic from other traffic arriving from the same instance of Session Manager.

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 FQDNs and IP addressing appropriate for the unique customer environment.

3.1. History Info and Diversion Headers

The Verizon Business IPCC Services suite does not support SIP History Info Headers or Diversion Headers. Therefore, Communication Manager was provisioned not to send History Info Headers or Diversion Headers.

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager	Release 5.2.1 R015x.02.1.016.4
Avaya Aura® System Manager	Release 6.2
Avaya Aura® Session Manager	Release 6.2
Avaya G450 Gateway	3.1.20.1
Avaya one-X® Communicator (H.323)	6.2.2.06_SP2-35791
Avaya 96x1-Series IP Telephones (H.323)	96x1-IPT-H323-R6_0-090610
Avaya 2400-Series Digital Telephones	N/A
Avaya Session Border Controller for Enterprise	Release 4.0.5 Q09

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Communication Manager Release 5.2.1

This section illustrates an example configuration allowing SIP signaling via the Processor Ethernet of Communication Manager to Session Manager. In configurations that use an Avaya G450 Media Gateway, it is also possible to use an Avaya C-LAN in the Avaya G450 Media Gateway for SIP signaling to Session Manager.

Note – For the Avaya servers and media gateways, the initial installation, configuration, and licensing are assumed to have been previously completed and are not discussed in these Application Notes. These Application Notes focus on describing the sample configuration as it relates to SIP Trunking to Verizon IPCC.

Configuration is illustrated via the Communication Manager SAT interface. Screens are abridged for brevity in presentation.

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** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business IPCC Services and any other SIP applications. Each call from the Verizon Business IPCC Services to a non-SIP endpoint uses one SIP trunk for the duration of the call. Each call from Verizon Business IPCC Services to a SIP endpoint 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:		8000 0
Maximum Concurrently Registered IP Stations:		18000 2
Maximum Administered Remote Office Trunks:		0 0
Maximum Concurrently Registered Remote Office Stations:		0 0
Maximum Concurrently Registered IP eCons:		128 0
Max Concur Registered Unauthenticated H.323 Stations:		18000 0
Maximum Video Capable Stations:		18000 0
Maximum Video Capable IP Softphones:		18000 0
Maximum Administered SIP Trunks:		5000 283
Maximum Administered Ad-hoc Video Conferencing Ports:		8000 0
Maximum Number of DS1 Boards with Echo Cancellation:		522 0
Maximum TN2501 VAL Boards:		10 0
Maximum Media Gateway VAL Sources:		250 1
Maximum TN2602 Boards with 80 VoIP Channels:		128 0
Maximum TN2602 Boards with 320 VoIP Channels:		128 0
Maximum Number of Expanded Meet-me Conference Ports:		300 0
(NOTE: You must logoff & login to effect the permission changes.)		

On **Page 4** of the **display system-parameters customer-options** form, verify that **IP Trunks** and **IP Stations** are enabled. If the use of SIP REFER messaging 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		
Enhanced Conferencing? y		ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y		Local Survivable Processor? n
Extended Cvg/Fwd Admin? y		Malicious Call Trace? y
External Device Alarm Admin? y		Media Encryption Over IP? n
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		

Forced Entry of Account Codes? y	Multifrequency Signaling? y
Global Call Classification? y	Multimedia Call Handling (Basic)? y
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y
IP Trunks? y	

On **Page 5** of the **display system-parameters customer-options** form, verify that the **Private Networking** and **Processor Ethernet** features are enabled if these features will be used, as is the case in the sample configuration.

display system-parameters customer-options		Page 5 of 11
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? y		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	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? n	
	Wireless? n	
Remote Office? n		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

On **Page 6** of the **display system-parameters customer-options** form, verify that any required call center features are enabled. In the sample configuration, **Vectoring** is enabled to refer calls to alternate destinations using SIP NCR. **Vector variables** are enabled in order to include User-User Information (UII) with the referred calls.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 5.0		
ACD? y	Reason Codes? y	
BCMS (Basic)? y	Service Level Maximizer? y	
BCMS/VuStats Service Level? y	Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y	
Business Advocate? n	Service Observing (VDNs)? y	
Call Work Codes? y	Timed ACW? y	
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y	
Dynamic Advocate? n	Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y	
EAS-PHD? y	Vectoring (3.0 Enhanced)? y	
Forced ACD Calls? n	Vectoring (ANI/II-Digits Routing)? y	
Least Occupied Agent? y	Vectoring (G3V4 Advanced Routing)? y	
Lookahead Interflow (LAI)? y	Vectoring (CINFO)? y	
Multiple Call Handling (On Request)? y	Vectoring (Best Service Routing)? y	
Multiple Call Handling (Forced)? y	Vectoring (Holidays)? y	

On **Page 7** of the **display system-parameters customer-options** form, verify that the required call center capacities can be met. In the sample configuration, agents will log in (using agent-login IDs) to staff the ACD and handle inbound calls from Verizon IP Toll Free.

display system-parameters customer-options		Page 7 of 11
CALL CENTER OPTIONAL FEATURES		
VDN of Origin Announcement? y	VuStats? n	
VDN Return Destination? y	VuStats (G3V4 Enhanced)? n	
	USED	
Logged-In ACD Agents: 5200	0	
Logged-In Advocate Agents: 5200	0	
Logged-In IP Softphone Agents: 5200	0	
Logged-In SIP EAS Agents: 500	0	

5.2. System Features

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

change system-parameters features		Page 1 of 18
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled? n		
Trunk-to-Trunk Transfer: all		
Automatic Callback with Called Party Queuing? n		
Automatic Callback - No Answer Timeout Interval (rings): 3		
Call Park Timeout Interval (minutes): 10		
Off-Premises Tone Detect Timeout Interval (seconds): 20		
AAR/ARS Dial Tone Required? y		

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

```

change system-parameters features
                                FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

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

```

5.3. Dial Plan

In the sample configuration, the Avaya CPE environment uses four digit local extensions, such as **4xxx** and **7xxx**. Trunk Access Codes (TAC) are 4 digits in length and begin with ***1**. The Feature Access Code (FAC) to access ARS is the single digit **9**. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used. The dial plan is modified with the **change dialplan analysis** command as shown below.

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

5.4. Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged display node-names ip output shows relevant node-names in the sample configuration. As shown in **bold**, the node name for Session Manager is “SM” with IP Address

“10.80.140.160”. The node name and IP Address “10.80.140.180” for the Processor Ethernet “procr” appears automatically due to the initial installation and configuration of the system.

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
GW3	10.64.90.112	
MM	205.3.3.55	
SM	10.80.140.160	
default	0.0.0.0	
procr	10.80.140.180	

5.5. IP Interface for Processor Ethernet

The **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the PE will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

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	
Subnet Mask: /24		

5.6. IP Codec Set

The following screen shows the configuration for IP codec set 2. IP codec set 2 is to be used for calls within Network Region 10 and for calls between Network Region 1 and Network Region 10. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls with Verizon IPCC via the SIP trunks would prefer to use **G.729A**, but also be capable of using **G.711MU**. Any calls using this same codec set that are between devices capable of the **G.722-64K** codec can use G.722. The specification of G.722 as the first choice is not required. That is, G.722 may be omitted from the codec set, but it is recommended that G.729A and G.711MU be included in the codec set for use with Verizon IPCC Services.

change ip-codec-set 2 Page 1 of 2

IP Codec Set

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.722-64K		2	20
2: G.729A	n	2	20
3: G.711MU	n	2	20
4:			
5:			
6:			
7:			

Media Encryption

1: none

On **Page 2** of the form, configure the **FAX Mode** field to **off**. Verizon IPCC does not support fax.

change ip-codec-set 2 Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy
FAX	off	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

5.7. IP Network Region

IP 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 10 was associated with other logical components used specifically for the Verizon IPCC 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 command **change media 3** shows that media gateway 3 is an Avaya G450 Media Gateway configured for region 1. It can also be observed that the **Controller IP Address** is the Processor Ethernet (10.80.140.180), and that the **G450 MGP IPV4 Address** is **10.64.90.112**. These fields are not configured in this screen, but rather display the current information for the gateway.

The following screen also shows media gateway 3 has an **MM712** media module supporting Avaya digital phones in slot **v7**, an **MM711** supporting analog devices in slot **v8**, and the capability to provide announcements and music on hold via “gateway-announcements” in logical slot **v9**

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

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 10 was chosen for the service provider trunk. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. Use the **change ip-network-region 10** command to configure region 10 with the following parameters:

- Set the **Location** field to match the enterprise location for this SIP trunk.
- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **adevc.avaya.globalipcom.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. To enable shuffling, set both **Intra-region** and **Inter-region IP-IP Direct Audio** fields to **yes**. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.6**.
- Default values can be used for all other fields.

change ip-network-region 10		Page 1 of 19	
		IP NETWORK REGION	
Region: 10			
Location: 1	Authoritative Domain: adevc.avaya.globalipcom.com		
Name: SIP Trunks			
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 2		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? n	
UDP Port Max: 3329			
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y	
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46		Use Default Server Parameters? y	
Video PHB Value: 26			
802.1P/Q PARAMETERS			
Call Control 802.1p Priority: 6			
Audio 802.1p Priority: 6			
Video 802.1p Priority: 5		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS		RSVP Enabled? n	
H.323 Link Bounce Recovery? y			
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			

On **Page 3**, define the IP codec set to be used for traffic between region 10 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 10 (the service provider region) and region 1 (the rest of the enterprise).

change ip-network-region 10										Page 3 of 19		
Source Region: 10 Inter Network Region Connection Management										I	M	
										G	A	t
dst rgn	codec set	direct WAN	WAN-BW-limits Units		Video Norm		Intervening Prio Shr Regions		Dyn CAC	A	G	c
1	2	y	NoLimit							n		t
2	2	y	NoLimit							n		t
3												
4												
5												
6												
7												
8												
9												
10	2									all		

5.8. Signaling Group

Use the **change signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.

- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of **TCP**. Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port. For compliance testing the **Near-end Listen Port** and **Far-end Listen Port** were set to **5060** and **tcp** was used so traces could be taken.
- Set the **Peer Detection Enabled** field to **y**. The **Peer Server** field will initially be set to **Others** and cannot be changed via administration. The Peer Server field will automatically change to **SM** once Communication Manager detected a Session Manager peer.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.4**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.4**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.7**
- Set the **Far-end Domain** to the domain of the enterprise.
Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value sends the DTMF digits in the RTP audio stream.
- Default values may be used for all other fields.

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

5.9. SIP Trunk Groups

This section illustrates the configuration of the SIP Trunks Groups corresponding to the SIP signaling groups from **Section 5.8**.

NOTE: For Verizon Business customers utilizing either Verizon **IP Contact Center** or **IP-IVR** service offers, at least one **Elite Agent license is required** to support the ability to utilize the Network Call Redirection capabilities of those services with Communication Manager. This license is required to enable the **ISDN/SIP Network Call Redirection** feature. This licensed feature must be turned on to support Network Call Redirection. Additional details on how to configure Network Call Redirection in Communication Manager can be found within the supporting text and figures contained within this section.

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.8**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an appropriate Class of Restriction (COR) designated for SIP Trunks in the **COR** field.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set the **Signaling Group** to the signaling group defined in **Section 5.8**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

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

The following shows Page 2 for trunk group 1. All parameters shown are default values. Although it is not strictly necessary to change the **Preferred Minimum Session Refresh Interval**, from the default “600” to “900” (seconds), some SIP products prefer a higher session refresh interval than the Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of “600” seconds was used.

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

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

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

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

The following **Page 4** for trunk group shows the Protocol Variations. The **Telephone Event Payload Type** has been set to “101” to match Verizon expectation. 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 for NCR nor “send-only” signaling is required for calls held at the enterprise, the **Network Call Redirection** field may be left at the default “n” value. In the testing associated with these Application Notes, the **Network Call Redirection** flag was set to “y” to allow REFER to be exercised with the Verizon IP Toll Free Service.

The Verizon IPCC Services do not support the Diversion header or the History-Info header, and therefore both **Support Request History** and **Send Diversion Header** are set to “n”.

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

5.10. Contact Center Configuration

This section describes the basic commands used to configure VDNs and corresponding vectors. These vectors contain steps that invoke the Communication Manager SIP NCR functionality. These Application Notes provide rudimentary vector definitions to demonstrate and test the SIP NCR and UII functionalities. In general, call centers will use vector functionality that is more complex and tailored to individual needs. Call centers may also use customer hosts running applications used in conjunction with Application Enablement Services (AES) to define call routing and provide associated UII. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

5.10.1 Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command **add announcement x** where **x** is the extension used screen not shown. The screen below shows the list of announcements already configured.

list announcement				
ANNOUNCEMENTS/AUDIO SOURCES				
Announcement			Source	Num
of				
Extension	Type	Name	Pt/Bd/Grp	
Files				
4000	integ-mus	holdmusic	003V9	1
4001	integrated	announcement_1	003V9	1

5.10.2 Post-Answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use post-answer redirection to a PSTN destination. In this example, the inbound toll-free call is routed to VDN 12309 as shown in the following screen. The originally dialed Verizon IP Toll Free number may be mapped to VDN 12309 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

display vdn 12309	Page	1 of	3
VECTOR DIRECTORY NUMBER			
Extension: 12309			
Name*: Refer to PSTN			
Destination: Vector Number			203
Attendant Vectoring? n			
Meet-me Conferencing? n			
Allow VDN Override? n			
COR: 1			
TN*: 1			
Measured: none			

VDN 12309 is associated with **vector 203**, which is shown below. Step 02 for vector 203 plays announcement 4003 to answer the call. After the announcement, the “route-to number” in step 03 includes “~r+13035380023” where the number 303-538-0023 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes “+13035380023” as the user portion. Note that Verizon IP Contact Center services require the “+” in the Refer-To header for this type of call redirection.

display vector 203	Page 1 of 6
CALL VECTOR	
Number: 203	Name: Blind TRF2 PSTN
Multimedia? n	Attendant Vectoring? n
Basic? y	Meet-me Conf? n
EAS? y	Lock? n
G3V4 Enhanced? y	ANI/II-Digits? y
ASAI Routing? y	
Prompting? y	LAI? y
G3V4 Adv Route? y	CINFO? y
BSR? y	Holidays? y
Variables? y	3.0 Enhanced? Y
01 wait-time 2 secs hearing ringback	
02 announcement 4003	
03 route-to number ~r+13035380023 with cov n if unconditionally	
04 stop	

5.10.3 Post-Answer Redirection With UII to a SIP Destination

This section provides an example of post-answer redirection with UII passed to a SIP destination. In this example, the inbound call is routed to VDN 12309 shown in the following screen. The originally dialed Verizon toll-free number may be mapped to VDN 12309 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

display vdn 12309	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 12309	
Name*: Refer-with-UII	
Destination: Vector Number	5
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	

To facilitate testing of NCR with UII, the vector variables were defined.

change variables	Page 1 of 39
VARIABLES FOR VECTORS	
Var Description	Type Scope Length Start Assignment
VAC	
A Test1	asaiuui L 16 1
B Test2	asaiuui L 16 17
C	

VDN 12309 is associated with vector 1 which is shown below. Vector 1 sets data in the vector variables A in step 02 and plays an announcement to answer the call (step 04). After the announcement, the “route-to” number step includes “~r+18002422121”. This step causes a REFER message to be sent where the Refer-To header includes “+18002422121” as the user portion. The Refer-To header will also contain the UII set in variables A. Verizon will include this UII in the INVITE ultimately sent to the SIP-connected target of the REFER, which is toll-free number “18002422121”. In the sample configuration, where only one location was used, 800-242-2121 is another toll-free number assigned to the same circuit as the original call. In practice, NCR with UII would allow Communication Manager to send call or customer-related data along with the call to another contact center.

display vector 1		Page 1 of 6
CALL VECTOR		
Number: 1	Name: UII	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y	ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y	CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y	
01 wait-time	2 secs hearing ringback	
02 set	A = none CATR 1234567890987421	
03 wait-time	2 secs hearing ringback	
04 announcement	4002	
05 route-to	number ~r+18002422121 with cov n if unconditionally	
06 disconnect	after announcement 4003	

5.11. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table is not necessary. In alternative configurations, if the toll-free number sent by Verizon was not changed before reaching Communication Manager, then the Verizon IPCC number could be mapped to a Communication Manager extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of toll-free number **8668502380** to extension **12203** when the call arrives on trunk group 1.

change inc-call-handling-trmt trunk-group 1					Page	1 of	30
INCOMING CALL HANDLING TREATMENT							
Service/	Number	Number	Del Insert				
Feature	Len	Digits					
public-ntwrk	10	8668502380	10	12203			
public-ntwrk							
public-ntwrk							
public-ntwrk							

5.12. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.9**), use the **change public-unknown-numbering** command to create an entry for each extension which has a 866 assigned. The 866 number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the bolded rows shown in the example abridged output below, Communication Manager extensions are mapped to DID numbers that are known to Verizon for this SIP Trunk connection when the call uses trunk group 5.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	12203	1	8668502380	10	Total Administered: 0
					Maximum Entries: 9999

5.13. Outbound Routing

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

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

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

change feature-access-codes		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:	*10	
Abbreviated Dialing List2 Access Code:	*12	
Abbreviated Dialing List3 Access Code:	*13	
Abbreviated Dial - Prgm Group List Access Code:	*14	
Announcement Access Code:	*19	
Answer Back Access Code:		
Auto Alternate Routing (AAR) Access Code:	*00	
Auto Route Selection (ARS) - Access Code 1:	9	Access Code 2:
Automatic Callback Activation:	*33	Deactivation: #33
Call Forwarding Activation Busy/DA:	*30 All: *31	Deactivation: #30
Call Forwarding Enhanced Status:	Act:	Deactivation:

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9.

- **Dialed String:** enter the leading digits (e.g., **1303**) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., **11**) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., **11**) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., **1**) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type:** enter **fnpa**, the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter **hnpa**. For 411 and 911 calls use **svcl** and **emer** respectively. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1.

The example below shows a subset of the dialed strings tested as part of the compliance test. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 1						Page	1 of	2
ARS DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 0		
	Dialed String	Total		Route Pattern	Call Type	Node Num	ANI	
		Min	Max				Reqd	
	1303	11	11	1	fnpa		n	
	1502	11	11	1	fnpa		n	
	17	11	11	1	fnpa		n	
	1720	11	11	1	fnpa		n	
	18	11	11	1	fnpa		n	
	1866	11	11	1	fnpa		n	
	1877	11	11	1	fnpa		n	
	1888	11	11	1	fnpa		n	
	1908	11	11	1	fnpa		n	

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group **5** was used.
- **FRL:** Set the Facility Restriction Level field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 1** The prefix mark of **1** will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNP 10 digit numbers are left unchanged.

