



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Controller for Enterprise 7.0 with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.0

Abstract

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Controller for Enterprise 7.0 with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. This service suite provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Communication Manager. The Communication Manager Network Call Redirection (NCR) and SIP User-to-User Information (UII) features can be utilized together to transmit UII within SIP signaling messages to alternate destinations via the Verizon network. These Application Notes update previously published Application Notes with newer versions of Communication Manager, Session Manager, and Avaya Session Border Controller for Enterprise.

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

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as any observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	6
2.2.	Test Results.....	7
2.3.	Support.....	8
2.3.1	Avaya	8
2.3.2	Verizon.....	8
3.	Reference Configuration.....	9
3.1.	History Info and Diversion Headers	10
3.2.	Call Flows	11
3.2.1	Inbound IP Toll Free Call with no Network Call Redirection.....	11
3.2.2	Inbound IP Toll Free Call with Post-Answer Network Call Redirection	11
3.2.3	Inbound IP Toll Free Call with Unsuccessful Network Call Redirection	12
4.	Equipment and Software Validated	14
5.	Configure Avaya Aura® Communication Manager Release 7.0	14
5.1.	Verify Licensed Features	15
5.2.	Dial Plan.....	18
5.3.	Node Names.....	18
5.4.	Processor Ethernet Configuration	18
5.5.	Network Regions	19
5.6.	IP Codec Sets	23
5.7.	SIP Signaling Group	24
5.8.	SIP Trunk Group.....	26
5.9.	Contact Center Configuration	30
5.9.1	Announcements.....	30
5.9.2	Post-Answer Redirection to a PSTN Destination	31
5.9.3	Post-Answer Redirection With UUI to a SIP Destination.....	31
5.9.4	ACD Configuration for Call Queued for Handling by Agent.....	33
5.10.	Public Numbering	35
5.11.	Incoming Call Handling Treatment for Incoming Calls	36
5.12.	Communication Manager Stations.....	36
5.13.	Saving Communication Manager Configuration Changes	37
6.	Configure Avaya Aura® Session Manager Release 7.0	38
6.1.	Domains	39
6.2.	Locations.....	40
6.3.	Adaptations	43
6.4.	SIP Entities.....	45
6.5.	Entity Links.....	50
6.6.	Time Ranges	51
6.7.	Routing Policies.....	51
6.8.	Dial Patterns.....	51
7.	Configure Avaya Session Border Controller for Enterprise Release 7.0.....	53
7.1.	Network Management.....	55
7.2.	Server Interworking Profile	55
7.3.	Signaling Manipulation.....	56

7.4.	Server Configuration.....	58
7.4.1	Server Configuration – Session Manager	58
7.4.2	Server Configuration - Verizon Business IPCC	59
7.5.	Routing Profile.....	61
7.6.	Topology Hiding Profile	63
7.7.	Application Rule	65
7.8.	Media Rule.....	65
7.9.	Signaling Rule.....	67
7.10.	Endpoint Policy Group	68
7.11.	Media Interface	69
7.12.	Signaling Interface	69
7.13.	End Point Flows - Server Flow	70
8.	Verizon Business IPCC Services Suite Configuration	73
8.1.	Service Access Information	73
9.	Verification Steps.....	74
9.1.	Avaya Aura® Communication Manager Verifications	74
9.1.1	Example Incoming Call from PSTN via Verizon IPCC to Telephone	74
9.1.2	Example Incoming Call Referred via Call Vector to PSTN Destination.....	76
9.2.	Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications	79
9.3.	Avaya Session Border Controller for Enterprise Verification	80
9.3.1	Welcome Screen	80
9.3.2	Alarms.....	80
9.3.3	Incidents.....	80
9.3.4	Diagnostics.....	82
9.3.5	Tracing	83
10.	Conclusion	84
11.	Additional References.....	84
11.1.	Avaya	84
11.2.	Verizon Business	85

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Controller for Enterprise 7.0 with Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite includes the IP Toll Free VoIP Inbound and IP-IVR SIP trunk service offers. This service suite provides toll free inbound calling via standards-based SIP trunks as well as re-routing of inbound toll free calls to alternate destinations based upon SIP messages (i.e., REFER) generated by Communication Manager. The Communication Manager Network Call Redirection (NCR) and SIP User-to-User Information (UUI) features can be utilized together to transmit UUI within SIP signaling messages to alternate destinations via the Verizon network. These Application Notes update previously published Application Notes [VZ-IPCC] with a newer version of Session Manager, Communication Manager, and Avaya Session Border Controller for Enterprise.

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

In the sample configuration, an Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between the Avaya CPE and Verizon Business. The Avaya SBCE performs SIP header manipulation and provides topology hiding to convert the private Avaya CPE IP addressing to IP addressing or domains appropriate for the Verizon access method. Session Manager is used as the Avaya SIP trunking “hub” connecting to Communication Manager, the Avaya SBCE, and other applications.

The Verizon Business IPCC Services suite described in these Application Notes is designed for business customers. The suite provides inbound toll-free service via standards-based SIP trunks. Using SIP Network Call Redirection (NCR), trunk-to-trunk connections of certain inbound calls at Communication Manager can be avoided by requesting that the Verizon network transfer the inbound caller to an alternate destination. In addition, the Communication Manager SIP User-to-User Information (UUI) feature can be utilized with the SIP NCR feature to transmit UUI within SIP signaling messages to alternate destinations. This capability allows the service to transmit a limited amount of call-related data between call centers to enhance customer service and increase call center efficiency. Examples of UUI data might include a customer account number obtained during a database query or the best service routing data exchanged between sites using Communication Manager.

Verizon Business IPCC Services suite is a portfolio of IP Contact Center (IPCC) interaction services that includes VoIP Inbound and IP Interactive Voice Response (IP IVR). Access to these features may use Internet Dedicated Access (IDA) or Private IP (PIP). PIP was used for the sample configuration described in these Application Notes. VoIP Inbound is the base service offering that offers core call routing and termination features. IP IVR is an enhanced service offering that includes features such as menu-routing, custom transfer, and additional media capabilities.

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

2. General Test Approach and Test Results

The Avaya equipment depicted in **Figure 1** was connected to the commercially available Verizon Business IPCC Services. This allowed PSTN users to dial toll-free numbers assigned by Verizon. The toll-free numbers were configured to be routed within the enterprise to Communication Manager numbers, including Vector Directory Numbers (VDNs). The VDNs were associated with vectors configured to exercise Communication Manager ACD functions as well as Verizon Business IPCC Services such as network call redirection to PSTN destinations and network call redirection with UUI.

The test approach was manual testing of inbound and referred calls using the Verizon Business IPCC Services on a production Verizon PIP access circuit, as shown in **Figure 1**.

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

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

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

See **Section 3.2** for an overview of key call flows and **Section 9** for detailed verifications and traces illustrating key call flows.

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

2.1. Interoperability Compliance Testing

The interoperability compliance testing included the execution of test cases details in the Verizon-authored interoperability test plan.

- SIP OPTIONS monitoring of the health of the SIP trunks was verified. Both the Avaya enterprise equipment and Verizon Business can monitor health using SIP OPTIONS.
- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya location. Configuration was varied such that these incoming toll-free calls were directed to Communication Manager telephone extensions, and Communication Manager VDNs containing call routing logic to exercise SIP Network Call Redirection.
- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a toll free call before the call has been answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a toll-free number directed to a busy user or resource when no redirection on busy conditions was configured (which would be unusual in a contact center).
- Proper termination of an inbound IP Toll Free call left in a ringing state for a relatively long duration, which again would be unusual in a contact center. In the sample configuration, Verizon sent a SIP CANCEL to cancel the call after three minutes of ring no answer conditions, returning busy tone to the PSTN caller.
- Privacy requests for inbound toll-free calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67 from a mobile phone), the inbound toll-free call can be successfully completed while withholding presentation of the PSTN caller id to user displays. (When the caller requests privacy, Verizon IPCC sends the caller ID in the P-Asserted-Identity header and includes “Privacy: id” which is honored by Communication Manager).
- Inbound toll-free call long holding time call stability. The Avaya CPE sends a re-INVITE with SDP to refresh the session at the configured session refresh interval specified on the Communication Manager trunk group handling the call. In the sample configuration, the session refresh re-INVITE was sent after 900 seconds (15 minutes), the interval configured for the trunk group in **Section 5.8**. The call continued with proper talk path.
- Telephony features such as hold and resume. When a Communication Manager user holds a call in the sample configuration, Communication Manager will send a re-INVITE to Verizon IP Toll Free service with a media attribute “sendonly”. The Verizon 200 OK to this re-INVITE will include media attribute “recvonly”. While the call remains on hold, RTP will flow from the Avaya CPE to Verizon, but no RTP will flow from Verizon to the Avaya CPE (i.e., as intended). When the user resumes the call from hold, bi-directional media path resumes. Although it would be unexpected in a contact center, calls on hold for longer than the session refresh interval were tested, and such calls could be resumed after the session refresh re-asserted the “sendonly” state.
- Transfer of toll-free calls between Communication Manager users.
- Incoming voice calls using the G.729a and G.711 ULAW codecs, and proper protocol procedures related to media.

- DTMF transmission using RFC2833. For inbound toll-free calls, PSTN users dialing post-answer DTMF digits are recognized properly by the Avaya CPE.
- Proper DiffServ markings for SIP signaling and RTP media flowing from the Avaya CPE to Verizon.
- Remote Workers

2.2. Test Results

The interoperability compliance testing of the sample configuration was completed with successful results as described in **Section 2.1**. The following observations may be noteworthy:

- Verizon Business IPCC Services suite does not support fax.
- Verizon Business IPCC Services suite does not support History Info or Diversion Headers. The Avaya CPE will not send History-Info or Diversion header to Verizon IPCC in the sample configuration.
- Verizon Business IPCC Services suite does not support SIP 302 Redirect.
- Verizon Business IPCC Services suite does not support G.729 Annex b. When using G729, the Avaya CPE will always include “annexb=no” in SDP in the sample configuration.
- **Section 3.3.3** summarizes a call flow that would theoretically allow a call to remain in Communication Manager vector processing upon failure of a vector-triggered REFER attempt. However, most such call scenarios could not be verified on the production Verizon circuit used for testing. On the production circuit, Verizon would send a BYE to terminate the call upon encountering REFER transfer failures, so there was no opportunity for the call to remain in Communication Manager vector processing. See **Section 3.3.3** for additional information.
- During testing, Verizon’s IP Interactive Voice Response (IP IVR) service did not accept the SIP REFER method unless the URI in the Refer-To header included the IP address presented in the From header within the original SIP INVITE. This IP address was different from the IP address included in the Contact header. The Avaya SBCE Topology Hiding profile was used to populate the From header IP address in the Refer-To header for both the IP IVR and IP Toll Free services. Calls were successfully diverted using REFER for both Verizon services with this Topology Hiding profile in place. See **Section 7.6** for additional information.

