



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and Avaya Aura™ Session Border Controller with Verizon Business IP Trunk SIP Trunk Service – Issue 1.3

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura™ Session Manager Release 6, Avaya Aura™ Communication Manager Release 6, and the Avaya Aura™ Session Border Controller with the Verizon Business Private IP (PIP) IP Trunk service. These Application Notes update previously published Application Notes with newer versions of Communication Manager and Session Manager, **including a declaration of support for Communication Manager Release 6.0.1 and Session Manager Release 6.1, as noted in Section 3.**

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab., utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunking service.

Table of Contents

1.	Introduction.....	4
1.1.	Interoperability Compliance Testing	4
1.2.	Support.....	4
1.2.1	Avaya	4
1.2.2	Verizon.....	4
1.3.	Known Limitations	5
2.	Reference Configuration.....	7
2.1.	History Info and Diversion Headers	8
3.	Equipment and Software Validated	9
4.	Configure Avaya Aura™ Communication Manager Release 6.....	10
4.1.	Processor Ethernet Configuration on S8800 Server	10
4.2.	Verify Licensed Features	14
4.3.	Dial Plan.....	15
4.4.	Node Names.....	16
4.5.	IP Interface for procr.....	16
4.6.	Network Regions for Gateway, Telephones	17
4.7.	IP Codec Sets	20
4.8.	SIP Signaling Groups.....	21
4.9.	SIP Trunk Groups	24
4.10.	Route Pattern Directing Outbound Calls to Verizon	27
4.11.	Public Numbering	27
4.12.	ARS Routing For Outbound Calls	28
4.13.	Incoming Call Handling Treatment for Incoming Calls	29
4.14.	Modular Messaging Hunt Group	29
4.15.	AAR Routing to Modular Messaging via Session Manager.....	30
4.16.	Uniform Dial Plan (UDP) Configuration.....	30
4.17.	Route Pattern for Internal Calls via Session Manager	30
4.18.	Private Numbering.....	31
4.19.	Avaya Aura™ Communication Manager Stations	31
4.20.	Coverage Path	32
4.21.	EC500 Configuration for Diversion Header Testing.....	33
4.22.	Saving Communication Manager Configuration Changes	33
5.	Configure Avaya Aura™ Session Manager Release 6	33
5.1.	Domains	37
5.2.	Locations.....	38
5.3.	Adaptations	41
5.4.	SIP Entities.....	44
5.5.	Entity Links.....	51
5.6.	Time Ranges	52
5.7.	Routing Policies	53
5.8.	Dial Patterns.....	55
6.	Configure Avaya Aura™ Session Border Controller (SBC).....	56
6.1.	Avaya Aura™ SBC Installation.....	57
6.2.	Avaya Aura™ SBC Licensing.....	69

6.3.	Avaya Aura™ SBC Element Manager Configuration.....	74
6.3.1	Configuration of the Verizon SIP Signaling Port	74
6.3.2	Stripping SIP Headers using P-Site as an Example	77
6.3.3	Use of REFER With Verizon.....	80
6.3.4	Quality Of Service (QoS) Markings for SIP Signaling	82
6.3.5	Disabling Third Party Call Control.....	83
6.3.6	Diversion Header Domain Mapping.....	84
6.3.7	Modular Messaging Find-Me PAI Insertion.....	88
6.4.	Saving and Activating Configuration Changes.....	90
7.	Verizon Business IP Trunk Service Offer Configuration	91
7.1.	Fully Qualified Domain Name (FQDN)s	91
8.	General Test Approach and Test Results.....	91
9.	Verification Steps.....	92
9.1.	Avaya Aura™ Communication Manager Verifications	93
9.1.1	Example Incoming Call from PSTN via Verizon SIP Trunk	93
9.1.2	Example Outgoing Call to PSTN via Verizon SIP Trunk	96
9.2.	Avaya Aura™ System Manager and Session Manager Verification.....	99
9.2.1	Verify SIP Entity Link Status	99
9.2.2	Verify System State	101
9.2.3	Call Routing Test.....	102
9.3.	Avaya Aura™ Session Border Controller Verification	105
9.3.1	Avaya Aura™ Session Border Controller Call Logs.....	108
10.	Conclusion	111
11.	Additional References.....	111
11.1.	Avaya	111
11.2.	Verizon Business	112
12.	Addendum – DNS on Avaya Aura™ SBC Public Interface	113
12.1.	Avaya Aura™ SBC Configuration Changes for DNS to Verizon.....	113
12.1.1	Add the Verizon DNS Server	113
12.1.2	Add DNS Group	115
12.1.3	Disable the sip-gateway Telco Created by the Installation Wizard.....	118
12.1.4	Configure the Dial-plan to Use the New DNS-Group.....	119
12.1.5	Set Fail-over Detection for New DNS-Group to use OPTIONS	120
12.1.6	Save the Configuration and Force DNS.....	121
12.2.	Avaya Aura™ SBC Verifications of DNS to Verizon	121
12.2.1	Avaya Aura™ SBC Status Tab.....	121
12.2.2	Avaya Aura™ SBC Actions Tab.....	122
12.2.3	Wireshark Illustration of DNS Usage.....	124
12.2.4	Wireshark Illustration of SIP OPTIONS	125

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura™ Session Manager Release 6, Avaya Aura™ Communication Manager Release 6, and the Avaya Aura™ Session Border Controller (SBC) with the Verizon Business Private IP (PIP) IP Trunk service. The Verizon Business IP Trunk service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

1.1. Interoperability Compliance Testing

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

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

1.2. Support

1.2.1 Avaya

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

1.2.2 Verizon

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

1.3. Known Limitations

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

- Following a loss and restoration of Ethernet connectivity, the Avaya Aura™ SBC may not recover quickly without manual intervention. This problem has been reported to the Avaya Aura™ SBC product team for resolution in a future software version. To trigger recovery of service following a loss and restoration of Ethernet connectivity, an arp request can be issued from the SBC for the default gateway IP address of the previously failed network interface. More specifically, the following actions will trigger recovery. Select the **Actions** tab, as shown in Section 12.2.2. From the left side menu, click the “arp” action. In the resultant right panel, select “request” from the **type** drop-down menu, and enter the IP Address of the default gateway for the previously failed interface. Click the **Invoke** button. Assuming the previously failed Ethernet connectivity has been restored, the arp request will succeed and stimulate full service recovery.
- Although Avaya Aura™ Session Manager 6.0 supports the use of SIP phones, and SIP phones were present in the sample configuration, the configuration of SIP phones is not covered by these Application Notes.
- At the time of original publication of these Application Notes, Verizon Business IP Trunking service supported fax over G.711 but did not support T.38 fax. As noted in reference [JF-JRR-VZIPT], the use of an AudioCodes SIP Gateway between Communication Manager and the fax device has long been recommended for G.711 fax with Verizon IP Trunk service. Since original publication of these Application Notes, Verizon Business IP Trunking service has been enhanced to support T.38 fax. A customer connecting fax devices to an AudioCodes SIP Gateway may continue to use fax over G.711. Alternatively, if the AudioCodes gateway version and Communication Manager Service Pack are up to date, the customer may now choose to enable T.38 on the AudioCodes gateway and Communication Manager codec set. For example, for an AudioCodes MP-114, the AudioCodes gateway should use version 6.20A.035.001 or later. If T.38 fax will be used with Verizon IP Trunk service, and the fax device will be connected to a SIP gateway, Communication Manager 6.0.1 Service Pack 6 (SP6) is recommended. Communication Manager 6.0.1 SP6 includes a change that enables Communication Manager to relay a SIP 488 response from Verizon to the SIP gateway for call scenarios where the SIP gateway requests T.38 but Verizon can not comply. By relaying the SIP 488 response from Verizon to the SIP gateway, Communication Manager 6.0.1 SP6 gives the SIP gateway the opportunity to “fallback to G.711” to complete the fax call using fax over G.711, if T.38 is not available for a particular fax call.
- If calls requiring in-band DTMF (rather than RFC 2833 signaling) will be required, the “DTMF over IP” parameter on the Avaya Aura™ Communication Manager SIP signaling group carrying such calls can be set to “in-band” rather than “rtp-payload”. If the Communication Manager SIP signaling group is set to “rtp-payload”, and a call is established using RFC 2833, Communication Manager will not subsequently switch to using “in-band” procedures to signal DTMF. Avaya is considering an enhancement for a future release of Communication Manager that would allow a call initially established with RFC 2833 to switch to using in-band DTMF based on subsequent SIP SDP exchanges.
- Verizon Business IP Trunking service does not support G.711A codec for domestic service (EMEA only).

- Verizon Business IP Trunking service does not support G.729B codec.

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

2. Reference Configuration

Figure 1 shows the sample configuration.. As shown in **Figure 1**, the Avaya Aura™ SBC receives traffic from the Verizon Business IP Trunk service on port 5060 and sends traffic to the Verizon Business IP trunk service to port 5071, using UDP protocol for network transport (required by the Verizon Business IP Trunk service). The Verizon Business IP Trunk service provided Direct Inward Dial (DID) 10 digit numbers. These DID numbers were mapped by Avaya Aura™ Session Manager or Avaya Aura™ Communication Manager to Avaya telephone extensions.

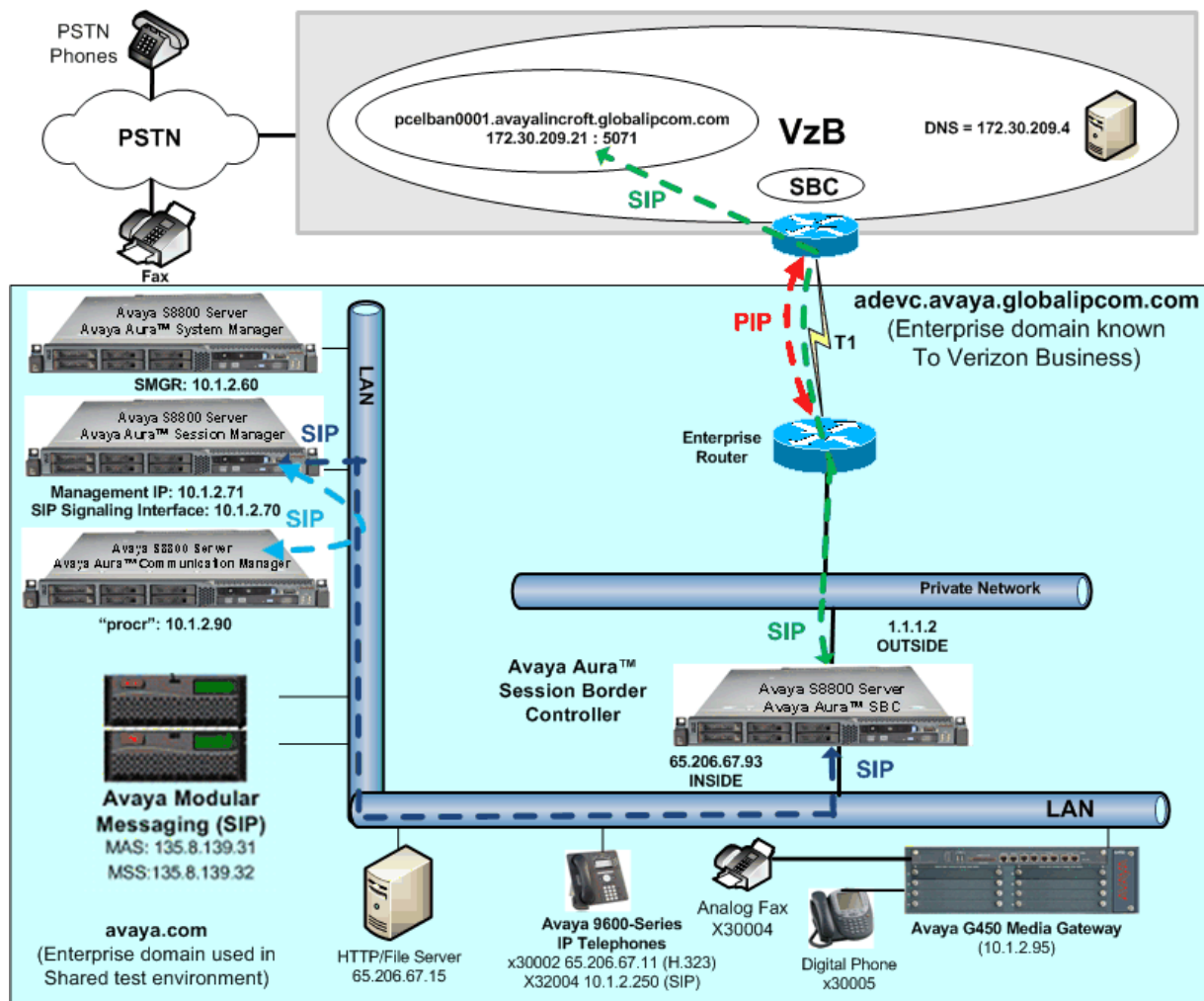


Figure 1: Avaya Interoperability Test Lab Configuration

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk Service as FQDN *adevc.avaya.globalipcom.com*, as in reference [JF-JRR-VZIPT]. For efficiency, the Avaya CPE environment utilizing Session Manager Release 6 and Communication Manager Release 6 was shared among many ongoing test efforts at the Avaya Interoperability lab. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain “avaya.com” at the enterprise. Avaya Aura™ Session Manager or the Avaya Aura™ SBC are used to adapt the “avaya.com” domain to the domains known to Verizon. 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 the Verizon Business IP Trunk service.

The following components were used in the sample configuration:

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

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
 - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN)
 - *adevc.avaya.globalipcom.com*
- Avaya Aura™ Session Border Controller (SBC)
- Avaya Aura™ Communication Manager Release 6
- Avaya Aura™ Session Manager Release 6
- Avaya 4600 Series IP telephones using the H.323 software bundle
- Avaya 9600 Series IP telephones using the H.323 software bundle
- Avaya Digital phones

2.1. History Info and Diversion Headers

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

If Avaya Aura™ Communication Manager sends the History Info Header for a redirected call, Avaya Aura™ Session Manager can convert the History Info header into the Diversion Header. This is performed by specifying the “*VerizonAdapter*” adaptation in Avaya Aura™ Session Manager.

The Avaya Aura™ Communication Manager call forwarding or Extension to Cellular (EC500) features may be used for call scenarios testing Diversion Header.

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server (Communication Manager)	Avaya Aura™ Communication Manager Release 6.0 (load 345.0, patch 18246)
Avaya S8800 Server (System Manager)	Avaya Aura™ System Manager Release 6.0 (load 6.0.0.0.556-3.0.6.1)
Avaya S8800 Server (Session Manager)	Avaya Aura™ Session Manager Release 6.0 (load 6.0.0.0.600020)
Avaya S8800 Server (Session Border Controller)	Avaya Aura™ Session Border Controller Release 6.0 SBC Template SBCT 6.0.0.1.4
Avaya Modular Messaging (Application Server)	Avaya Modular Messaging (MAS) 5.2 Service Pack 3 Patch 1
Avaya Modular Messaging (Storage Server)	Avaya Modular Messaging (MSS) 5.2, Build 5.2-11.0
Avaya 4600-Series Telephones (H.323)	Release 2.9.1 – H.323
Avaya 9600-Series Telephones (H.323)	Release 3.1.1 – H.323
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
Brother Intellifax 1360	N/A

Table 1: Equipment and Software Used in the Sample Configuration

Note - The solution integration validated in these Application Notes should be considered valid for deployment with Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1. Avaya agrees to provide service and support for the integration of Avaya Aura® Communication Manager release 6.0.1 and Avaya Aura® Session Manager release 6.1 with Verizon Business IP Trunk service offer, in compliance with existing support agreements for Avaya Aura® Communication Manager release 6.0 and Avaya Aura® Session Manager 6.0, and in conformance with the integration guidelines as specified in this document. As noted in Section 1.3, Communication Manager 6.0.1 Service Pack 6 (SP6) is recommended if fax devices will be connected to a SIP gateway, and T.38 fax will be used.

4. Configure Avaya Aura™ Communication Manager Release 6

This section illustrates an example configuration allowing SIP signaling via the “Processor Ethernet” of the Avaya S8800 Server to Session Manager.

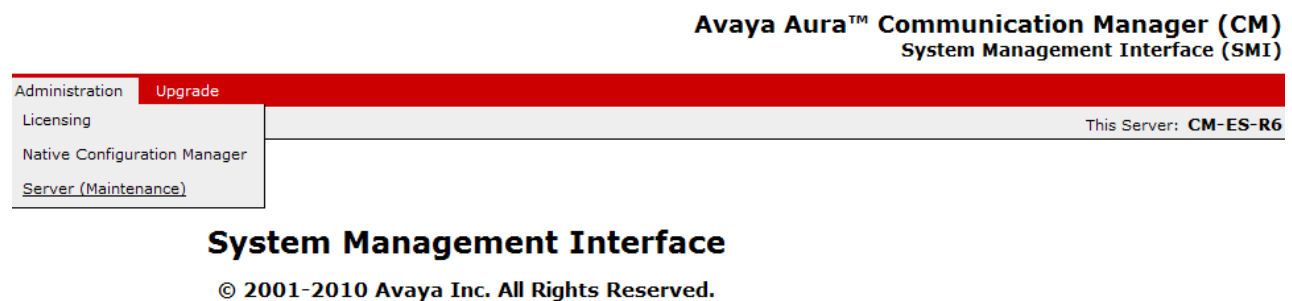
Note - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Avaya Aura™ Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

Except for the web configuration shown in Section 4.1, all remaining configuration is performed via the Communication Manager SAT interface of the Avaya S8800 Server. Screens are abridged for brevity in presentation.

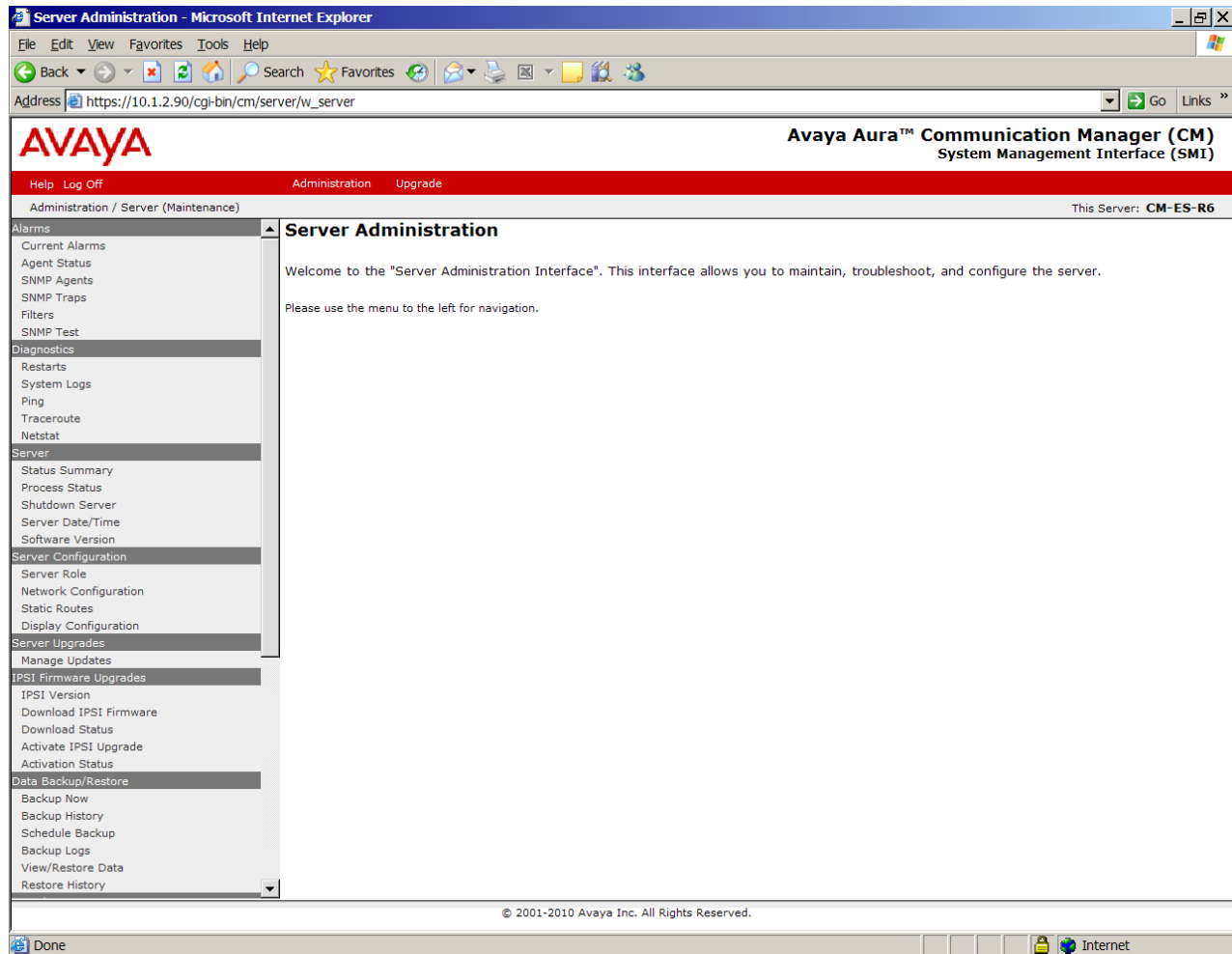
4.1. Processor Ethernet Configuration on S8800 Server

The Processor Ethernet must be configured via the Web pages on the S8800 server. The screens in this section illustrate a previously completed configuration. Consult product documentation for further procedural guidance.

The S8800 Server can be accessed via a web interface in an internet browser. In the sample configuration, enter <http://10.1.2.90> and log in with appropriate credentials (not shown). From the System Management Interface screen, select **Administration → Server (Maintenance)** as shown below.



The resulting **Server Administration** screen is shown below.



Under **Server Configuration**, select **Server Role** to view the server role. In the sample configuration, the Avaya S8800 server is a **main server**, as shown below.

Server Role

This page allows for the specification of the Server's Role.



WARNING:

- Changing the role of this server will **erase any translations** residing on this server and will cause a **Communication Manager reset**. If you wish to preserve existing translations, execute a backup prior to completing this page.
- This server appears to be the **ACTIVE** server. Continuing the process may cause the Standby to become **ACTIVE**. This server will be unavailable for telephony during the configuration process.

Server Settings

This Server is:

- ☒ a main server
- ☐ an enterprise survivable server (ESS)
- ☐ a local survivable server (LSP)

System ID and Module ID:

SID:

MID:

Configure Memory

This Server's Memory Setting:

Large ▼

[Change](#)

[Restart CM](#)

[Help](#)

Under **Server Configuration**, select **Network Configuration** to view the network configuration. The following screen shows the upper portion of the **Network Configuration**.

Network Configuration

This implementation is used to configure the IP related settings for this server. Please note that some changes made on this page may affect settings on other pages under the "Server Configuration" category - please make sure to check all pages for an accurate configuration.



Notes

- The host name and ID of each server in the system must be unique.
- The below fields is used to indicate how each Ethernet port is to be used (functional assignment) and to configure the IP related settings of each port. Ethernet ports may be used for multiple purposes, except for the port assigned to the laptop, which must be dedicated to only that purpose.
- An Ethernet port can be configured without a functional assignment. However, any port intended for use with the Communication Manager application must be assigned the correct functional assignment.
- Physical connections to the Ethernet ports must match settings provided below. Please keep in mind that the labels on the physical ports may be shifted by 1, e.g.: eth0 could be labeled 1, eth1 could be labeled 2, etc.
- Note that any configuration data obtained from an external source will be displayed read-only. To change these settings, please navigate to the external tool used to configure those settings.
- A restart of Communication Manager is needed after the server has been successfully configured. Click the **Restart CM** button below to do so. Please note that this should be done after all configuration is completed. Too many restarts may escalate to a full Communication Manager reboot.
- This server appears to be the **ACTIVE** server. Continuing the process may cause the Standby to become **ACTIVE**. This server will be unavailable for telephony during the configuration process.

Host Name:	<input type="text" value="CM-ES-R6"/>
DNS Domain:	<input type="text"/>
Search Domain List:	<input type="text" value="cm-es-r6"/> (comma separated)
Primary DNS:	<input type="text" value="192.168.1.200"/>
Secondary DNS:	<input type="text"/>
Tertiary DNS:	<input type="text"/>
Server ID:	<input type="text" value="1"/> (Range 1 to 256)

Scrolling down, the following screen shows the lower portion of the Network Configuration. Note that the IPv4 Address of the server is 10.1.2.90, and that the **Functional Assignment** drop-down has assigned the **Corporate LAN/Processor Ethernet/Control Network** to the same "eth0" interface.