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

5.14. Saving Communication Manager Configuration Changes

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

6. Avaya Aura® Session Manager Configuration for SIP Trunking

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. Access the web management interface by entering **https://<ip-addr of System Manager>/SMGR** this is the management IP address assigned during installation. 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 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.

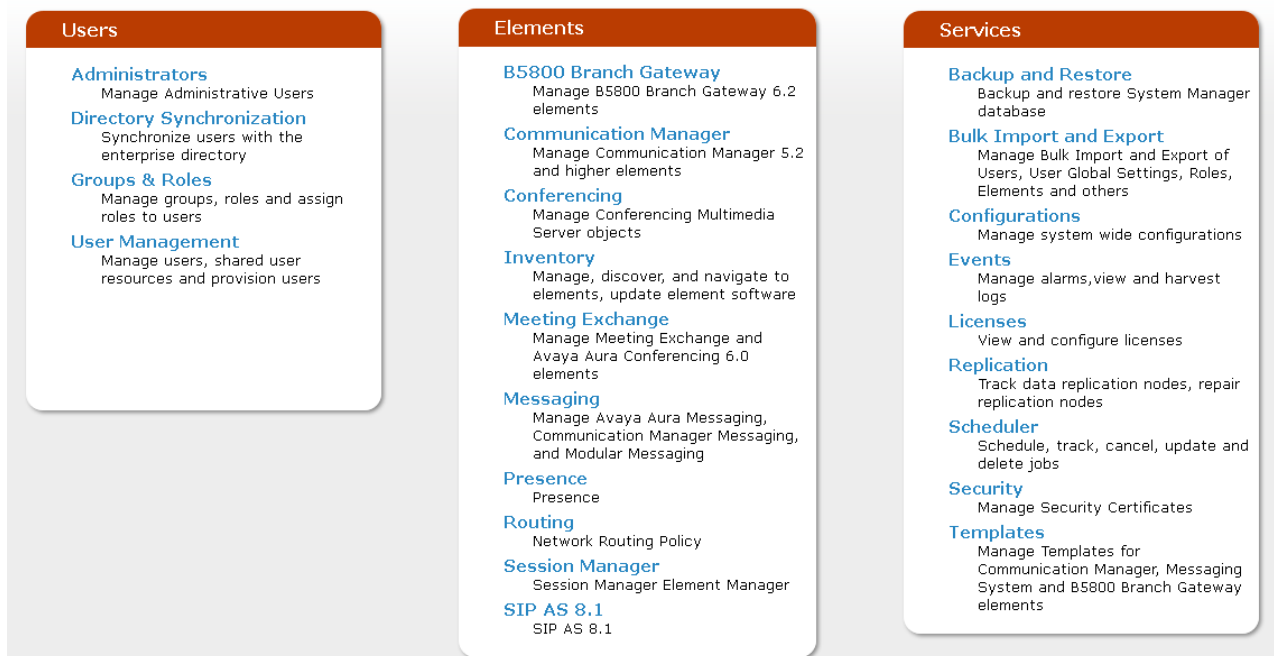
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

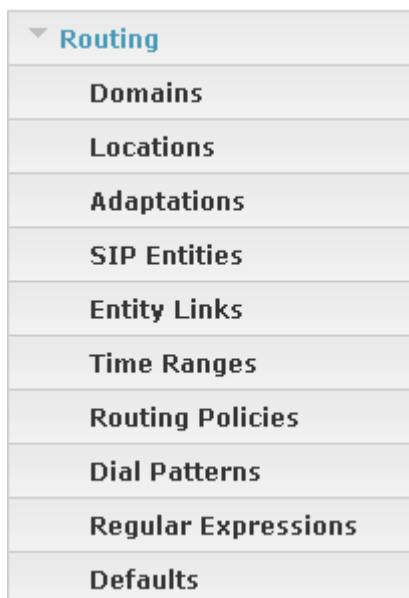
Password:

[Change Password](#)

Once logged in, a screen similar to the abridged screen shown below is displayed.



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. Specify SIP Domain

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

Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

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

Click **Commit**. The screen below shows the list of configured SIP domains.

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

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

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

6.2. Add Location

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

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.

Location

5 Items	Refresh	Filter: Enable
<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"/>	Avaya-SBCE-3	Avaya SBCE-3
<input type="checkbox"/>	CM521	CM 5.2.1
<input type="checkbox"/>	Location_140	Subnet 140
Select : All, None		

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

Location Details

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

The following image shows the lower portion of the screen for the location details for the location named “Avaya-SBCEE-3”. The IP Address “10.64.914.150” of the inside (private) interface of the SBCE is entered in the **IP Address Pattern** field. In the sample configuration, other location parameters (not shown) retained default values.

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.91.150	Sipera SBCE-3 private side IP

Select : All, None

* Input Required

If desired, additional locations can be configured with IP Address Patterns corresponding to other elements in the configuration.

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.

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

EditNewDuplicateDeleteMore Actions

5 Items | Refresh

<input type="checkbox"/>	Name	Module name
<input type="checkbox"/>	CM-ES-VZ	DigitConversionAdapter odstd=avayalab.com
<input type="checkbox"/>	CM-ES-VZ-IPCC	DigitConversionAdapter odstd=avayalab.com fromto=true
<input type="checkbox"/>	History_Diversion_IPT	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true
<input type="checkbox"/>	SBC-VzB-IPCC	DigitConversionAdapter osrcd=adevc.avaya.globalipccom.com
<input type="checkbox"/>	Verizon_Test	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com

The adapter named “CM-ES-VZ-IPCC” shown in the following screen will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Verizon IPCC. This adaptation uses the “DigitConversionAdapter” and specifies the “odstd=avayalab.com”. More specifically, this configuration enables the destination domain to be overwritten with “avayalab.com” for calls that egress to a SIP entity using this adapter. For example, for inbound toll-free calls from Verizon IPCC to the Avaya CPE, the Request-URI header sent to Communication Manager will contain “avayalab.com”, which was the domain used by Communication Manager in the shared Avaya Interoperability Test Lab configuration. Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion. The parameter “fromto=true” enables Session Manager to adapt the domain in the To header (to “avayalab.com”) as well.

Similarly, an abridged portion of the settings for **Digit Conversion for Incoming Calls to SM** is shown below. Although the direction of actual calls involving Verizon IPCC service are “inbound” to Communication Manager, SIP headers in responses from Communication Manager can be adapted using the **Digit Conversion for Incoming Calls to SM** area.

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

5 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"/>	* 12203	* 5	* 5		* 5	8668502380	both ▼		
<input type="checkbox"/>	* 12204	* 5	* 5		* 5	8668506850	both ▼		

An example portion of the settings for **Digit Conversion for Outgoing Calls from SM** (i.e., inbound to Communication Manager) is shown below. During the testing, this digit conversion was varied to allow the same toll-free number to be used to test different Communication Manager destinations.

Digit Conversion for Outgoing Calls from SM

Add Remove

12 Items Refresh

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 8666735877	* 10	* 10		* 10	2011	both ▼	
<input type="checkbox"/>	* 8666747056	* 10	* 10		* 10	3698	both ▼	
<input type="checkbox"/>	* 8666747057	* 10	* 10		* 10	3690	both ▼	
<input type="checkbox"/>	* 8668502380	* 10	* 10		* 10	12203	both ▼	
<input type="checkbox"/>	* 8668506850	* 10	* 10		* 10	12204	both ▼	

6.4. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected which includes Communication Manager and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.

- **Time Zone:** Select the time zone for the location above.

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

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit
Cancel

General

* Name:
ASM-62

* FQDN or IP Address:
10.80.140.160

Type:
Session Manager

Notes:

Location:
CMS21

Outbound Proxy:

Time Zone:
America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring:
Use Session Manager Configuration

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

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

- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

Entity Links

Add
Remove

9 Items
Refresh
Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	ASM-62	TLS	* 5061	CMS21_tg3	* 5061	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	ModularMessaging	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	CMS21_tg1	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5060	CM6.2	* 5060	Trusted
<input type="checkbox"/>	ASM-62	TCP	* 5063	CM-Evolution-procr-5063	* 5063	Trusted

Select : All, None

< Previous
Page 1 of 2
Next >

The following screen shows the addition of Communication Manager. The **FQDN or IP Address** field is set to the IP address defined in **Section 5.4** of the procr interface on Communication Manager. The Location is set to the one defined for Communication Manager in **Section 6.2**.

Home / Elements / Routing / SIP Entities

SIP Entity Details Help ?

Commit Cancel

General

* Name: CM521_tg1

* FQDN or IP Address: 10.80.140.180

Type: CM

Notes: CM521

Adaptation: CM-ES-VZ-IPCC

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

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “Avaya-ASBCE-3”. The **FQDN or IP Address** field is configured with the Avaya SBCE inside IP Address “10.64.91.150”. “SIP Trunk” is selected from the **Type** drop-down menu for SBCE SIP Entities. This SBCE has been assigned to **Location** “Avaya-ASBCE-3”. **Link Monitoring** was used as SIP OPTIONS were exchanged between Verizon and Avaya for the test. Other parameters (not shown) retain default values.

Home / Elements / Routing / SIP Entities

[Help ?](#)

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

6.5. Entity Links

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

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.8**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the

Near-end Listen Port defined on the Communication Manager signaling group in **Section 5.8**.

- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE.