2.3. Support

2.3.1 Avaya

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

2.3.2 Verizon

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

3. Reference Configuration

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

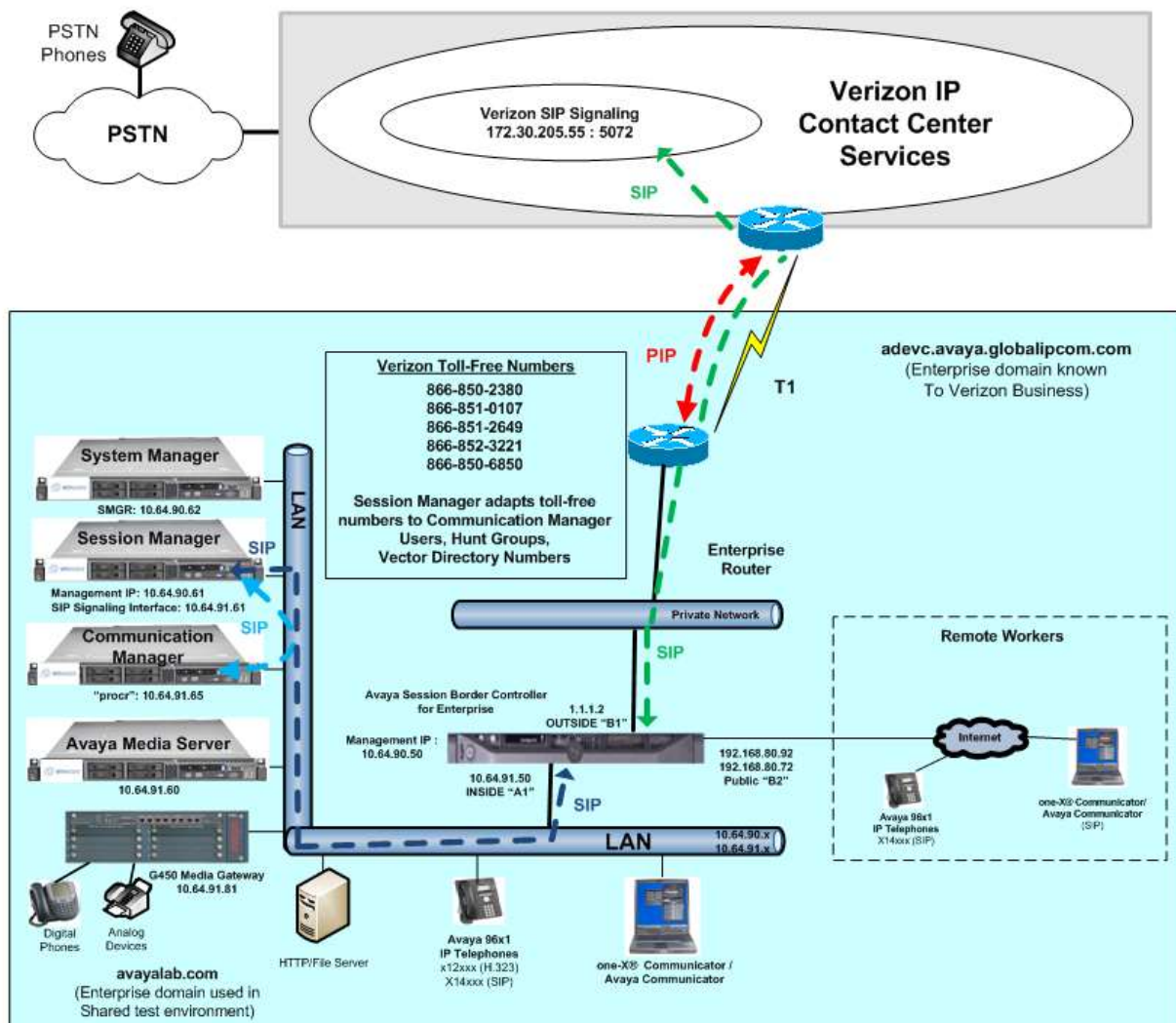


Figure 1: Avaya Interoperability Test Lab Configuration

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

The Avaya CPE environment was known to Verizon Business IPCC Service as FQDN “*adevc.avaya.globalipcom.com*”. For efficiency, the Avaya CPE environment utilizing Session Manager Release 7.0 and Communication Manager Release 7.0 was shared among other ongoing test efforts at the Avaya Solutions and Interoperability Test lab. Access to the Verizon Business IPCC services was added to a configuration that already used domain “*avayalab.com*” at the enterprise. As such, the Avaya SBCE is used to adapt the domains as needed. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Manager and Session Manager match the CPE domain known to Verizon.

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

- Verizon Business IPCC Services node sends the following in the initial INVITE to the CPE:
 - The CPE FQDN of *adevc.avaya.globalipcom.com* in the Request URI.
 - The Verizon Business IPCC Services gateway IP address in the From header.
 - The enterprise SBC outside IP address (e.g., 1.1.1.2) in the To header.
 - Sends the INVITE to Avaya CPE using destination port 5060 via UDP
- Avaya Session Border Controller for Enterprise sends Session Manager:
 - The Request URI contains *avayalab.com*.
 - The host portion of the From header and PAI header contains *avayalab.com*
 - The host portion of the To header contains *avayalab.com*
 - Sends the packet to Session Manager using destination port 5060 via TCP
- Session Manager sends Communication Manager
 - The Request URI contains *avayalab.com*, to match the shared Avaya SIL test environment.
 - Sends the packet to Communication Manager using destination port 5071 via TLS to allow Communication Manager to distinguish Verizon traffic from other traffic arriving from the same instance of Session Manager.

Note – The Fully Qualified Domain Names and IP addressing specified in these Application Notes apply only to the reference configuration shown in **Figure 1**. Verizon Business customers will use FQDNs and IP addressing appropriate for the unique customer environment.

3.1. History Info and Diversion Headers

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

3.2. Call Flows

To understand how inbound Verizon toll-free calls are handled by Session Manager and Communication Manager, key call flows are summarized in this section.

3.2.1 Inbound IP Toll Free Call with no Network Call Redirection

The first call scenario illustrated in **Figure 3** is an inbound Verizon IP Toll Free call that is routed to Communication Manager, which in turn routes the call to a vector, agent, or phone. No redirection is performed in this simple scenario. A detailed verification of such a call with Communication Manager traces can be found in **Section 9.1.1**.

1. A PSTN phone originates a call to a Verizon IP Toll Free number.
2. The PSTN routes the call to the Verizon IP Toll Free service network.
3. The Verizon IP Toll Free service routes the call to the Avaya Session Border Controller for Enterprise.
4. The Avaya Session Border Controller for Enterprise performs any configured SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any configured SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed. In this case, Session Manager routes the call to Communication Manager using a unique port so that Communication Manager can distinguish this call as having arrived from Verizon IPCC.
6. Depending on the called number, Communication Manager routes the call to a) a hunt group or vector, which in turn routes the call to an agent or phone, or b) directly to a phone.

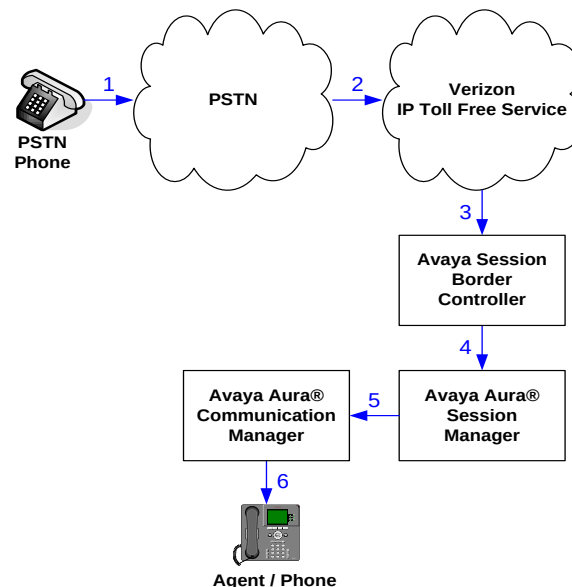


Figure 3: Inbound Verizon IP Toll Free Call – No Redirection

3.2.2 Inbound IP Toll Free Call with Post-Answer Network Call Redirection

The second call scenario illustrated in **Figure 4** is an inbound Verizon IP Toll Free call that is routed to a Communication Manager Vector Directory Number (VDN) to invoke call handling logic in a vector. The vector answers the call and then redirects the call back to the Verizon IP Toll Free service for routing to an alternate destination. Note that Verizon IP Toll Free service does not

support redirecting a call before it is answered (using a SIP 302), and therefore the vector must include a step that results in answering the call, such as playing an announcement, prior to redirecting the call using REFER.

A detailed verification of such call with Communication Manager traces can be found in **Section 9.1.2** for a Verizon IP Toll Free SIP-connected alternate destination. In this example, the Verizon IP Toll Free service can be used to pass User to User Information (UI) from the redirecting site to the alternate destination.

1. Same as the first five steps in **Figure 3**.
2. Communication Manager routes the call to a vector, which answers the call, plays an announcement, and attempts to redirect the call by sending a SIP REFER message out the SIP trunk from which the inbound call arrived. The SIP REFER message specifies the alternate destination in the Refer-To header. The SIP REFER message passes back through Session Manager and the Avaya SBCE to the Verizon IP Toll Free service network.
3. The Verizon IP Toll Free service places a call to the target party contained in the Refer-To header. Upon answer, the calling party is connected to the target party.
4. The Verizon IP Toll Free service notifies the Avaya CPE that the referred call has been answered (NOTIFY/sipfrag 200 OK). Communication Manager sends a BYE. The calling party and the target party can talk. The trunk upon which the call arrived in Step 1 is idle.

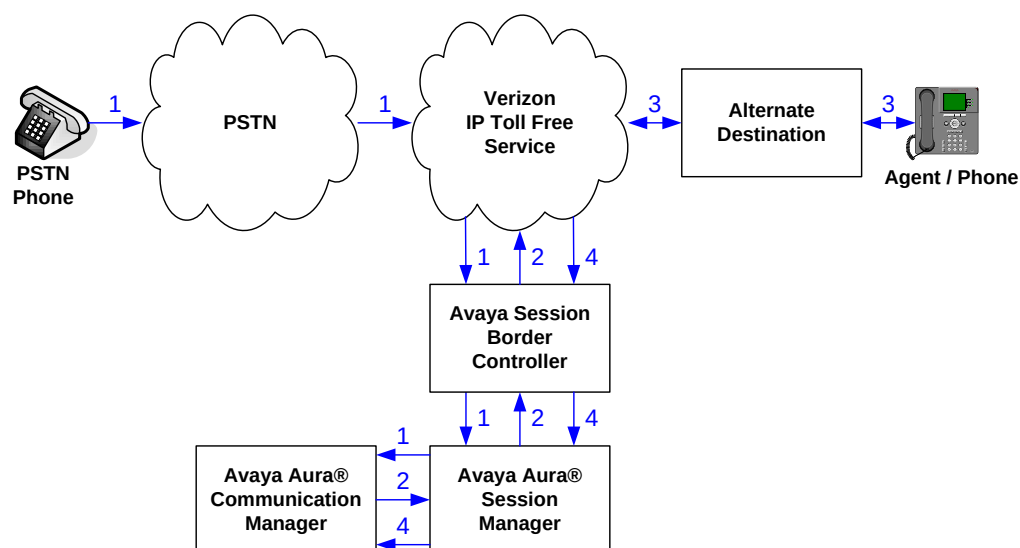


Figure 4: Inbound Verizon IP Toll Free– Post-Answer SIP REFER Redirection Successful

3.2.3 Inbound IP Toll Free Call with Unsuccessful Network Call Redirection

The next call scenario illustrated in **Figure 5** is similar to the previous call scenario, except that the redirection is unsuccessful. In theory, if redirection is successful, Communication Manager can “take the call back” and continue vector processing. For example, the call may route to an alternative agent, phone, or announcement after unsuccessful NCR.

1. Same as **Figure 4**.
2. Same as **Figure 4**.

3. The Verizon IP Toll Free service places a call to the target party (alternate destination), but the target party is busy or otherwise unavailable.
4. The Verizon IP Toll Free service notifies the redirecting/referring party (Communication Manager) of the error condition.
5. Communication Manager routes the call to a local agent, phone, or announcement.

However, as noted in **Section 2.2**, except for egregious configuration errors, this “REFER error handling” scenario could not be verified on the production Verizon circuit used for testing. On the production circuit, Verizon sends a SIP BYE which terminates Communication Manager vector processing for failure scenarios. For example, if a 486 Busy is received from the target of the REFER, Verizon will send a BYE immediately after a “NOTIFY/sipfrag 486”, which precludes any further call processing by Communication Manager. As another example, in cases where mis-configuration is introduced to cause the Refer-To header to be malformed (e.g., no “+” in Refer-To), Verizon will send a BYE immediately after a “NOTIFY/sipfrag 603 Server Internal Error”. If REFER is configured in the vector, but Network Call Redirection is not enabled for the SIP trunk group, Communication Manager will not send the REFER to Verizon, and vector processing will continue at the step following the route-to step that would normally trigger the REFER.

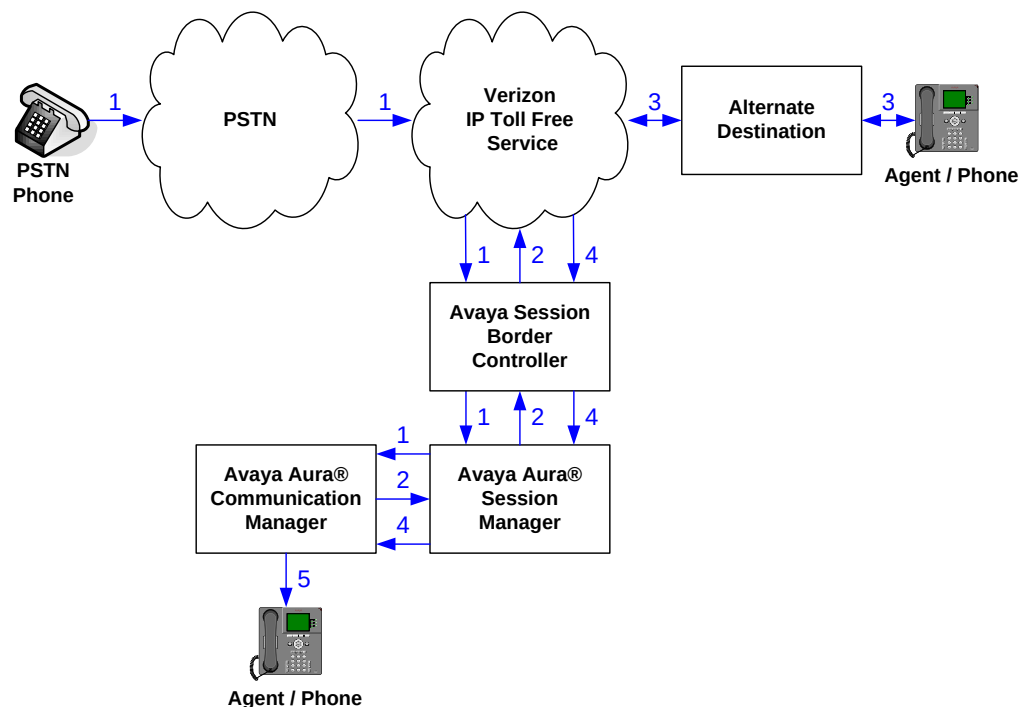


Figure 5: Inbound Verizon IP Toll Free– Post-Answer SIP REFER Redirection Unsuccessful