Server ID:	<input type="text" value="1"/> (Range 1 to 256)			
Default Gateway:	IPv4 <input type="text" value="10.1.2.1"/>		IPv6 <input type="text"/>	
eth0:	IPv4 Address	Mask	IPv6 Address	Prefix
IP Configuration:	<input type="text" value="10.1.2.90"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text"/>
Functional Assignment:	<input type="text" value="Corporate LAN/Processor Ethernet/Control Network"/>			

[Change](#)

[Restart CM](#)

[Help](#)

4.2. Verify Licensed Features

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

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

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	100
Maximum Concurrently Registered IP Stations:		18000	3
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	146
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	1
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		300	0

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

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

On **Page 4** of the *display system-parameters customer-options* form, verify that the **Enhanced EC500, IP Trunks, IP Stations, and ISDN-PRI** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required (see also Section 4.9), 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		
IP Attendant Consoles? y		

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

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

4.3. Dial Plan

In the sample configuration the Avaya CPE environment uses five digit local extensions, such as 30xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with 1. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR

is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

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

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all			Percent Full: 2			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	3	fac							
1	3	dac							
2	5	ext							
3	5	ext							
4	4	ext							
5	5	ext							
6	3	fac							
60	5	ext							
7	5	ext							
8	1	fac							
9	1	fac							
*	2	fac							
#	2	fac							

4.4. Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged “change node-names ip” output shows relevant node-names in the sample configuration. As shown in bold, the node name for Avaya Aura™ Session Manager is “SM1” with IP Address 10.1.2.70. The node name and IP Address (10.1.2.90) for the Processor Ethernet “procr” appears automatically due to the web configuration in Section 4.1.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
SM1	10.1.2.70	
procr	10.1.2.90	

4.5. IP Interface for procr

The “add ip-interface procr” or “change ip-interface procr” command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet 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: 1700	
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.1.2.90	
Subnet Mask: /24		

4.6. Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the shared Avaya Aura™ Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 4 was associated with other components used specifically for the Verizon testing.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that media gateway 1 is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the “Controller IP Address” is the Avaya S8800 processor Ethernet (10.1.2.90), and that the gateway IP Address is 10.1.2.95. These fields are not configured in this screen, but rather simply display the current information for the gateway.

change media-gateway 1		Page 1 of 2
MEDIA GATEWAY 1		
Type: g450		
Name: G450 Evolution Srvr		
Serial No: 08IS43202588		
Encrypt Link? y	Enable CF? n	
Network Region: 1	Location: 1	
	Site Data:	
Recovery Rule: none		
Registered? y		
FW Version/HW Vintage: 30 .13 .2 /1		
MGP IPV4 Address: 10.1.2.95		
MGP IPV6 Address:		
Controller IP Address: 10.1.2.90		
MAC Address: 00:1b:4f:03:57:b0		

The following screen shows **Page 2** for media gateway 1. The gateway has an MM712 media module supporting Avaya digital phones in slot v3, an MM714 supporting analog devices in slot v5, and the capability to provide announcements and music on hold via “gateway-announcements” in logical slot v9.

change media-gateway 1				Page 2 of 2	
MEDIA GATEWAY 1					
Type: g450					
Slot	Module	Type	Name	DSP Type	FW/HW version
V1:				MP80	45 3
V2:					
V3:	MM712		DCP MM		
V4:					
V5:	MM714		ANA MM		
V6:					
V7:					
V8:					Max Survivable IP Ext: 8
V9:	gateway-announcements		ANN VMM		

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the “gatekeeper” (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 65.206.67.11 would be mapped to network region 4, based on the bold configuration below. In production environments, different sites will typically be on different networks, and ranges of IP Addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 10.1.2.0	/24	1	n		
TO: 10.1.2.255					
FROM: 65.206.67.0	/24	4	n		
TO: 65.206.67.255					

The following screen shows IP Network Region 4 configuration. In the shared test environment, network region 4 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 4 will be used for calls within region 4. The “Authoritative Domain” is set to the enterprise SIP domain “adevc.avaya.globalipcom.com” known to Verizon, as shown in **Figure 1**. Verizon supports domains that are longer than the maximum number of characters accepted by the **Authoritative Domain** field. If a domain is required that is longer than the maximum length of the **Authoritative Domain** field, a Session Manager adaptation can be used to manipulate the domain.

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

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

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

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the Codec Set parameter on **Page 1**, but codec set 4 will be used for connections between region 1 and region 4 as noted previously. In the shared test environment, network region 1 was in place prior to adding the Verizon test environment and already used **Authoritative Domain** “avaya.com”. Where necessary, Avaya Aura™ Session Manager will adapt the domain from “avaya.com” to “adevc.avaya.globalipcom.com” and vice-versa. In production environments, it is likely that the enterprise SIP domain known to Verizon will be the same as the Authoritative Domain in the Communication Manager network regions.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain: avaya.com	
Name: HQ CM and SIP Phones		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? y
UDP Port Max: 65535		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

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

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

4.7. IP Codec Sets

The following screen shows the configuration for codec set 4, the codec set configured to be used for calls within region 4 and for calls between region 1 and region 4. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls to and from the PSTN via the SIP trunks would use G.729A, since G.729A is preferred by both Verizon and the Avaya ip-codec-set. Any calls using this same codec set that are between devices capable of the G.722-64K codec (e.g., Avaya 9600-Series IP Telephone) can use G.722. Note that if G.711MU is omitted from the list of allowed codecs in ip-codec-set 4, calls from Verizon that are answered by Avaya Modular Messaging will use G450 VoIP resources to convert from G.729A (facing Verizon) to G.711MU (facing Modular Messaging). If G.711MU is included in ip-codec-set 4, then calls from Verizon that are answered by Modular Messaging will not use G450 VoIP resources, but rather be “ip-direct” using G.711MU from Modular Messaging to the inside of the Avaya Aura™ SBC. Include G.711MU in the ip-codec-set if fax will be used.

change ip-codec-set 4 Page 1 of 2

IP Codec Set

Codec Set: 4

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

On **Page 2** of the form:

- Configure the **FAX Mode** field to **off**. See Section 1.3 for additional fax considerations arising from Verizon’s introduction of support for T.38 fax.
- Configure the **FAX Redundancy** field to **0**.

change ip-codec-set 4 Page 2 of 2

IP Codec Set

Allow Direct-IP Multimedia? n

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

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

change ip-codec-set 1 Page 1 of 2

IP Codec Set

Codec Set: 1

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

4.8. SIP Signaling Groups

This section illustrates the configuration of the SIP Signaling Groups that use the Processor Ethernet. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM1”. In the example screens, the **Transport Method** for all signaling groups is “tcp”. In production, TLS transport between Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager may be used. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the

signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 67. Signaling group 67 will be used for processing incoming PSTN calls from Verizon via Session Manager. The **Far-end Network Region** is configured to region 4. Port 5062 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Verizon DID numbers to a route policy that uses a SIP Entity link to Communication Manager specifying port 5062. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. The **Peer Detection Enabled** field may be set to “no”. Other parameters may be left at default values.

change signaling-group 67		Page 1 of 1
SIGNALING GROUP		
Group Number: 67	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? n	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: SM1	
Near-end Listen Port: 5062	Far-end Listen Port: 5062	
	Far-end Network Region: 4	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

The following screen shows signaling group 68. Again, the **Near-end Node Name** is “procr”, the **Far-end Node Name** is “SM1”, the node name of the Session Manager, and the **Far-end Network Region** is 4. Signaling group 68 will be used for outgoing calls to Session Manager destined for the PSTN via Verizon. Although not strictly necessary in the sample configuration since Session Manager is adapting the Request-URI to the expected Verizon network domain, the **Far-end Domain** is set to “pcelban0001.avayaInc.com”.

Note that the **Alternate Route Timer** that defaults to 6 seconds impacts fail-over timing for outbound calls. If Communication Manager does not get an expected response, Look-Ahead Routing (LAR) can be triggered, after the expiration of the Alternate Route Timer. Detailed examples of the use of LAR can be found in reference [PE] and reference [LAR].

```

change signaling-group 68                                     Page 1 of 1
                                SIGNALING GROUP

Group Number: 68                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
    Q-SIP? n                                SIP Enabled LSP? n
    IP Video? n                        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? n Peer Server: Others

Near-end Node Name: procr                Far-end Node Name: SM1
Near-end Listen Port: 5062                Far-end Listen Port: 5062
                                Far-end Network Region: 4

Far-end Domain: pcelban0001.avayalincroft.globalipcom.com
                                Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate        RFC 3389 Comfort Noise? n
    DTMF over IP: rtp-payload                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3          IP Audio Hairpinning? n
    Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n      Alternate Route Timer(sec): 6

```

The following screen shows signaling group 60, the signaling group to Session Manager that was in place prior to adding the Verizon SIP Trunking configuration to the shared Avaya Interoperability lab configuration. This signaling group reflects configuration not specifically related to Verizon trunking. For example, calls using Avaya SIP Telephones and calls routed to other Avaya applications, such as Avaya Modular Messaging, use this signaling group. Again, the **Near-end Node Name** is “procr” and the **Far-end Node Name** is “SM1”, the node name of the Session Manager. Unlike the signaling groups used for the Verizon signaling, the **Far-end Network Region** is 1. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected. The **Far-end Domain** is set to “avaya.com” matching the configuration in place prior to adding the Verizon SIP Trunking configuration. Session Manager will adapt avaya.com to adevc.avaya.globalipcom.com where necessary for calls involving Verizon.

```

change signaling-group 60                                     Page 1 of 1
                                SIGNALING GROUP

Group Number: 60                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
    Q-SIP? n                                SIP Enabled LSP? n
    IP Video? n                        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: procr                Far-end Node Name: SM1
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                Far-end Network Region: 1

Far-end Domain: avaya.com
                                Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate        RFC 3389 Comfort Noise? n
    DTMF over IP: rtp-payload                Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3          IP Audio Hairpinning? n
    Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n      Alternate Route Timer(sec): 10

```

4.9. SIP Trunk Groups

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

The following shows **Page 1** for trunk group 67, which will be used for incoming PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to “public-ntwrk” for the trunks that will handle calls with Verizon. The **Direction** has been configured to “incoming” to emphasize that trunk group 67 is used for incoming calls only in the sample configuration.

change trunk-group 67		Page 1 of 21	
TRUNK GROUP			
Group Number: 67	Group Type: sip	CDR Reports: y	
Group Name: From-SM-Acme-VZ	COR: 1	TN: 1	TAC: 167
Direction: incoming	Outgoing Display? n		
Dial Access? n	Night Service:		
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 67	
		Number of Members: 6	

The following shows **Page 2** for trunk group 67. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than the Avaya Aura™ Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

change trunk-group 67		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Delay Call Setup When Accessed Via IGAR? n			

The following shows **Page 3** for trunk group 67. All parameters except those in bold are default values. Optionally, replacement text strings can be configured using the “system-parameters features” screen, such that incoming “private” calls can display an Avaya-configured text string on called party telephones.

change trunk-group 67		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		UI Treatment: service-provider
Replace Restricted Numbers? y		Replace Unavailable Numbers? y
Show ANSWERED BY on Display? y		

The following shows **Page 4** for trunk group 67. The **PROTOCOL VARIATIONS** page is one reason why it can be advantageous to configure incoming calls from Verizon to arrive on specific signaling groups and trunk groups. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field is new in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to “y” for the trunk group handling inbound calls from Verizon produces this result. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to “y” enables advanced services associated with the use of the SIP REFER message, while also implicitly enabling Communication Manager to signal “send-only” media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor “send-only” media signaling is required, this field may be left at the default “n” value. In the testing associated with these Application Notes, transfer testing using INVITE was successfully completed with the **Network Call Redirection** flag set to “n”. Transfer testing with the **Network Call Redirection** flag set to “y” was also completed successfully, but the use of REFER to Verizon requires the complementary configuration the Avaya Aura™ SBC shown in Section 6.3.3.

For redirected calls, Verizon supports the Diversion header, but not the History-Info header. Communication Manager can send the Diversion header by marking **Send Diversion Header** to “y”. Alternatively, Communication Manager can send the History-Info header by setting **Support Request History** to “y”, and Session Manager can adapt the History-Info header to the Diversion header using the “VerizonAdapter”.

change trunk-group 67		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? y		
Support Request History? n		
Telephone Event Payload Type: 101		
Convert 180 to 183 for Early Media? y		
Always Use re-INVITE for Display Updates? n		
Enable Q-SIP? n		

The following shows **Page 1** for trunk group 68. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to “public-ntwrk” for the trunks that will handle calls with Verizon. The **Direction** has been

configured to “outgoing” to emphasize that trunk group 68 is used for outgoing calls to Session Manager destined for the PSTN. The remaining pages for trunk group 68 can match trunk group 67 and therefore will not be illustrated here.

change trunk-group 68		Page 1 of 21	
TRUNK GROUP			
Group Number: 68	Group Type: sip	CDR Reports: y	
Group Name: To-ASM-6-VZ	COR: 1	TN: 1	TAC: 168
Direction: outgoing	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 68	
		Number of Members: 10	

The following shows **Page 1** for trunk group 60, the bi-directional tie trunk group to Session Manager that existed before adding the Verizon SIP Trunk configuration to the shared Avaya Interoperability lab network. Recall that this trunk is used for communication with other Avaya applications, such as Avaya Modular Messaging, and does not reflect any unique Verizon configuration.

change trunk-group 60		Page 1 of 21	
TRUNK GROUP			
Group Number: 60	Group Type: sip	CDR Reports: y	
Group Name: SM1	COR: 1	TN: 1	TAC: 160
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 60	
		Number of Members: 100	

The following shows **Page 3** for trunk group 60. Note that unlike the trunks associated with Verizon calls that use “public” numbering, this tie trunk group uses a “private” **Numbering Format**.

change trunk-group 60		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private		UUI Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			

The following shows **Page 4** for trunk group 60. Note that unlike the trunks associated with Verizon calls that have non-default “protocol variations”, this trunk group maintains all default

change trunk-group 60	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type:	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Enable Q-SIP? n	

Route pattern 68 will be used for calls destined for the PSTN via the Verizon IP Trunk Service. Digit manipulation can be performed on the called number, if needed, using the **No. Del Dgts** and **Inserted Digits** parameters. Digit manipulation can also be performed by Session Manager.

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

The “change public-unknown-numbering” command may be used to define the format of numbers sent to Verizon in SIP headers such as the “From” and “PAI” headers. In general, the mappings of internal extensions to Verizon DID numbers may be done in Session Manager (via Digit

Conversion in adaptations) or in Communication Manager (via public-unknown-numbering, and incoming call handling treatment for the inbound trunk group).

In the bolded rows shown in the example abridged output below, a specific Communication Manager extension (x30002) is mapped to a DID number that is known to Verizon for this SIP Trunk connection (7329450285), when the call uses trunk group 67 or 68. Alternatively, Communication Manager can send the extension to Session Manager by leaving the **CPN Prefix** field blank and setting the **CPN Len** to 5 (i.e., similar to the first row in the screen), and Session Manager can adapt the number to the Verizon DID. Both approaches were tested successfully.

change public-unknown-numbering 5					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	3	60		5	Total Administered: 3
5	556			5	Maximum Entries: 9999
5	30002	67-68	7329450285	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.

4.12. ARS Routing For Outbound Calls

Although not illustrated in these Application Notes, location-based routing may be configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns. Various example scenarios for a multi-location network with failover routing are provided in reference [PE]. In these Application Notes, the ARS “all locations” table directs ARS calls to specific SIP Trunks to Session Manager. Appropriate ARS entries can be added to match the various dial patterns (e.g., long distance, operator assist, x11 service numbers, etc.) to be sent to Verizon.

The following screen shows a sample specific ARS configuration for a number that will be dialed in the Verification section of these Application Notes. If a user dials the ARS access code followed by 1-908-848-5704, the call will select route pattern 68. Of course, matching of the dialed string need not be this specific.

change ars analysis 19088485704							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
19088485704	11	11	68	hnpa		n	

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

list ars route-chosen 19088485704						
ARS ROUTE CHOSEN REPORT						
Location: 1			Partitioned Group Number: 1			
Dialed	Total		Route	Call	Node	
String	Min	Max	Pattern	Type	Number	Location
19088485704	11	11	68	hnpa		all

4.13. Incoming Call Handling Treatment for Incoming Calls

In general, the “incoming call handling treatment” for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Avaya Aura™ Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Verizon is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of DID number 7329450285 to extension 30002. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were tested successfully.

change inc-call-handling-trmt trunk-group 67				Page	1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del Insert		
Feature	Len	Digits			
public-ntwrk	10	7329450285	all 30002		

4.14. Modular Messaging Hunt Group

Although not specifically related to Verizon, this section shows the hunt group used for access to Avaya Modular Messaging. In the sample configuration, users with voice mail have a coverage path containing hunt group 60. Users can dial extension 33000 to reach Modular Messaging (e.g., for message retrieval). The following screen shows **Page 1** of hunt-group 60.

display hunt-group 60		Page 1 of 60	
HUNT GROUP			
Group Number: 60		ACD? n	
Group Name: MM Coverage		Queue? n	
Group Extension: 33000		Vector? n	
Group Type: ucd-mia		Coverage Path:	
TN: 1		Night Service Destination:	
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display: mbr-name			

The following screen shows **Page 2** of hunt-group 60, which routes to the AAR access code 8 and **Voice Mail Number 33000**.

display hunt-group 60			Page 2 of 60
HUNT GROUP			
Message Center: sip-adjunct			
Voice Mail Number	Voice Mail Handle	Routing Digits	
		(e.g., AAR/ARS Access Code)	
33000	33000	8	

4.15. AAR Routing to Modular Messaging via Session Manager

Although not specifically related to Verizon, this section shows a portion of the AAR routing for the number used in the hunt group in the previous section. The bold row shows that calls to the number range 33xxx, which includes the Modular Messaging hunt group 33000, will use **Route Pattern 60**. As can be observed from the other rows, various other dial strings also route to other internal destinations (i.e., not to Verizon) via route pattern 60.

change aar analysis 0						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 0	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
300	5	5	60	unku		n	
301	5	5	60	unku		n	
305	5	5	60	unku		n	
3100	5	5	60	unku		n	
32	5	5	60	unku		n	
33	5	5	60	unku		n	
3400	5	5	60	unku		n	

4.16. Uniform Dial Plan (UDP) Configuration

Although not specifically related to Verizon, this section shows a portion of the UDP configuration, with the bold row showing the calls of the form 33xxx will be routed via AAR.

change uniform-dialplan 3					Page 1 of 2		
UNIFORM DIAL PLAN TABLE							
					Percent Full: 0		
Matching Pattern	Len	Del	Insert Digits	Node Net Conv	Num		
33	5	0		aar n			
3400	5	0		aar n			

4.17. Route Pattern for Internal Calls via Session Manager

Although not specifically related to Verizon, this section shows the AAR routing for the number used in the hunt group for Modular Messaging. Route pattern 60 contains trunk group 60, the tie “private” trunk group to Session Manager.

change route-pattern 60													Page 1 of 3								
Pattern Number: 60													Pattern Name: SM FS								
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:	60	0					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				none				
2:	y	y	y	y	y	n	n						rest				none				
3:	y	y	y	y	y	n	n						rest				none				
4:	y	y	y	y	y	n	n						rest				none				
5:	y	y	y	y	y	n	n						rest				none				
6:	v	v	v	v	v	n	n						rest				none				

4.18. Private Numbering

Although not specifically related to Verizon, this section shows the private numbering configuration associated with the calls using trunk group 60. The bold row configures any five digit number beginning with 3 (i.e., 3xxxx) that uses trunk group 60 to retain the original 5 digit number (i.e., no digit manipulation is specified, and the **Total Len** is 5).

change private-numbering 0										Page 1 of 2		
NUMBERING - PRIVATE FORMAT												
Ext	Ext		Trk		Private		Total					
Len	Code		Grp(s)		Prefix		Len					
5	2						5			Total Administered:	5	
5	3		60				5			Maximum Entries:	540	
5	4						5					
5	5						5					

4.19. Avaya Aura™ Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 3xxxx. The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone. Coverage path 60 is assigned to give this user coverage to Avaya Modular Messaging.

change station 30002															Page 1 of 5		
STATION																	
Extension: 30002																	
Type: 9620																	
Port: S00038																	
Name: Joey Votto																	
Lock Messages? n															BCC: 0		
Security Code: *															TN: 1		
Coverage Path 1: 60															COR: 1		
Coverage Path 2:															COS: 1		
Hunt-to Station:																	
STATION OPTIONS																	
Loss Group: 19																	
Speakerphone: 2-way																	
Time of Day Lock Table:																	
Personalized Ringing Pattern: 1																	
Message Lamp Ext: 30002																	
Mute Button Enabled? y																	

On **Page 2**, the **MWI Served User Type** is set to “sip-adjunct” for the SIP integration to Avaya Modular Messaging.

change station 30002		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer:	
none		
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type: sip-adjunct	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 30002	Always Use? n IP Audio Hairpinning? n	

4.20. Coverage Path

This section illustrates an example coverage path for a station with a mailbox on Avaya Modular Messaging. Hunt group 60, the hunt group to Modular Messaging, is **Point1** in coverage path 60.

change coverage path 60		Page 1 of 1
COVERAGE PATH		
Coverage Path Number: 60		
Cvg Enabled for VDN Route-To Party? y	Hunt after Coverage? n	
Next Path Number:	Linkage	
COVERAGE CRITERIA		
Station/Group Status	Inside Call	Outside Call
Active?	n	n
Busy?	y	y
Don't Answer?	y	y
All?	n	n
DND/SAC/Goto Cover?	y	y
Holiday Coverage?	n	n
COVERAGE POINTS		
Terminate to Coverage Pts. with Bridged Appearances? n		
Point1: h60	Rng: Point2:	
Point3:	Point4:	
Point5:	Point6:	

4.21. EC500 Configuration for Diversion Header Testing

When EC500 is enabled on the Avaya Aura™ Communication Manager station, a call to that station will generate a new outbound call from Avaya Aura™ Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 30002. Use the command **change off-pbx-telephone station mapping x** where x is the Communication Manager station (e.g. **30002**).

- **Station Extension** – This field will automatically populate
- **Application** – Enter **EC500**
- **Dial Prefix** – Enter a prefix (e.g., 1) if required by the routing configuration
- **Phone Number** – Enter the phone that will also be called (e.g., **7326870755**)
- **Trunk Selection** – Enter **ARS**. This means ARS will be used to determine how Communication Manager will route to the **Phone Number** destination.
- **Config Set** – Enter **1**
- Other parameters can retain default values

change off-pbx-telephone station-mapping 30002							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual
Extension		Prefix			Selection	Set	Mode
30002	EC500	1	-	7326870755	ars	1	

4.22. Saving Communication Manager Configuration Changes

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

5. Configure Avaya Aura™ Session Manager Release 6

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

Note – The following sections assume that Avaya Aura™ Session Manager and Avaya Aura™ System Manager have been installed and that network connectivity exists between the two. For more information on Avaya Aura™ Session Manager see [3].

Session Manager is managed via Avaya Aura™ System Manager. Using a web browser, access “https://<ip-addr of System Manager>/SMGR”. In the **Log On** screen, enter appropriate **Username** and **Password** and press the **Log On** button (not shown).