Entity Link to Communication Manager:

Home / Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM-CM521_tg1	* ASM-62	TCP	* 5060	* CM521_tg1	* 5060	Trusted	

Entity Link to Avaya SBCE:

Home / Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Avaya-SBCE-3	* ASM-62	TCP	* 5060	* Avaya-SBCE-3	* 5060	Trusted	SBC outside 1112

6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added; one for Communication Manager and one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

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

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**

(not shown). The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

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

Routing Policy for Communication Manger:

[Home](#) / [Elements](#) / [Routing](#) / [Routing Policies](#)

Routing Policy DetailsHelp ?
Commit Cancel

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM521_tg1	10.80.140.180	CM	CM521

Routing Policy for Avaya SBCE:

[Home](#) / [Elements](#) / [Routing](#) / [Routing Policies](#)

Routing Policy DetailsHelp ?
Commit Cancel

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Select

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

6.7. Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Verizon and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing** →

Dial Patterns in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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

An example of an inbound dial pattern used for the compliance test is shown below. The example shows that 11 digit dialed numbers that begin with **1866** originating from **Avaya-SBCE-3** uses route policy **CM521_tg1_RPolicy**.

Home / Elements / Routing / Dial Patterns

[Help ?](#)

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

4 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-VZIPCC	0	<input type="checkbox"/>	CM-Evolution-procr-5063	Verizon IPCC Service
<input type="checkbox"/>	Avaya-SBCE-2	Avaya SBCE-2	CM-ES-VZIPCC	0	<input type="checkbox"/>	CM-Evolution-procr-5063	Verizon IPCC Service
<input checked="" type="checkbox"/>	Avaya-SBCE-3	Avaya SBCE-3	ASM to CM521	0	<input type="checkbox"/>	CM521_tg1	inbound VZ to CM521
<input type="checkbox"/>	CM521	CM 5.2.1	Avaya-SBCE-3-to-Verizon	0	<input type="checkbox"/>	Avaya-SBCE-3	verizon IPCC via ASBCE-3

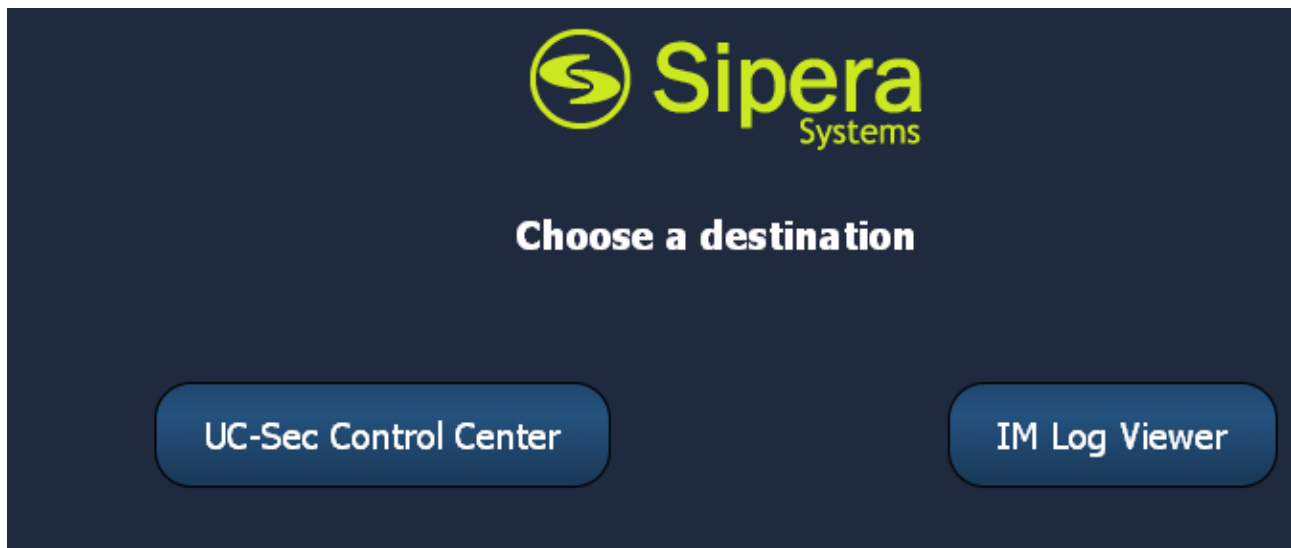
7. Avaya Session Border Controller for Enterprise

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**.

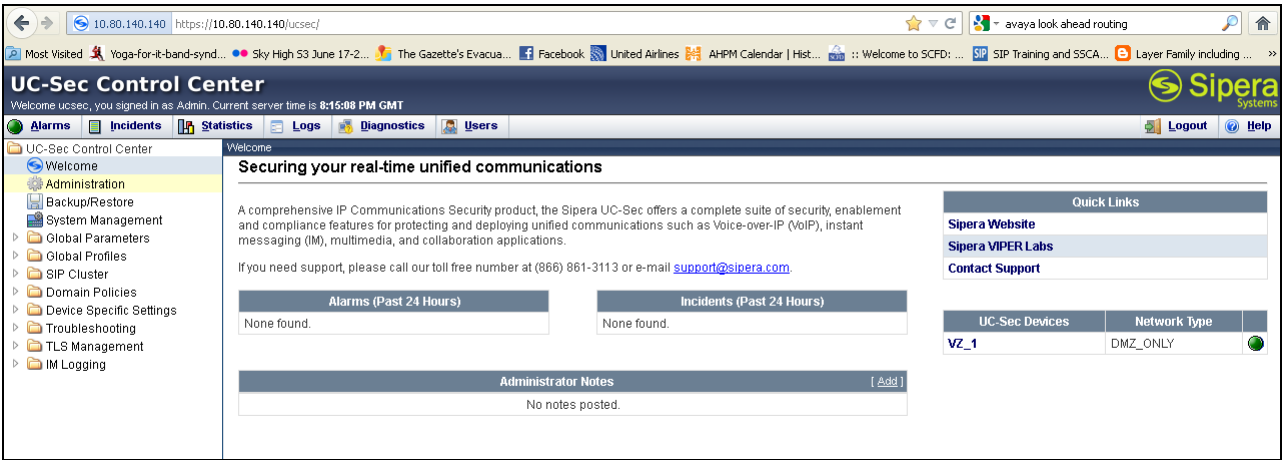


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

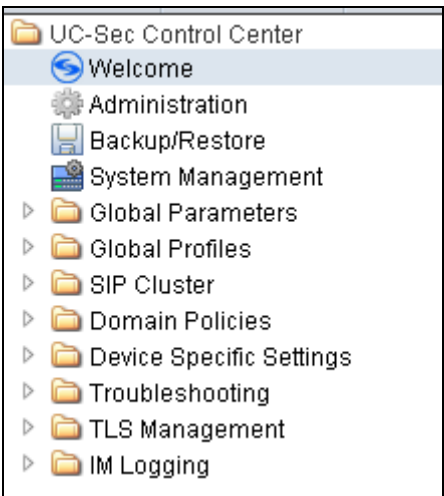
[Visit the Sipera Systems website to learn more.](#)

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.



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



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 **ASBCE-3** 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: ASBCE-3				
Network Configuration				
General Settings		Device Settings		
Appliance Name	ASBCE-3	HA Mode	No	
Box Type	SIP	Secure Channel Mode	None	
Deployment Mode	Proxy	Two Bypass Mode	No	
Network Settings				
IP	Public IP	Netmask	Gateway	Interface
10.64.91.150	10.64.91.150	255.255.255.0	10.64.91.1	A1
1.1.1.2	1.1.1.2	255.255.255.0	1.1.1.1	B1
DNS Configuration		Management IP(s)		
Primary DNS	10.80.150.201	IP	10.64.90.150	
Secondary DNS	4.2.2.2			
DNS Location	DMZ			
DNS Client IP	10.64.91.150			

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.

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:

Buttons: Add IP, Save Changes, Clear Changes

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

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

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 internal 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.

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

7.2.3 Media Interfaces

To define the media 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 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 internal address for the media
- **Port Range:** Enter port ranges for the media path

Repeat the process for the internal Avaya network.

Name	Media IP	Port Range
Avaya_Int_Media	10.64.91.150	35000 - 40000
Ext_Media_to_Verizon	1.1.1.2	35000 - 40000

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:** (Optional) Checked only 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 Avaya SBCE Entity Link created on Session Manager in **Section 6.5**.

[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	*	10.80.140.160:5060	---	<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 that Verizon uses for the IPCC Service Director. Enter **UDP** for the **Outgoing Transport** field.

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	*	172.30.205.55:5072	---	<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.

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

Enter a descriptive name for the new profile and click **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 for Session Manager in **Section 6.1** and the Communication Manager signaling group Far-end Domain in **Section 5.8**. Click **Finish** to save the changes.

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

It is not necessary to modify the **Verizon** profile from the default values. The following screen shows the Topology Hiding Policy created for Verizon

Topology Hiding Profiles

default

cisco_th_profile

Avaya

Verizon-IPCC

Click here to add a description.

Topology Hiding

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

Edit

7.3.3 Server Interworking

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

Interworking Profile

Profile Name

Verizon-IPCC

Next

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

Editing Profile: Verizon-IPCC

General

Hold Support

☐ None
☐ RFC2543 - c=0.0.0.0
☒ RFC3264 - a=sendonly

180 Handling

☐ None
☐ SDP
☒ No SDP

181 Handling

☒ None
☐ SDP
☐ No SDP

182 Handling

☒ None
☐ SDP
☐ No SDP

183 Handling

☒ None
☐ SDP
☐ No SDP

Refer Handling

☐

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

T.38 Support

☒

URI Scheme

☒ SIP
☐ TEL
☐ ANY

Via Header Format

☒ RFC3261
☐ 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 leave the following default settings:

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

Click **Finish** to save changes.