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	7.0-441.0-22477
Avaya Aura® System Manager	7.0.0.0.3929
Avaya Aura® Session Manager	7.0.0.0.700007
Avaya Session Border Controller for Enterprise	7.0.0-21-6602
Avaya Aura® Messaging	6.3.2 SP 2
Avaya Aura® Media Server	7.7.0.235
G450 Gateway	37.19.0
Avaya 96X1- Series Telephones (SIP)	R7.0.0.39
Avaya 96X1- Series Telephones (H323)	R6.2313
Avaya One-X Communicator	6.2.7
Avaya Communicator for Windows	2.1.2.75
Avaya 2400-Series and 6400-Series Digital Telephones	N/A

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager Release 7.0

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

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

5.1. Verify Licensed Features

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 IPCC Services and any other SIP applications. Each call from the Verizon Business IPCC Services to a non-SIP endpoint uses one SIP trunk for the duration of the call. Each call from Verizon Business IPCC Services to a SIP endpoint uses two SIP trunks for the duration of the call.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks: 4000		0	
Maximum Concurrently Registered IP Stations: 2400		1	
Maximum Administered Remote Office Trunks: 4000		0	
Maximum Concurrently Registered Remote Office Stations: 2400		0	
Maximum Concurrently Registered IP eCons: 68		0	
Max Concur Registered Unauthenticated H.323 Stations: 100		0	
Maximum Video Capable Stations: 2400		3	
Maximum Video Capable IP Softphones: 2400		4	
Maximum Administered SIP Trunks: 4000		30	
Maximum Administered Ad-hoc Video Conferencing Ports: 4000		0	
Maximum Number of DS1 Boards with Echo Cancellation: 80		0	

On **Page 4** of the *display system-parameters customer-options* form, verify that **ARS** is enabled.

display system-parameters customer-options		Page	4 of 12
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 5** 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 will be required verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

display system-parameters customer-options		Page 5 of 12
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	ISDN-BRI Trunks? y
Enterprise Survivable Server? n		ISDN-PRI? y
Enterprise Wide Licensing? n		Local Survivable Processor? n
ESS Administration? y		Malicious Call Trace? y
Extended Cvg/Fwd Admin? y		Media Encryption Over IP? n
External Device Alarm Admin? y		Mode Code for Centralized Voice Mail? n
Five Port Networks Max Per MCC? n		
Flexible Billing? n		Multifrequency Signaling? y
Forced Entry of Account Codes? y		Multimedia Call Handling (Basic)? y
Global Call Classification? y		Multimedia Call Handling (Enhanced)? y
Hospitality (Basic)? y		Multimedia IP SIP Trunking? y
Hospitality (G3V3 Enhancements)? y		
IP Trunks? y		
IP Attendant Consoles? y		

On **Page 6** 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 6 of 12
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		Wideband Switching? y
Processor Ethernet? y		Wireless? n
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

```

display system-parameters customer-options
CALL CENTER OPTIONAL FEATURES

Call Center Release: 7.0

ACD? y
BCMS (Basic)? y
BCMS/VuStats Service Level? y
BSR Local Treatment for IP & ISDN? y
Business Advocate? n
Call Work Codes? y
DTMF Feedback Signals For VRU? y
Dynamic Advocate? n
Expert Agent Selection (EAS)? y
EAS-PHD? y
Forced ACD Calls? n
Least Occupied Agent? y
Lookahead Interflow (LAI)? y
Multiple Call Handling (On Request)? y
Multiple Call Handling (Forced)? y
PASTE (Display PBX Data on Phone)? y

Reason Codes? y
Service Level Maximizer? n
Service Observing (Basic)? y
Service Observing (Remote/By FAC)? y
Service Observing (VDNs)? y
Timed ACW? y
Vectoring (Basic)? y
Vectoring (Prompting)? y
Vectoring (G3V4 Enhanced)? y
Vectoring (3.0 Enhanced)? y
Vectoring (ANI/II-Digits Routing)? y
Vectoring (G3V4 Advanced Routing)? y
Vectoring (CINFO)? y
Vectoring (Best Service Routing)? y
Vectoring (Holidays)? y
Vectoring (Variables)? y

```

```

display system-parameters customer-options
CALL CENTER OPTIONAL FEATURES

V   VDN of Origin Announcement? y
V   VDN Return Destination? y
V   VuStats? y
V   VuStats (G3V4 Enhanced)? y

V   Logged-In ACD Agents: 500
V   Logged-In Advocate Agents: 500
V   Logged-In IP Softphone Agents: 500
V   Logged-In SIP EAS Agents: 50
V   USED
V   1
V   0
V   0
V   0

```

5.2. Dial Plan

In the reference configuration the Avaya CPE environment uses five digit local extensions, such as 12xxx, 14xxx or 20xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with *. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

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

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

5.3. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following ***change node-names ip*** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is “**SM**” with IP address **10.64.91.61**. The node name and IP address for the Processor Ethernet “**procr**” is **10.64.61.65**.

change node-names ip		IP NODE NAMES		Page 1 of 2	
Name	IP Address				
AMS	10.64.91.60				
SM	10.64.91.61				
default	0.0.0.0				
procr	10.64.91.65				
procr6	::				

5.4. Processor Ethernet Configuration

The ***add ip-interface procr*** or ***change ip-interface procr*** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the 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: 4800
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: 10.64.91.65	
Subnet Mask: /24		

5.5. Network Regions

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 2 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 Processor Ethernet (10.64.91.65), and that the gateway IP address is 10.64.91.81. These fields are not configured in this screen, but just display the current information for the Media Gateway.

change media-gateway 1		Page 1 of 2
MEDIA GATEWAY 1		
Type: g450		
Name: G450-1		
Serial No: 08IS38199678		
Link Encryption Type: any-ptls/tls	Enable CF? n	
Network Region: 1	Location: 1	
	Site Data:	
Recovery Rule: 1		
Registered? y		
FW Version/HW Vintage: 36 .14 .0 /1		
MGP IPV4 Address: 10.64.91.81		
MGP IPV6 Address:		
Controller IP Address: 10.64.91.65		
MAC Address: 00:1b:4f:03:52:18		

The following screen shows **Page 2** for **Media Gateway 1**. The gateway has an **MM712** media module supporting Avaya digital phones in slot V2, an **MM711** supporting analog devices in slot V3, and the capability to provide announcements and music on hold via **gateway-announcements** in logical slot V9.

change media-gateway 1		MEDIA GATEWAY 1		Page 2 of 2	
		Type: g450			
Slot	Module Type	Name	DSP Type	FW/HW version	
V1:			MP80	134 3	
V2:	MM712	DCP MM			
V3:	MM711	ANA MM			
V4:					
V5:					
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 10.64.91.39 would be mapped to network region 1, based on the configuration in bold below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map		IP ADDRESS MAPPING		Page 1 of 63	
		Subnet	Network	Emergency	
IP Address		Bits	Region	VLAN	Location Ext
-----		-----	-----	-----	-----
FROM: 10.64.91.30		/	1	n	
TO: 10.64.91.49					

The following screen shows IP Network Region 2 configuration. In the shared test environment, network region 2 is used to allow unique behaviors for the Verizon IPCC test environment. In this example, codec set 2 will be used for calls within region 2. The shared Avaya Interoperability Lab test environment uses the domain “**avayalab.com**” (i.e., for network region 1 including the region of the Processor Ethernet “procr”). Session Manager also uses this domain to determined routes for calls based on the domain information of the calls and for SIP phone registration.

```
change ip-network-region 2                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location: 1      Authoritative Domain: avayalab.com
Name: SIP TRUNK      Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2      Inter-region IP-IP Direct Audio: yes
      UDP Port Min: 2048      IP Audio Hairpinning? n
      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
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 2. The first bold row shows that network region 2 is directly connected to network region 1, and that codec set 2 will also be used for any connections between region 2 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 2 for region 2 to region 1 connectivity.

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

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 2 will be used for connections between region 1 and region 2 as noted previously.

```

change ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: avayalab.com
Name: Enterprise Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
Codec Set: 1          IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5

```

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 2, and that codec set 2 will be used for any connections between region 2 and region 1.

```

change ip-network-region 1                                     Page 4 of 20

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

```

5.6. IP Codec Sets

The following screen shows the configuration for codec set 2, the codec set configured to be used for calls within region 2 and for calls between region 1 and region 2. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls with Verizon IPCC via the SIP trunks would prefer to use **G.729A**, but also be capable of using **G.711MU**.

change ip-codec-set 2 Page 1 of 2

IP CODEC SET

Codec Set: 2

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.729A	n	2	20
2: G.711MU	n	2	20
3:			
4:			

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

change ip-codec-set 2 Page 2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? y

Maximum Call Rate for Direct-IP Multimedia: 384:Kbits

Maximum Call Rate for Priority Direct-IP Multimedia: 384:Kbits

	Mode	Redundancy	Packet Size(ms)
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Although codec set 1 is not used for connections with Verizon IPCC, the following screen shows the configuration for codec set 1. Codec set 1 is used for local Avaya CPE 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: G.729A	n	2	20
3:			

5.7. SIP Signaling Group

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM”. In the example screens, the **Transport Method** for all signaling groups is “tls”. 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 “avayalab.com” matching the configuration in place prior to adding the Verizon IP SIP Trunking configuration. 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 2. Signaling group 2 will be used for processing incoming calls from Verizon IPCC via Session Manager. The **Far-end Network Region** is configured to region “2”. Port “5071” 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 toll-free numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5071. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. Other parameters may be left at default values.

change signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr		Far-end Node Name: SM
Near-end Listen Port: 5071		Far-end Listen Port: 5071
		Far-end Network Region: 2
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

The following screen shows signaling group 3, the signaling group to Session Manager that was in place prior to adding the Verizon IPCC configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon IPCC but will be used to enable SIP phones to register to Session Manager and to use features from Communication Manager. Again, the **Near-end Node Name** is “**procr**” and the **Far-end Node Name** is “**SM**”, the node name of the Session Manager. Unlike the signaling group used for the Verizon IPCC 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.

change signaling-group 3		Page 1 of 2
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y Peer Server: SM		
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.8. SIP Trunk Group

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

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

The following shows **Page 1** for trunk group 2, which will be used for incoming and outgoing PSTN calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field is set to “**public-ntwrk**” for the trunks that will handle calls with Verizon. Although not strictly necessary, the **Direction** has been configured to “incoming” to emphasize that trunk group 1 is used for incoming calls only in the sample configuration.

change trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: Verizon IPCC	COR: 1	TN: 1	TAC: *02
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 2	
		Number of Members: 10	

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

change trunk-group 2	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	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 1xC: station-extension	

The following screen shows **Page 3** for trunk group 2. All parameters except those in bold are default values. The **Numbering Format** will use “**public**” numbering, meaning that the public numbering table would be consulted for any mappings of Communication Manager extensions to alternate numbers to be sent to Session Manager. Replacement text strings can be configured using the “system-parameters features” screen (page 9, not shown), such that incoming “private” (anonymous) or “restricted” calls can display a configurable text string on called party telephones. If it is desired to see the configurable replacement text strings on user displays, the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields may be set to “y”.

change trunk-group 2	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	
Hold/Unhold Notifications? y	
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

The following screen shows **Page 4** for trunk group 2. The bold fields have non-default values. Setting the **Network Call Redirection** flag to “y” enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal “send-only” media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor “send-only” media signaling is required, this field may be left at the default “n” value. In the testing associated with these Application Notes, the **Network Call Redirection** flag was set to “y” to allow REFER to be exercised with the Verizon Business IPCC Service. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting **Convert 180 to 183 for Early Media** 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.

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

change trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? n	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

The following screen shows **Page 1** for trunk group 3, 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 to enable SIP phones to use features from Communication Manager and to communicate with other Avaya applications, such as Avaya Aura® Messaging, and does not reflect any unique Verizon configuration.

change trunk-group 3		Page 1 of 21	
TRUNK GROUP			
Group Number: 3	Group Type: sip	CDR Reports: y	
Group Name: To SM Enterprise	COR: 1	TN: 1	TAC: *03
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 3	
		Number of Members: 20	

The following shows **Page 3** for trunk group 3. Note that this tie trunk group uses a “**private**” **Numbering Format**.

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

The following screen shows **Page 4** for trunk group 3. Note that unlike the trunks associated with Verizon calls that have non-default “protocol variations”, this trunk group maintains all default values. **Support Request History** must remain set to the default “**y**” to support proper subscriber mailbox identification by Avaya Aura® Messaging.

PROTOCOL VARIATIONS

```

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

                                Send Diversion Header? n
                                Support Request History? y
                                Telephone Event Payload Type: 120

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

Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits

```

5.9. Contact Center Configuration

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

5.9.1 Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command “**add announcement <extension>**”.