Avaya Aura™ System Manager 6.0

[Home](#) / [Log On](#)

Log On

Username :

Password :

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



Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at April 29, 2010 5:07 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

- Elements
- Events
- Groups & Roles
- Licenses
- Routing
- Security
- System Manager Data
- Users

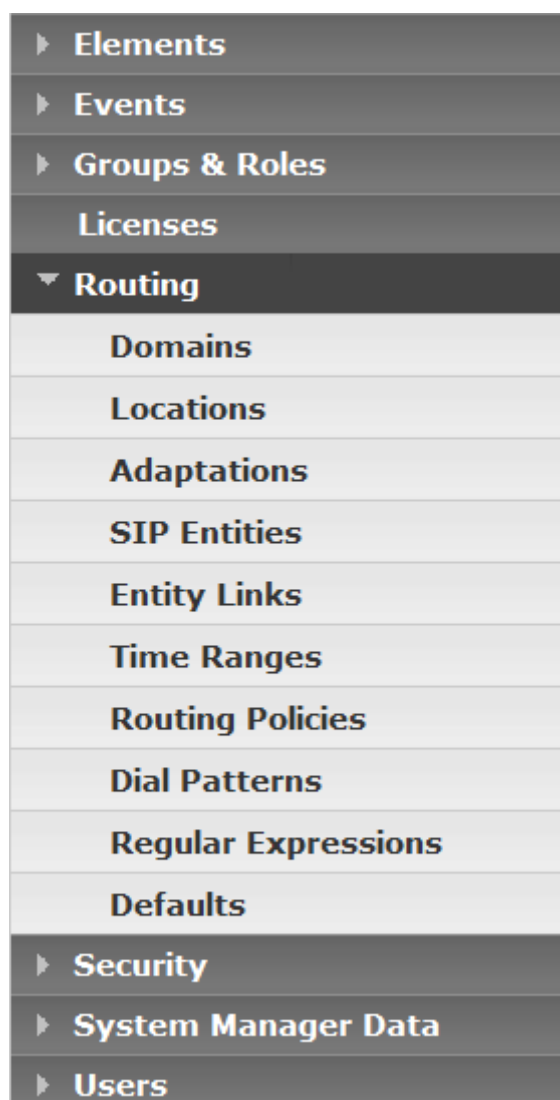
Help

Home Screen

Sub Pages

Action	Description	Help
Elements	This section provides various functionality related to elements. Some functionality is implemented by SMGR generic services and some are provided by product specific element managers.	Help for RTS
Events	Event Management section of the System Manager Console. This part of SMGR lets you view and administer logs and alarms related to the individual domains of SMGR.	Help to manage events like logs and alarms
Groups & Roles	Groups and Roles administration section of System Manager Console. This part of SMGR lets you create and manage groups , roles and permissions.	Help to manage groups and roles
Licenses	Licence Administration section of the system Manager Console. This part of SMGR lets you view and administer licenses.	Help to administer

For readers familiar with prior releases of Session Manager, the configurable items under **Routing** in Release 6 were located under a heading called **Network Routing Policy** in prior releases. Select **Routing**. The screen shown below shows the various sub-headings.



When Routing is selected, the right side 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 (NRP)** 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"

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

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

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

5.1. Domains

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

The following screen shows the list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among many Avaya interoperability test efforts. The domain “avaya.com” was already being used for communication among a number of Avaya systems and applications, including an Avaya Modular Messaging system with SIP integration to Session Manager. The domain “avaya.com” is not known to the Verizon production service.

Domain Management

EditNewDuplicateDeleteMore Actions ▾

5 Items | RefreshFilter: Enable

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avaya.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Trunk Test
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	avocs.contoso.com	sip	<input type="checkbox"/>	Microsoft OCS Test Environment
<input type="checkbox"/>	contosomed1.avocs.contoso.com	sip	<input type="checkbox"/>	Mediation server inserts this
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk

Select : All, None

The domain “adevc.avaya.globalipcom.com” is the domain known to Verizon as the enterprise SIP domain. For example, for calls from the enterprise site to Verizon, this domain can appear in the P-Asserted-Identity in the INVITE message sent to Verizon.

Home / Routing / Domains

▸ Elements

▸ Events

▸ Groups & Roles

Licenses

▼ Routing

Domains

Locations

Adaptations

Domain Management

CommitCancel

1 Item | RefreshFilter: Enable

Name	Type	Default	Notes
* adevc.avaya.globalipcom.com	sip ▾	<input type="checkbox"/>	CPE domain for Verizon Trunk Test

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

> Elements
> Events
> Groups & Roles
Licenses
▼ Routing
Domains
Locations
Adaptations

Domain Management

Commit Cancel

1 Item | Refresh Filter: Enable

Name	Type	Default	Notes
* pcelban0001.avayalincroft.globalipcom.	slip	<input type="checkbox"/>	Verizon network domain for IP Trunk

5.2. Locations

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

Location

Edit New Duplicate Delete More Actions ▼ Commit

13 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	AC-BR2	Branch 2 for AudioCodes MP-118
<input type="checkbox"/>	Acme1	Net-Net SD1 Inside
<input type="checkbox"/>	Acme2	Net-Net SD2 Inside
<input type="checkbox"/>	adevc	Inside network used for VZ test
<input type="checkbox"/>	Aura-SBC	Location for Avaya Aura SBC
<input type="checkbox"/>	BaskingRidge_HQ	Fred's ACM & ASM's

The following screen shows the location details for the location named “Aura-SBC”, corresponding to the Avaya Aura™ Session Border Controller. Later, the location with name “Aura-SBC” will be assigned to the corresponding SIP Entity. The IP Address 65.206.67.93 of the inside (private) interface of the SBC is entered in the **IP Address Pattern** field.

Location Details

CommitCancel

General

* Name: Aura-SBC

Notes: Location for Avaya Aura SBC

Managed Bandwidth: Kbit/sec

* Average Bandwidth per Call: 80 Kbit/sec

Location Pattern

AddRemove

1 Item | Refresh

Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	* 65.206.67.93	Inside IP Address of Aura SBC

The following screen shows the location details for the location named “BaskingRidge HQ”. The SIP Entities and associated IP Addresses for this location correspond to the shared components of the Avaya Interoperability Lab test environment, such as Avaya Aura™ Communication Manager Release 6, Avaya Aura™ Session Manager Release 6, and Avaya Modular Messaging servers.

Location Details

[Commit](#)[Cancel](#)

General

* **Name:**

Notes:

Managed Bandwidth:

* **Average Bandwidth per Call:**

Location Pattern

[Add](#)[Remove](#)

4 Items | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* <input type="text" value="10.32.1.*"/>	<input type="text"/>
<input type="checkbox"/>	* <input type="text" value="10.32.2.*"/>	<input type="text"/>
<input type="checkbox"/>	* <input type="text" value="172.28.43.*"/>	<input type="text"/>
<input type="checkbox"/>	* <input type="text" value="10.1.2.*"/>	<input type="text"/>

5.3. Adaptations

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

The following screen shows a portion of the list of adaptations in the sample configuration.

Adaptations				
<div>EditNewDuplicateDeleteMore Actions ▼Commit</div>				
14 Items Refresh			Filter: Enable	
<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	Avaya-R6.0	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	Cisco-UCM6	CiscoAdapter avaya.com		
<input type="checkbox"/>	Cisco-UCM7	CiscoAdapter avaya.com		
<input type="checkbox"/>	CiscoUCME	CiscoAdapter avaya.com		
<input type="checkbox"/>	CM-ES Inbound	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	CM-ES-VZ Inbound	DigitConversionAdapter odstd=avaya.com		Avaya.com for shared SIL ntwk

After scrolling down, the following screen shows another portion of the list of adaptations in the sample configuration.

<input type="checkbox"/>	History_Diversion_IPT	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com
<input type="checkbox"/>	MM Normalized	DigitConversionAdapter avaya.com

The adapter named “History_Diversion_IPT” will later be assigned to the SIP Entity for the Avaya Aura™ SBC. This adaptation uses the “VerizonAdapter” and specifies two parameters that are used to adapt the FQDN to the domains expected by the Verizon network in the sample configuration.

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

For example, for outbound PSTN calls from the Avaya CPE to Verizon, the Request-URI header will contain “pcelban0001.avayalincroft.globalipcom.com” as expected by Verizon.

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domains in this fashion. In the sample configuration, where “avaya.com” was already in use in a shared Avaya environment, it was necessary for Session Manager to adapt the domain from “avaya.com” to “adevc.avaya.globalipcom.com” where the latter is the CPE domain known to Verizon.

The adapter named “CM-ES-VZ Inbound” will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls to and from Verizon. This adaptation uses the “DigitConversionAdapter” and specifies the “odstd=avaya.com” parameter to adapt the domain to the domain expected by Communication Manager in the sample configuration. More specifically, this configuration enables the destination domain to be overwritten with “avaya.com” for calls that egress to a SIP entity using this adapter. For example, for inbound PSTN calls from Verizon to the Avaya CPE, the Request-URI header sent to Communication Manager will contain “avaya.com” as expected by Communication Manager in the shared Avaya Interoperability Lab configuration. Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

Adaptation Details

CommitCancel

General

*** Adaptation name:**

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Scrolling down, the following screen shows a portion of the CM-ES-VZ Inbound adapter that can be used to convert digits between the extension numbers used on Communication Manager and the 10 digit DID numbers assigned by Verizon. Since this adapter will be assigned to the SIP Entity receiving calls from Communication Manager for routing to the PSTN, the settings for “incoming calls to SM” correspond with outgoing calls from Communication Manager to the PSTN using the Verizon IP Trunk Service. Similarly, the settings for “outgoing calls from SM” correspond to incoming calls from the PSTN to Communication Manager. In general, digit conversion such as this, that converts a Communication Manager extension (e.g., 30002) to a corresponding LDN or DID number known to the PSTN (e.g., 7329450285), can be performed in Communication Manager (e.g., using “public unknown numbering” and “incoming call handling treatment” for the Communication Manager trunk group) or in Session Manager as shown below.

Digit Conversion for Incoming Calls to SM

Add
Remove

1 Item | Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 30002	* 5	* 5	* 5	7329450285	both ▼	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add
Remove

6 Items | Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7329450285	* 10	* 10	* 10	30002	both ▼	

In the example shown above, if a user on the PSTN dials 732-945-0285, Session Manager will convert the number to 30002 before sending the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, if extension 30002 dials the PSTN, and if Communication Manager sends the extension 30002 to Session Manager as the calling number, Session Manager would convert the calling number to 7329450285. Alternatively, the Communication Manager public-unknown numbering form could have an entry to convert 30002 to 7329450285 before sending the call on the trunk group to Session Manager. Both methods were verified successfully in the testing associated with these Application Notes.

5.4. SIP Entities

To view or change SIP elements, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an element and **Edit** to edit an existing element, or the **New** button to add an element. Click the **Commit** button after changes are completed.

The following screen shows a portion of the list of configured SIP entities. In this screen, the SIP Elements named “AuraSBC”, “alpinemas1”, “CM-Evolution-procr-5062”, and “CM-Evolution-Server” are relevant to these Application Notes.

SIP Entities

Edit

New

Duplicate

Delete

More Actions ▾











Commit

27 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	Acme1		65.206.67.1	Other	Inside IP Acme1
<input type="checkbox"/>	Acme2		65.206.67.21	Other	Acme2 Inside
<input type="checkbox"/>	AllanC-S8300-G350		10.32.2.80	CM	For Survivability Test
<input type="checkbox"/>	alpinemas1		135.8.139.31	Modular Messaging	For use by Tony M's group
<input type="checkbox"/>	AudioCodes M1000		m1000.avaya.com	Other	QSIG/SIP GW for CS1000
<input type="checkbox"/>	AuraSBC		65.206.67.93	Other	Avaya Aura SBC Inside IP
<input type="checkbox"/>	BR2 AudioCodes MP114		192.168.75.110	Other	SIP Media Gateway
<input type="checkbox"/>	BR2 AudioCodes MP118		192.168.75.100	Other	SIP Media Gateway
<input type="checkbox"/>	CallCenter		10.1.2.233	CM	To Interop CUCME
<input type="checkbox"/>	Cisco-UCM6		60.1.1.9	Other	
<input type="checkbox"/>	Cisco-UCM7		172.29.5.20	Other	
<input type="checkbox"/>	CiscoUCME		192.45.131.1	Other	
<input type="checkbox"/>	CM-Evolution-procr-5062		10.1.2.90	CM	CM-ES procr IP, different port
<input type="checkbox"/>	CM-Evolution-procr-5065		10.1.2.90	CM	CM-ES procr IP, different port
<input type="checkbox"/>	CM Evolution Server		10.1.2.90	CM	

The following screen shows Page 2 of the list of SIP Entities. In this screen, only the SIP Entity named “SM1” (corresponding to Avaya Aura™ Session Manager) is relevant to these Application Notes.

<input type="checkbox"/>	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	Denver Nortel CS1000e		CS1KGateway.avaya.com	Other	
<input type="checkbox"/>	Juniper-SRX240		1.0.0.2	Other	
<input type="checkbox"/>	Microsoft-OCS-Mediation-Server		135.8.19.139	SIP Trunk	MS OCS Mediation Server in WM
<input type="checkbox"/>	MikeH-S8300-G450		10.32.2.20	CM	For Survivability Test
<input type="checkbox"/>	OITT Test Tool		135.8.19.109	Other	OITT Test Tool
<input type="checkbox"/>	RobertIP500		10.1.2.190	SIP Trunk	Robert's IP500
<input type="checkbox"/>	S8300-G250-JRWB		172.28.40.5	CM	S8300-in-G250 at JRR workbench
<input type="checkbox"/>	S8300-G450-BR1		135.8.139.118	CM	S8300 is an LSP
<input type="checkbox"/>	S87x0-Procr-CM521-VZ		65.206.67.3	CM	CM 5.2.1 Verizon Testbed
<input type="checkbox"/>	SM1		10.1.2.70	Session Manager	

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “SM1”. The **FQDN or IP Address** field for “SM1” is the Avaya Aura™ Session Manager Security Module IP Address (10.1.2.70), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is “Session Manager”. Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location “BaskingRidge HQ”. The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.

SIP Entity Details

Commit

Cancel

General

* Name:

SM1

* FQDN or IP Address:

10.1.2.70

Type:

Session Manager

Notes:

Location:

BaskingRidge HQ

Outbound Proxy:

Time Zone:

America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for “SM1”. The links relevant to these Application Notes are described in the following section.

Entity Links

Add

Remove

27 Items Refresh				Filter: Enable		
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM1	TCP	* 5060	Acme1	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	Acme2	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	AuraSBC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	CallCenter	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	Cisco-UCM6	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	Cisco-UCM7	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	CiscoUCME	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	CM Evolution Server	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5062	CM-Evolution-procr-5062	* 5062	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	Denver Nortel CS1000e	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM1	TCP	* 5060	alpinemas1	* 5060	<input checked="" type="checkbox"/>

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, a listing of the configured ports for “SM1”. In the sample configuration, TCP port 5060 was already in place for the shared test environment, using **Default Domain** “avaya.com”. To enable Communication Manager to distinguish inbound calls from Verizon from other types of SIP calls arriving from the same Session Manager, TCP port 5062 was added, with default domain “adevc.avaya.globalipcom.com”. Click the **Add** button to configure a new port. TCP is used in the sample configuration for improved visibility during testing; TLS may be used in production.

Port

Add

Remove

5 Items Refresh				Filter: Enable	
<input type="checkbox"/>	Port	Protocol	Default Domain	Notes	
<input type="checkbox"/>	5060	TCP	avaya.com		
<input type="checkbox"/>	5060	UDP	avaya.com		
<input type="checkbox"/>	5061	TLS	avaya.com		
<input type="checkbox"/>	5062	TCP	adevc.avaya.globalipcom.com	Verizon testing CPE-domain	
<input type="checkbox"/>	5070	TCP	avocs.contoso.com		

The following screen shows the **SIP Entity Details** corresponding to the SIP Entity with the **Name** “AuraSBC”. The **FQDN or IP Address** field is configured with the Avaya Aura™ SBC inside IP Address (65.206.67.93). “Other” is selected from the **Type** drop-down menu for SBC SIP Entities. The SBC has been assigned to **Location** “Aura-SBC” shown in Section 5.2, and the “History_Diversion_IPT” adapter shown in Section 5.3 is applied. This adaptation uses the “VerizonAdapter”.

SIP Entity Details

Commit

Cancel

General

* **Name:** AuraSBC

* **FQDN or IP Address:** 65.206.67.93

Type: Other

Notes: Avaya Aura SBC Inside IP

Adaptation: History_Diversion_IPT

Location: Aura-SBC

Time Zone: America/New_York

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 a portion of the **SIP Entity Details** corresponding to an Avaya Aura™ Communication Manager SIP Entity named “CM Evolution Server” This is the SIP Entity that was already in place in the shared Avaya Interoperability Lab test environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP Address of the “processor ethernet” (10.1.2.90). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the “processor ethernet”. “CM” is selected from the **Type** drop-down menu. In the shared test environment, the **Adaptation** “CM-ES Inbound” and **Location** “BaskingRidge HQ” had already been assigned to the Communication Manager SIP entity.

SIP Entity Details

Commit

Cancel

General

* Name: CM Evolution Server

* FQDN or IP Address: 10.1.2.90

Type: CM

Notes:

Adaptation: CM-ES Inbound

Location: BaskingRidge HQ

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

The following screen shows the **SIP Entity Details** for an entity named “CM-Evolution-procr-5062”. This entity uses the same **FQDN or IP Address** (10.1.2.90) as the prior entity with name “CM Evolution Server”; both correspond to the S8800 Processor Ethernet. Later, a unique port, 5062, will be used for the Entity Link to “CM-Evolution-procr-5062”. Using a different port is one approach that will allow Avaya Aura™ Communication Manager to distinguish traffic originally from Verizon from other SIP traffic arriving from the same IP Address of the Avaya Aura™ Session Manager. The adapter “CM-ES-VZ Inbound” is applied to this SIP entity. Recall that this adapter will be used to adapt the domain as well as map the Verizon 10 digit DID numbers to the corresponding Communication Manager extensions. If desired, a location can be assigned if location-based routing criteria will be used. In the sample configuration, no location was assigned to this entity, and “all locations” routing was used for outbound calls to Verizon.

SIP Entity Details

Commit

Cancel

General

* Name: CM-Evolution-procr-5062

* FQDN or IP Address: 10.1.2.90

Type: CM

Notes: CM-ES procr IP, different port

Adaptation: CM-ES-VZ Inbound

Location:

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

5.5. Entity Links

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

The following screen shows a partial list of configured links. In the screen below, the links named “AuraSBC”, “CM-ES-VZ-5062”, and “CM Evolution Server” are relevant to these Application Notes. Each of the links uses the entity named “SM1” as **SIP Entity 1**, and the appropriate entity, such as “AuraSBC” for **SIP Entity 2**. Note that there are two SIP Entity Links, using different TCP ports, linking the same SM1 with the processor Ethernet of Avaya Aura™ Communication Manager. For one link, named “CM Evolution Server”, both entities use port 5060. For the other, named “CM-ES-VZ-5062”, both entities use port 5062.

Entity Links

Edit

New

Duplicate

Delete

More Actions ▾

Commit

27 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	Acme1	SM1	TCP	5060	Acme1	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	Acme2	SM1	TCP	5060	Acme2	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	AuraSBC	SM1	TCP	5060	AuraSBC	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	Call Center	SM1	TCP	5060	CallCenter	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	Cisco-UCM6	SM1	TCP	5060	Cisco-UCM6	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	Cisco-UCM7	SM1	TCP	5060	Cisco-UCM7	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	CiscoUCME-Link	SM1	TCP	5060	CiscoUCME	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	CM-ES-VZ-5062	SM1	TCP	5062	CM-Evolution-procr-5062	5062	<input checked="" type="checkbox"/>	<div>Same IP, diff port</div>
<input type="checkbox"/>	CM Evolution Server	SM1	TCP	5060	CM Evolution Server	5060	<input checked="" type="checkbox"/>	————
<input type="checkbox"/>	Denver CS1000e	SM1	TCP	5060	Denver Nortel CS1000e	5060	<input checked="" type="checkbox"/>	————

The link named “CM Evolution Server” links Session Manager “SM1” with the Communication Manager processor Ethernet. This link existed in the shared configuration prior to adding the Verizon IP Trunk-related configuration. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with

Verizon, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Avaya Modular Messaging, which has SIP integration to Session Manager.

The link named “CM-ES-VZ-5062” also links Session Manager “SM1” with the Communication Manager processor Ethernet. However, this link uses port 5062 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired. For example, in a configuration using G650 Media Gateways, the use of one or more TN799DP C-LAN interface cards can provide additional Communication Manager SIP Signaling alternatives.

5.6. Time Ranges

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

Time Ranges

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

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7
<input type="checkbox"/>	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	
<input type="checkbox"/>	Off-Hours	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	18:00	23:59	for testing

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

5.7. Routing Policies

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

The following screen shows the **Routing Policy Details** for the policy named “CM-ES-R6-VZ-Inbound” associated with incoming PSTN calls from Verizon to Communication Manager, using the Avaya S8800 PE. Observe the **SIP Entity as Destination** is the entity named “CM-Evolution-procr-5062”.

Routing Policy Details

[Commit](#)[Cancel](#)

General

* **Name:**

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
CM-Evolution-procr-5062	10.1.2.90	CM	CM-ES procr IP, different port

Time of Day

[Add](#)[Remove](#)[View Gaps/Overlaps](#)

1 Item Refresh										Filter: Enable		
<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	<input type="text" value="0"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Ran 24/7

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

Routing Policy Details

Commit

Cancel

General

* Name: To-Aura-SBC

Disabled: ☐

Notes: Avaya Aura SBC for Verizon test

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AuraSBC	65.206.67.93	Other	Avaya Aura SBC Inside IP

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh											Filter: Enable	
<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Ran 24/7

5.8. Dial Patterns

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

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Verizon IP Trunk service, such as 732-945-0285, Verizon delivers the number to the enterprise, and the Avaya Aura™ SBC sends the call to Session Manager. The pattern below matches on 732-945-0285 specifically. Dial patterns can alternatively match on ranges of numbers (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named “CM-ES-R6-VZ-Inbound” is selected, which sends the call to Communication Manager using port 5062 as described previously. In the Avaya Interoperability Lab configuration, calls to this number from any of three originating locations, including the one with **Originating Location Name** “Aura-SBC” defined in Section 5.2, are routed to Communication Manager.

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add		Remove					
3 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	R P N
<input type="checkbox"/>	Acme1	Net-Net SD1 Inside	CM-ES-R6-VZ-Inbound	0	<input type="checkbox"/>	CM-Evolution-procr-5062	In V to C
<input type="checkbox"/>	Acme2	Net-Net SD2 Inside	CM-ES-R6-VZ-Inbound	0	<input type="checkbox"/>	CM-Evolution-procr-5062	In V to C
<input type="checkbox"/>	Aura-SBC	Location for Avaya Aura SBC	CM-ES-R6-VZ-Inbound	0	<input type="checkbox"/>	CM-Evolution-procr-5062	In V to C

The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 9-1-908-848-5704, Communication Manager sends the call to Session Manager, via the S8800 PE. Session Manager will match the dial pattern shown below and send the call to the Avaya Aura™ SBC via the **Routing Policy Name** “To-Aura-SBC”.

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	R P N
<input type="checkbox"/>	-ALL-	Any Locations	To-Aura-SBC	0	<input type="checkbox"/>	AuraSBC	Av Au fo Ve te

Select : All, None

6. Configure Avaya Aura™ Session Border Controller (SBC)

This section illustrates an example configuration of the Avaya Aura™ SBC. Similar to Avaya Aura™ Communication Manager Release 6, the Avaya Aura™ SBC runs on its own S8800 Server as an application template using Avaya Aura™ System Platform. The installation of the System Platform is assumed to have been previously completed.

The Avaya Aura™ SBC includes a configuration wizard that can be used as part of the installation of the SBC template on System Platform. As such, screens from the installation of the SBC template are presented in Section 6.1. The wizard pre-configures the underlying SBC for much of the required provisioning. After the Avaya Aura™ SBC has been installed as shown in Section 6.1, any subsequent changes to the network configuration (e.g., IP address, network mask,

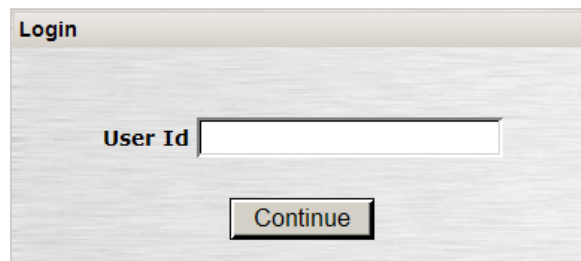
hostname) for the Avaya Aura™ SBC eth0 or eth2 interfaces must be done via the System Platform webconsole Network Configuration page. Any backup and restore actions should also use System Platform. Configuration of SBC behaviors (e.g., header manipulations) can be performed through the element manager GUI as shown in Section 6.3.

Although licensing tasks are not typically covered in Application Notes and this document does not aim to be an authoritative guide to licensing, example screens and procedures for the licensing of the Avaya Aura™ SBC used for the verification testing are provided in Section 6.2.