Editing Profile: Verizon-IPCC	
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 checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" 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"/>
Finish	

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

General	
Hold Support	RFC3264
180 Handling	No SDP
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

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

Profile Name	Verizon-IPCC
Clone Name	Avaya

Finish

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 Avaya SBCE. Using this language, a script can be written and tied to a given flow through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

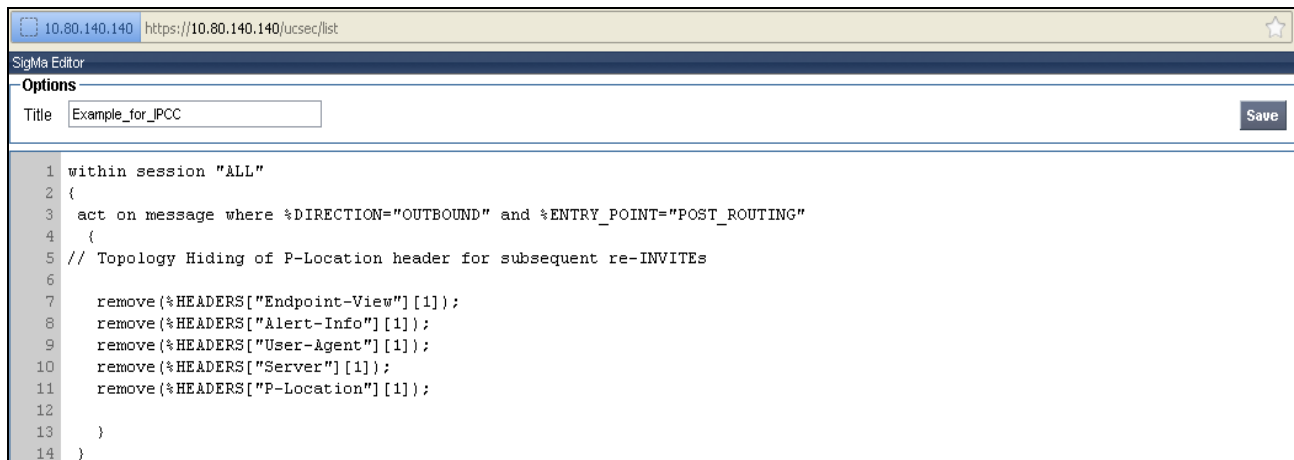
These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and to remove unwanted headers in the SIP messages to and from Verizon.

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. For more information on Signaling Manipulation see **Reference [8]** in **Section 11**.

The script will act on all outbound traffic to Verizon after the SIP message has been routed through the Avaya SBCE. The script is further broken down as follows:

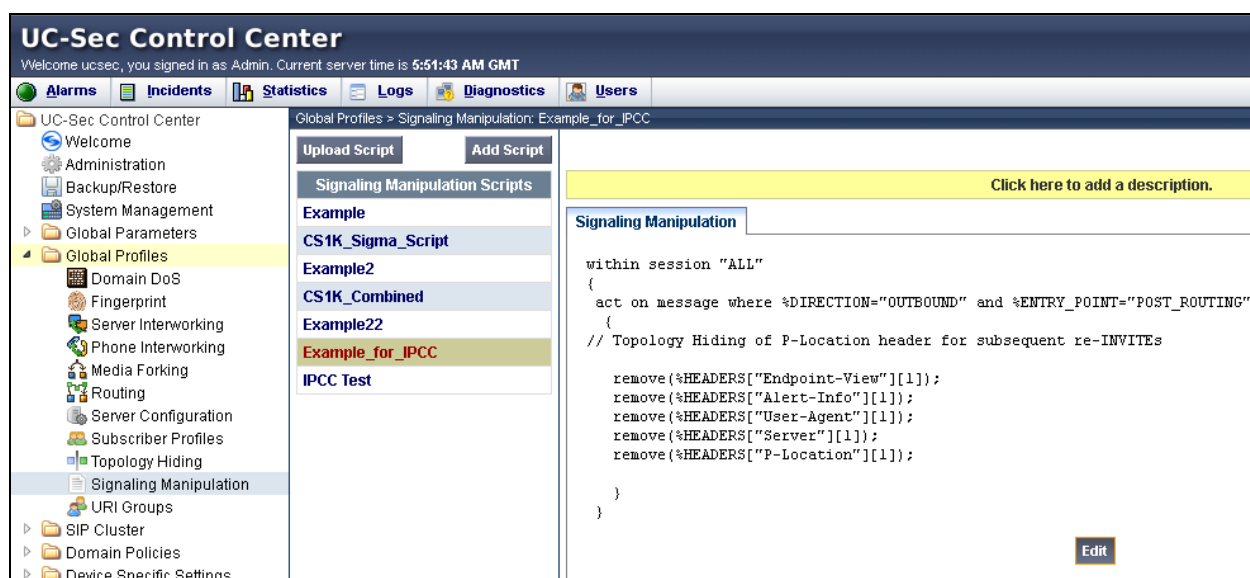
- **within session “All”** Transformations applied to all SIP sessions.
- **act on message** Actions to be taken to any SIP message.
- **%DIRECTION=“OUTBOUND”** Applied to a message leaving the Avaya SBCE.
- **%ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has 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.

With this script, the “Endpoint-View”, “Alert-Info”, “User-Agent”, “Server”, and “P-Location” headers will be removed.



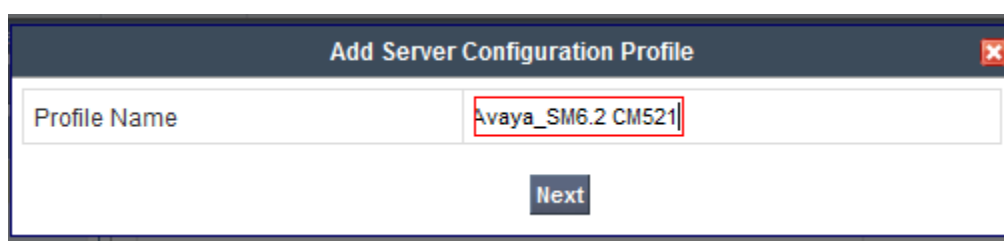
Click **Save**.

The following screen shows the finished Signaling Manipulation Script **Example_for_IPCC**. This script will later be applied to the Verizon Service Director and Service Host in the Server Configuration in **Section 7.3.5**. The details of these script elements can be found in **Appendix A**.



7.3.5 Server Configuration

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, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side (not shown). Click on **Add Profile** (not shown) and enter details in the pop-up menu.



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 Avaya SBCE 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 Avaya SBCE Entity Link on Session Manager in **Section 6.5**.

Click **Next** to continue.

The screenshot shows a configuration window with a sidebar on the left containing a list of profiles: 'Avaya_SM6.2 CM521' and 'VZ-IPCC SIP TRK'. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is selected, displaying a table with the following information:

General	
Server Type	Call Server
IP Addresses / FQDNs	10.80.140.160
Supported Transports	TCP
TCP Port	5060

Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

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

The screenshot shows the same configuration window with the 'Authentication' tab selected. It displays a single setting:

Authentication	
Enable Authentication	<input type="checkbox"/>

The 'Edit' button is visible at the bottom right of the table.

In the new window that appears, 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.
- **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.

Click **Next** to continue (not shown).

Note: Advanced and Authentication Tabs not shown are left as defaults (notice that external OPTIONS are not enabled since they are not used in this configuration).

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

Edit

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

Edit Server Configuration Profile - Heartbeat	Edit Server Configuration Profile - Advanced
Enable Heartbeat <input checked="" type="checkbox"/>	Enable DoS Protection <input type="checkbox"/>
Method OPTIONS	Enable Grooming <input type="checkbox"/>
Frequency 60 seconds	Interworking Profile Avaya
From URI ping@10.80.140.141	Signaling Manipulation Script None
To URI ping@10.80.150.206	TCP Connection Type SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING <input type="radio"/>
TCP Probe <input type="checkbox"/>	
TCP Probe Frequency seconds	
Finish	Finish

7.3.6 Server Configuration for Verizon IPCC

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

To define the Verizon Service Director and Service Host, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side (not shown). Click on **Add Profile** (not shown) and enter Profile Name in the pop-up menu.

Add Server Configuration Profile	
Profile Name	VZ-IPCC SIP TRK
Next	

The following screens illustrate the Server Configuration with Profile name “VZ_IPCC”. In the “General” parameters, select “Trunk Server” from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** field, the Verizon-provided Verizon IPCC IP Address is entered. This IP Address is **172.30.205.55**. In the **Supported Transports** field, **UDP** is selected, and the **UDP Port** is set to **5072**.

The screenshot shows the 'Global Profiles > Server Configuration: IPCC_Service' interface. On the left, a list of profiles includes 'Avaya_SM6.2 CM521' and 'VZ-IPCC SIP TRK'. The main area displays the 'General' tab for the 'VZ_IPCC' profile. The configuration details are as follows:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	172.30.205.55
Supported Transports	UDP
UDP Port	5072

Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

Authentication and Advanced Tabs (not shown) are left at defaults (external OPTIONS are not enabled since they are not used in this configuration):

Two side-by-side screenshots of the 'Global Profiles > Server Configuration: IPCC_Service' interface. The left screenshot shows the 'Authentication' tab with the 'Enable Authentication' checkbox unchecked. The right screenshot shows the 'Heartbeat' tab with the 'Enable Heartbeat' and 'TCP Probe' checkboxes unchecked. Both screenshots include an 'Edit' button.