```
list announcement
```

ANNOUNCEMENTS/AUDIO SOURCES

Announcement Extension	Type	Name	Source Pt/Bd/Grp	Num of Files
11001	integrated	callcenter-main	001V9	1
11002	integ-mus	holdmusic	001V9	1
11003	integrated	disconnect	001V9	1
11004	integrated	no_agents	001V9	1
11005	integrated	dtmf_test	001V9	1
11006	integrated	please_wait	001V9	1
11007	integrated	REFER_Test	001V9	1

5.9.2 Post-Answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use post-answer redirection to a PSTN destination. A corresponding detailed verification is provided in **Section 9.1.2**. In this example, the inbound toll-free call is routed to VDN 10001 shown in the following screen. The originally dialed Verizon IP Toll Free number may be mapped to VDN 10001 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```
display vdn 10001                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 10001
      Name*: Refer-to-PSTN
      Destination: Vector Number 1
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none
```

VDN 10001 is associated with vector 1, which is shown below. Vector 1 plays an announcement (step 03) to answer the call. After the announcement, the “**route-to number**” (step 05) includes “~r+13035387024” where the number 303-538-7024 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes “+13035387024” as the user portion. Note that Verizon Business IPCC Services require the “+” in the Refer-To header for this type of call redirection.

```
display vector 1                                       Page 1 of 6
                                         CALL VECTOR

      Number: 1                                         Name: Refer-to-PSTN
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
      Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
      Variables? y      3.0 Enhanced? y
01 wait-time      2      secs hearing ringback
02 #      Play announcement to caller in step 3. This answers the call.
03 announcement 11006
04 #      Refer the call to PSTN Destination in step 5 below.
05 route-to      number ~r+13035387024      with cov n if unconditionally
06 #      If Refer fails queue to skill 1
07 queue-to      skill 1      pri m
08
```

5.9.3 Post-Answer Redirection With UUI to a SIP Destination

This section provides an example of post-answer redirection with UUI passed to a SIP destination. A corresponding detailed verification is provided in **Section 9.2.3**. In this example, the inbound call is routed to VDN 10003 shown in the following screen. The originally dialed Verizon toll-free

number may be mapped to VDN 10003 by Session Manager digit conversion, or via the incoming call handling treatment for the Communication Manager trunk group handling the call.

```

display vdn 10003                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

Extension: 10003
Name*: REFER with UII
Destination: Vector Number 3
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

```

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

```

change variables                                     Page 1 of 39
                                         VARIABLES FOR VECTORS

Var Description                                     Type Scope Length Start Assignment VAC
A uui                                                asaiuui L 16 1
B uui                                                asaiuui L 16 17
C

```

VDN 10003 is associated with vector 3, which is shown below. Vector 3 sets data in the vector variables A and B (steps 03 and 04) and plays an announcement to answer the call (step 05). After the announcement, the “route-to” number step includes “~r+18668512649”. This step causes a REFER message to be sent where the Refer-To header includes “+18668512649” as the user portion. The Refer-To header will also contain the UII set in variables A and B. Verizon will include this UII in the INVITE ultimately sent to the SIP-connected target of the REFER, which is toll-free number “18668512649”. In the sample configuration, where only one location was used, 866-851-2649 is another toll-free number assigned to the same circuit as the original call. In practice, NCR with UII would allow Communication Manager to send call or customer-related data along with the call to another contact center.

```

display vector 3                                     Page 1 of 6
                                         CALL VECTOR

Number: 3 Name: Refer-with-UII
Multimedia? n Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y 3.0 Enhanced? y
01 wait-time 2 secs hearing ringback
02 set A = none CATR 1234567890123456
03 set B = none CATR 7890123456789012
04 # Play announcement to answer call and route to ~r to cause Refer
05 announcement 11007
06 route-to number ~r+18668512649 with cov n if unconditionally
07 # If Refer fails play announcement and disconnect
08 disconnect after announcement 11003

```

5.9.4 ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt group, and agent logins used to queue inbound Verizon IPCC calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

```
display hunt-group 1                                     Page 1 of 4
HUNT GROUP
Group Number: 1                                         ACD? y
Group Name: Agent Group                               Queue? y
Group Extension: 19991                                 Vector? y
Group Type: ucd-mia
TN: 1
COR: 1
Security Code:                                         MM Early Answer? n
ISDN/SIP Caller Display:                             Local Agent Preference? n
Queue Limit: unlimited
```

The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note Skill is set to “y”.

display hunt-group 1	Page 2 of 4
HUNT GROUP	
Skill? y	Expected Call Handling Time (sec): 180
AAS? n	Service Level Target (% in sec): 80 in 20

VDN 10004, shown below, is associated with vector 4.

display vdn 10004	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 10004	
Name*: Sales	
Destination: Vector Number	4
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	

In this simple example, vector 4 briefly plays ring back, then queues the call to skill 1. Announcement 11004 is a simple recurring announcement. If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear the announcement. Once an agent becomes available, the call will be delivered to the agent.

display vector 4	Page 1 of 6
CALL VECTOR	
Number: 4 Name: Sales	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 # Wait hearing ringback	
02 wait-time 2 secs hearing ringback	
03 # Simple queue to skill with recurring announcement until available	
04 queue-to skill 1 pri m	
05 announcement 11004	
06 wait-time 30 secs hearing music	
07 goto step 5 if unconditionally	
08 stop	

The following screen illustrates an example agent-loginID 20001. In the sample configuration, an Avaya one-X® Deskphone logged in using agent-loginID 20001 and the configured Password to staff and take calls for skill 1.

```

change agent-loginID 20001                                     Page 1 of 2
                                AGENT LOGINID

      Login ID: 20001                                           AAS? n
      Name: Agent 1                                           AUDIX? n
      TN: 1           Check skill TNs to match agent TN? n
      COR: 1
      Coverage Path: 1                                           LWC Reception: spe
      Security Code:                                           LWC Log External Calls? n
      Attribute:                                           AUDIX Name for Messaging:

                                           LoginID for ISDN/SIP Display? n
                                           Password:
                                           Password (enter again):
                                           Auto Answer: station
                                           MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                           Logout Reason Code Type: system

```

The following abridged screen shows Page 2 for agent-loginID 20001. Note that the Skill Number (SN) has been set to 1.

```

change agent-loginID 20001                                     Page 2 of 2
                                AGENT LOGINID

      Direct Agent Skill:                                           Service Objective? n
      Call Handling Preference: skill-level                         Local Call Preference? n

      SN   RL SL           SN   RL SL           31:           46:
      1: 1       1       16:           32:           47:
      2:           17:           33:           48:
      3:           18:

```

To enable a telephone or one-X® Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to “y” as shown in the screen below.

```

change system-parameters features                             Page 11 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
      CALL CENTER SYSTEM PARAMETERS
      EAS
      Expert Agent Selection (EAS) Enabled? y
      Minimum Agent-LoginID Password Length: 4

```

5.10. Public Numbering

The *change public-unknown-numbering* command may be used to define the format of numbers sent to Verizon in SIP headers such as the “Contact” and “P-Asserted-Identity” headers.

In the bolded rows shown in the example abridged output below, entries are made for the specific Communication Manager Vector Directory Numbers (VDN) illustrated in the prior section.

Without this configuration, calls to the VDNs would result in a 5-digit user portion of the Contact header in the 183 with SDP and 200 OK returned to Verizon. Although this did not present any user-perceivable problem in the sample configuration, the configuration in the bolded rows below illustrate how to cause Communication Manager to populate the Contact header with user portions that correspond with a Verizon Business IPCC number. In the course of the testing, multiple Verizon toll-free numbers were associated with different Communication Manager extensions and functions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	10001		18668523221	11	Total Administered: 16
5	10003		18668510107	11	Maximum Entries: 240
5	10004		18668502380	11	Note: If an entry applies to

5.11. 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 Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table is not necessary. In alternative configurations, if the toll-free number sent by Verizon was not changed before reaching Communication Manager, then the Verizon Business IPCC number could be mapped to a Communication Manager extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of toll-free number 8668502380 to extension 14000 when the call arrives on trunk group 2.

change inc-call-handling-trmt trunk-group 2					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			
public-ntwrk	10	8668502380	10	14000	

5.12. Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 120xx. Since this configuration is not unique to Verizon, a minimum of information is presented simply to assist in understanding verification traces presented in subsequent sections.

The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone also used by Avaya one-X® Communicator. Call appearances and desired features (e.g., call forwarding, EC500, etc.) can be assigned to the station on page 4 (not shown).

change station 12002		Page 1 of 5
STATION		
Extension: 12002	Lock Messages? n	BCC: 0
Type: 9621	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: 9621 IP Phone	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 12002	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? y	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

The following abbreviated screen shows an example extension used by an Avaya one-X® Agent client. Call appearances and appropriate features (e.g., uui-info, aux-work, etc.) can be assigned on page 4 (not shown).

change station 12003		Page 1 of 5
STATION		
Extension: 12003	Lock Messages? n	BCC: 0
Type: 9641	Security Code: *	TN: 1
Port: S00002	Coverage Path 1:	COR: 1
Name: Test Agent	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 12003	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	

5.13. Saving Communication Manager Configuration Changes

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

```
save translation all
```

6. Configure Avaya Aura® Session Manager Release 7.0

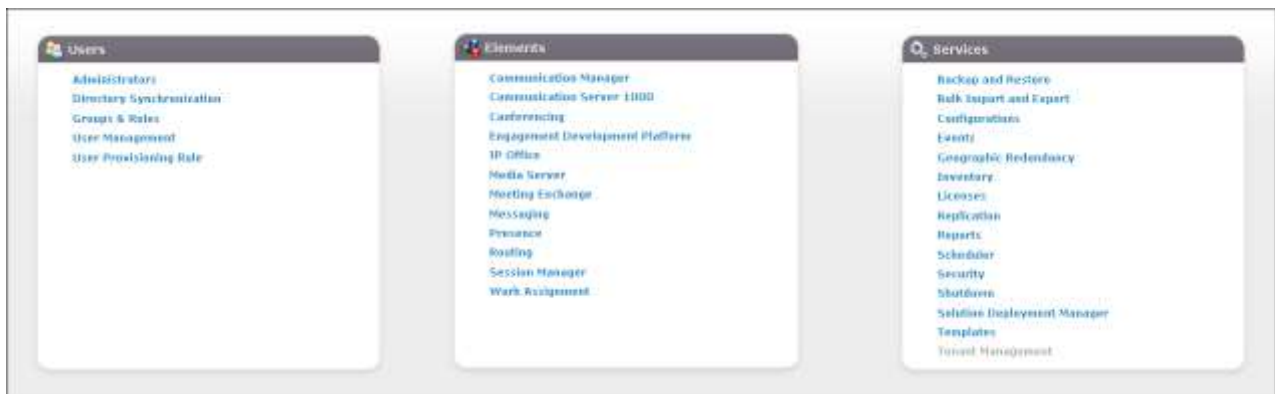
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

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

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



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



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

Introduction to Network Routing Policy

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

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

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"
- (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

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

Step 9: Create "Regular Expressions"

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

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

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

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

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

- Step 7: "Routing Policies" are defined
- Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)
- Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

6.1. Domains

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

The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among other Avaya interoperability test efforts. The domain “avayalab.com” was used for communication with Avaya SIP Telephones and other

Avaya systems and applications. The domain “avayalab.com” is not known to the Verizon production service.

The 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 From and P-Asserted-Identity headers in the INVITE message sent to Verizon.



Home / Elements / Routing / Domains

Domain Management

New Edit Delete Disable More Actions

3 Items Filter: Enable

Name	Type	Notes
adevc.avaya.globalipcom.com	sip	CEF Domain known by Verizon
avayalab.com	sip	Avaya STL Domain

Select : All, None

6.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button (not shown) after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.



Home / Elements / Routing / Locations

Location

New Edit Delete Disable More Actions

3 Items Filter: Enable

Name	Correlation	Notes
Avaya Denver	☐	Avaya STL
RemoteAccess	☐	Remote Access from SBCE1
Vz-ASBCE	☐	SBC to Verizon

Select : All, None

The following screen shows the location details for the location named “**Vz-ASBCE**”, corresponding to the Avaya SBCE relevant to these Application Notes. Later, the location with name “**Vz-ASBCE**” will be assigned to the corresponding Avaya SBCE SIP Entity.

The **Location Pattern** is used to identify call routing based on IP address. Session Manager matches the IP address of SIP Entities against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the Location administered in the SIP Entity form. In this sample configuration Locations are added to SIP Entities in **Section 6.4**, so it was not necessary to add a pattern.