In the sample configuration, the Avaya S8800 Server has four physical network interfaces, labeled 1 through 4. The port labeled “1” (virtual “eth0”) is used for the management and private (inside) network interface of the SBC. The port labeled “4” (virtual “eth2”) is used for the public (outside) network interface of the SBC.


6.1. Avaya Aura™ SBC Installation

To begin the SBC Template installation, log in to the System Platform console domain by entering `https://<ip-addr>/webconsole` as shown in the example screen below. In the sample configuration, the console domain uses the IP Address 65.206.67.92, and the system domain uses the IP Address 65.206.67.91. Enter an appropriate **User Id** and press the **Continue** button.



Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

On the subsequent screen, enter the appropriate **Password** and click the **Log On** button.

Address  https://65.206.67.92/webconsole/vslogin.action;jsessionid=79110794C38D3743B518C9F04DC34E85

AVAYA

Avaya Aura™

Login

User Id

Password

Reset

Log On

The following screen shows the left-hand side System Platform menu.



The following screen shows the right-hand side, showing the System Domain "Domain-0" and the Console Domain "cdom" in the sample configuration.

Avaya Aura™ System Platform
 admin
 Previous successful login: Mon Jun 07 14:44:43 EDT 2010
 Failed login attempts since: 0
 Failover status: [Not configured](#)
[About](#) | [Help](#) | [Log Out](#)

Virtual Machine Management

[Virtual Machine List](#)

System Domain Uptime: 23 days, 17 hours, 30 minutes, 31 seconds

Current template installed: No Template Installed [Refresh](#)

Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓ Domain-0	6.0.0.0.11	65.206.67.91	512.0 MB	8	1d 3h 59m 52s	Running	N/A
✓ cdom	6.0.0.0.11	65.206.67.92	1024.0 MB	1	11h 41m 52s	Running	N/A

From the left menu, select **Virtual Machine Management** → **Solution Template**. In the **Install Template From** area, choose where the template files are located. In the sample configuration, the template files were copied to the System Platform server /vsp-template/ directory prior to installation, but USB or other means may be used. Click **Search**.

Virtual Machine Management

[Search Local and Remote Template](#)

Current template installed: No Template Installed

Install Template From

Avaya Downloads (PLDS)
 HTTP
SP Server
 SP CD/DVD
 SP USB Disk

Template Location:

[Search](#)



Select the appropriate file, such as “SBCT.ovf”. Click the **Select** button.

Virtual Machine Management

Select Template

Current template installed: No Template Installed

Select Template From /vsp-template/

Select Template  /vsp-template/
 **SBCT.ovf**

In the resultant screen shown below, the **Selected Template** can be observed. If an EPW file is available, it may be uploaded and used. In the sample configuration, the **Continue without EPF file** button was used.

Virtual Machine Management

Select Template

Current template installed: No Template Installed

Select EPW File

Selected Template

EPW file may be used for this template.

The **Template Details** screen is presented. If satisfied that the information is correct, click the **Install** button.

Virtual Machine Management

Template Details

Current template installed: No Template Installed

Product ID: SBCT
Product Vendor: Avaya
Product Version: 6.0.0.1.4

Virtual Machines:

sbc

Product ID: sbc
Product Vendor: Avaya
Product Version: E36M2

Install

Cancel

After clicking the Install button, the screen will update similar to the following, showing “Processing your request, please wait”

Virtual Machine Management

Template Details

Current template installed: No Template Installed

Processing your request, please wait..... ▼

Product ID: SBCT
Product Vendor: Avaya
Product Version: 6.0.0.1.4

Virtual Machines:

sbc

Product ID: sbc
Product Vendor: Avaya
Product Version: E36M2

Install

Cancel

The installation will proceed until user input is expected, as shown below.

Virtual Machine Management

Template Installation

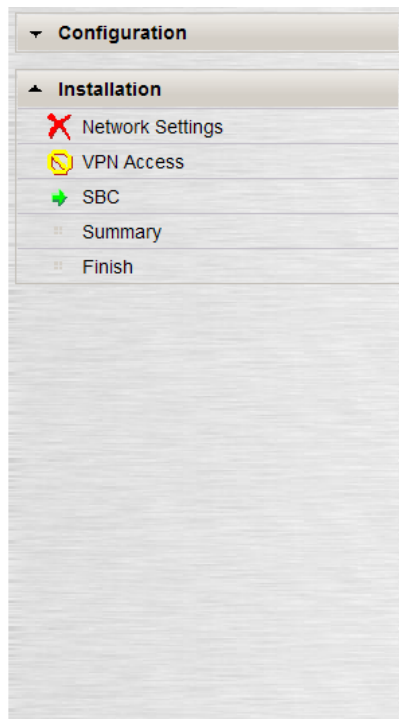
Cancel Installation

Template Installation In Progress

Workflow Status						
Start Time	Task Description	State	% Complete	Estimate	Actual	
09:39:42	Download disk image for sbc	Complete	100		37s	✓
09:39:42	Download plugins for VMs	Complete	100		2s	✓
09:39:45	Check Template for Web Application	Complete	100		14s	✓
09:40:00	Download pre-install web application	Complete	100		0s	✓
09:40:00	Pre-Install Web Application Deployment	Complete	100		7s	✓
09:40:07	Wait For User To Complete Data Entry	In Progress	0			<div><div></div></div>

The following shows the first screen in a series of Installation screens, beginning with **Network Settings**. In the top portion of the screen, the System Domain **Domain-0 IP Address**, Console Domain **CDom IP Address**, **Gateway IP Address**, and **Network Mask** are pre-populated with information from System Platform. In the sample configuration, no DNS was entered during the System Platform installation. The Avaya Aura™ SBC Installation requires that the Primary DNS be populated, even if a DNS is not really used. In the screen below, the Primary DNS is configured to be the same address as the Console Domain.

In the bottom portion of the screen, the **IP Address** and **Hostname** of the Avaya Aura™ SBC are configured. The IP Address 65.206.67.93 becomes the private, inside IP Address as well as the management address for the Avaya Aura™ SBC.



Network Settings

Enter network settings

Domain-0 IP Address	<input type="text" value="65.206.67.91"/>
CDom IP Address	<input type="text" value="65.206.67.92"/>
Gateway IP Address	<input type="text" value="65.206.67.254"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Primary DNS	<input type="text" value="65.206.67.92"/>
Secondary DNS	<input type="text"/>
HTTPS Proxy (if required) [IP Address:Port Number]	<input type="text"/>

Virtual Machine	IP Address	Hostname
SBC	<input type="text" value="65.206.67.93"/>	<input type="text" value="AuraSBC"/>

Scroll down if necessary, and click **Next Step**.

Virtual Machine	IP Address	Hostname
SBC	65.206.67.93	AvayaSBC

[Next Step](#) 

The resulting screen allows VPN Access parameters to be configured. Configure as appropriate, or skip, and click **Next Step**.

VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

☐ Yes ☒ No

VPN Access Configuration

VPN Router IP Address

Remote Access Network

Remote Access Network Subnet Mask

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

 [Previous Step](#)

[Next Step](#) 

The following screen shows the **Session Border Controller Data** configuration screen.

In the upper portion of the screen with heading **SIP Service Provider Data**, select “Verizon” from the **Service Provider** drop-down menu. The **IP Address** and **Port** fields are configured with the Verizon supplied IP Address (172.30.209.21) and port (5071) for the service as shown in **Figure 1**. If it is desired to use DNS to the Verizon network DNS server, the IP Address and port can still be specified here. Use of DNS on the public interface to Verizon can be configured later using the procedures shown in **Appendix 1**. The **Media Network** and **Media Netmask** fields are configured with the appropriate network routing information for the subnet. In the sample configuration, Verizon media IP addresses (signaled in SDP) are on the 172.30.209.0/24 network with network mask 255.255.255.0.

In the middle portion of the screen with heading **SBC Network Data**, the **Public IP Address** of the Avaya Aura™ SBC known to the Verizon network is configured. As shown in **Figure 1**, Verizon will signal to IP Address 1.1.1.2. In the sample configuration, the **Gateway** for the public interface is 1.1.1.1. Note that the Private (Management) Interface information has already been completed with the IP Address (65.206.67.93) provided as the **Virtual Machine IP Address** on the first screen of the series.

In the lower portion of this screen with heading **Enterprise SIP Server**, the **IP Address** of the Avaya Aura™ Session Manager is configured. As shown in **Figure 1**, the Avaya Aura™ SBC will signal to the Avaya Aura™ Session Manager at **IP Address** 10.1.2.70. TCP Transport was selected in the sample configuration to facilitate tracing visibility. The **SIP Domain** is configured to “adevc.avaya.globalipcom.com” to match the Verizon configuration of the enterprise SIP domain.

SBC

Session Border Controller Data

SIP Service Provider Data				
Service Provider	IP Address	Port	Media Network	Media Netmask
Verizon	172.30.209.21	5071	172.30.209.0	255.255.255.0

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	65.206.67.93	255.255.255.0	65.206.67.254
Public	1.1.1.2	255.255.255.0	1.1.1.1

Enterprise SIP Server		
IP Address	Transport	SIP Domain
10.1.2.70	TCP	adevc.avaya.glob

 [Previous Step](#)

[Next Step](#) 

Once complete, click **Next Step**. A summary screen will be presented. The lower portion of the summary screen for the sample configuration is shown below.

Virtual Machine	IP Address	Hostname
SBC	65.206.67.93	AuraSBC

VPN Access	
VPN Access	Not Configured

SBC	
Service Provider	vzb
Service Provider IP Address	172.30.209.21
Service Provider Port	5071
Service Provider Media Network	172.30.209.0
Service Provider Media Netmask	255.255.255.0
Public IP Address	1.1.1.2
Public Netmask	255.255.255.0
Public Gateway	1.1.1.1
Enterprise SIP Server IP	10.1.2.70
Enterprise SIP Server Domain	adevc.avaya.globalipcom.com
Enterprise SIP Server Transport	TCP

A **Confirm Installation** screen is presented. After reading and heeding the Warning, click the **Accept** button if satisfied.

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook, 555-025-600*.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

Accept

Install

After clicking **Accept**, the screen is updated, and the **Install** button may be clicked to proceed.

The following required fields have not been set, these must be completed before installing

The following optional fields have not been set

[Secondary DNS](#)

[HTTPS Proxy](#)

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook, 555-025-600*.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

Accept

Install

The Virtual Machine Management window, which had previously been at the “Wait for User to Complete Data Entry” step, has now continued, as shown in the abridged screen below.

Virtual Machine Management

Template Installation

Cancel Installation

Template Installation In Progress

Workflow Status						
Start Time	Task Description	State	% Complete	Estimate	Actual	
09:39:42	Download disk image for sbc	Complete	100		37s	✓
09:39:42	Download plugins for VMs	Complete	100		2s	✓
09:39:45	Check Template for Web Application	Complete	100		14s	✓
09:40:00	Download pre-install web application	Complete	100		0s	✓
09:40:00	Pre-Install Web Application Deployment	Complete	100		7s	✓
09:40:07	Wait For User To Complete Data Entry	Complete	100		26m 25s	✓
10:06:33	Undeploy Web Application	Complete	100		0s	✓

Wait for the “Finalize Installation” task to reach the “Complete” State, as shown below. This same information is available via the **View Install/Upgrade Log** link on the left (not shown).

09:40:07	Wait For User To Complete Data Entry	Complete	100	26m 25s	✓
10:06:33	Undeploy Web Application	Complete	100	0s	✓
10:06:34	Process EPW properties file if present	Complete	100	19s	✓
10:06:54	Configure Network	Complete	100	4s	✓
10:06:58	Install plugins	Complete	100	1s	✓
10:07:00	Install sbc	Complete	100	8m 11s	✓
10:15:11	Restart network	Complete	100	23s	✓
10:15:35	Start all VMs	Complete	100	13s	✓
10:15:49	Wait until system and all VMs are stabilised	Complete	100	40s	✓
10:16:30	Run post-install plugin if present	Complete	100	2m 20s	✓
	- SBC:Creating SBC Configuration File				
	- SBC:Checking ssh connection to SBC				
	- SBC:Connecting to SBC web service				
	- SBC:Can't connect, trying again				
	- SBC:Connecting to SBC web service				
	- SBC:Copying configuration file to SBC				
	- SBC:Checking ssh connection to SBC				
	- SBC:Connecting to SBC web service				
	- SBC:Merging SBC configuration				
10:18:50	- SBC:Connecting to SBC web service				
	- SBC:Saving SBC configuration file				
	- SBC:Connecting to SBC web service				
	- SBC:Restarting SBC				
	- main: Wizard completed successfully				
	Finalize Installation	Complete	100	15s	✓


Once the SBC template install has completed, select **Virtual Machine Management** on the left. Now, the **Virtual Machine List** shows that the SBC Template is installed.

Virtual Machine Management

Virtual Machine List


System Domain Uptime: 23 days, 18 hours, 27 minutes, 42 seconds

Current template installed: SBCT 6.0.0.1.4 (sbc E36M2) Refresh

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	65.206.67.91	512.0 MB	8	1d 4h 11m 28s	Running	N/A
✓ 	sbc	E36M2	65.206.67.93	4.0 GB	1	2m 14s	Running	N/A
✓	cdom	6.0.0.0.11	65.206.67.92	1024.0 MB	1	11h 48m 16s	Running	N/A

6.2. Avaya Aura™ SBC Licensing

After the Avaya Aura™ SBC has been installed, the system can be licensed. The license, which is a function of the “box-identifier” shown in the output of the “show system-info” CLI command, can be obtained from an Avaya authorized representative. The procedures in this section assume the license file is available.

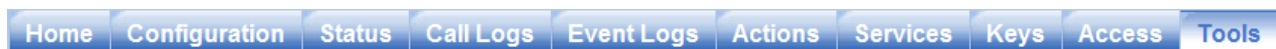
To log in, either select the wrench  [sbc](#) icon shown in the prior screen, or enter https://<ip-addr> where <ip-addr> is the management IP Address of the SBC. In the example configuration, the IP Address 65.206.67.93 can be used  to access a log in screen. Enter appropriate **Username** and **Password** and click **Login**.

Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name

Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Login"/>

The following shows an abridged screen after logging in. From the tabs available at the top, select the **Tools** tab.



Choose a tool to view from the left panel

From the menu on the left panel, select **Upload license file** as shown in the abridged menu below.

Tools

Update software

Retrieve license

Upload license file

The following screen shows the right panel after **Upload license file** has been selected on the left.

Upload License File

You can upload a license file from your computer to Net-Net OS-E. You can optionally apply the license file immediately. Otherwise, the license file will not take effect until Net-Net OS-E is restarted.

BOX:

File:

Apply License ☐

Use the **Browse...** button to select the location of the license file obtained from the Avaya authorized representative. Check the **Apply License** box. Click the **Upload** button.

Upload License File

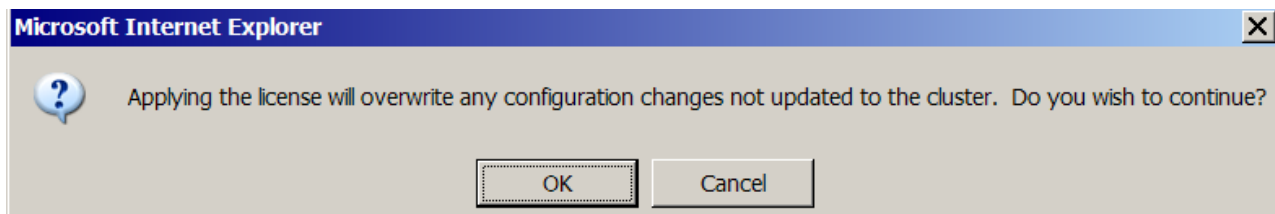
You can upload a license file from your computer to Net-Net OS-E. You can optionally apply the license file immediately. Otherwise, the license file will not take effect until Net-Net OS-E is restarted.

BOX:

File:

Apply License ☒

Heed the warning, and select **OK** if appropriate to proceed.



The following screen shows an example of a successfully uploaded license file.

Upload License File

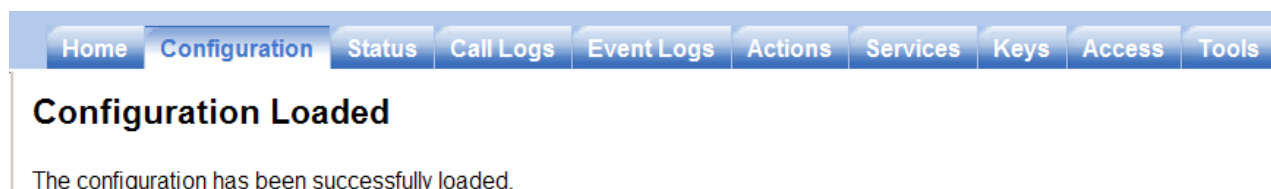
Uploaded License File : E:\Verizon-testing\Aura-SBC\SBCT_6.0.0.1.4
\Licensing\8bcebf67-f08b-4373-ab2a-6f3a59e9e493.xml

Result

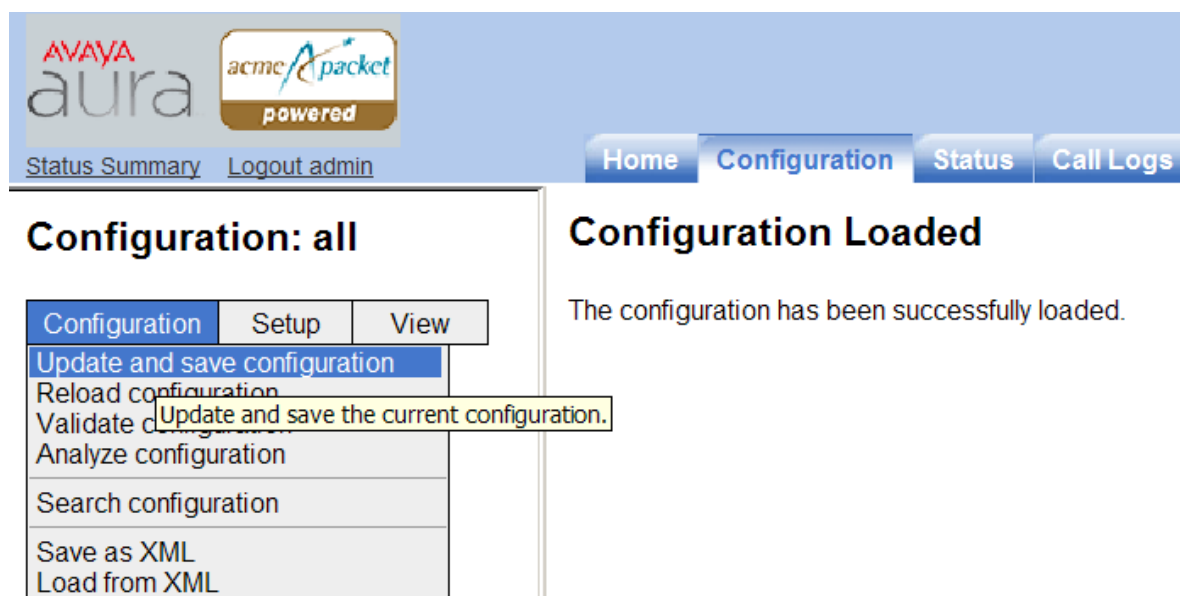
Success

You can upload a license file from your computer to Net-Net OS-E. You can optionally apply the license file immediately. Otherwise, the license file will not take effect until Net-Net OS-E is restarted.

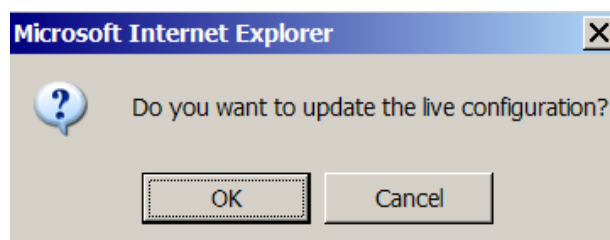
After the license has been uploaded, select the **Configuration** tab as shown below.



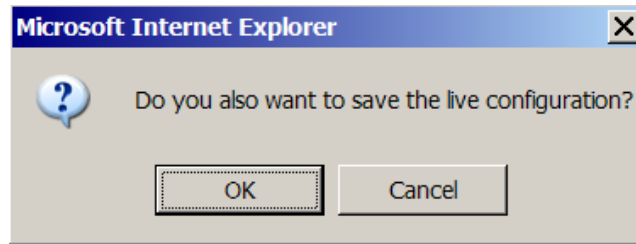
From the left, select **Configuration** → **Update and save configuration** as shown below.



Click **OK** to update the live configuration.



Click **OK** to save the live configuration.



Select the **Actions** tab as shown below.



Choose an action to invoke from the left panel

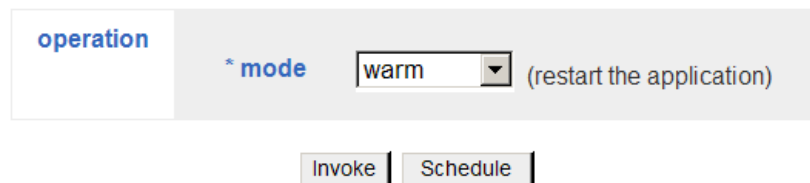
Scroll down the actions menu on the left and select **restart** as shown in the abridged screen below.

- ping
- playback
- presence
- presence-end-subscription
- presence-subscribe
- prune-assoc
- pt-script
- radius
- radius-authorize
- raid-check-consistency
- raid-set-adapter
- reg-lookup
- reg-lookup-detail
- registration
- remove-device
- restart**

From the right panel, select “warm” from the **mode** drop-down menu, and click the **Invoke** button, as shown below.

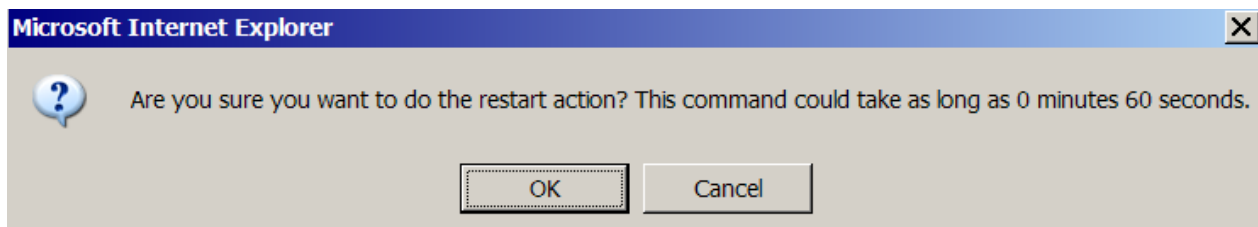
restart

restart the Net-Net OS-E



The screenshot shows a configuration panel with a tab labeled "operation". To its right, there is a label "* mode" followed by a dropdown menu currently set to "warm". To the right of the dropdown is the text "(restart the application)". Below this panel are two buttons: "Invoke" and "Schedule".

Select **OK** to proceed with the warm restart.



A screen such as the following will be displayed to show that the SBC is restarting. After the restart, the licensing procedure is complete. If further configuration is required, log back in, as described in the next section.


restart


restart the Net-Net OS-E

Net-Net OS-E is restarting...

6.3. Avaya Aura™ SBC Element Manager Configuration

After the installation wizard is completed, subsequent configuration can be performed through the element manager of the SBC. The configuration screens will be familiar to the reader experienced with the Acme Packet Net-Net OS-E.