In the Advanced Tab select Verizon-IPCC for Internetworking Profile and Example_for_IPCC as the Signaling Manipulation Script:

The screenshot shows the 'Global Profiles > Server Configuration: IPCC_Service' interface with the 'Advanced' tab selected. The configuration details are as follows:

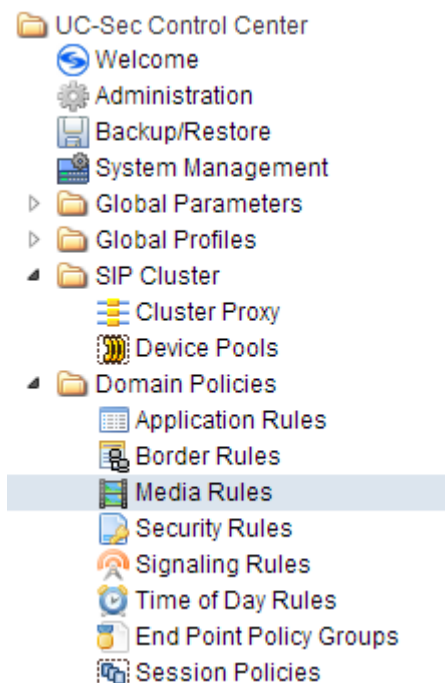
Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Verizon-IPCC
Signaling Manipulation Script	Example_for_IPCC
UDP Connection Type	SUBID

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

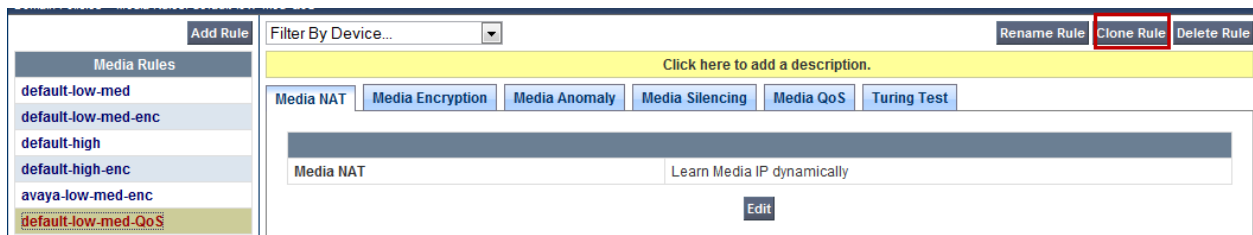
Click **Finish** to save changes (not shown).

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.



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
<div>Finish</div>	

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 the **DSCP** radio button. Select “EF” from the drop down menu for both **Audio** and **Video**. 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
<div>Finish</div>			

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

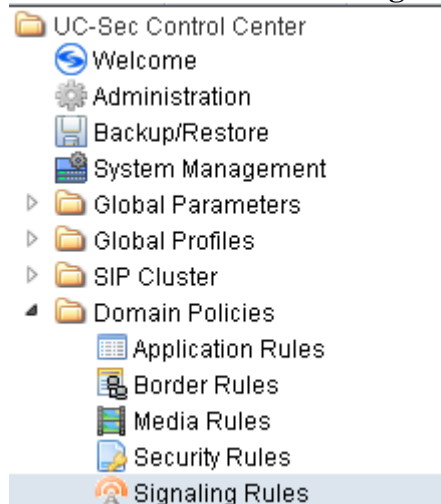
Video QoS

Video DSCP EF

Edit

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.

Signaling Rules	
default	
No-Content-Type-Checks	
Block_Hdr_Remark	

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 **Application Rule** which was set to “Verizon_App_Rule”, **Media Rule** which was set to

“default-low-med-QoS”, and the **Signaling Rule**, which was set to “Block_Hdr_Remark” as shown below. The selected non-default media rule and signaling rule chosen were created in previous sections. Click **Finish**.

Edit Policy Set ✕

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

Finish

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

Add Group
Filter By Device... ▼
Rename Group
Delete Group

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- default-low-remark

Click here to add a description.

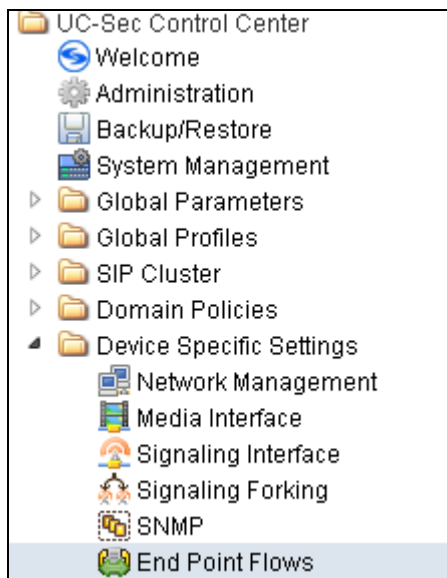
Click here to add a row description.

Policy Group
View Summary Add Policy Set

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

7.7. Device Specific Settings – End Point Flows

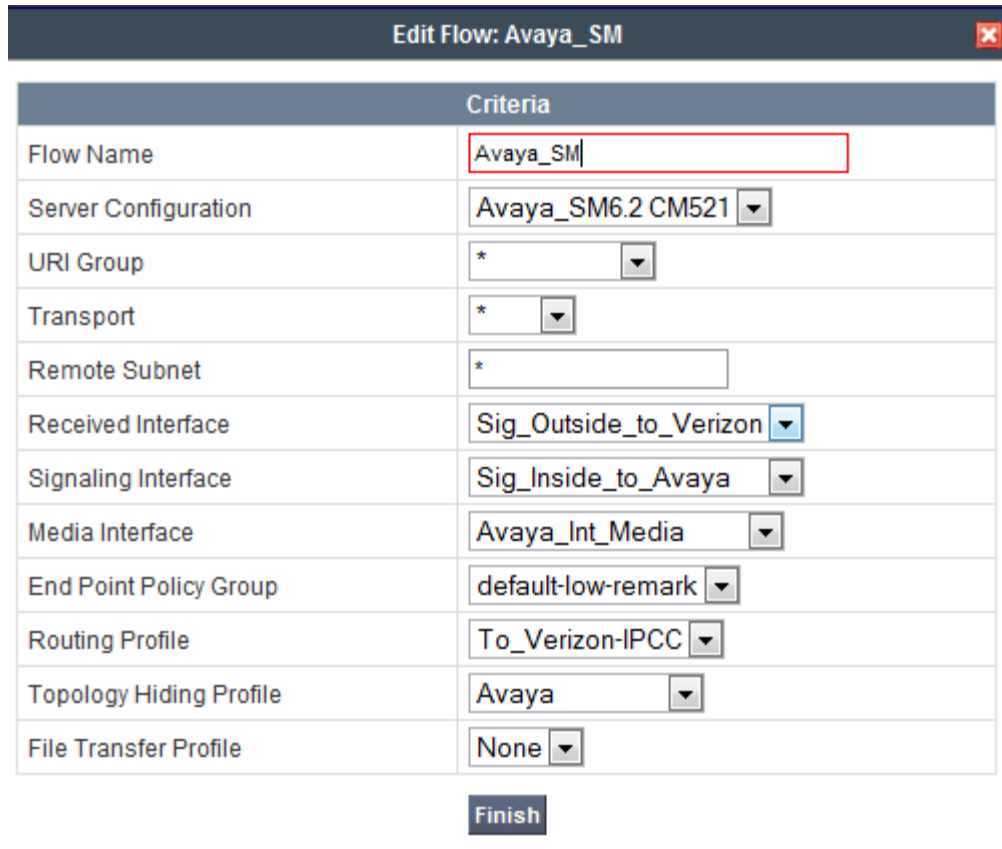
Select **Device Specific Setting** → **End Point Flows** from the left-side menu as shown below.



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



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



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

Finish

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

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

Edit Flow: VZ-IPCC SIP_Trunk
✕

Criteria	
Flow Name	VZ-IPCC SIP_Trunk
Server Configuration	VZ-IPCC SIP TRK ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Sig_Inside_to_Avaya ▼
Signaling Interface	Sig_Outside_to_Verizon ▼
Media Interface	Ext_Media_to_Verizon ▼
End Point Policy Group	default-low-remark ▼
Routing Profile	To_Avaya SM6.2 ▼
Topology Hiding Profile	Verizon-IPCC ▼
File Transfer Profile	None ▼
<div style="background-color: #4f81bd; color: white; padding: 5px 15px; display: inline-block; border: 1px solid black;">Finish</div>	

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

UC-Sec Devices

ASBCE-3

Subscriber Flows

Server Flows

Add Flow

[Click here to add a row description.](#)

Server Configuration: Avaya_SM6.2 CM521

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

Server Configuration: VZ-IPCC SIP TRK

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	VZ-IPCC SIP_Trunk	*	*	*	Sig_Inside_to_Avaya	Sig_Outside_to_Verizon	Ext_Media_to_Verizon	default-low-remark	To_Avaya SM6.2	Verizon-IPCC	None			

8. Verizon Business IPCC Services Suite Configuration

Information regarding Verizon Business IPCC Services suite offer can be found at <http://www.verizonbusiness.com/products/contactcenter/ip/> or by contacting a Verizon Business sales representative.

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

9. Verification Steps

This section provides example verifications of the sample configuration illustrated in these Application Notes.