The screenshot shows the 'Location Details' configuration page for a location named 'Vz-ASBCE'. The page is divided into several sections:

- General:** Contains fields for 'Name' (Vz-ASBCE) and 'Notes' (SBCE to Verizon). There are 'Commit' and 'Cancel' buttons.
- Dial Plan Transparency in Survivable Mode:** Includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth:** Includes a 'Managed Bandwidth Units' dropdown (set to Kbit/sec), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.
- Per-Call Bandwidth Parameters:** Includes fields for 'Maximum Multimedia Bandwidth (Intra-Location):' (2000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location):' (2000 Kbit/Sec), '* Minimum Multimedia Bandwidth:' (64 Kbit/Sec), and '* Default Audio Bandwidth:' (80 Kbit/Sec).
- Alarm Threshold:** Includes 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' (both set to 80 %), and latency fields for both (both set to 5 Minutes).
- Location Pattern:** A table with columns for 'IP Address Pattern' and 'Notes'. It shows 0 items and has 'Add' and 'Remove' buttons. A 'Filter: Enable' button is also present.

The following screen shows the location details for the location named “**Avaya Denver**”, corresponding to SIP entities within the enterprise. Later, the location with name “**Avaya Denver**” will be assigned to the corresponding Communication Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.

Location Details Commit Cancel Help ?

General

* Name:

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

* Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth: Kbit/Sec

Alarm Threshold

Overall Alarm Threshold: %

Multimedia Alarm Threshold: %

* Latency before Overall Alarm Trigger: Minutes

* Latency before Multimedia Alarm Trigger: Minutes

Location Pattern

0 Items Filter: Enable

IP Address Pattern	Notes
--------------------	-------

6.3. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed (not shown).



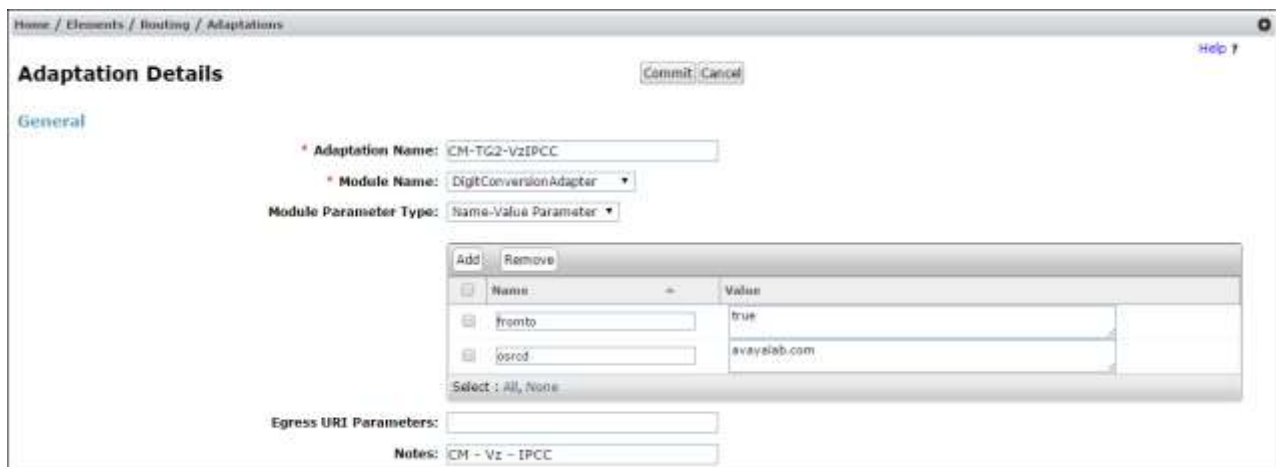
The screenshot shows the 'Adaptations' page in the Avaya Element Manager. It features a table with 14 items. The table has columns for Name, Module Name, Module Parameters, Egress URI Parameters, and Notes. The first three items are highlighted: CM-TG1-VzIPT, CM-TG2-VzIPCC, and Verizon-SBC. The CM-TG2-VzIPCC item is selected, and its details are shown in the table.

Name	Module Name	Module Parameters	Egress URI Parameters	Notes
CM-TG1-VzIPT	DigitConversionAdapter	fromto=true osrcd=avayalab.com		CM - V2 - IPT
CM-TG2-VzIPCC	DigitConversionAdapter	fromto=true osrcd=avayalab.com		CM - V2 - IPCC
Verizon-SBC	VerizonAdapter	fromto=true sRhdns="AV-Global-Session-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, P-Charana-Vector, P-Location"		SBC - Verizon IPT

The adapter named “CM-TG2-VzIPCC” shown in the following screen will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Verizon Business IPCC service. This adaptation uses the “DigitConversionAdapter” and specifies the following parameters:

- **Name: “fromto” Value: “true”**
 - This adapts the From and To headers along with the Request-Line and PAI headers.
- **Name: “osrcd” Value: “avayalab.com”**
 - This enables the source domain to be overwritten with “avayalab.com”. For example, for inbound PSTN calls from Verizon to Communication Manager, the PAI header will contain “avayalab.com”.

Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.



The screenshot shows the 'Adaptation Details' form for the 'CM-TG2-VzIPCC' adaptation. The form includes fields for Adaptation Name, Module Name, and Module Parameter Type. Below these is a table for adding parameters. The 'fromto' parameter is set to 'true' and the 'osrcd' parameter is set to 'avayalab.com'. There are also fields for Egress URI Parameters and Notes.

Name	Value
fromto	true
osrcd	avayalab.com

Scrolling down, the following screen shows a portion of the “**CM-TG2-VzIPCC**” adapter that can be used to convert digits between the Communication Manager extension numbers (user extensions, VDNs) and the toll-free numbers assigned by Verizon.

An example portion of the settings for “**Digit Conversion for Outgoing Calls from SM**” (i.e., inbound to Communication Manager) is shown below.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
*	12	12		*		origination		E.164 Calling Number Conversion
8668502380	10	10		*	10004	destination		Call Center
8668506850	10	10		*	14000	destination		DTHF Test
8668510107	10	10		*	10003	destination		REFER with UII
8668512649	10	10		*	12003	destination		Refer-To Target of UII Test VDN
8668523221	10	10		*	10001	destination		Refer-To PSTN Test VDN

In general, digit conversion such as this that converts a Verizon Business IPCC number to a Communication Manager extension can be performed in Communication Manager or in Session Manager. In the example screens shown above, before sending the SIP INVITE to Communication Manager, Session Manager would adapt a dialed number of 8668510107 to the VDN 10003 associated with testing Refer with UII. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the toll-free number to its corresponding extension.

The adapter named “**Verizon-SBC**” shown below will later be assigned to the SIP Entity for the Avaya SBCE, specifying that all communication from Session Manager to the Avaya SBCE will use this adapter.

This adaptation uses the “**VerizonAdapter**” module and specifies the “**eRHdrs**” and “**fromto**” parameters. The “**eRHdrs**” parameter will remove the specified headers during adaptation in the egress direction. In the sample configuration, unnecessary headers were removed to reduce the size of the SIP message to prevent packet fragmentation by adding the following **Value**, including the quotes, “**AV-Global-Sesison-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, PCharging-vector, P-Location**”.

The screenshot shows the 'Adaptation Details' window with the following configuration:

- Adaptation Name:** Verizon-SBC
- Module Name:** VerizonAdapter
- Module Parameter Type:** Name-Value Parameter
- Parameters:**

Name	Value
eRHdrs	"AV-Global-Sesison-ID, Alert-Info, Endpoint-View, P-AV-Message-Id, PCharging-vector, P-Location"
- Egress URI Parameters:** (Empty)
- Notes:** SBC - Verizon

6.4. SIP Entities

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

The following screen shows the list of configured SIP entities in the shared test environment.

Name	FQDN or IP Address	Type	Notes
Aura Messaging	10.64.91.54	Modular Messaging	Aura Messaging
CM-TG1	10.64.91.65	CM	Trunk Group 1 - CM to Vz-IPT
CM-TG2	10.64.91.65	CM	Trunk Group 2 - Toll-Free Inbound
CM-TG3	10.64.91.65	CM	Trunk Group 3 - CM to Enterprise
SessionManager	10.64.91.61	Session Manager	Session Manager
Vz-SBC-1	10.64.91.50	SIP Trunk	Avaya SBC-1 to Verizon

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “**SessionManager**”. The **FQDN or IP Address** field for “**SessionManager**” is the Session Manager Security Module IP Address (10.64.91.61), 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 test environment, the Session Manager used location “**Avaya Denver**”. 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.

Home / Elements / Routing / SIP Entities

Help ?

SIP Entity Details

CommitCancel

General

* Name:

SessionManager

* FQDN or IP Address:

10.64.91.61

Type:

Session Manager

Notes:

Session Manager

Location:

Avaya Denver

Outbound Proxy:

Time Zone:

America/Denver

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 “**SessionManager**”. The links relevant to these Application Notes are described in the subsequent section.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
SM to AAM	SessionManager	TCP	5060	Aura Messaging	5060	trusted	☐
SM to CM TG1	SessionManager	TLS	5081	CM-TG1	5081	trusted	☐
SM to CM TG2	SessionManager	TLS	5071	CM-TG2	5071	trusted	☐
SM to CM TG3	SessionManager	TLS	5061	CM-TG3	5061	trusted	☐
SM to V2-SBC1	SessionManager	TCP	5060	V2-SBC1	5060	trusted	☐

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, illustrating the configured ports for “**SessionManager**”. This section is only present for Session Manager SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

Listen Ports	Protocol	Default Domain	Notes
5060	TCP	avayalab.com	
5060	UDP	avayalab.com	
5061	TLS	avayalab.com	

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “**Vz-SBC-1**”. The **FQDN or IP Address** field is configured with the Avaya SBCE inside IP Address (**10.64.91.50**). “**SIP Trunk**” is selected from the **Type** drop-down menu for Avaya SBCE SIP Entities. This Avaya SBCE has been assigned to **Location “Vz-ASBCE”**, and the “**Verizon-SBC**” adapter is applied. Other parameters (not shown) retain default values.

The screenshot shows the 'SIP Entity Details' window for 'Vz-SBC-1'. The 'General' tab is active. Fields include: Name (Vz-SBC-1), FQDN or IP Address (10.64.91.50), Type (SIP Trunk), Notes (Avaya SBC-1 to Verizon), Adaptation (verizon-SBC), Location (Vz-ASBCE), Time Zone (America/Denver), SIP Timer B/F (in seconds) (4), Credential name (empty), Securable (unchecked), Call Detail Recording (egress), Loop Detection Mode (Off), and SIP Link Monitoring (Use Session Manager Configuration).

The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named “**CM-TG3**”. This is the SIP Entity that was already in place in the Avaya Interoperability Test Lab environment, prior to adding the Verizon Business IPCC configuration. The **FQDN or IP Address** field contains the IP Address of the “processor Ethernet” (**10.64.91.65**). “**CM**” is selected from the **Type** drop-down menu and “**Avaya Denver**” is selected for the **Location**.

The screenshot shows the 'SIP Entity Details' window for 'CM-TG3'. The 'General' tab is active. Fields include: Name (CM-TG3), FQDN or IP Address (10.64.91.65), Type (CM), Notes (Trunk Group 3 - CM to Enterprise), Adaptation (empty), Location (Avaya Denver), Time Zone (America/Denver), SIP Timer B/F (in seconds) (4), Credential name (empty), Securable (unchecked), Call Detail Recording (none), Loop Detection Mode (Off), and SIP Link Monitoring (Use Session Manager Configuration).

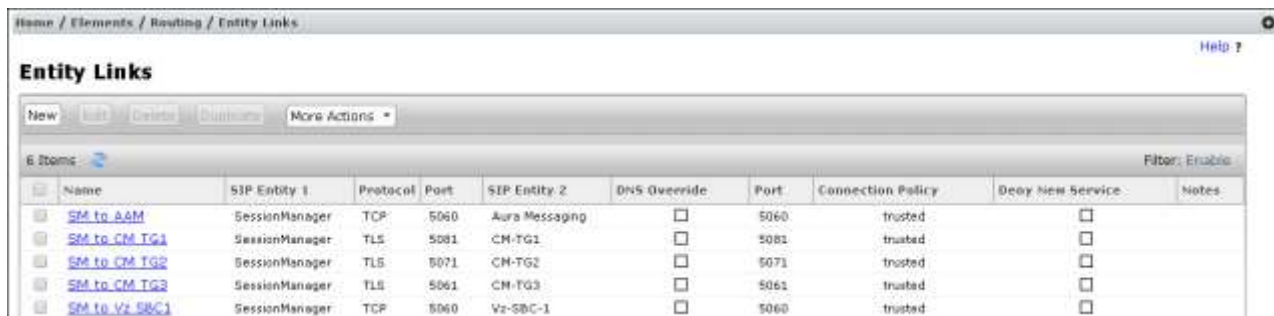
The following screen shows the **SIP Entity Details** for an entity named “**CM-TG2**”. This entity uses the same **FQDN or IP Address (10.64.91.65)** as the prior entity with name “**CM-TG3**”; both correspond to Communication Manager processor Ethernet IP address. Later, a unique port, 5071, will be used for the Entity Link to “**CM-TG2**”. Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon Business IPCC from other SIP traffic arriving from the same IP Address of the Session Manager, such as SIP traffic associated with SIP Telephones or other SIP-integrated applications. “**CM**” is selected from the **Type** drop-down menu. The **Adaptation** “**CM-TG2-VzIPCC**” is applied to this SIP entity. Recall that this adapter is used to map the Verizon Business IPCC toll-free numbers to the corresponding Communication Manager extensions. “**Avaya Denver**” is selected for the **Location**.