To log in, either select the wrench  [sbc](#) icon shown in the final screen in Section 6.1, or enter the `https://<ip-addr>` where `<ip-addr>` is the management IP Address of the SBC. In the example configuration, the IP Address 65.206.67.93 can be used

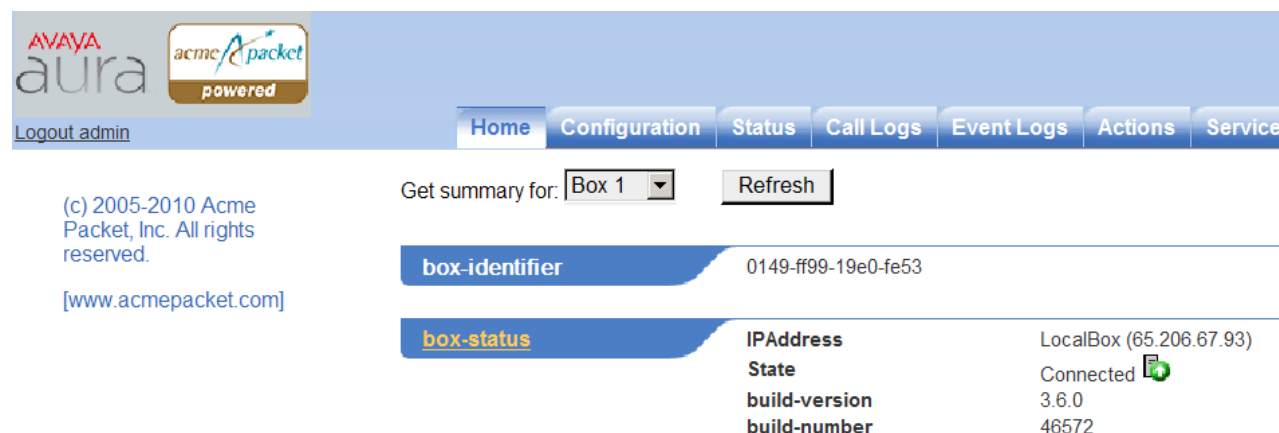
Address  `https://65.206.67.93/` to access a log in screen. Enter appropriate **Username** and **Password** and click **Login**.


Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name

Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Login"/>

The following shows an abridged **Home** screen after logging in. Note the tabs at the top.

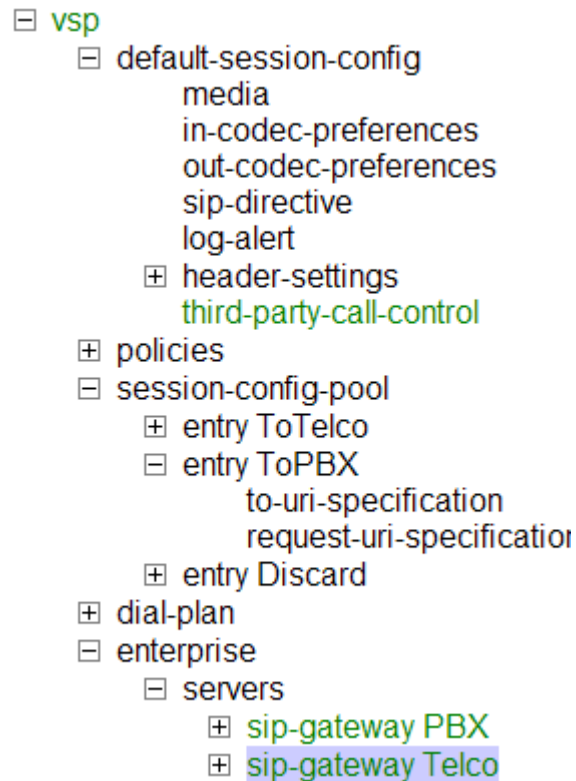


box-identifier		0149-ff99-19e0-fe53
box-status		
IPAddress	LocalBox (65.206.67.93)	
State	Connected 	
build-version	3.6.0	
build-number	46572	

6.3.1 Configuration of the Verizon SIP Signaling Port

Pre-GA versions of the configuration wizard did not allow the SIP signaling port to be configured to a port other than the default 5060. Although the version shown in these Application Notes allowed configuration of the SIP signaling port (5071) via the wizard, the information in this section is included in case the signaling port may need to be changed at any time. The following configuration should not be required using the GA version of the Avaya Aura™ SBC.

Select the **Configuration** tab. Using the menu on the left hand side, expand **vsp** → **enterprise** → **servers** → **sip-gateway Telco**, as shown below.



Under the **servers:** heading, select **Edit** for the “server_Telco1” entry corresponding to the Verizon network (i.e., host 172.30.209.21 in the screen below).

Configure vsplenterprise\servers\sip-gateway Telco

Show advanced

[Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Copy](#) [Delete](#)

[Manage connections](#), [Log instant messages](#), [Record media](#), [Record files](#),
[Set up accounting](#), [Change "from:" URI](#), [Change "to:" URI](#)

general:	
* name	<input type="text" value="Telco"/>
admin	<input type="button" value="enabled"/> (Resource is active)
domain	<input type="text"/>
failover-detection	<input type="button" value="ping"/> (Use OPTIONS to detect failures)

servers:								
	server	server	admin	host	transport	port	outbound-normalization	inbound-normalization
<input checked="" type="checkbox"/> server-pool [Delete]								
	Edit Delete	server Telco1	enabled	172.30.209.21	UDP	5060	Configure	Configure

In the **port** field, enter the proper SIP signaling port used by the Verizon network. In the sample configuration, Verizon is expecting SIP signaling to UDP port 5071. as shown below. Click the **Set** button.

Home	Configuration	Status	Call Logs	Event Logs	Actions	Services	Keys	Access	Tools												
<h3>Configure vsplenterprise\servers\sip-gateway Telco\server-pool\server Telco1</h3> <p>Show advanced Help Index</p> <p>Set Reset Back Copy Delete</p>																					
<table border="1"> <thead> <tr> <th colspan="2">General:</th> </tr> </thead> <tbody> <tr> <td>* server-name</td> <td><input type="text" value="Telco1"/></td> </tr> <tr> <td>admin</td> <td><input type="button" value="enabled"/> (Resource is active)</td> </tr> <tr> <td>* host</td> <td><input type="text" value="172.30.209.21"/> (host name or n.n.n.n)</td> </tr> <tr> <td>transport</td> <td>transport <input type="button" value="UDP"/> (User Datagram Protocol)</td> </tr> <tr> <td>port</td> <td><input type="text" value="5071"/> (at minimum 1,default=5060)</td> </tr> </tbody> </table>										General:		* server-name	<input type="text" value="Telco1"/>	admin	<input type="button" value="enabled"/> (Resource is active)	* host	<input type="text" value="172.30.209.21"/> (host name or n.n.n.n)	transport	transport <input type="button" value="UDP"/> (User Datagram Protocol)	port	<input type="text" value="5071"/> (at minimum 1,default=5060)
General:																					
* server-name	<input type="text" value="Telco1"/>																				
admin	<input type="button" value="enabled"/> (Resource is active)																				
* host	<input type="text" value="172.30.209.21"/> (host name or n.n.n.n)																				
transport	transport <input type="button" value="UDP"/> (User Datagram Protocol)																				
port	<input type="text" value="5071"/> (at minimum 1,default=5060)																				

6.3.2 Stripping SIP Headers using P-Site as an Example

The Avaya Aura™ SBC can be used to strip SIP headers. For headers that have relevance only within the enterprise, it may be desirable to prevent the header from being sent to the public SIP Service Provider. For example, Avaya Aura™ Session Manager Release 6 inserts the P-Site header. The following procedures may be used to strip the P-Site header.

Select the **Configuration** tab. Using the menu on the left hand side, select **vsp** → **default-session-config**. Scroll down on the right and select **header-settings** as shown in the screen below.

The screenshot displays the Avaya Aura SBC Configuration web interface. At the top, there is a navigation bar with tabs: Status Summary, Logout admin, Home, Configuration (selected), Status, Call Logs, Event Logs, and Actions. Below the navigation bar, the main content area is titled "Configuration: all". On the left side, there is a tree view showing the configuration hierarchy. The tree is expanded to show the "vsp" node, which is further expanded to show "default-session-config". Under "default-session-config", there are sub-nodes: media, sip-directive, log-alert, and third-party-call-control. The "media" node is selected. On the right side, there is a list of configuration items, each with a "Configure" link. The items are: out-media-normalization, in-hold-translation, out-hold-translation, sdp-regeneration, playback-call-settings, codec-specific-parameters, and media-scanner-settings. Below this list, there are two sections: "dtmf:" and "header:". The "dtmf:" section contains "in-dtmf-translation" and "out-dtmf-translation", each with a "Configure" link. The "header:" section contains "header-settings" with a "Configure" link.

Configuration	Setup	View
cluster		
box:AuraSBC		
vsp		
default-session-config		
media		
sip-directive		
log-alert		
third-party-call-control		
tls		
session-config-pool		
dial-plan		
enterprise		
dns		
settings		

Configuration	Configure
out-media-normalization	Configure
in-hold-translation	Configure
out-hold-translation	Configure
sdp-regeneration	Configure
playback-call-settings	Configure
codec-specific-parameters	Configure
media-scanner-settings	Configure

dtmf:	
in-dtmf-translation	Configure
out-dtmf-translation	Configure

header:	
header-settings	Configure

Select the **blocked-header** link on the right.

Status Summary Logout admin Home Configuration Status Call Logs Event Logs Actions Service

Configuration: all

Configuration Setup View

- cluster
 - box:AuraSBC
- vsp
 - default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control
 - tls
 - session-config-pool

Configure vsp\default-session-config\header-settings

Show advanced

Set Reset Back Delete

allowed-header	Edit allowed-header
blocked-header	Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header

The following screen appears allowing configuration of the header to block.

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configure vsp\default-session-config\header-settings blocked-header

Back

X

Add Remove All

OK

To block the P-Site header, enter “P-Site” and click **OK** as shown in the screen below.

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configure vsp\default-session-config\header-settings blocked-header

Back

P-Site X

Add Remove All

OK

The following screen shows the resulting configuration. The P-Site header is a blocked-header.

Home	Configuration	Status	Call Logs	Event Logs	Actions	Services	Keys	Access	Tools
------	---------------	--------	-----------	------------	---------	----------	------	--------	-------

Configure vsp\default-session-config\header-settings
[Show advanced](#)
[Help](#)
[Index](#)

[Set](#)
[Reset](#)
[Back](#)
[Delete](#)

allowed-header	Edit allowed-header
blocked-header	<div>P-Site</div> Edit blocked-header
altered-header	Add altered-header

Similar procedures can be used to strip headers in a more specific session-config-pool. For example, to strip the P-Site header in the session-config-pool “To-Telco”, navigate to **vsp → session-config-pool → entry ToTelco → header-settings** as shown below.

Configuration	Setup	View
---------------	-------	------

- [-] cluster
 - ⊕ box:AuraSBC
- [-] vsp
 - [-] default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control
 - ⊕ tls
 - [-] session-config-pool
 - [-] entry ToTelco
 - header-settings
 - ⊕ entry ToPBX
 - ⊕ entry Discard
 - ⊕ dial-plan
 - ⊕ enterprise
 - ⊕ dns
 - settings

In the resultant screen shown below, click **Edit blocked-header** and proceed to add the P-Site header as previously described in this section.

Configure vsp\session-config-pool\entry ToTelco\header-settings

[Index](#)

Show advanced

Set

Reset

Back

Delete

allowed-header	Edit allowed-header
blocked-header	Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization
altered-body	Add altered-body
reg-ex-collector	Add reg-ex-collector

The resultant configuration showing P-Site as a blocked-header within the session-config-pool entry “ToTelco” is shown below. Proceed to save and activate the configuration as described in Section 6.4.

Configure vsp\session-config-pool\entry ToTelco\header-settings

[Index](#)

Show advanced

Set

Reset

Back

Delete

allowed-header	Edit allowed-header
blocked-header	<div>P-Site</div> Edit blocked-header

6.3.3 Use of REFER With Verizon

After running the installation wizard with the Verizon service provider profile as shown in Section 6.1, the default configuration of the Avaya Aura™ SBC will not use REFER messages towards Verizon. That is, REFER messages received from the private side of the SBC will result in INVITE messages on the public side to Verizon. This section shows how the configuration can be changed to enable the use of REFER messages towards Verizon. Assuming the Network Call Redirection parameter on the relevant Communication Manager trunk groups is set to “y” (see Section 4.9), example call flows that would utilize REFER towards Verizon are as follows:

- An incoming call from a PSTN telephone 1 via Verizon to a Communication Manager station. The station answers, and transfers the call to a PSTN telephone 2 via Verizon. Communication Manager will send a REFER to complete the transfer. The changes in this section allow REFER to be sent to Verizon.
- An outgoing call from a Communication Manager station to a PSTN telephone 1 via Verizon. The calling station then transfers the call to a PSTN telephone 2 via Verizon. Communication Manager will send a REFER to complete the transfer. The changes in this section allow REFER to be sent to Verizon.

To cause the REFER sent by Communication Manager to result in a REFER sent to Verizon, the following change can be made to the Avaya Aura™ SBC. Navigate to **vsp → default-session-config → third-party-call-control** as shown below.

Configuration	Setup	View
<div>cluster</div> <div> <div>box:AuraSBC</div> </div> <div>vsp</div> <div> <div>default-session-config</div> <div>media</div> <div>sip-directive</div> <div>log-alert</div> <div>header-settings</div> <div>third-party-call-control</div> </div> <div> <div>tls</div> <div>session-config-pool</div> </div>		

On the right, select “disabled” from the **handle-refer-locally** drop-down menu. Click the **Set** button. Proceed to save and activate the configuration as described in Section 6.4.

Configure vsp\default-session-config\third-party-call-control		Show advanced
<div>Set</div> <div>Reset</div> <div>Back</div> <div>Delete</div>		
admin	enabled	(Resource is active)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)
refer-maintain-identity	false	

6.3.4 Quality Of Service (QoS) Markings for SIP Signaling

The procedure in this section is optional. The procedure can be used to achieve SIP signaling re-marking using the Avaya Aura™ SBC similar to the approach previously documented in Section 11.4 of reference [JF-JRR-VZIPT] for the Acme Packet Net-Net Session Director.

The default QoS behavior after using the installation wizard will be to preserve the TOS values. That is, the TOS value received from the private side of the Avaya Aura™ SBC will be transmitted to Verizon on the public side of the SBC. For example, for an outbound call to Verizon, if Avaya Aura™ Session Manager sends a SIP INVITE to the Avaya Aura™ SBC with a Differentiated Services Code Point (DSCP) value of 46, then the Avaya Aura™ SBC will send a SIP INVITE to Verizon with a DSCP of 46. The following screen, accessible via **vsp → session-config-pool → entry ToTelco → sip-settings**, shows the settings as configured by the installation wizard. Note that the **outleg-tos** is set to “preserve”.

Configure vsp\session-config-poolentry ToTelco\sip-settings [Show advanced](#) [Help](#)
[Index](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

general:

mode	<input type="text" value="auto-determine"/> (The Net-Net OS-E determines the mode, either back-to-back user agent or proxy.)
transport	transport <input type="text" value="any"/> (All protocol types)
port	directive <input type="text" value="auto-determine"/> (The Net-Net OS-E sets the SIP port.)

message-options:

preserve-call-id	<input type="text" value="disabled"/> (Resource is inactive)
handle-3xx-locally	<input type="text" value="disabled"/> (Resource is inactive)
handle-3xx-locally-server-arbitration	<input type="text" value="disabled"/> (Resource is inactive)
handle-3xx-locally-lookup-original-invite	<input type="text" value="disabled"/> (Resource is inactive)
inleg-tos	mode <input type="text" value="preserve"/>
outleg-tos	mode <input type="text" value="preserve"/>

If it is desired to have the Avaya Aura™ SBC re-mark SIP signaling to a different DSCP towards Verizon, the outleg-tos parameter can be changed. Select “overwrite” from the **outleg-tos mode** drop-down menu.

outleg-tos	mode <div> <div>preserve</div> <div>preserve</div> <div>overwrite</div> </div>
auto-accept-reinvite-with-no-sdp-on-in-leg	<div>disabled</div> <div>(Resource is inactive)</div>

In the **value** field that appears after selecting “overwrite”, enter the decimal value corresponding to the byte containing the ToS field. For example, if the value is set to 104 (0x68) as shown below, the DSCP value 26 (0x1A) will be sent to Verizon (decoded by Wireshark as “Assured Forwarding 31”). Click the **Set** button. Proceed to save and activate the configuration as described in Section 6.4. If DSCP value 28 (0x1C) is desired (decoded by Wireshark as “Assured Forwarding 32”), then the **value** field can be set to 112.

outleg-tos	mode <div>overwrite</div>
	value <div>104</div> <div>(from 0 to 255)</div>

Proceed to save and activate the configuration as described in Section 6.4.

6.3.5 Disabling Third Party Call Control

The installation wizard for Verizon in the release documented in these Application Notes will enable the **admin** field for third party call control.

Navigate to **vsp → default-session-config → third-party-call-control**. As shown below, the installation wizard in the release covered by these Application Notes sets the **admin** field to enabled.

Configuration: all

Configuration

Setup

View

cluster

box:AuraSBC

vsp

default-session-config

media

sip-directive

log-alert

header-settings

third-party-call-control

tls

session-config-pool

dial-plan

enterprise

dns

Configure vsp\default-session-config\third-party-call-control

Show advanced

Set

Reset

Back

Delete

admin	enabled	(Resource is active)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)
refer-maintain-identity	false	
ringback-file	<input type="text"/> Browse System Files	
busy-file	<input type="text"/> Browse System Files	

To disable third-party-call-control, select disabled from the **admin** drop-down and click **Set** as shown below.

Configure vsp\default-session-config\third-party-call-control [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

admin	disabled (Resource is inactive)
status-events	both (both call-legs)
handle-refer-locally	disabled (Resource is inactive)

After disabling, the third-party-call-control link becomes red as shown below.

Configuration: all

[Configuration](#) [Setup](#) [View](#)

- cluster
 - box:AuraSBC
- vsp
 - default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control**

Configure vsp\default-session-config\third-party-call-control [Show advanced](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

admin	disabled (Resource is inactive)
status-events	both (both call-legs)
handle-refer-locally	disabled (Resource is inactive)
refer-maintain-identity	false

Proceed to save and activate the configuration as described in Section 6.4.

6.3.6 Diversion Header Domain Mapping

The configuration in this section is not required if the Avaya CPE domain configured in Communication Manager matches the domain configured in the Verizon network for the Avaya CPE.

Avaya Aura™ Session Manager can adapt the domain in various SIP headers such as the Request-URI, P-Asserted-Identity, and History-Info headers. As described in these Application Notes, the Session Manager capability to adapt the domain in various headers allowed a shared Avaya Interoperability Lab configuration already configured for the CPE domain “avaya.com” to be used for Verizon IP Trunk Testing, even though the Verizon IP Trunk Service understood the CPE domain to be “adevc.avaya.globalipcom.com”. To allow diverted calls to be processed properly in the shared configuration, the SBC was used to convert the domain in the Diversion header to the Verizon expected “adevc.avaya.globalipcom.com”.

Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. The screen below shows the configuration before making changes for the Diversion header. The P-Site header is configured as a blocked-header per Section 6.3.2. To create a SIP header manipulation to change the host domain in the Diversion header, click **Add altered-header**.

Set

Reset

Back

Delete

allowed-header	Edit allowed-header
blocked-header	<div>P-Site</div> Edit blocked-header
altered-header	Add altered-header
reg-ex-header	Add reg-ex-header
header-normalization	Add header-normalization
altered-body	Add altered-body
reg-ex-collector	Add reg-ex-collector
apply-allow-block-to	requests-and-responses (apply to requests and responses)
apply-to-allow-block-to-dialog	both (Apply to both inbound and outbound dialogs.)

In the **number** field, enter an appropriate unused number. Since this is the first altered-header rule, number 1 was used. In the **source-header** field, enter “Diversion”. In the source-field area,

- select “selection” from the **type** drop-down menu
- in the **value** field, either enter a value to match directly, or click the **regular expression** link for assistance in creating the proper **value**. In the sample configuration, the rule will match on “avaya.com” appearing in the Diversion header.
- in the **replacement** field, enter the domain to appear in the host portion of the Diversion header, in place of “avaya.com”. In the sample configuration, Verizon expects “adevc.avaya.globalipcom.com” as shown below.

In the **destination** area, enter “Diversion”. In the **destination-field** area, select “host” from the **type** drop-down menu, since it is the host portion of the Diversion header that the rule should replace with “adevc.avaya.globalipcom.com”. Click the **Create** button.

Create vsp\session-config-pool\entry ToTelco\header-settings\altered-header 0 - Step 1 of 1: Edit altered-header 0

Please provide some basic information for altered-header 0. Then press "Create".

* number	<input type="text" value="1"/>	
* source-header	enter <input type="text" value="Diversion"/> or select from <input type="button" value="Diversion"/> <Not configured> ▼	
* source-field	<div><div>* type</div><div><input type="button" value="selection"/> ▼ (Regular expression based selection of portion of the URI.)</div><div>* value</div><div><input type="text" value="*.avaya.com"/> (regular expression)</div><div>* replacement</div><div><input type="text" value="adefc.avaya.globalipcom.c"/></div></div>	
* destination	enter <input type="text" value="Diversion"/> or select from <input type="button" value="Diversion"/> <Not configured> ▼	
* destination-field	<div><div>* type</div><div><input type="button" value="host"/> ▼ (Host portion of the URI.)</div></div>	

If the **regular expression** link is clicked in the screen shown above, the screen shown below is presented for assistance in generating the regular expression using simple language choices like "Match Any". Enter the string to match in the **Enter String Pattern** field, and click the appropriate radio button such as **Match Any**, and press **OK**.

(regular expression)

You can set the match option so that the system matches the entire string, the beginning or end of the string, or any part of the string.

Enter String Pattern	<input type="text" value="avaya.com"/>
Match option	<input type="radio"/> Exact Match <input type="radio"/> Match Beginning <input type="radio"/> Match End <input checked="" type="radio"/> Match Any
<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

Additional configuration can be applied to the altered-header rule using the screen shown below. In the sample configuration, the defaults were retained. Click the **Set** button.

Configure vsp\session-config-pool\entry ToTelco\header-settings\altered-header 1 [Show advanced](#)

[Set](#)
[Reset](#)
[Back](#)
[Copy](#)
[Delete](#)

admin	enabled <input type="button" value="v"/> (Resource is active)
* number	1
* source-header	enter <input type="text" value="Diversion"/> or select from <input type="button" value="Diversion"/> <input type="button" value="v"/>
* source-field	<div> <div>* type</div> <div>selection <input type="button" value="v"/> (Regular expression based selection of portion of the URI.)</div> </div> <div> <div>* value</div> <div><input type="text" value=".*avaya\.com"/> (regular expression)</div> </div> <div> <div>* replacement</div> <div><input type="text" value="adevc.avaya.globalipcom.com"/></div> </div>
* destination	enter <input type="text" value="Diversion"/> or select from <input type="button" value="Diversion"/> <input type="button" value="v"/>
* destination-field	<div> <div>* type</div> <div>host <input type="button" value="v"/> (Host portion of the URI.)</div> </div>
apply-to-methods	<div> <div>INVITE</div> <div>REFER</div> <div>MESSAGE</div> <div>INFO</div> </div> <div> <div>Select All</div> <div>Unselect All</div> </div>
apply-to-responses	<div> <div>* type</div> <div>no <input type="button" value="v"/> (Do not apply to responses (requests only))</div> </div>

The following screen shows a summary of the altered-header rule configured in this section.

Configure vsp\session-config-pool\entry ToTelco\header-settings [Show advanced](#) [Help](#) [Index](#)

[Set](#)
[Reset](#)
[Back](#)
[Delete](#)

allowed-header	Edit allowed-header																													
blocked-header	<input type="text" value="P-Site"/> Edit blocked-header																													
altered-header	<table border="1"> <thead> <tr> <th></th> <th>altered-header</th> <th>admin</th> <th>source-header</th> <th>source-field</th> <th>destination</th> <th>destination-field</th> <th>apply-to-methods</th> <th>apply-to-responses</th> <th>apply-to-dialog</th> </tr> </thead> <tbody> <tr> <td>Edit Delete</td> <td>altered-header 1</td> <td>enabled</td> <td>Diversion</td> <td>selection .*avaya\.com adevc.avaya.globalipcom.com</td> <td>Diversion</td> <td>host</td> <td>INVITE</td> <td>no</td> <td>both</td> </tr> </tbody> </table> Add altered-header											altered-header	admin	source-header	source-field	destination	destination-field	apply-to-methods	apply-to-responses	apply-to-dialog	Edit Delete	altered-header 1	enabled	Diversion	selection .*avaya\.com adevc.avaya.globalipcom.com	Diversion	host	INVITE	no	both
	altered-header	admin	source-header	source-field	destination	destination-field	apply-to-methods	apply-to-responses	apply-to-dialog																					
Edit Delete	altered-header 1	enabled	Diversion	selection .*avaya\.com adevc.avaya.globalipcom.com	Diversion	host	INVITE	no	both																					

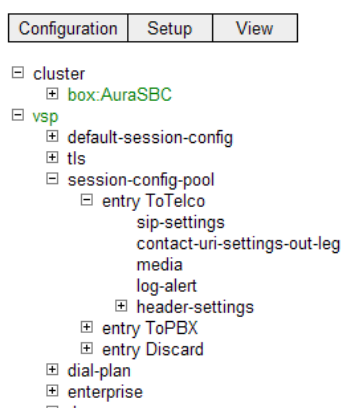
Proceed to save and activate the configuration as described in Section 6.4.