9.1. Communication Manager and Wireshark Trace Call Verifications

This section illustrates verifications using Communication Manager and Wireshark to illustrate key SIP messaging and call flows.

9.1.1 Wireshark Example of Incoming Call from PSTN via Verizon IPCC

Incoming toll-free calls arrive from Verizon at the Avaya SBCE, which sends the call to Session Manager. Session Manager sends the call to Communication Manager via the entity link corresponding to Communication Manager Processor Ethernet using port 5060. On Communication Manager, the incoming call arrives via signaling group 5 and trunk group 5.

Filter: sip					
Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
1	0.000000	63.79.178.21	12.71.19.138	SIP/SDP	Request: INVITE sip:8666735877@iptf7.interoplab.21sip.com;transport=udp
2	0.001668	12.71.19.138	63.79.178.21	SIP	Status: 100 Trying
3	0.035776	12.71.19.138	63.79.178.21	SIP/SDP	Status: 183 Session Progress, with session description
190	3.792756	12.71.19.138	63.79.178.21	SIP/SDP	Status: 200 OK, with session description
198	3.949220	63.79.178.21	12.71.19.138	SIP	Request: ACK sip:8666735877@12.71.19.138:5060;transport=udp
1100	13.001505	63.79.178.21	12.71.19.138	SIP/SDP	Request: INVITE sip:8666735877@12.71.19.138:5060;transport=udp, in-dia
1101	13.002951	12.71.19.138	63.79.178.21	SIP	Status: 100 Trying
1103	13.020734	12.71.19.138	63.79.178.21	SIP/SDP	Status: 200 OK, with session description
1104	13.070582	63.79.178.21	12.71.19.138	SIP	Request: ACK sip:8666735877@12.71.19.138:5060;transport=udp
1105	13.083705	63.79.178.21	12.71.19.138	SIP	Request: BYE sip:8666735877@12.71.19.138:5060;transport=udp
1106	13.119841	12.71.19.138	63.79.178.21	SIP	Status: 200 OK

Frame 1: 963 bytes on wire (7704 bits), 963 bytes captured (7704 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: 63.79.178.21 (63.79.178.21), Dst: 12.71.19.138 (12.71.19.138)
User Datagram Protocol, Src Port: 34056 (34056), Dst Port: sip (5060)
Session Initiation Protocol
Request-Line: INVITE sip:8666735877@iptf7.interoplab.21sip.com;transport=udp SIP/2.0
Message Header
Call-ID: 21113012261815257392@63.79.178.21
Via: SIP/2.0/UDP 63.79.178.21:5060;branch=z9hG4bK3F4FB215BADF00D00000137379FBE701478
Via: SIP/2.0/UDP app.ubiquitousoftware.com;branch=z9hG4bK3F4FB215BADF00D00000137379FBE70
From: <sip:+13035387022@199.173.94.16:5060;user=phone>;tag=36632949.1.pdpeclebiameejmnmkfbfan
To: sip:18666735877@iptf7.interoplab.21sip.com
CSeq: 1 INVITE
Contact: sip:63.79.178.20:5060
Allow: INVITE, ACK, BYE, OPTIONS, CANCEL, SUBSCRIBE, REFER
P-Asserted-Identity: "UNAVAILABLE" <sip:+13035387022@199.173.94.16;user=phone>
Accept: application/sdp
Content-Type: application/sdp
Content-Length: 201
Max-Forwards: 70
Message Body

The following abridged and annotated Communication Manager **list trace tac *015** output shows a call incoming on trunk group 5. The PSTN telephone 3035387022 dialed 866-674-7056. Session Manager can map the number received from Verizon to the extension of a Communication Manager telephone (Extension 7689), or the incoming call handling table for trunk group 5 can do the same. In the trace below, Communication Manager receives the DID of 866-674-7056 and translates that to local extension 7689.

list trace tac *105	Page 1
LIST TRACE	
time	data
17:39:29	TRACE STARTED 06/20/2012 CM Release String cold-00.1.510.1-19528
	/* Incoming call arrives to Communication Manager for DID 8666747056 */
17:39:37	SIP<INVITE sip: 8666747056@avayalab.com;transport=tcp SIP/2.
17:39:37	SIP<0
17:39:37	Call-ID: 1137110669543718452@63.79.178.21
17:39:37	active trunk-group 5 member 249 cid 0x1aa
	/* Communication Manager sends 183 with SDP as a result of TG 5 configuration */
17:39:37	SIP>SIP/2.0 183 Session Progress
17:39:37	Call-ID: 1137110669543718452@63.79.178.21
	/* Communication Manager translates the DID to extension 7689 */
17:39:37	dial 7689
17:39:37	ring station 7689 cid 0x1aa
	/* G450 Gateway at 10.80.140.15, ringback tone heard by caller */
17:39:37	G729A ss:off ps:20
	rgn:1 [10.80.140.40]:32670
	rgn:1 [10.80.140.15]:16394
17:39:37	G729 ss:off ps:20
	rgn:1 [10.80.140.141]:35020
	rgn:1 [10.80.140.15]:16386
17:39:37	xoip options: fax:off modem:off tty:US uid:0x50107
	xoip ip: [10.80.140.15]:16386
	/* User Answers call, Communication Manager sends 200 OK */
17:39:42	SIP>SIP/2.0 200 OK
17:39:42	Call-ID: 1137110669543718452@63.79.178.21
17:39:42	active station 7689 cid 0x1aa
	/* Communication Manager receives ACK to 200 OK */
17:39:42	SIP<ACK sip: 8666747056@10.80.140.22;transport=tcp SIP/2.0
17:39:42	Call-ID: 1137110669543718452@63.79.178.21
	/* Communication Manager Extension terminates the call */
17:39:44	SIP>BYE sip:10.80.140.141:5060;transport=tcp SIP/2.0
17:39:44	Call-ID: 1137110669543718452@63.79.178.21
17:39:44	idle station 7689 cid 0x1aa

9.1.2 Example Incoming Call Referred with UII to Alternate SIP Destination

The following Communication Manager **list trace vdn** output shows a different example incoming Verizon toll-free call. The call was routed to a Communication Manager VDN 7690 associated with a vector 5. As in previous illustrations, this vector will answer the call, play an announcement to the caller, and then use a “route-to” step to cause a REFER message to be sent to Verizon. In this case, the Refer-To number will cause Verizon to route the call to another SIP-connected destination. In the sample configuration, where only one site is available, this was tested by including a different IP Toll Free number (1-866-674-7056) assigned to the same site in the Route-To step in the vector. The vector also sets UII data that will be included in the

Refer-To header. When Verizon originates a new call to the “alternate” destination, the INVITE message sent by Verizon will contain a User-To-User header containing the UUI data originally sent by the referring site in the Refer-To header. In practice, this would allow a Communication Manager at one site to pass call or customer-related data to another site via the Verizon network.

LIST TRACE

```
time          data
17:27:13 TRACE STARTED 06/20/2012 CM Release String cold-00.1.510.1-19528
/* Inbound call arrives to DID 8666747057 -- VDN 7690 associated with vector 5 */
17:27:40 SIP<INVITE sip:8666747057@avayaalab.com;transport=tcp SIP/2.
17:27:40 SIP<0 Call-ID: -2087842424-449653436@63.79.178.21
17:27:40         active trunk-group 5 member 249      cid 0x1a5
17:27:40         0 0 ENTERING TRACE cid 421
17:27:40         5 1 vdn e7690 bsr appl      0 strategy 1st-found override n
/* Steps in vector 5 add UUI */
17:27:40         5 1 set A = none CATR 1234567890123456
17:27:40         5 1      operand      = []
17:27:40         5 1      operand      = [1234567890123456]
17:27:40         5 1      ===== CATR =====
17:27:40         5 1      variable A = [1234567890123456] asaiuui local
17:27:40         5 1      asaiuui chg from [] to [1234567890123456]
17:27:40         5 2 set B = none CATR 7890123456789012
17:27:40         5 2      operand      = []
17:27:40         5 2      operand      = [7890123456789012]
17:27:40         5 2      ===== CATR =====
17:27:40         5 2      variable B = [7890123456789012] asaiuui local
17:27:40         5 2      asaiuui chg from [] to [7890123456789012]
17:27:40         5 3 wait 2 secs hearing ringback
17:27:40 SIP>SIP/2.0 183 Session Progress
17:27:40         Call-ID: -2087842424-449653436@63.79.178.21
17:27:40         dial 7690
17:27:40         ring vector 5      cid 0x1a5
17:27:40         G729 ss:off ps:20
17:27:40         rgn:1 [10.80.140.141]:35012
17:27:40         rgn:1 [10.80.140.15]:16390
17:27:42         5 4 # Play announcement to answer c...
17:27:42         5 5 announcement 7697
17:27:42 SIP>SIP/2.0 183 Session Progress
17:27:42         Call-ID: -2087842424-449653436@63.79.178.21
17:27:42         5 5      announcement: board 001V9 ann ext: 7697
/* Pre-refer announcement answers call,200 OK sent to Verizon */
17:27:42 SIP>SIP/2.0 200 OK
17:27:42         Call-ID: -2087842424-449653436@63.79.178.21
17:27:42         hear annc board 001V9 ext 7697 cid 0x1a5
17:27:42 SIP<ACK sip:10.80.140.22;transport=tcp SIP/2.0
17:27:42         Call-ID: -2087842424-449653436@63.79.178.21
17:27:49         idle announcement      cid 0x1a5
/* Announcement completes, route-to step executes and REFER (with UUI) is sent */
17:27:49         5 6 route-to number ~r+18666747056 cov n if unconditionally
17:27:49 SIP>REFER sip:10.80.140.141:5060;transport=tcp SIP/2.0
17:27:49         Call-ID: -2087842424-449653436@63.79.178.21
/* Communication Manager receives 202 Accepted for the REFER */
17:27:49 SIP<SIP/2.0 202 Accepted
17:27:49         Call-ID: -2087842424-449653436@63.79.178.21
/* Verizon sends re-INVITE with c=0.0.0.0 SDP */
17:27:49 SIP<INVITE sip:10.80.140.22;transport=tcp SIP/2.0
17:27:49         Call-ID: -2087842424-449653436@63.79.178.21
17:27:49 SIP>SIP/2.0 100 Trying
17:27:49         Call-ID: -2087842424-449653436@63.79.178.21
17:27:49 SIP>SIP/2.0 200 OK
17:27:49         Call-ID: -2087842424-449653436@63.79.178.21
17:27:50 SIP<ACK sip:8776735877@10.80.140.22;transport=tcp SIP/2.0
/* Communication Manager receives SIP NOTIFY with sipfrag 200 OK,agent answered */
17:27:50 SIP<NOTIFY sip:8776735877@10.80.140.22;transport=tcp SIP/2.
17:27:50 SIP<0 Call-ID: -2087842424-449653436@63.79.178.21
17:27:50 SIP>SIP/2.0 200 OK
17:27:50         Call-ID: -2087842424-449653436@63.79.178.21
17:27:56 SIP<NOTIFY sip:10.80.140.22;transport=tcp SIP/2.0
17:27:56         Call-ID: -2087842424-449653436@63.79.178.21
17:27:56 SIP>SIP/2.0 200 OK
17:27:56         Call-ID: -2087842424-449653436@63.79.178.21
17:27:56         5 6 LEAVING VECTOR PROCESSING cid 421
17:27:56 SIP>BYE sip:10.80.140.141:5060;transport=tcp SIP/2.0
17:27:56         idle vector 0      cid 0x1a5
```