The screenshot shows the 'SIP Entity Details' configuration window for an entity named 'CM-TG2'. The window has a title bar with 'Phone / Elements / Routing / SIP Entities' and a 'Help ?' button. The main content area is divided into three sections: 'General', 'Loop Detection', and 'SIP Link Monitoring'. The 'General' section contains the following fields: 'Name' (CM-TG2), 'FQDN or IP Address' (10.64.91.65), 'Type' (CM), 'Notes' (Trunk Group 2 - Toll-Free Inbound), 'Adaptation' (CM-TG2-VzIPCC), 'Location' (Avaya Denver), 'Time Zone' (America/Fortaleza), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), 'Securable' (checkbox), 'Call Detail Recording' (none), and 'Loop Detection Mode' (Off). The 'SIP Link Monitoring' section contains 'SIP Link Monitoring' (Use Session Manager Configuration). The 'Commit' and 'Cancel' buttons are at the top right.

6.5. Entity Links

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

The following screen shows a list of configured links. In the screen below, the links named “**SM to Vz-SBC-1**” and “**SM to CM-TG2**” are most relevant to these Application Notes. Each link uses the entity named “**SessionManager**” as **SIP Entity 1**, and the appropriate entity, such as “**Vz-SBC-1**”, for **SIP Entity 2**. Note that there are multiple SIP Entity Links, using different TLS ports, linking the same “**SessionManager**” with the processor Ethernet of Communication Manager. For example, for one link named “**SM to CM-TG3**”, both entities use TLS and port 5061. For the entity link used by Verizon Business IPCC named “**SM to CM-TG2**”, both entities use TLS and port 5071.



Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Delay New Service	Notes
SM to AGM	SessionManager	TCP	5060	Aura Messaging	☐	5060	trusted	☐	
SM to CM-TG1	SessionManager	TLS	5081	CM-TG1	☐	5081	trusted	☐	
SM to CM-TG2	SessionManager	TLS	5071	CM-TG2	☐	5071	trusted	☐	
SM to CM-TG3	SessionManager	TLS	5061	CM-TG3	☐	5061	trusted	☐	
SM to Vz-SBC-1	SessionManager	TCP	5060	Vz-SBC-1	☐	5060	trusted	☐	

The link named “**SM to CM-TG3**” links Session Manager “**SessionManager**” with Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Verizon Business IPCC-related configuration. This link, using port 5061, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager.

The link named “**SM to CM-TG2**” also links Session Manager “**SessionManager**” with Communication Manager processor Ethernet. However, this link uses port 5071 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon Business IPCC from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

6.6. Time Ranges

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

Home / Elements / Routing / Time Ranges [Help ?](#)

Time Ranges

[New](#) [Edit](#) [Delete](#) [Duplicate](#) [More Actions](#)

1 Item | [Refresh](#) [Filter: Enable](#)

☐	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
☐	24/7	☒	☒	☒	☒	☒	☒	☒	00:00	23:59	Time Range 24/7

Select : All, None

6.7. Routing Policies

To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click the **Commit** button after changes are completed (not shown).

The following screen shows the **Routing Policy Details** for the policy named “To CM TG2” associated with incoming toll-free calls from Verizon Business IPCC to Communication Manager. Observe the **SIP Entity as Destination** is the entity named “CM-TG2”.

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

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

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select	Name	FQDN or IP Address	Type	Notes
☐	CM-TG2	10.64.51.65	CM	Trunk Group 2 - Toll-Free inbound

Time of Day

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

1 Item | [Filter: Enable](#)

☐	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
☐	0	24/7	☒	☒	☒	☒	☒	☒	☒	00:00	23:59	

Select : All, None

6.8. 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 toll-free number such as 866-850-2380, Verizon delivers the number to the enterprise, and the Avaya SBCE sends the call to Session Manager. The dial pattern below matches on 866-850-2380 specifically. Dial patterns can alternatively match on ranges of numbers. Under **Originating Locations and Routing Policies**, the routing policy named “**To CM TG2**” is chosen when the call originates from **Originating Location Name** “**Vz-ASBCE**”. This sends the call to Communication Manager using port 5071 as described previously.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Vz-ASBCE	SBC to Verizon	To CM TG2	0	☐	CM-TG2	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise Release 7.0

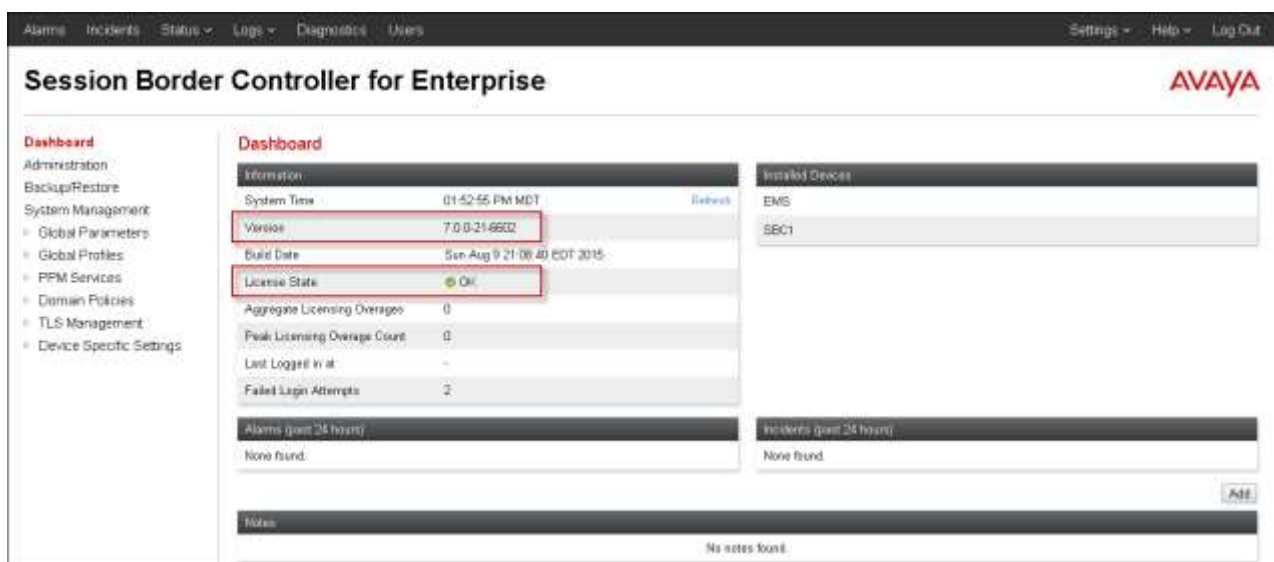
These Application Notes assume that the installation of the Avaya SBCE and the assignment of all IP addresses have already been completed, including the management IP address.

In the sample configuration, the management IP is 10.64.90.50. Access the web management interface by entering `https://<ip-address>` where `<ip-address>` is the management IP address assigned during installation. Log in with the appropriate credentials. Click **Log In**.



The login page features the Avaya logo and the text "Session Border Controller for Enterprise". It includes a "Log In" section with fields for "Username" (containing "UCSEC") and "Password" (containing "XXXXXXXXXX"), and a "Log In" button. Below the login fields, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The use of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and/or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Another disclaimer states: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." A final note says: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 2011 - 2015 Avaya Inc. All rights reserved."

The main page of the Avaya SBCE will appear. Note that the installed software version is displayed. Verify that the **License State** is “OK”. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



The dashboard shows the "Session Border Controller for Enterprise" title and the Avaya logo. It has a navigation menu on the left with options like "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "PPM Services", "Domain Policies", "TLS Management", and "Device Specific Settings". The main content area is titled "Dashboard" and contains several sections: "Information" with fields for "System Time" (01:52:55 PM MDT), "Version" (7.0.0-21.6602), "Build Date" (Sun Aug 9 21:08:40 EDT 2015), "License State" (OK), "Aggregate Licensing Overages" (0), "Peak Licensing Overage Count" (0), "Last Logged in at" (-), and "Failed Login Attempts" (2); "Installed Devices" with "EMS" and "SBC1"; "Alarms (past 24 hours)" (None found); "Incidents (past 24 hours)" (None found); and "Notes" (No notes found).

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named “SBC1” is shown. To view the configuration of this device, click **View** as highlighted below.



The **System Information** screen shows the **Network Settings**, **DNS Configuration**, and **Management IP** information provided during installation and corresponds to **Figure 1**. The highlighted **A1** and **B1** IP addresses are the ones relevant to the configuration of the SIP trunk to Verizon. Other IP addresses assigned to these interfaces and interface **B2** on the screen below are used to support remote workers and are not the focus of these Application Notes. Note that the **Management IP** must be on a separate subnet from the IP interfaces designated for SIP traffic.

System Information: SBC1

General Configuration

Appliance Name	SBC1
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions	500
Requested: 500	
Advanced Sessions	500
Requested: 500	
Scopia Video Sessions	0
Requested: 500	
CES Sessions	0
Requested: 0	
Encryption	☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.64.91.49	10.64.91.49	255.255.255.0	10.64.91.1	A1
10.64.91.50	10.64.91.50	255.255.255.0	10.64.91.1	A1
1.1.1.2	1.1.1.2	255.255.255.0	1.1.1.1	B1
192.168.80.72	192.168.80.72	255.255.255.128	192.168.80.1	B2
192.168.80.92	192.168.80.92	255.255.255.128	192.168.80.1	B2

DNS Configuration

Primary DNS	10.64.19.201
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.64.91.50

Management IP(s)

IP	10.64.90.50
----	-------------

7.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the internal interface is assigned to **A1** and the external interface is assigned to **B1**.



The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle State** button.



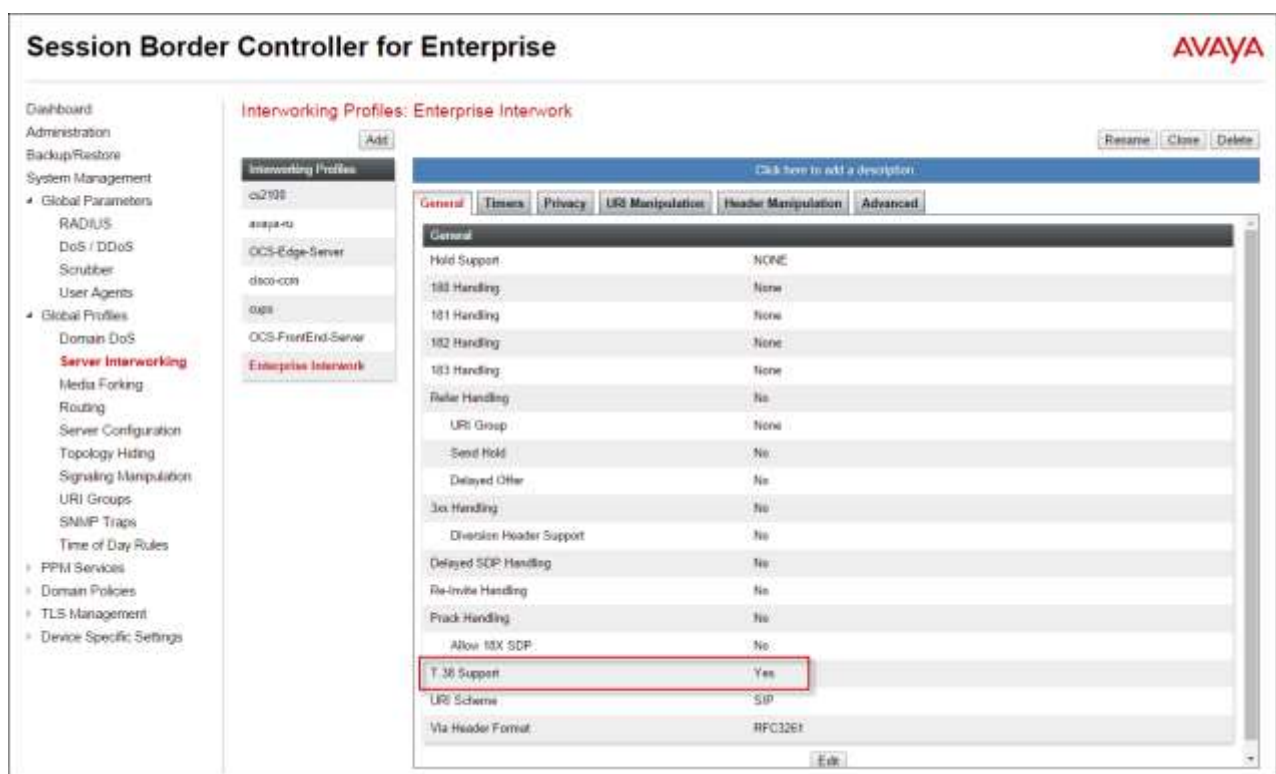
7.2. Server Interworking Profile

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing.