6.3.7 Modular Messaging Find-Me PAI Insertion

The configuration in this section is not required unless the Modular Messaging Find-Me application will be used to direct Find-Me calls out to the PSTN via the Verizon IP Trunk service. The Modular Messaging Find-Me feature allows a subscriber to set Find-Me reach number(s). If a caller is directed to the mailbox of a Modular Messaging subscriber with Find-Me active, the caller will have the option to leave a voice message or allow Modular Messaging to try to “find” the subscriber. If the caller opts to have Modular Messaging find the subscriber, Modular Messaging generates an outbound Find-Me call to the reach number active at that time. The P-Asserted-Identity in the INVITE for this outbound Find-Me call generated by Modular Messaging will not necessarily contain a DID number provisioned in the Verizon network for the IP Trunk Service. To allow Verizon to route the outbound Find-Me call, the SBC can be used to insert a PAI with a DID number provisioned for the IP Trunk Service. The DID number inserted in the PAI can be the external number callers would use to reach Modular Messaging. With the SIP header manipulation in place, the call will be routed by Verizon to the Find-Me reach number, and the caller ID presented to the Find-Me destination will be the Verizon DID associated with Modular Messaging (i.e., rather than the caller’s information). Note that the Modular Messaging Find-Me application announces the caller’s spoken name when the Find-Me call is answered, so the answering user can still identify the caller to decide whether to connect to the caller. If the user answering the Find-Me call does not opt to connect to the caller, the caller is returned to the subscriber’s mailbox greeting to leave a message.

The procedure below may be used to have the Avaya Aura™ SBC create the proper PAI. The approach is to look for the presence of “Modular Messaging” in the User-Agent header of an INVITE message, and ensure a specific PAI header is sent to Verizon. In the sample configuration, the PAI sent to Verizon contains “sip:7329450287@adevc.avaya.globalipcom.com” where the number “732-945-0287” is a DID number on the Verizon IP Trunk circuit that is associated with Modular Messaging, and the host portion of the PAI is the enterprise domain known to Verizon. Navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. Click **Add altered-header**. The resultant screen is shown below.

Configuration: all



Create vsp\session-config-pool\entry ToTelco\header-settings\altered-header 0 - Step 1 of 1

Please provide some basic information for altered-header 0. Then press "Create".

* number	<input type="text"/>
* source-header	enter <input type="text"/> or select from <input type="button" value="v"/> <Not configured>
* source-field	* type <input type="button" value="v"/> <Not configured>
* destination	enter <input type="text"/> or select from <input type="button" value="v"/> <Not configured>
* destination-field	* type <input type="button" value="v"/> <Not configured>

In the **number** field, enter a unique number. In the **source-header** field, enter “User-Agent”. From the **source-field type** drop-down, choose “selection”, which will cause two new fields to appear. For the **source-field value**, enter “.*Modular Messaging”. For the **source-field replacement**, enter the Verizon DID number associated with Modular Messaging access, such as “7329450287”. In the **destination** field, enter “P-Asserted-Identity”. From the **destination-field type** drop-down, select “user”. Click **Create**.

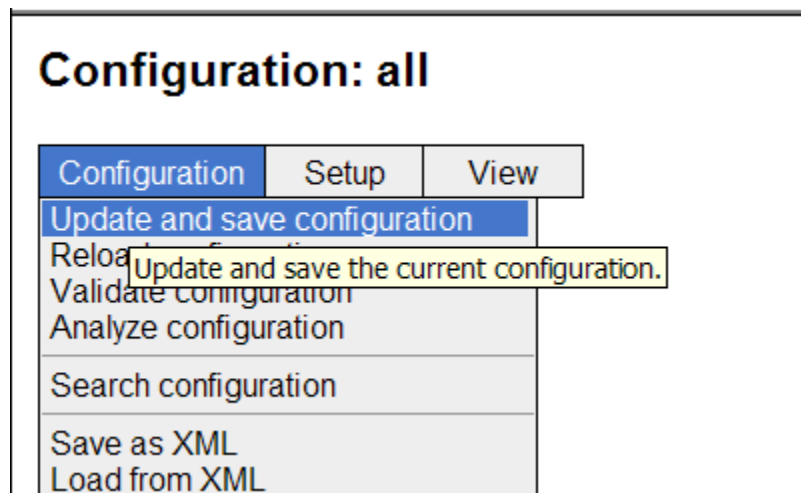
In the resultant screen, select “INVITE” from the **apply-to-methods**, as shown below. Click **Set**. Proceed to save and activate the configuration as described in Section 6.4.

Configure vsp\session-config-pool\entry ToTelco\header-settings\altered-header 4 [Show advanced](#)

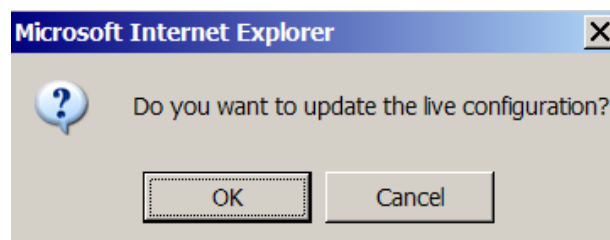
admin	enabled (Resource is active)
* number	4
* source-header	enter User-Agent or select from User-Agent
* source-field	<div> <div>* type</div> <div>selection (Regular expression based selection of portion of the URI.)</div> </div> <div> <div>* value</div> <div>.*Modular Messaging (regular expression)</div> </div> <div> <div>* replacement</div> <div>7329450287</div> </div>
* destination	enter P-Asserted-Identity or select from P-Asserted-Identity
* destination-field	<div> <div>* type</div> <div>user (User portion of the URI.)</div> </div>
apply-to-methods	<div> <div>INVITE</div> <div>REFER</div> <div>MESSAGE</div> <div>INFO</div> </div> <div> <input type="button" value="Select All"/> <input type="button" value="Unselect All"/> </div>
apply-to-responses	<div> <div>* type</div> <div>no (Do not apply to responses (requests only))</div> </div>
apply-to-dialog	<div> <div>both</div> <div>(Apply to both inbound and outbound dialogs.)</div> </div>
session-persistent	<div> <div>disabled</div> <div>(Resource is inactive)</div> </div>

6.4. Saving and Activating Configuration Changes

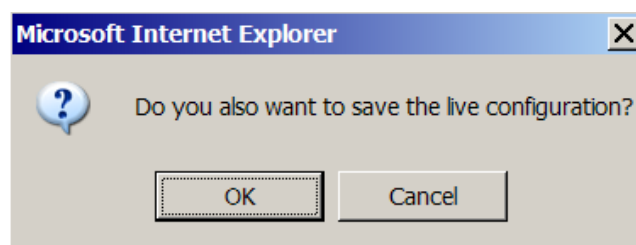
To save and activate configuration changes, select **Configuration → Update and save configuration** from the upper left hand side of the user interface, as shown below.



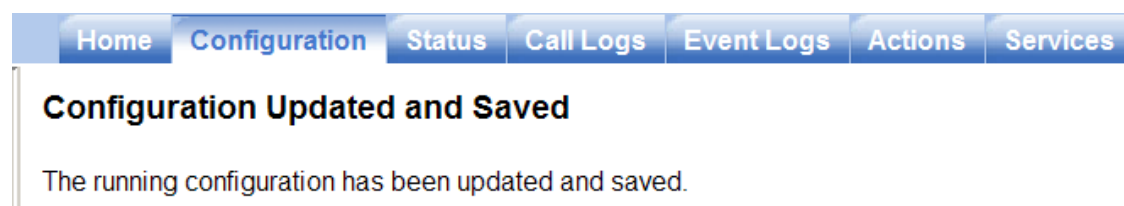
Click **OK** to update the live configuration.



Click **OK** to save the live configuration.



A screen that includes the following should appear.



7. Verizon Business IP Trunk Service Offer Configuration

Information regarding Verizon Business IP Trunk service offer can be found at <http://www.verizonbusiness.com/us/products/voip/trunking/> or by contacting a Verizon Business sales representative.

The sample configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Lab. The Verizon Business IP trunk service was accessed via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

7.1. Fully Qualified Domain Name (FQDN)s

The following Fully Qualified Domain Name (FQDN)s were provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i>	<i>pcelban0001.avayalincroft.globalipcom.com</i>

8. General Test Approach and Test Results

The test approach was manual testing of inbound and outbound calls using the Verizon IP Trunk Service on a production Verizon PIP access circuit, as shown in **Figure 1**. Testing was successful. Examples of the verified call scenarios are detailed in Section 9.

9. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business Private IP (PIP) IP Trunk service. Verification scenarios for the configuration described in these Application Notes included the following:

- Inbound and outbound voice calls between telephones controlled by Avaya Aura™ Communication Manager and the PSTN can be made using G.711MU or G.729A codecs.
- Direct IP-to-IP Media (also known as “Shuffling”) when applicable.
- DTMF Tone Support
 - Outbound call to PSTN application requiring post-answer DTMF (e.g., an IVR or voice mail system)
 - Inbound call from PSTN to Avaya CPE application requiring post-answer DTMF (e.g., Avaya Modular Messaging, Avaya vector digit collection steps)
- Additional PSTN numbering plans (e.g. International, operator assist, 411)
- Hold / Retrieve with music on hold
- Call transfer
- Conference calls
- Voicemail Coverage and Retrieval
- SIP Diversion Header for call re-direction
 - Call Forwarding
 - EC500
- Long hold time calls

9.1. Avaya Aura™ Communication Manager Verifications

This section illustrates verifications from Avaya Aura™ Communication Manager.

9.1.1 Example Incoming Call from PSTN via Verizon SIP Trunk

Incoming PSTN calls arrive from Verizon at the Avaya Aura™ SBC, which sends the call to Avaya Aura™ Session Manager. Session Manager sends the call to Avaya Aura™ Communication Manager via the entity link corresponding to the Avaya S8800 PE using port 5062. On Communication Manager, the incoming call arrives via signaling group 67 and trunk group 67.

The following Communication Manager “list trace” trace output shows a call incoming on trunk group 67. The PSTN telephone dialed 732-945-0285. Session Manager converted the number received from Verizon to the extension of a Communication Manager telephone (x30002). Alternatively, the incoming call handling table for trunk group 67 could have done the same. Extension 30002 is an IP Telephone with IP Address 65.206.67.11 in Region 4. Initially, the G450 Media Gateway (10.1.2.95) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is “ip-direct” from the IP Telephone (65.206.67.11) to the “inside” of the Avaya Aura™ SBC (65.206.67.93).

```
list trace tac 167                                     Page 1
LIST TRACE
time          data
15:58:19 TRACE STARTED 07/07/2010 CM Release String cold-00.0.345.0-18246
16:02:20 SIP<INVITE sip:30002@avaya.com:5060 SIP/2.0
16:02:20      active trunk-group 67 member 1 cid 0xbbd
16:02:20 SIP>SIP/2.0 183 Session Progress
16:02:20      dial 30002
16:02:20      ring station 30002 cid 0xbbd
16:02:20      G729A ss:off ps:20
16:02:20      rgn:4 [65.206.67.11]:2250
16:02:20      rgn:1 [10.1.2.95]:2050
16:02:20      G729 ss:off ps:20
16:02:20      rgn:4 [65.206.67.93]:20096
16:02:20      rgn:1 [10.1.2.95]:2052
16:02:20      xoip options: fax:off modem:off tty:US uid:0x500f1
16:02:20      xoip ip: [10.1.2.95]:2052
16:02:28 SIP>SIP/2.0 200 OK
16:02:28      active station 30002 cid 0xbbd
16:02:28 SIP<ACK sip:7329450285@adevc.avaya.globalipcom.com:5060
16:02:28 SIP< SIP/2.0
16:02:28 SIP>INVITE sip:9088485704@65.211.120.226:5060;transport
16:02:28 SIP>=tcp;maddr=65.206.67.93 SIP/2.0
16:02:28 SIP<SIP/2.0 100 Trying
16:02:28 SIP<SIP/2.0 200 OK
16:02:28 SIP>ACK sip:9088485704@65.211.120.226:5060;transport=tc
16:02:28 SIP>p;maddr=65.206.67.93 SIP/2.0
16:02:28      G729A ss:off ps:20
16:02:28      rgn:4 [65.206.67.93]:20096
16:02:28      rgn:4 [65.206.67.11]:2250
16:02:28      G729 ss:off ps:20
16:02:28      rgn:4 [65.206.67.11]:2250
16:02:28      rgn:4 [65.206.67.93]:20096
```

The following screen shows **Page 2** of the output of the “status trunk” command pertaining to this same call. Note the signaling using port 5062 between Communication Manager and Session Manager. Note the media is “ip-direct” from the IP Telephone (65.206.67.11) to the inside IP Address of the Avaya Aura™ SBC (65.206.67.93) using G.729.

status trunk 67/1		Page 2 of 3
CALL CONTROL SIGNALING		
Near-end Signaling Loc: PROCR		
Signaling	IP Address	Port
Near-end:	10.1.2.90	: 5062
Far-end:	10.1.2.70	: 5062
H.245 Near:		
H.245 Far:		
H.245 Signaling Loc:		H.245 Tunneler in Q.931? no
Audio Connection Type: ip-direct		Authentication Type: None
Near-end Audio Loc:		Codec Type: G.729
Audio	IP Address	Port
Near-end:	65.206.67.11	: 2250
Far-end:	65.206.67.93	: 20096

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

status trunk 67/1		Page 3 of 3
SRC PORT TO DEST PORT TALKPATH		
src port: T00241		
T00241:TX:65.206.67.93:20096/g729/20ms		
S00038:RX:65.206.67.11:2250/ g729a /20ms		
dst port: S00038		

The following portion of a filtered Wireshark trace (from the inside private side of the SBC) shows an incoming PSTN call. In frame 153, the Avaya Aura™ SBC (65.206.67.93) sends an INVITE to Session Manager (10.1.2.70). In frame 158, Session Manager sends the INVITE to the S8800 PE (10.1.2.90). In frame 163, Communication Manager sends a 183 Session Progress with SDP. Note that in prior releases of Communication Manager, a 180 with SDP would have been sent, but enhancements in Communication Manager Release 6 allow a 183 with SDP to be configured to be sent, as desired by Verizon. In frame 333, Communication Manager sends the 200 OK when the user answers the call. In frame 344, Communication Manager sends the INVITE to begin the process of shuffling the media paths to “ip-direct”, which concludes with the ACK in frame 366.

Filter: (sip && ip.addr == 65.206.67.93) || (sip && ip.addr == 10.1.2.90) Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
135	7.080612	65.206.67.93	10.1.2.70	SIP	Request: OPTIONS sip:10.1.2.70;transport=tcp
137	7.084615	10.1.2.70	65.206.67.93	SIP	Status: 200 OK
153	7.957317	65.206.67.93	10.1.2.70	SIP/SD	Request: INVITE sip:7329450285@adevc.avaya.globalipcom.com:5060, w
154	7.959172	10.1.2.70	65.206.67.93	SIP	Status: 100 Trying
158	8.003025	10.1.2.70	10.1.2.90	SIP/SD	Request: INVITE sip:30002@avaya.com:5060, with session description
160	8.005066	10.1.2.90	10.1.2.70	SIP	Status: 100 Trying
163	8.017746	10.1.2.90	10.1.2.70	SIP/SD	Status: 183 Session Progress, with session description
168	8.019890	10.1.2.70	65.206.67.93	SIP/SD	Status: 183 Session Progress, with session description
333	15.643716	10.1.2.90	10.1.2.70	SIP/SD	Status: 200 OK, with session description
336	15.647028	10.1.2.70	65.206.67.93	SIP/SD	Status: 200 OK, with session description
342	15.933765	65.206.67.93	10.1.2.70	SIP	Request: ACK sip:7329450285@adevc.avaya.globalipcom.com:5060
343	15.937089	10.1.2.70	10.1.2.90	SIP	Request: ACK sip:7329450285@adevc.avaya.globalipcom.com:5060
344	15.940276	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:9088485704@65.211.120.226:5060;transport=tcp;m
347	15.975446	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
349	15.976624	10.1.2.70	65.206.67.93	SIP	Request: INVITE sip:9088485704@65.211.120.226:5060;transport=tcp;m
350	15.977800	65.206.67.93	10.1.2.70	SIP	Status: 100 Trying
352	15.992907	10.1.2.70	10.1.2.90	SIP	Request: OPTIONS sip:avaya.com:5065;transport=tcp;monent=10.1.2.90
353	15.995816	10.1.2.90	10.1.2.70	SIP/SD	Status: 200 OK, with session description
361	16.300072	65.206.67.93	10.1.2.70	SIP/SD	Status: 200 OK, with session description
363	16.302240	10.1.2.70	10.1.2.90	SIP/SD	Status: 200 OK, with session description
365	16.316691	10.1.2.90	10.1.2.70	SIP/SD	Request: ACK sip:9088485704@65.211.120.226:5060;transport=tcp;madd
366	16.319087	10.1.2.70	65.206.67.93	SIP/SD	Request: ACK sip:9088485704@65.211.120.226:5060;transport=tcp;madd

The following portion of the same filtered Wireshark trace shows the INVITE sent by Session Manager in frame 158 expanded to illustrate the use of destination port 5062 on the S8800 processor ethernet (10.1.2.90) of Communication Manager. Communication Manager can apply Verizon-appropriate behaviors, such as the use of 183 rather than 180 with SDP, since it can distinguish that the call is inbound from Verizon by the use of an alternative port such as 5062 (i.e., arriving from the same Session Manager as other non-Verizon traffic).

No.	Time	Source	Destination	Protocol	Info
135	7.080612	65.206.67.93	10.1.2.70	SIP	Request: OPTIONS sip:10.1.2.70;transport=tcp
137	7.084615	10.1.2.70	65.206.67.93	SIP	Status: 200 OK
153	7.957317	65.206.67.93	10.1.2.70	SIP/SD	Request: INVITE sip:7329450285@adevc.avaya.globalipcom.com:5060,
154	7.959172	10.1.2.70	65.206.67.93	SIP	Status: 100 Trying
158	8.003025	10.1.2.70	10.1.2.90	SIP/SD	Request: INVITE sip:30002@avaya.com:5060, with session description
160	8.005066	10.1.2.90	10.1.2.70	SIP	Status: 100 Trying
163	8.017746	10.1.2.90	10.1.2.70	SIP/SD	Status: 183 Session Progress, with session description
168	8.019890	10.1.2.70	65.206.67.93	SIP/SD	Status: 183 Session Progress, with session description
333	15.643716	10.1.2.90	10.1.2.70	SIP/SD	Status: 200 OK, with session description
336	15.647028	10.1.2.70	65.206.67.93	SIP/SD	Status: 200 OK, with session description
342	15.933765	65.206.67.93	10.1.2.70	SIP	Request: ACK sip:7329450285@adevc.avaya.globalipcom.com:5060
343	15.937089	10.1.2.70	10.1.2.90	SIP	Request: ACK sip:7329450285@adevc.avaya.globalipcom.com:5060
344	15.940276	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:9088485704@65.211.120.226:5060;transport=tcp;m
347	15.975446	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
349	15.976624	10.1.2.70	65.206.67.93	SIP	Request: INVITE sip:9088485704@65.211.120.226:5060;transport=tcp;m
350	15.977800	65.206.67.93	10.1.2.70	SIP	Status: 100 Trying
352	15.992907	10.1.2.70	10.1.2.90	SIP	Request: OPTIONS sip:avaya.com:5065;transport=tcp;monent=10.1.2.90
353	15.995816	10.1.2.90	10.1.2.70	SIP/SD	Status: 200 OK, with session description
361	16.300072	65.206.67.93	10.1.2.70	SIP/SD	Status: 200 OK, with session description
363	16.302240	10.1.2.70	10.1.2.90	SIP/SD	Status: 200 OK, with session description
365	16.316691	10.1.2.90	10.1.2.70	SIP/SD	Request: ACK sip:9088485704@65.211.120.226:5060;transport=tcp;madd
366	16.319087	10.1.2.70	65.206.67.93	SIP/SD	Request: ACK sip:9088485704@65.211.120.226:5060;transport=tcp;madd

Source: 10.1.2.70 (10.1.2.70)
Destination: 10.1.2.90 (10.1.2.90)
Transmission Control Protocol, Src Port: 51095 (51095), Dst Port: 5062 (5062), Seq: 1462, Ack: 1, Len: 292

9.1.2 Example Outgoing Call to PSTN via Verizon SIP Trunk

The following trace shows an outbound ARS call from IP Telephone x30002 to the PSTN number 9-1-908-848-5704. The call is routed to route pattern 68 and trunk group 68. The call initially uses the gateway (10.1.2.95), but after the call is answered, the call is “shuffled” to become an “ip-direct” connection between the IP Telephone (65.206.67.11) and the “inside” of the Avaya Aura™ SBC (65.206.67.93). In this case, the mapping from the caller’s extension to the full DID number was performed in Session Manager.

```
list trace tac 168                                     Page 1
LIST TRACE
time          data
14:13:49 TRACE STARTED 07/06/2010 CM Release String cold-00.0.345.0-18246
14:14:00      Calling party station      30002 cid 0xb35
14:14:00      Calling Number & Name 30002 Joey Votto
14:14:00      dial 919088485704 route:PREFIX|HNPA|ARS
14:14:00      term trunk-group 68      cid 0xb35
14:14:00      dial 919088485704 route:PREFIX|HNPA|ARS
14:14:00      route-pattern 68 preference 1 cid 0xb35
14:14:00      seize trunk-group 68 member 7 cid 0xb35
14:14:00      Calling Number & Name NO-CPNumber NO-CPName
14:14:00 SIP>INVITE sip:19088485704@pcelban0001.avayalincroft.gl
14:14:00 SIP>obalipcom.com SIP/2.0
14:14:00      Setup digits 19088485704
14:14:00      Calling Number & Name 30002 Joey Votto
14:14:00 SIP<SIP/2.0 100 Trying
14:14:00      Proceed trunk-group 68 member 7 cid 0xb35
14:14:01 SIP<SIP/2.0 183 Session Progress
14:14:01      G729 ss:off ps:20
14:14:01      rgn:4 [65.206.67.93]:23066
14:14:01      rgn:1 [10.1.2.95]:2058
14:14:01      xoip options: fax:off modem:off tty:US uid:0x500ed
14:14:01      xoip ip: [10.1.2.95]:2058
14:14:03 SIP<SIP/2.0 200 OK
14:14:03 SIP>ACK sip:19088485704@pcelban0001.avayalincroft.globa
14:14:03 SIP>lipcom.com:5060;transport=tcp;maddr=65.206.67.93 SI
14:14:03 SIP>P/2.0
14:14:03      active trunk-group 68 member 7 cid 0xb35
14:14:03 SIP>INVITE sip:19088485704@pcelban0001.avayalincroft.gl
14:14:03 SIP>obalipcom.com:5060;transport=tcp;maddr=65.206.67.93
14:14:03 SIP> SIP/2.0
14:14:03 SIP<SIP/2.0 100 Trying
14:14:03 SIP<SIP/2.0 200 OK
14:14:03      G729 ss:off ps:20
14:14:03      rgn:4 [65.206.67.11]:2250
14:14:03      rgn:4 [65.206.67.93]:23066
14:14:03 SIP>ACK sip:19088485704@pcelban0001.avayalincroft.globa
14:14:03 SIP>lipcom.com:5060;transport=tcp;maddr=65.206.67.93 SI
14:14:03 SIP>P/2.0
14:14:03      G729A ss:off ps:20
14:14:03      rgn:4 [65.206.67.93]:23066
14:14:03      rgn:4 [65.206.67.11]:2250
```


The following screen shows **Page 2** of the output of the “status trunk” command pertaining to this same call. Note the media is “ip-direct” from the IP Telephone (65.206.67.11) to the inside IP Address of the Avaya Aura™ SBC (65.206.67.93) using G.729.

```
status trunk 68/7                                     Page 2 of 3
                                     CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
  Near-end: 10.1.2.90                               : 5062
  Far-end:  10.1.2.70                               : 5062
H.245 Near:
H.245 Far:
H.245 Signaling Loc:                               H.245 Tunneled in Q.931? no

Audio Connection Type: ip-direct           Authentication Type: None
  Near-end Audio Loc:                               Codec Type: G.729
  Audio       IP Address                             Port
  Near-end: 65.206.67.11                         : 2250
  Far-end:  65.206.67.93                         : 23066
```

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

```
status trunk 68/7                                     Page 3 of 3
                                     SRC PORT TO DEST PORT TALKPATH

src port: T00237
T00237:TX:65.206.67.93:23066/g729/20ms
S00038:RX:65.206.67.11:2250/g729a/20ms
dst port: S00038
```

The following portion of a filtered Wireshark trace taken on the inside network shows an outgoing call. In frame 190, Communication Manager uses the S8800 PE to send an INVITE to Session Manager. In highlighted frame 195, Session Manager sends the INVITE to the Avaya Aura™ SBC. The frame 195 INVITE is selected and expanded so that the contents of the PAI can be observed. In the selected row, observe that the Request URI contains the Verizon FQDN “pcelban0001.avayalincroft.globalipcom.com”. In the details in the center, observe that the PAI contains the enterprise FQDN known to Verizon, “adevc.avaya.globalipcom.com”. The call proceeds with 100 Trying, 183 Session Progress, and 200 OK upon answer by the PSTN phone. In frame 281, Communication Manager sends an INVITE to begin the shuffling process, which concludes with the ACKs in frames 299 and 300.