9.2. System Manager and Session Manager Verifications

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

9.2.1 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
▶ Performance

A screen such as the following is displayed.

Call Routing Test

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

SIP INVITE Parameters

Called Party URI	Calling Party Address
<input type="text"/>	<input type="text"/>
Calling Party URI	Session Manager Listen Port
<input type="text"/>	<input type="text" value="5060"/>
Day Of Week	Time (UTC)
<input type="text" value="Wednesday"/>	<input type="text" value="23:45"/>
Called Session Manager Instance	Transport Protocol
<input type="text" value="ASM"/>	<input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

Populate the fields for the call parameters of interest and click **Execute Test**.

For example, the following shows a call routing test for an inbound toll-free call from the PSTN to the enterprise via the Avaya SBCE (10.80.140.141). Under **Routing Decisions**, observe that the call will route to the Communication Manager using the SIP entity named “Vz_CM601”. The digits are manipulated such that the Verizon toll-free number (i.e., 866-674-5877) is converted to a Communication Manager extension by the Communication Manager **incoming-call-handling-treatment-trunk-group** form. 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

Help ?

Call Routing Test

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

SIP INVITE Parameters

Called Party URI	Calling Party Address
<input type="text" value="8666745877@avayalab.com"/>	<input type="text" value="10.80.140.141"/>
Calling Party URI	Session Manager Listen Port
<input type="text" value="anycaller@anydomain.com"/>	<input type="text" value="5060"/>
Day Of Week	Time (UTC)
<input type="text" value="Wednesday"/>	<input type="text" value="23:45"/>
Called Session Manager Instance	Transport Protocol
<input type="text" value="ASM"/>	<input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

Routing Decisions

Route < sip:8666745877@avayalab.com > to SIP Entity Vz_CM601 (10.80.140.22). Terminating Location is Location_140_CM.

Below is an example of the **status trunk 5** output for an active call in Communication Manager.

status trunk 5				
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/active	no	S00000
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

Verify the port returns to **in-service/idle** after the call has ended.

status trunk 5				
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/idle	no	
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

9.3. Troubleshooting

1. Communication Manager:

- **list trace station** <extension number> - Traces calls to and from a specific station.
- **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
- **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk number> - Displays trunk group information.

2. Session Manager:

- **traceSM -x -uni** - Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

3. Avaya SBCE:

- **Incidences** - Displays alerts captured by the UC-Sec appliance.

Incident Viewer

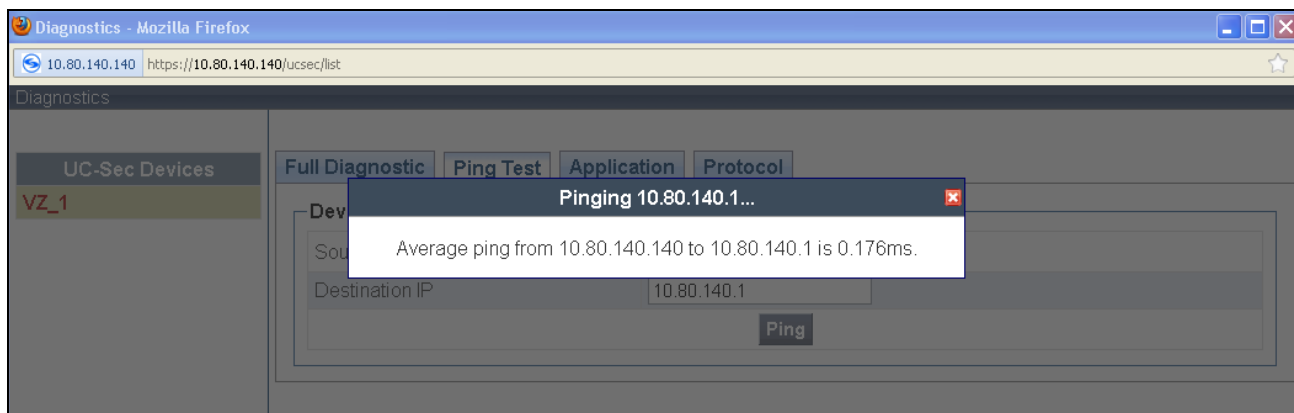
Device **All** Category **All** **Clear Filters** **Refresh** **Show Chart** **Generate Report**

Displaying results 1 to 15 out of 2000.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
Call Denied	670662031896742	7/3/12	2:01 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661994168844	7/3/12	1:59 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661954276260	7/3/12	1:58 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661945964975	7/3/12	1:58 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661925281781	7/3/12	1:57 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Call Denied	670661836385435	7/3/12	1:54 PM	Policy	VZ_1	No Server Flow Matched for Outgoing Message
Server Heartbeat	670544586913020	6/30/12	8:46 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	670544560072813	6/30/12	8:45 PM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	670395413600112	6/27/12	9:53 AM	Policy	VZ_1	Server Heartbeat is UP
Call Denied	670395398129528	6/27/12	9:53 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Call Denied	670395390129764	6/27/12	9:53 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Call Denied	670395389651406	6/27/12	9:52 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Server Heartbeat	670395386597209	6/27/12	9:52 AM	Policy	VZ_1	Server Heartbeat is failed
Call Denied	670395386129139	6/27/12	9:52 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message
Call Denied	670395384128531	6/27/12	9:52 AM	Policy	VZ_1	No Server Flow Matched for Incoming Message

<< < 1 2 3 4 5 > >>

- **Diagnostics** - Allows for PING tests and displays application and protocol use.



- **Troubleshooting → Trace Settings** - Configure and display call traces and packet captures for the UC-Sec appliance.

Packet Trace	Call Trace	Packet Capture	Captures
Packet Capture Configuration			
Currently capturing		No	
Interface		A1 ▼	
Local Address (ip:port)		All ▼ : <input type="text"/>	
Remote Address (*, *:port, ip, ip:port)		* <input type="text"/>	
Protocol		All ▼	
Maximum Number of Packets to Capture		9999	
Capture Filename <small>Existing captures with the same name will be overwritten</small>		Test_Trace.pcap	
		<input type="button" value="Start Capture"/> <input type="button" value="Clear"/>	

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise can be configured to interoperate successfully with Verizon Business IP Contact Center Services IP Toll Free VoIP Inbound service. This solution enables inbound toll free calls over a Verizon Business VoIP Inbound SIP trunk service connection. In addition, these Application Notes further demonstrate that the Avaya Aura® Communication Manager implementation of SIP Network Call Redirection (SIP-NCR) can work in conjunction with Verizon Business IP Contact Center services implementation of SIP-NCR to support call redirection over SIP trunks inclusive of passing User-User Information (UII).

Please note that the sample configurations shown in these Application Notes are intended to provide configuration guidance to supplement other Avaya product documentation.

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.

11. Additional References

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 6.0 June, 2010 available at <http://support.avaya.com/css/P8/documents/100089133>
- [2] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, Issue 6.0 June 2010 available at <http://support.avaya.com/css/P8/documents/100089333>
- [3] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [4] *Installing and Upgrading Avaya Aura® System Manager Release 6.2*, November 2010.

- [5] *Installing and Configuring Avaya Aura® Session Manager*, January 2011, Document Number 03-603473
- [6] *Administering Avaya Aura® Session Manager*, March 2011, Document Number 03-603324.
- [7] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org>
- [8] UC-Sec Administration Guide (010-5423-400v106)

Appendix A

Included below is the Sigma Script used during the compliance testing.

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

©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.