In the sample configuration, a single server interworking profile was created to define the connection to Session Manager. The Session Manager server interworking profile was cloned from the default **avaya-ru** profile. To clone a server interworking profile for, navigate to **Global Profiles → Server Interworking**, select the “**avayu-ru**” profile and click the **Clone** button. Enter a **Clone Name** and click **Finish** to continue.



The following screen shows the “**Enterprise Interwork**” profile used in the sample configuration, with **T.38 Support** set to “**Yes**”. To modify the profile, scroll down to the bottom of the screen and click **Edit**. Select the **T.38 Support** parameter and then click **Next** and then **Finish** (not shown). Default values can be used for all other fields.



7.3. Signaling Manipulation

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

The sample script show below is used to remove the “**gsid**” and “**epv**” parameters Session Manager places in the Contact header. These parameters contain unnecessary information for Verizon, including the internal domain. Removing these parameters helps to mask the internal topology of the enterprise and reduces the size of the SIP packet sent to Verizon. The Endpoint-View header and other proprietary headers are removed using an adaptation as illustrated in **Section Error! Reference source not found.**

To create a new Signaling Manipulation, navigate to **Global Profiles** → **Signaling Manipulation** and click on **Add**. A new blank SigMa Editor window will pop up.

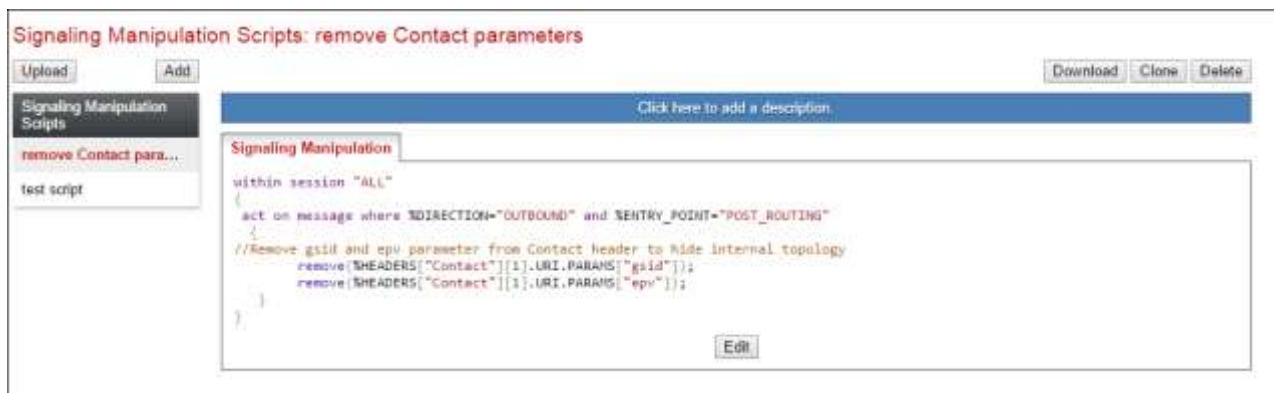


The following screen illustrates the “**remove Contact parameters**” script.