No.	Time	Source	Destination	Protocol	Info
190	7.530293	10.1.2.90	10.1.2.70	SIP/SD	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
193	7.532725	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
195	7.536533	10.1.2.70	65.206.67.93	SIP/SD	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
197	7.538080	65.206.67.93	10.1.2.70	SIP	Status: 100 Trying
228	9.154807	65.206.67.93	10.1.2.70	SIP/SD	Status: 183 Session Progress, with session description
231	9.157552	10.1.2.70	10.1.2.90	SIP/SD	Status: 183 Session Progress, with session description
270	10.714642	65.206.67.93	10.1.2.70	SIP/SD	Status: 200 OK, with session description
274	10.717103	10.1.2.70	10.1.2.90	SIP/SD	Status: 200 OK, with session description
277	10.720095	10.1.2.90	10.1.2.70	SIP	Request: ACK sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
278	10.722528	10.1.2.70	65.206.67.93	SIP	Request: ACK sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
281	10.777323	10.1.2.90	10.1.2.70	SIP	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
283	10.779184	10.1.2.70	10.1.2.90	SIP	Status: 100 Trying
284	10.780393	10.1.2.70	65.206.67.93	SIP	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
286	10.781530	65.206.67.93	10.1.2.70	SIP	Status: 100 Trying
296	11.060783	65.206.67.93	10.1.2.70	SIP/SD	Status: 200 OK, with session description
297	11.063267	10.1.2.70	10.1.2.90	SIP/SD	Status: 200 OK, with session description
299	11.078509	10.1.2.90	10.1.2.70	SIP/SD	Request: ACK sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
300	11.081180	10.1.2.70	65.206.67.93	SIP/SD	Request: ACK sip:19088485704@pcelban0001.avayalincroft.globalipcom.com

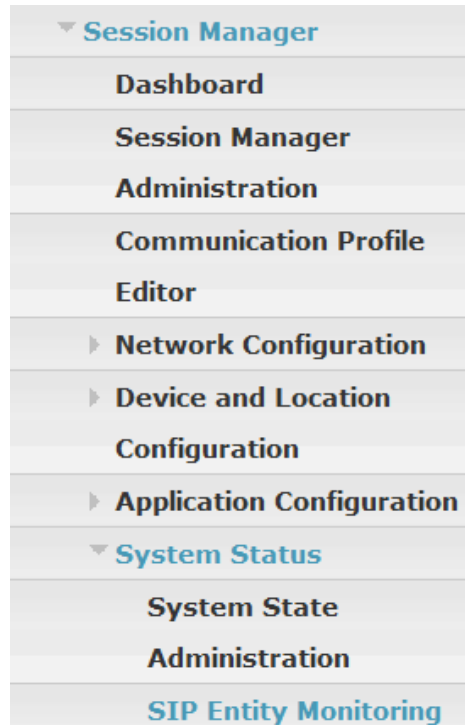
<div> P-Asserted-Identity: "Joey Votto" <sip:7329450285@adevc.avaya.globalipcom.com> SIP Display info: "Joey Votto" </div> <div> SIP PAI Address: sip:7329450285@adevc.avaya.globalipcom.com SIP PAI User Part: 7329450285 SIP PAI Host Part: adevc.avaya.globalipcom.com </div>

9.2. Avaya Aura™ System Manager and Session Manager Verification

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

9.2.1 Verify SIP Entity Link Status

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



From the list of monitored entities, select an entity of interest, such as “AuraSBC”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. The **Reason Code** column indicates that the Aura SBC has responded to SIP OPTIONS from Session Manager with a SIP 404 message, which is sufficient for SIP Link Monitoring to consider the link up.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: AuraSBC

Refresh

Summary View

1 Item							Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM1	65.206.67.93	5060	TCP	Up	404 Not found	Up
Time Last Down		Time Last Up		Last Message Sent		Last Response Latency (ms)	
Jun 30, 2010 10:15:36 AM EDT		Jun 30, 2010 2:35:49 PM EDT		Jul 6, 2010 2:09:13 PM EDT		7	

Return to the list of monitored entities, and select another entity of interest, such as “CM-Evolution-procr-5062”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. In this case, “Show” under Details was selected to view additional information. Note the use of port 5062.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CM-Evolution-procr-5062

Refresh

Summary View

1 Item							Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM1	10.1.2.90	5062	TCP	Up	200 OK	Up
Time Last Down		Time Last Up		Last Message Sent		Last Response Latency (ms)	
Never		Jun 9, 2010 9:57:41 AM EDT		Jul 6, 2010 2:14:38 PM EDT		9	

9.2.2 Verify System State

Expand **Elements** → **Session Manager** → **System Status** → **System State Administration**, as shown below.

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

Verify that the **Management State** is “Management Enabled” and the **Service State** is “Accept New Service.” In this case, the screen was captured while a call was up to Verizon.

System State Administration

This page shows the current service and management state of configured Session Managers. You can use this page to make state changes in the context of an upgrade or necessary maintenance.

Session Manager Instances

1 Item						Filter: Enable
<input type="checkbox"/>	Session Manager	Management State	Service State	Last Service State Change	Active Call Count	Version
<input type="checkbox"/>	SM1	Management Enabled	Accept New Service	No last service state change	1	6.0.0.0.600020

9.2.3 Call Routing Test

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



A screen such as the following is displayed.

Call Routing Test

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

SIP INVITE Parameters

Called Party URI <input type="text"/>		Calling Party Address <input type="text"/>
Calling Party URI <input type="text"/>		Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Monday"/>	Time (UTC) <input type="text" value="16:59"/>	Transport Protocol <input type="text" value="TCP"/>
Called Session Manager Instance <input type="text" value="SM1"/>		<input type="button" value="Execute Test"/>

Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. Under **Routing Decisions**, observe that the call will route via the Avaya Aura™ SBC on the path to Verizon. The domain is “pcelban0001.avayalincroft.globalipcom.com”. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

SIP INVITE Parameters

Called Party URI 19088485704@pcelban0001.avayalincroft.globalipcom		Calling Party Address 10.1.2.90
Calling Party URI 30002@avaya.com		Session Manager Listen Port 5062
Day Of Week Tuesday ▼	Time (UTC) 18:28	Transport Protocol TCP ▼
Called Session Manager Instance SM1 ▼		Execute Test

Routing Decisions

Route < sip:19088485704@pcelban0001.avayalincroft.globalipcom.com > to SIP Entity AuraSBC (65.206.67.93).
Terminating Location is Aura-SBC.

As another example, the following screen shows a call routing test for an inbound call from the PSTN to the enterprise, arriving via the Avaya Aura™ SBC. Under **Routing Decisions**, observe that the call will route to the S8800 processor ethernet (10.1.2.90) using the SIP entity named “CM-Evolution-procr-5062” Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Call Routing Test

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

SIP INVITE Parameters

Called Party URI

7329450285@adevc.avaya.globalipcom.com

Calling Party URI

9088485704@65.206.67.93

Day Of Week

Tuesday

Time (UTC)

18:28

Called Session Manager Instance

SM1

Calling Party Address

65.206.67.93

Session Manager Listen Port

5060

Transport Protocol

TCP

Execute Test

Routing Decisions

Route < sip:30002@avaya.com > to SIP Entity CM-Evolution-procr-5062 (10.1.2.90). Terminating Location is BaskingRidge HQ.

9.3. Avaya Aura™ Session Border Controller Verification

This section contains verification steps that may be performed using the Avaya Aura™ Session Border Controller.


The status of the virtual machines can be checked via the System Platform Console Domain of the S8800 Server running the Avaya Aura™ SBC. The following screen, available via the **Virtual Machine Management** link in the console domain, shows the “Running” State of the SBC.

Virtual Machine Management



Virtual Machine List

System Domain Uptime: 29 days, 23 hours, 43 minutes, 17 seconds

Current template installed: SBCT 6.0.0.1.4 (sbc E36M2) [Refresh](#)

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓	Domain-0	6.0.0.0.11	65.206.67.91	512.0 MB	8	1d 11h 30m 28s	Running	N/A
✓ 	sbc	E36M2	65.206.67.93	4.0 GB	1	6h 5m 53s	Running	Running
✓	cdom	6.0.0.0.11	65.206.67.92	1024.0 MB	1	14h 54m 14s	Running	N/A

Click on the wrench icon to the left of the name “sbc” to access the element manager user interface of the SBC. The following “Home” screen was accessed when one call was active.



[Logout admin](#)

[Home](#) [Configuration](#) [Status](#) [Call Logs](#) [Event Logs](#) [Actions](#) [Service](#)

(c) 2005-2010 Acme Packet, Inc. All rights reserved.
www.acmepacket.com

Get summary for: Box 1 [Refresh](#)

box-identifier

0149-ff99-19e0-fe53

box-status

IPAddress

LocalBox (65.206.67.93)

State

Connected 

build-version

3.6.0

build-number

46572

master-services

accounting, database

up-time

time

15:36:07 Tue 2010-07-06

timezone

EDT

uptime

6 days 00:23:54

system-info

cpu-usage-one-second

0%

call-info

active-calls

1

From the screen above, the “box-status” link provides basic information on the ethernet interfaces.

Status Summary for Box 1 :: box-status for Box 1 ▼ Refresh

interfaces **process-info** **sensors**

interface	name	op-state
eth0	inside	up
eth2	outside	up

A wealth of status information is available via the **Status** tab. For example, in the following screen, the left side Menu expands **Media** and **media-ports-sessions** is selected, revealing the information on the right about the active call.

AVAYA aura acme packet powered

Status Summary Logout admin

Home Configuration **Status** Call Logs Event Logs Actions Service

⊕ Location
⊕ MX
⊖ Media
 codec-info
 file-transfer-files
 file-transfer-summary
 media-clip-stats
 media-files
 media-ports-free-blocks
 media-ports-held
 media-ports-process-units
 media-ports-sessions
 media-ports-summary
 media-scanner-interval
 media-scanner-summary
 media-session-record

media-ports-sessions - Addresses used

View: Basic ▼ Search

ip-address	port	session-id
1.1.1.2	20220	0x04C29BE35D53DA10
65.206.67.93	23068	0x04C29BE35D53DA10

Page 1 ▼ of 1 showing 25 ▼ items

In the same **Status** tab, there is a SIP heading on the left that can be expanded as shown below.

- ⊕ Registration
- ⊖ SIP
 - active-association
 - active-call-peers
 - active-call-summary
 - active-calls**
 - active-session

In the example screen, **active-calls** was selected, revealing details about an active incoming call on the right. A scroll bar allows viewing of information about the active inbound call.

active-calls - currently active calls

View:

Basic

Search

seconds

Refresh

session-id	from	to
0x04C29BE35D53DA10	"AVAYA ALPHA" <sip:9088485704@65.211.120.226;user=phone>;tag=982278403-1278444984895-	"Lincroft Lab LINCROFT LAB" <sip:7329450285@adevc.avaya.globalip

Taken Jul 6, 2010 3:39:50 PM

XML

Scrolling right, the next screen presents additional information about this same inbound call. Additional information is available by continuing to scroll right (not shown).

state	previous-hop-ip	next-hop-domain	duration (seconds)	inbound-connection	outbound-connection
CONNECTED	172.30.209.21	adevc.avaya.globalipcom.com	237		65.206.67.93:5060-10.1.2.70:60599 TCP

9.3.1 Avaya Aura™ Session Border Controller Call Logs

The **Call Logs** tab can provide useful diagnostic or troubleshooting information. In the following screen, the **SIP Messages** search capability can be observed.

The following screen shows the **Call Logs** tab selected after making an inbound call.

Sessions seconds Refresh

Search Type: All Sessions View All Sessions Search

Page 1 of 1 showing 30 items View: User Messages

Created	Method	Result	From	To
09:51:59.110 Tue 2010-07-13	INVITE	sip:9088485704@65.211.120.226	sip:7329450285@adevc.avaya.globalipcom.com	

As shown below, select the **Session Diagram** link to view a ladder diagram for the session.

Created **Method** **Result** **From** **To**

Detail Call Diagram Session Diagram Call Record Delete Media Disconnect Play Call-out Files IM Archive Statistics

09:51:59.110
Tue 2010-07-13

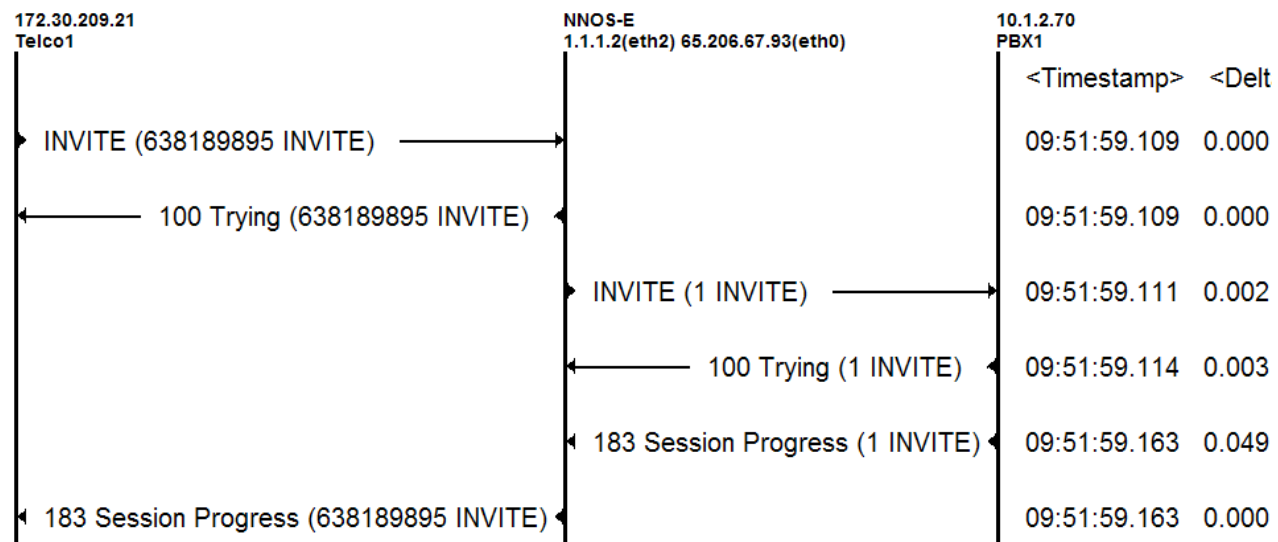
INVITE

sip:9088485704@65.211.120.226

sip:7329450285@adevc.avaya.globalipcom.com

Show Event Sequence Diagram For Session Only

For example, the following screen shows a portion of the ladder diagram for an inbound call. Note that the activity for both the inside private and outside public side of the SBC can be seen. Scroll down (not shown) to see additional ladder diagram information for the session.



At the top right of the screen, the session may be saved as a text or XML file. If the session is saved as an XML file, using the **Save as XML** link, the xml file can be provided to support personnel that can open the session on another Avaya Aura™ SBC for analysis.

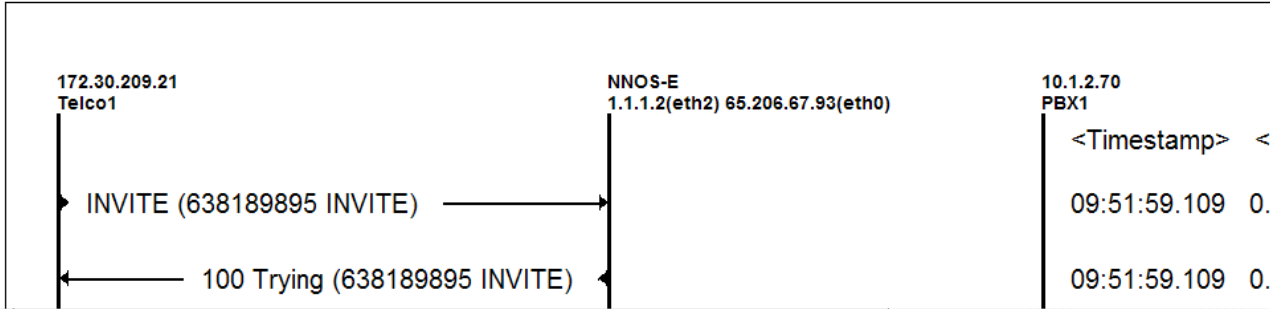
Back

[Save as text](#) [Save as XML](#)

Call Sequence for Session 0x04C29D107163AA7C

[Add Se](#)

Call IDs: BW0952303491307101477040542@65.211.120.226 CXC-54-5c37a790-5d43ce41-13c4-4c3c6f7



The **Call Logs** tab also provides search capabilities. The following screen shows the result of selecting the **SIP Messages** link (not shown) within the left-side menu of the **Call Logs** tab. The number “50” was entered to view the last 50 SIP messages.

Past 50 SIP messages

SIP Messages:
[Simple Search](#)
[Advanced Search](#)

☒ Show the last messages
 ☐ Show messages from the past:
☐ Show messages for call ID:

Show:
 Page of 3 showing items

Timestamp	Direction	Remote IP/Port	Local IP/Port
15:42:56.226 2010-07-06	RX	10.1.2.70:5060	65.206.67.93(eth0):3457
Message: More SIP/2.0 200 OK			
15:42:56.126 2010-07-06	RX	172.30.209.21:5071	1.1.1.2(eth2):5060
Message: More SIP/2.0 200 OK			

Scrolling down, the following screen shows a sampling of SIP messages for an inbound call. The received (RX) INVITE from Verizon that begins the process is at the bottom. The Avaya Aura™ SBC transmits (TX) the INVITE to Session Manager in the third row from the bottom, and the call proceeds.

15:44:15.420 2010-07-06	TX	172.30.209.21:5071	1.1.1.2(eth2):5060	UDP
Message: More SIP/2.0 200 OK				
15:44:15.419 2010-07-06	RX	10.1.2.70:5060	65.206.67.93(eth0):3457	TCP
Message: More SIP/2.0 200 OK				
15:44:14.740 2010-07-06	TX	172.30.209.21:5071	1.1.1.2(eth2):5060	UDP
Message: More SIP/2.0 183 Session Progress				
15:44:14.739 2010-07-06	RX	10.1.2.70:5060	65.206.67.93(eth0):3457	TCP
Message: More SIP/2.0 183 Session Progress				
15:44:14.679 2010-07-06	RX	10.1.2.70:5060	65.206.67.93(eth0):3457	TCP
Message: More SIP/2.0 100 Trying				
15:44:14.676 2010-07-06	TX	10.1.2.70:5060	65.206.67.93(eth0):3457	TCP
Message: More INVITE sip:7329450285@adevc.avaya.globalipcom.com:5060 SIP/2.0				
15:44:14.675 2010-07-06	TX	172.30.209.21:5071	1.1.1.2(eth2):5060	UDP
Message: More SIP/2.0 100 Trying				
15:44:14.674 2010-07-06	RX	172.30.209.21:5071	1.1.1.2(eth2):5060	UDP
Message: More INVITE sip:7329450285@1.1.1.2:5060 SIP/2.0				

10. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and the Avaya Aura™ SBC can be configured to interoperate successfully with Verizon Business IP trunk service. This solution allows Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager users access to the PSTN using a Verizon Business IP Trunk public SIP trunk service connection.

11. Additional References

This section references documentation relevant to these Applications.

11.1. Avaya

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

- [1] *Installing and Configuring Avaya Aura™ Communication Manager*, Doc ID 03-603558, Release 6.0 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™ Session Manager*, Doc ID 03-603324, Release 6.0, June 2010 available at <http://support.avaya.com/css/P8/documents/100082630>
- [4] *Installing and Configuring Avaya Aura™ Session Manager*, Doc ID 03-603473 Release 6.0, June 2010 available at <http://support.avaya.com/css/P8/documents/100089152>
- [5] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, Release 6.0, June 2010 available at <http://support.avaya.com/css/P8/documents/100089154>
- [6] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, Release 5.2, November 2009 available at <http://support.avaya.com/css/P8/documents/100089681>

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

Application Notes Reference [JF-JRR-VZIPT] documents Verizon IP Trunk Service with previous versions of Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. The version coverage in [JF-JRR-VZIPT] goes beyond the versions in the title, with the addition of Addendum 2 in Issue 1.3 covering Communication Manager 5.2.1 and Session Manager 5.2.

[JF-JRR-VZIPT] Application Notes for Avaya Aura™ Communication Manager 5.2, Avaya Aura™ Session Manager 1.1, and Acme Packet Net-Net Session Director with Verizon Business IP Trunk SIP Trunk Service – Issue 1.3

https://devconnect.avaya.com/public/download/dyn/AvayaSM_VzB_IPT.pdf

Application Notes Reference [PE] documents a configuration with testing results using Processor Ethernet on a main Communication Manager and an ESS for survivable SIP Trunking. The verifications in this document illustrate additional survivability considerations.

[PE] Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunking Using Processor Ethernet and Acme Packet Net-Net 4500 Session Director –

Issue 1.0

<https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/CM-PE-NN4500.pdf>

Application Notes Reference [CLAN] documents a similar configuration to [PE] using survivable SIP Trunks signaled from C-LAN interfaces rather than processor Ethernet. [CLAN] Sample Configuration Illustrating Avaya Aura™ Communication Manager SIP Trunk Survivability with Enterprise Survivable Server and Acme Packet Net-Net 4500 Session Director, Issue 1.0

<https://devconnect.avaya.com/public/flink.do?f=/public/download/interop/CM-ESS-NN4500.pdf>

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

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

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

11.2. Verizon Business

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

[7] *Retail VoIP Interoperability Test Plan*

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

12. Addendum – DNS on Avaya Aura™ SBC Public Interface

The procedure in this section is optional. The installation wizard for Verizon in the Avaya Aura™ SBC software release documented in these Application Notes requires knowledge of the IP Address and port associated with the Verizon IP Trunk SIP Signaling entity. That is, the installation wizard does not account for using DNS procedures to a Verizon DNS server rather than statically configured IP Address and port. Future versions of the installation wizard may account for using DNS on the public interface. This addendum shows an example configuration and associated verifications for modifying the configuration to use DNS on the public interface to Verizon, after the installation wizard has been run as shown in Section 6. These DNS changes are isolated to the Avaya Aura™ SBC. That is, no changes are required to Avaya Aura™ Session Manager or Avaya Aura™ Communication Manager.

12.1. Avaya Aura™ SBC Configuration Changes for DNS to Verizon

Log in to the Avaya Aura™ SBC element manager using the access procedures described in Section 6.3. Select the **Configuration** tab.

12.1.1 Add the Verizon DNS Server

Navigate to **vsp → dns → resolver** as shown below. Click the **Add server** link to add the Verizon-supplied IP Address of the Verizon DNS server to the configuration.

The screenshot shows the Avaya Aura SBC Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The 'Configuration' tab is selected. On the left, a tree view shows the configuration hierarchy: 'cluster' (box: AuraSBC), 'vsp', 'default-session-config', 'tis', 'session-config-pool', 'dial-plan', 'enterprise', 'dns', and 'resolver' (selected). The main content area is titled 'Configure vsp\dns\resolver' and includes a 'Show advanced' button and links for 'Help' and 'Index'. Below the title are 'Set', 'Reset', 'Back', and 'Delete' buttons. The configuration table shows the following settings:

Field	Value	Notes
admin	enabled	(Resource is active)
server	Add server	
server-scheme	preference-order	(Try DNS lookups to the most preferred server)
query-timeout	2	seconds(from 1 to 10,default=2)

In the **address** field, enter the IP Address of the Verizon DNS server. In the sample configuration, the IP Address for the Verizon DNS server is 172.30.209.4. Click **Create**.

The screenshot shows the 'Create vsp\dns\resolver\server - Step 1 of 1: Edit server' form. It includes a 'Help' and 'Index' link. The instruction reads: 'Please provide some basic information for server. Then press "Create".' The form has a single input field for the 'address' with the value '172.30.209.4' and a placeholder '(n.n.n.n)'. Below the input field are 'Create', 'Reset', and 'Cancel' buttons.

In the resultant screen, enter an appropriate **name** and click **Set**. In the sample configuration, the default values were retained for the other fields.

Configure vsp\dns\resolver\server 172.30.209.4 [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

* address	<input type="text" value="172.30.209.4"/> (n.n.n.n)
protocol	<input type="button" value="UDP"/> (User Datagram Protocol)
port	<input type="text" value="53"/> (from 0 to 65,535)
preference	<input type="text" value="100"/>
type	<input type="button" value="both"/>
name	<input type="text" value="VZ-IPTrunk-DNS"/>

[Set](#) [Reset](#) [Back](#)

The new server configuration is summarized as shown below.

Configure vsp\dns\resolver [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Delete](#)

admin	<input type="button" value="enabled"/> (Resource is active)														
server	<table><thead><tr><th></th><th>server</th><th>protocol</th><th>port</th><th>preference</th><th>type</th><th>name</th></tr></thead><tbody><tr><td>Edit Delete</td><td>server 172.30.209.4</td><td>UDP</td><td>53</td><td>100</td><td>both</td><td>VZ-IPTrunk-DNS</td></tr></tbody></table>		server	protocol	port	preference	type	name	Edit Delete	server 172.30.209.4	UDP	53	100	both	VZ-IPTrunk-DNS
	server	protocol	port	preference	type	name									
Edit Delete	server 172.30.209.4	UDP	53	100	both	VZ-IPTrunk-DNS									

12.1.2 Add DNS Group

Navigate to **vsp** → **enterprise** → **servers**. In the right-hand side, click the **Show advanced** button (not shown). Scroll down below the list of configured servers and click **Add dns-group**. The **Add dns-group** link will not be shown unless **Show advanced** has been selected.

server										
	server	peer-identity	admin	domain	directory	user	password-tag	failover-detection	description	
Edit Delete	sip-gateway PBX		enabled	adevc.avaya.globalipcom.com	Configure			ping		
Edit Delete	sip-gateway Telco		enabled		Configure			ping		
Edit Delete	sip-gateway VZ-IPCC		enabled		Configure			ping		

[Add avaya](#)
[Add h323-server](#)
[Add sip-host](#)
[Add lcs](#)
[Add mcs](#)
[Add sametime](#)
[Add sip-gateway](#)
[Add sip-connection](#)
[Add dns-group](#)

Enter an appropriate **name** for the DNS group to be created, and click **Create**.

Create vsp\enterprise\servers\dns-group - Step 1 of 1: Edit dns-group

[Show basic](#)

[Help](#) [Index](#)

Please provide some basic information for dns-group. Then press "Create".

general:

* name

VZ-IPTrunk-DNS-Group

Create

Reset

Cancel

In the resultant screen, enter the Verizon domain in the **domain** field. In the sample configuration, "pcelban0001.avayalincroft.globalipcom.com" was entered. If desired, scroll down and set **failover-detection** to ping and configure the desired **ping-interval**. The procedures to

enable periodic OPTIONS are shown separately in Section 12.1.5, but may be done at this stage. Click **Set**.

Configure vsplenterprise\servers\dns-group VZ-IPTrunk-DNS-Group

Show basic

Set

Reset

Back

Copy

Delete

[Manage connections](#), [Log instant messages](#), [Record media](#), [Record files](#),
[Set up accounting](#), [Change "from:" URI](#), [Change "to:" URI](#)

general:	
* name	VZ-IPTrunk-DNS-Group
peer-identity	
admin	enabled (Resource is active)
domain	pcelban0001.avayalincroft.

The newly added dns-group now appears at the end of the list of servers, as shown below.

Configure vsplenterprise\servers

Show basic

[Help](#) [Index](#)

Set

Reset

Back

Delete

server		server	peer-identity	admin	domain	directory	user	password-tag	failov-detec
	Edit Delete	sip-gateway PBX		enabled	adevc.avaya.globalipcom.com	Configure			ping
	Edit Delete	sip-gateway Telco		enabled		Configure			ping
	Edit Delete	sip-gateway VZ-IPCC		enabled		Configure			ping
	Edit Delete	dns-group VZ-IPTrunk-DNS-Group		enabled	pcelban0001.avayalincroft.globalipcom.com	Configure			none

If desired, edit the newly created dns-group and assign appropriate attributes and policies that had been assigned to the “sip-gateway Telco” created by the installation wizard . For example, in the sample configuration, an “outbound-session-config-pool-entry” was assigned to the “sip-gateway Telco” created by the installation wizard. The procedure below assigns the same “outbound-

session-config-pool-entry” to the new dns-group, since the new dns-group will be used instead of the “sip-gateway Telco” created by the wizard.

Navigate to **vsp** → **enterprise** → **servers**. In the left menu, select the newly added dns-group to Verizon, as shown below. In the right-hand side, scroll down to the **policy** section. In the **outbound-session-config-pool-entry**, select the appropriate policy from the list. In the sample configuration, the entry “vsp\session-config-pool\entry ToTelco” is selected. Click **Set** (not shown).

The screenshot displays the Avaya Session Manager configuration interface. On the left, a tree view shows the navigation path: **vsp** > **enterprise** > **servers** > **sip-gateway VZ-IPCC** > **dns-group VZ-IPTTrunk-DNS-Group**. The right pane shows the configuration for the selected dns-group. The **registration:** section includes fields for **peer-max-interval** (86400 seconds), **peer-min-interval** (3600 seconds), and **registration-request-timeout** (10 seconds). The **policy:** section includes a **default-policy** dropdown with a **Create** link, a **user-group-policy** field with an **Add user-group-policy** link, an **inbound-session-config-pool-entry** dropdown with a **Create** link, and an **outbound-session-config-pool-entry** dropdown with the selected entry **vsp\session-config-pool\entry ToTelco** and **Edit** and **Create** links.

domain-alias	Edit domain-alias
domain-subnet	Edit domain-subnet
loop-detection	tight (Compare source and destination address/port/transport)
service-type	provider (Provider peer)
ping-interval	10 seconds

registration:

peer-max-interval	86400 seconds
peer-min-interval	3600 seconds
registration-request-timeout	10 seconds

policy:

default-policy	Create
user-group-policy	Add user-group-policy
inbound-session-config-pool-entry	Create
outbound-session-config-pool-entry	vsp\session-config-pool\entry ToTelco Edit Create

12.1.3 Disable the sip-gateway Telco Created by the Installation Wizard

Navigate to **vsp** → **enterprise** → **servers**. In the left menu, select **sip-gateway Telco** as shown below. In the right panel, select “disabled” from the **admin** drop-down menu. Click **Set**.

The screenshot shows the Avaya Aura SBC configuration interface. On the left, the 'Configuration: all' tree is expanded to 'vsp' > 'enterprise' > 'servers' > 'sip-gateway Telco'. The right panel is titled 'Configure vsp\enterprise\servers\sip-gateway Telco' and includes a 'Show basic' button. Below the title are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. A link bar contains: 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. The 'general:' section contains the following fields:

general:	
* name	Telco
peer-identity	
admin	disabled (Resource is inactive)
domain	
directory	<input type="button" value="v"/> Create

The disabled “sip-gateway Telco”, whose “server-pool” contains the statically provisioned IP-Address and port of the Verizon IP Trunk Service entered in the installation wizard (Section 6.1), now appears in red.

This screenshot is identical to the one above, but the 'sip-gateway Telco' entry in the left-hand configuration tree is highlighted in red, indicating its disabled status. The right-hand configuration panel remains the same, showing the 'admin' dropdown set to 'disabled'.

12.1.4 Configure the Dial-plan to Use the New DNS-Group

Navigate to **vsp** → **dial-plan** → **source-route FromTelco**. This source-route previously used the “sip-gateway Telco” as the source-server, but will be changed to use the new dns-group. As shown below, use the **source-server** drop-down menu to select the DNS-group configured in Section 12.1.2 Click **Set**.

Configure vsp\dial-plan\source-route FromTelco [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Copy](#) [Delete](#)

general:	
* name	FromTelco
description	
* source-match	<div>* type server</div> <div>* source-server vsp\enterprise\servers\dns-group VZ-IPTrunk-DNS-Group Edit Create</div>
peer	<div>type server (Peer is a SIP server)</div> <div>server vsp\enterprise\servers\sip-gateway PBX Edit Create</div>

Navigate to **vsp** → **dial-plan** → **source-route FromPBX**. This source-route previously used the “sip-gateway Telco” as its peer server, but will be changed to use the new dns-group. Use the **server** drop-down menu in the peer area to select the DNS-group configured in Section 12.1.2 Click **Set**.

Configure vsp\dial-plan\source-route FromPBX [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Copy](#) [Delete](#)

general:	
* name	FromPBX
description	
* source-match	<div>* type server</div> <div>* source-server vsp\enterprise\servers\sip-gateway PBX Edit Create</div>
peer	<div>type server (Peer is a SIP server)</div> <div>server vsp\enterprise\servers\dns-group VZ-IPTrunk-DNS-Group Edit Create</div>

12.1.5 Set Fail-over Detection for New DNS-Group to use OPTIONS

If not already completed as part of creation of the dns-group in Section 12.1.2, the procedure in this section can be used to configure the dns-group to use OPTIONS to check the health of the link, and set the period between OPTIONS messages sent by the Avaya Aura™ SBC.

Navigate to **vsp → enterprise → servers**. Select the dns-group created in Section 12.1.2. Recall that dns-group configuration requires clicking the **Show advanced** button, as illustrated below. Click **Show advanced**.

Configure vsp\enterprise\servers\dns-group VZ-IPTrunk-DNS-Group

Show advanced

Set

Reset

Back

Copy

Delete

[Manage connections](#), [Log instant messages](#), [Record media](#), [Record files](#),
[Set up accounting](#), [Change "from:" URI](#), [Change "to:" URI](#)

This configuration is not in the "basic" view. To see the configuration, please press "Show advanced".

Scroll down to the “general” area and select **failover-detection** “ping” from the drop-down menu.

general:	
* name	VZ-IPTrunk-DNS-Group
peer-identity	
admin	enabled (Resource is active)
domain	pcelban0001.avayaalincroft.
directory	Create
user	
password-tag	Manage Password
failover-detection	ping (Use OPTIONS to detect failures)

To view or change the typical period between OPTIONS messages, scroll down and locate the **ping-interval** field under the “routing” heading. Enter the desired time (in seconds) between OPTIONS messages sourced by the Avaya Aura™ SBC for the new dns-group. The installation wizard for Verizon uses 10 seconds as the **ping-interval**, and this value can be retained or changed for the dns-group according to customer preference.

loop-detection	tight (Compare source and destination address/port/transport)
service-type	provider (Provider peer)
ping-interval	10 seconds

12.1.6 Save the Configuration and Force DNS

Proceed to save and activate the configuration as described in Section 6.4. If appropriate, use the warm restart procedure shown at the end of Section 6.2 to cause a restart the Aura SBC application and test the new DNS configuration.

12.2. Avaya Aura™ SBC Verifications of DNS to Verizon

After changing the configuration (as shown in Section 12.1) to use a dns-group rather than the static Verizon IP address and port in the “sip-gateway Telco” configured by the installation wizard, make outbound and inbound calls to verify the configuration. No further action is necessary. The remaining sub-sections are for illustration and aid in troubleshooting if necessary.

12.2.1 Avaya Aura™ SBC Status Tab

Select the **Status** tab. On the left-hand side menu, expand **DNS** → **dns-resolver** as shown below.

Status

BOX: Display:

- ☐ Trends
- ☐ Access
- ☐ Accounting
- ☐ Archives
- ☐ Authentication
- ☐ CSTA Call Control
- ☐ Carrier
- ☒ DNS
 - dns-cache
 - dns-resolver**
 - dns-server

In the right-side panel, select “Verbose” from the **View** menu. The following example screen shows that the DNS resolver is up and six successful **requests** and **responses** have been made.

Home Configuration **Status** Call Logs Event Logs Actions Services Keys Access Tools

dns-resolver - DNS resolver statistics

View: seco

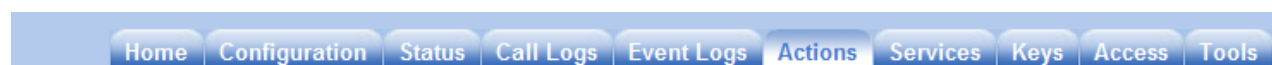
server	type	name	preference	cost	protocol	state	requests	responses	request-fails	discards	time-outs	server-failures	pending queries
172.30.209.4:53	both	VZ-IPTrunk-DNS	100	500	UDP	up	6	6	0	0	0	0	0

Using the left-hand menu shown above, select **DNS** → **dns-cache**. The following screen shows an abridged output from the sample configuration, after scrolling right so that the full “data” column could be illustrated. Refer to the wireshark traces in Section 12.2.3 for related information in the sample configuration.

name	type	server-name	TTL	data
1.1.1.2	PTR		static	AuraSBC.
aurasbc.	A		static	65.206.67.93
aurasbc.	A		static	1.1.1.2
127.0.0.1	PTR		static	localhost
localhost.	A		static	127.0.0.1
65.206.67.93	PTR		static	AuraSBC.
pcelban0001.avayalincroft.globalipcom.com.	NAPTR	VZ-IPTrunk-DNS	3531	
pc-n0001-elba.avayalincroft.globalipcom.com.	A	VZ-IPTrunk-DNS	20555	172.30.209.21
_sip_udp.pcelban0001.avayalincroft.globalipcom.com.	SRV	VZ-IPTrunk-DNS	20554	pc-n0001-elba.avayalincroft.globalipcom.com priority:100, weight:50, port:5071

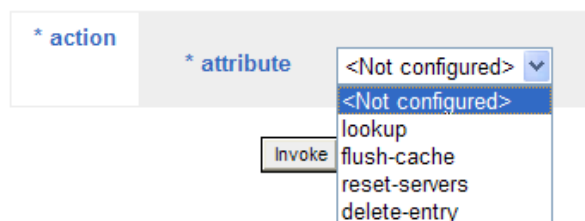
12.2.2 Avaya Aura™ SBC Actions Tab

Select the **Actions** tab. On the left-hand side menu, scroll down the alphabetical list of actions and select **dns**. In the following example screen, the drop-down menu for **attribute** is selected to illustrate available options. To force a “lookup”, select “lookup” from the **attribute** drop-down menu.



dns

DNS actions



The following example screen shows a successful “SRV” lookup. In the **host-name** field, “_sip._udp.pcelban0001.avayalincroft.globalipcom.com” was entered, “SRV” was selected from the **type** drop-down, and the **Invoke** button was clicked. Recall that “pcelban0001.avayalincroft.globalipcom.com” is the domain associated with the Verizon network. The “Success” results showing additional information are shown in the upper left. Note the name “pc-n0001-elba.avayalincroft.globalipcom.com”, and the SIP signaling port “5071” in the output.

DNS actions

Success

_sip._udp.pcelban0001.avayalincroft.globalipcom.com IN
SRV VZ-IPTTrunk-DNS Resolved 21600 100 50 5071 pc-n0001-elba.avayalincroft.globalipcom.com

* action

* attribute
lookup (Lookup DNS name)
* host-name
_sip._udp.pcelban0001.av
type
SRV (Server resource)
server-name
timeout-in-milliseconds
enter default or select from default (Default value in milliseconds)

Invoke

The following example screen shows a successful “A” lookup. In the **host-name** field, the name returned by Verizon in the SRV lookup, “pc-n0001-elba.avayalincroft.globalipcom.com” was entered, “A” was selected from the **type** drop-down, and the **Invoke** button was clicked. The “Success” results showing additional information are shown in the upper left. Note the IP Address “172.30.209.21” in the output. As can be observed, the IP Address 172.30.209.21 and port 5071 that were statically configured in the installation wizard in Section 6.1 can instead be learned through DNS procedures using the procedures in this Appendix.

dns

DNS actions

Success

pc-n0001-elba.avayalincroft.globalipcom.com IN
A VZ-IPTTrunk-DNS Resolved 21600 172.30.209.21

* action

* attribute
lookup (Lookup DNS name)
* host-name
pc-n0001-elba.avayalincro
type
A (IPv4 address)
server-name
timeout-in-milliseconds
enter default or select from default (Default value in milliseconds)

Invoke

12.2.3 Wireshark Illustration of DNS Usage

The following filtered wireshark trace shows the first outbound call to the Verizon IP Trunk service after the procedures in Section 12.1.1 to 12.1.6 were followed. Frame 523 shows a DNS Naming Authority Pointer (NAPTR) query for “pcelban0001.avayalincroft.globalipcom.com” from the Avaya Aura™ SBC public interface (1.1.1.2) to the Verizon DNS Server (172.30.209.4), with the Verizon response in frame 524. Frame 525 shows a DNS Service Location (SRV) query for “_sip._UDP.pcelban0001.avayalincroft.globalipcom.com”, with the Verizon response in frame 526 providing the port “5071” and name “pc-n0001-elba.avayalincroft.globalipcom.com”. Frame 527 shows a DNS Host address “A” query for “pc-n0001-elba.avayalincroft.globalipcom.com”, the name that was returned by Verizon in the DNS SRV response in frame 526. Frame 528 shows the Verizon A query response with the IP Address 172.30.209.21. At this point, the Avaya Aura™ SBC has determined via DNS procedures the same Verizon IP Address (172.30.209.21) and port (5071) for SIP signaling shown in Section 6.1 The Avaya Aura™ SBC sends the INVITE in frame 529 and the call proceeds as usual.

No.	Time	Source	Destination	Protocol	Info
523	791.043741	1.1.1.2	172.30.209.4	DNS	Standard query NAPTR pcelban0001.avayalincroft.globalipcom.com
524	791.152626	172.30.209.4	1.1.1.2	DNS	Standard query response
525	791.153339	1.1.1.2	172.30.209.4	DNS	Standard query SRV _sip._UDP.pcelban0001.avayalincroft.globalipcom.com
526	791.259237	172.30.209.4	1.1.1.2	DNS	Standard query response SRV 100 50 5071 pc-n0001-elba.avayalincroft.globalipcom.com
527	791.260311	1.1.1.2	172.30.209.4	DNS	Standard query A pc-n0001-elba.avayalincroft.globalipcom.com
528	791.366374	172.30.209.4	1.1.1.2	DNS	Standard query response A 172.30.209.21
529	791.369764	1.1.1.2	172.30.209.21	SIP/SD	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com
530	791.489366	172.30.209.21	1.1.1.2	SIP	Status: 100 Trying
535	793.071918	172.30.209.21	1.1.1.2	SIP/SD	Status: 183 Session Progress, with session description
779	795.413868	172.30.209.21	1.1.1.2	SIP/SD	Status: 200 OK, with session description
782	795.423894	1.1.1.2	172.30.209.21	SIP	Request: ACK sip:19088485704@172.30.209.21:5071;transport=udp
793	795.517599	1.1.1.2	172.30.209.21	SIP	Request: INVITE sip:19088485704@172.30.209.21:5071;transport=udp
820	795.819785	172.30.209.21	1.1.1.2	SIP/SD	Status: 200 OK, with session description
821	795.829142	1.1.1.2	172.30.209.21	SIP/SD	Request: ACK sip:19088485704@172.30.209.21:5071;transport=udp, with

The following screen shows frame 526 expanded to show additional details about the SRV query and response. Note the **Priority**, **Weight**, **Port**, and **Target** match the cached DNS information shown in the “data” column shown in Section 12.2.1. In the sample configuration, the Verizon network supplied just one “answer”.

No.	Time	Source	Destination	Protocol	Info
523	791.043741	1.1.1.2	172.30.209.4	DNS	Standard query NAPTR pcelban0001.avayalincroft.globalipcom.com
524	791.152626	172.30.209.4	1.1.1.2	DNS	Standard query response
525	791.153339	1.1.1.2	172.30.209.4	DNS	Standard query SRV _sip._UDP.pcelban0001.avayalincroft.globalipcom.com
526	791.259237	172.30.209.4	1.1.1.2	DNS	Standard query response SRV 100 50 5071 pc-n0001-elba.avayalincroft.globalipcom.com

Queries

- _sip._UDP.pcelban0001.avayalincroft.globalipcom.com: type SRV, class IN
 - Name: _sip._UDP.pcelban0001.avayalincroft.globalipcom.com
 - Type: SRV (Service location)
 - Class: IN (0x0001)

Answers

- _sip._UDP.pcelban0001.avayalincroft.globalipcom.com: type SRV, class IN, priority 100, weight 50, port 5071, target pc-n0001-elba.avayalincroft.globalipcom.com
 - Name: _sip._UDP.pcelban0001.avayalincroft.globalipcom.com
 - Type: SRV (Service location)
 - Class: IN (0x0001)
 - Time to live: 5 hours, 43 minutes, 42 seconds
 - Data length: 22
 - Priority: 100
 - Weight: 50
 - Port: 5071
 - Target: pc-n0001-elba.avayalincroft.globalipcom.com

The following screen shows frame 528 expanded to show additional details about the A query and response. Note the “Addr” matches the cached DNS information shown in the “data” column shown in Section 12.2.1.

No. ↓	Time	Source	Destination	Protocol	Info
525	791.153339	1.1.1.2	172.30.209.4	DNS	Standard query response
526	791.259237	172.30.209.4	1.1.1.2	DNS	Standard query response SRV 100 50 5071 pc-n0001-elba.avaya-incroft.globalipcom.com
527	791.260311	1.1.1.2	172.30.209.4	DNS	Standard query A pc-n0001-elba.avaya-incroft.globalipcom.com
528	791.366374	172.30.209.4	1.1.1.2	DNS	Standard query response A 172.30.209.21

Queries

pc-n0001-elba.avaya-incroft.globalipcom.com: type A, class IN

Name: pc-n0001-elba.avaya-incroft.globalipcom.com

Type: A (Host address)

Class: IN (0x0001)

Answers

pc-n0001-elba.avaya-incroft.globalipcom.com: type A, class IN, addr 172.30.209.21

Name: pc-n0001-elba.avaya-incroft.globalipcom.com

Type: A (Host address)

Class: IN (0x0001)

Time to live: 5 hours, 43 minutes, 43 seconds

Data length: 4

Addr: 172.30.209.21

12.2.4 Wireshark Illustration of SIP OPTIONS

The following filtered wireshark trace shows SIP OPTIONS exchanges on an idle line. Note that the Avaya Aura™ SBC sends SIP OPTIONS every 10 seconds as configured in Section 12.1.5 for the dns-group. For example, frames 3, 8, and 15 are 10 seconds apart. In frame 30, the Verizon network sends an OPTIONS message to the Avaya Aura™ SBC, which responds with the 200 OK in the frame 31.

Filter: sip && ip.addr == 172.30.209.21

▼ Expression... Clear Apply

No. ↓	Time	Source	Destination	Protocol	Info
3	2.310399	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:172.30.209.21;transport=udp
4	2.422749	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
8	12.310262	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:172.30.209.21;transport=udp
9	12.421655	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
15	22.308650	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:172.30.209.21;transport=udp
16	22.422625	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
22	32.308986	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:172.30.209.21;transport=udp
23	32.421803	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
27	42.307819	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:172.30.209.21;transport=udp
28	42.419144	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
30	47.948766	172.30.209.21	1.1.1.2	SIP	Request: OPTIONS sip:1.1.1.2:5060
31	47.949832	1.1.1.2	172.30.209.21	SIP	Status: 200 OK
34	52.307441	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:172.30.209.21;transport=udp
35	52.418716	172.30.209.21	1.1.1.2	SIP	Status: 200 OK

©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.