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    //Remove gsid and epv parameter from Contact header to hide internal topology
    remove(%HEADERS["Contact"][1].URI.PARAMS["gsid"]);
    remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
  }
}
```

In the Signaling Manipulation script above, the statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** specifies the portion of the script that will take effect on all outbound SIP messages and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

The following screen shows the finished Signaling Manipulation Script “**remove Contact parameters**” used during compliance testing. This script will later be applied to the Verizon Server Configuration in **Section 7.4.2**.



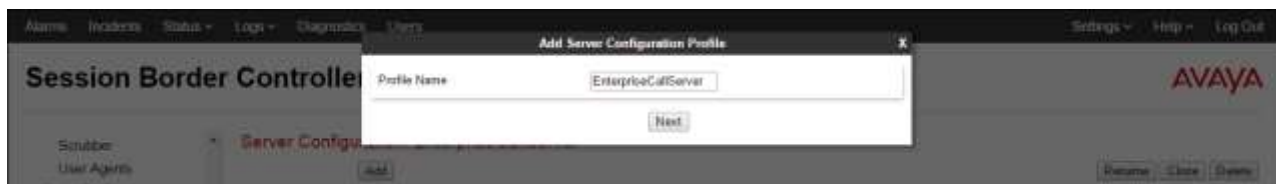
7.4. Server Configuration

The Server Configuration contains parameters to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

In the sample configuration, separate Server Configurations were created for Session Manager and Verizon Business IPCC.

7.4.1 Server Configuration – Session Manager

To add a Server Configuration Profile for Session Manager, navigate to **Global Profiles → Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



The following screens illustrate the Server Configuration for the Profile name “**EnterpriseCallServer**”. In the **General** parameters, the **Server Type** is set to “**Call Server**”. In the **IP Address / FQDN** field, the IP Address of the Session Manager SIP signaling interface is entered. In the sample configuration this IP Address is “**10.64.91.61**”. Under **Port**, “**5060**” is entered, and the **Transport** parameter is set to “**TCP**”. This configuration corresponds with the Session Manager entity link configuration for the entity link to the Avaya SBCE created in **Section 6.4**. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

IP Address / FQDN	Port	Transport
10.64.91.61	5060	TCP

If adding the profile, click **Next** to accept default parameters for the **Authentication** tab (not shown), and advance to the Heartbeat area. If editing an existing profile, select the **Heartbeat** tab and click **Edit** (not shown).

Avaya SBCE can be configured to source “heartbeats” in the form of SIP OPTIONS. In the sample configuration, with one Session Manager, this configuration is optional. If Avaya SBCE-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select “**OPTIONS**” from the **Method** drop-down menu. Select the desired frequency that the Avaya SBCE will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE towards Session Manager. If adding a new profile, click **Next** (not shown). If editing an existing profile, click **Finish** (not shown).

The screenshot shows the 'Heartbeat' configuration tab. It includes a table with the following settings:

Setting	Value
Enable Heartbeat	☒
Method	OPTIONS
Frequency	60 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com

Below the table is an 'Edit' button.

If adding a profile, click **Next** to continue to the **Advanced** settings (not shown). If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select **Enable Grooming** to allow the same TCP connection to be used for all SIP messages from this device. Select the **Interworking Profile** “**Enterprise Interwork**” created previously. Click **Finish**.

The screenshot shows the 'Advanced' configuration tab. It includes a table with the following settings:

Setting	Value
Enable DoS Protection	☐
Enable Grooming	☒
Interworking Profile	Enterprise Interwork
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	☐

Below the table is an 'Edit' button.

7.4.2 Server Configuration - Verizon Business IPCC

To add a Server Configuration Profile for Verizon, navigate to **Global Profiles → Server Configuration** and click **Add**. Enter a descriptive name for the new profile and click **Next**.



The following screens illustrate the Server Configuration for the Profile name “**Verizon Server**”. In the **General** parameters, the **Server Type** is set to “**Trunk Server**”. In the **IP Address / FQDN** field, the Verizon-provided IP address is entered. This is “**172.30.209.55**”. Under **Port**, “**5072**” is entered, and the **Transport** parameter is set to “**UDP**”. If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.

IP Address / FQDN	Port	Transport
172.30.209.55	5072	UDP

Default values can be used on the **Authentication** tab (not shown), click **Next** (not shown) to proceed to the **Heartbeats** tab. The ASBCE can be configured to source “heartbeats” in the form of SIP OPTIONS towards Verizon. This configuration is optional. Independent of whether the ASBCE is configured to source SIP OPTIONS towards Verizon, Verizon will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends SIP OPTIONS to the inside private IP Address of the Avaya SBCE, the Avaya SBCE will send SIP OPTIONS to Verizon. When Verizon responds, the Avaya SBCE will pass the response to Session Manager.

Select “**OPTIONS**” from the **Method** drop-down menu. Select the desired frequency that the SBCE will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the Avaya SBCE. If adding a new profile, click **Next** to continuing to the **Advanced** settings. If editing an existing profile, click **Finish** (not shown).

General	Authentication	Heartbeat	Advanced
Enable Heartbeat ☒			
Method		OPTIONS	
Frequency		60 seconds	
From URI		ping@adevc.avaya.globalipcom.com	
To URI		ping@pcelban0001.avayalincroft.globalipcom.com	
Edit			

On the **Advanced** tab, **Enable Grooming** is not used for UDP connections and left unchecked. The Interworking Profile is left at its default setting of “None”. This will prevent Avaya SBCE from inserting “Supported: replaces” in the SIP message toward Session Manager. See **Section 2.2**. Select the **Signaling Manipulation Script** created in the previous section titled “**remove Contact parameters**”. Click **Finish**.

General	Authentication	Heartbeat	Advanced
Enable DoS Protection ☐			
Enable Grooming ☐			
Interworking Profile		None	
Signaling Manipulation Script		remove Contact parameters	
Connection Type		SUBID	
Securable ☐			
Edit			

7.5. Routing Profile

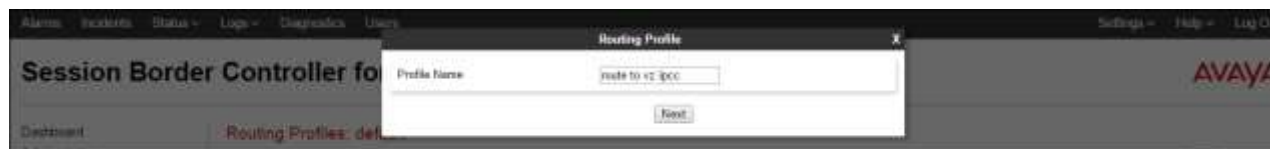
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

Create a Routing Profile for Session Manager and Verizon Business IPCC service. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.

The following screen shows the Routing Profile “**route to sm**” created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to “1”, and the Session Manager **Server Configuration**, created in **Section 7.4.1**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the Server Configuration, and **Transport** becomes greyed out. Select **Finish**.

Profile : route to sm - Edit Rule			
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☒
Next Hop In-Dialog	☐	Ignore Route Header	☐
Add			
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	EnterpriseCallServer	10.64.91.61:5060 (TCP)	None
Delete			
Finish			

Similarly add a Routing Profile to Verizon Business IPCC.



The following screen shows the Routing Profile “**route to vz ipcc**” created in the sample configuration. The parameters in the top portion of the profile are left at their default settings. The **Priority / Weight** parameter is set to “1”, and the Verizon **Server Configuration**, created in **Section 7.4.2**, is selected from the drop-down menu. The **Next Hop Address** is automatically selected with the values from the Server Configuration, and **Transport** becomes greyed out. Click **Finish**.

Routing Profile			
URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☒
Next Hop In-Dialog	☐	Ignore Route Header	☐
Add			
Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Vz IPCC Server	172.30.205.55:5072 (UDP)	None
Delete			
Back Finish			

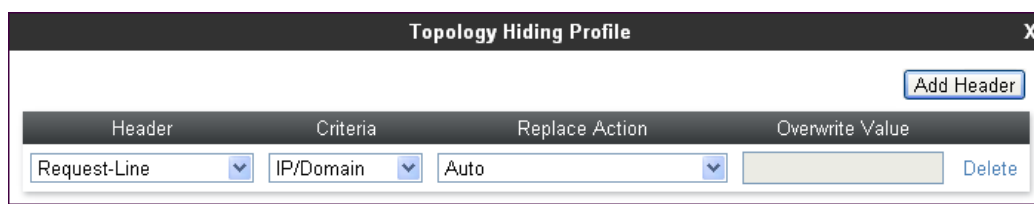
7.6. Topology Hiding Profile

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

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

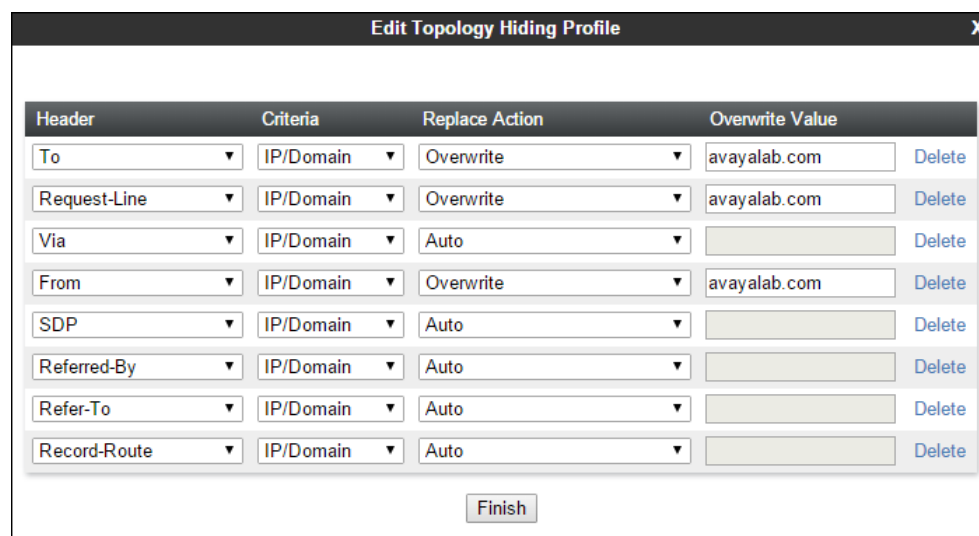


In the resultant screen, click the **Add Header** button in the upper right multiple times to reveal additional headers.

A screenshot of the 'Topology Hiding Profile' configuration window. It has an 'Add Header' button in the top right. Below is a table with one row: 'Request-Line' in the 'Header' column, 'IP/Domain' in the 'Criteria' column, 'Auto' in the 'Replace Action' column, and an empty 'Overwrite Value' field. A 'Delete' button is at the end of the row.

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

In the **Replace Action** column an action of “**Auto**” will replace the header field with the IP address of the Avaya SBCE interface and the “**Overwrite**” will use the value in the **Overwrite Value**. In the example shown, this profile will later be applied in the direction of the Session Manager and “**Overwrite**” has been selected for the To/From and Request-Line headers and the shared interop lab domain of “**avayalab.com**” has been inserted. Click **Finish**.

A screenshot of the 'Edit Topology Hiding Profile' window. It displays a table with eight rows of header configurations. Each row has a 'Header' dropdown, a 'Criteria' dropdown (all set to 'IP/Domain'), a 'Replace Action' dropdown, an 'Overwrite Value' text field, and a 'Delete' button. The 'Finish' button is at the bottom.

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

After configuration is completed, the Topology Hiding for profile “**enterprise th profil**” will appear as follows. This profile will later be applied to the Server Flow for Avaya.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like DoS/DDoS, Scrubber, User Agents, Global Profiles, and Topology Hiding. The main area is titled 'Topology Hiding Profiles: enterprise th profil'. It features a list of profiles on the left: default, disco_th_profile, verizon_th_profile, and enterprise th profil (highlighted). The main content area shows the configuration for the 'enterprise th profil' profile. It includes a table with the following headers: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following data:

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

Similarly, create a Topology Hiding profile for Verizon. Overwrite the headers as shown below with the FQDNs known by Verizon. The Refer-To header’s domain is overwritten with the IP address presented in the original INVITE from Verizon’s IP-IVR service. If the IP-IVR service is not used, the Refer-To header can retain the default **Replace Action** of “**Auto**”. The following screen shows Topology Hiding profile “**Verizon ipcc th profile**” created for Verizon. This profile will later be applied to the Server Flow for Verizon.

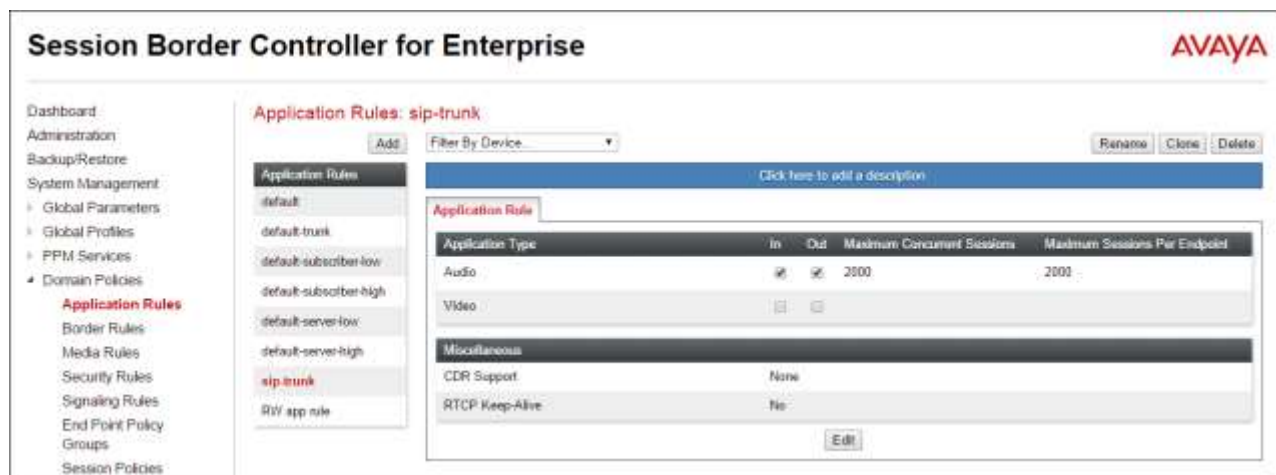
The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Topology Hiding. The main area is titled 'Topology Hiding Profiles: vz ipcc th profile'. It features a list of profiles on the left: default, disco_th_profile, verizon_th_profile, enterprise th profil, and vz ipcc th profile (highlighted). The main content area shows the configuration for the 'vz ipcc th profile' profile. It includes a table with the following headers: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following data:

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	poelbar0001.avayaalab.com
From	IP/Domain	Overwrite	advc.avaya.globalipcom.com
Refer-To	IP/Domain	Overwrite	199.173.54.16
SDP	IP/Domain	Auto	—
Record-Route	IP/Domain	Auto	—
Request-Line	IP/Domain	Overwrite	poelbar0001.avayaalab.com
Refered-By	IP/Domain	Overwrite	advc.avaya.globalipcom.com
Via	IP/Domain	Auto	—

7.7. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Select **Domain Policies** → **Application Rules** from the left-side menu as shown below. Click the **Add** button to add a new profile, or select an existing topology hiding profile to edit. In the sample configuration, the “**sip-trunk**” profile was created from cloning the **default-trunk** application rule. In an actual customer installation, set the **Maximum Concurrent Sessions** for the **Audio** application to a value slightly larger than the licensed sessions. For example, if licensed for 1500 session set the values to “**2000**”. The **Maximum Session Per Endpoint** should match the **Maximum Concurrent Sessions**.

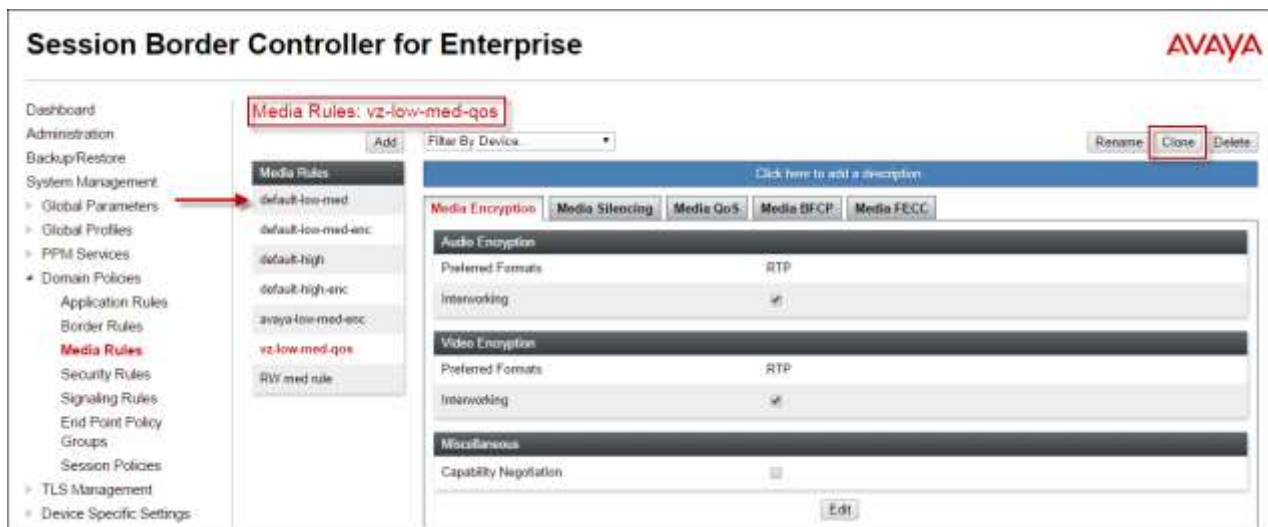


7.8. Media Rule

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

Select **Domain Policies** → **Media Rules** from the left-side menu as shown below. In the sample configuration, a single media rule is created by cloning the default rule called **default-low-med**. With the **default-low-med** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

In the sample configuration, signaling rule “**vz-low-med-qos**” was used as shown below.

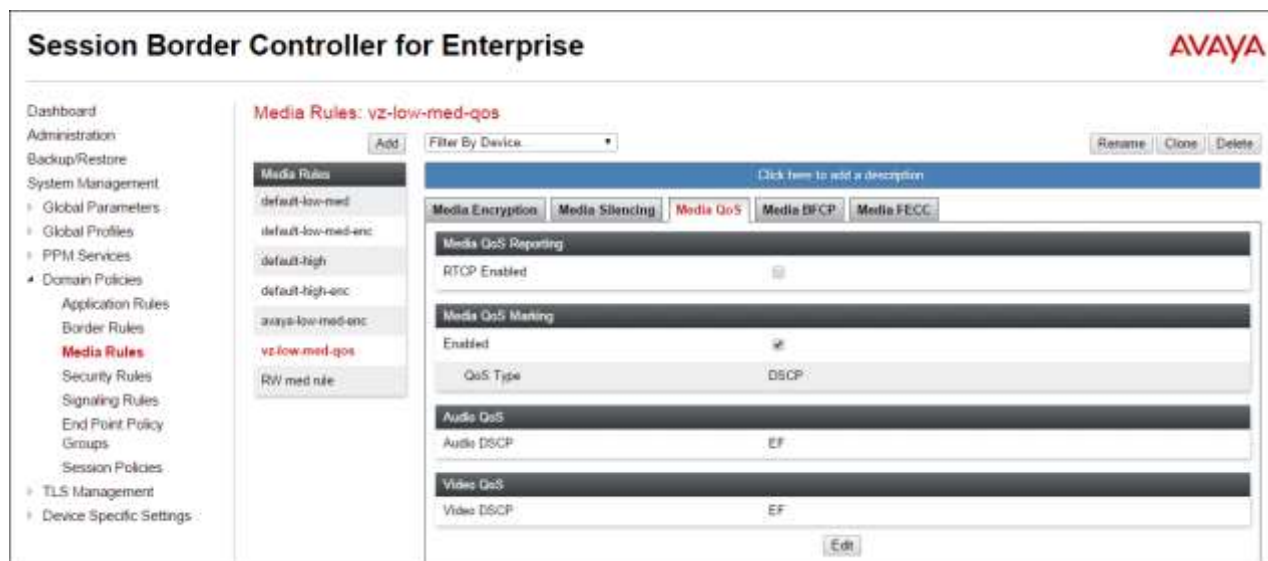


Select the newly created rule, select the **Media QoS** tab and click the **Edit** button (not shown). In the resulting screen below, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select “EF” for expedited forwarding as shown below. Click **Finish**.

The screenshot shows the 'Media QoS' configuration window. The 'Media QoS Reporting' section has 'RTCP Enabled' checked. The 'Media QoS Marking' section is expanded, showing 'Enabled' checked. Under the 'DSCP' section, 'Audio' and 'Video' are both set to 'EF' (Expedited Forwarding). The 'Finish' button is at the bottom.

Media QoS Reporting		
RTCP Enabled	☒	
Media QoS Marking		
Enabled	☒	
ToS		
Audio Precedence	Routine	000
Audio ToS	Minimize Delay	1000
Video Precedence	Routine	000
Video ToS	Minimize Delay	1000
DSCP		
Audio	EF	101110
Video	EF	101110
Finish		

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

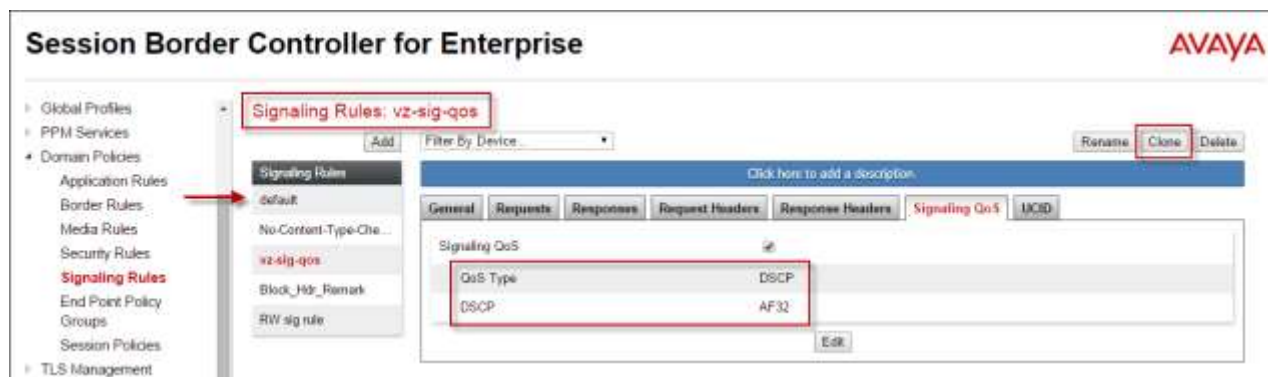


7.9. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the **default** signaling rule to add the proper quality of service to the SIP signaling towards Verizon. To clone a signaling rule, navigate to **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click **Clone**. Enter a descriptive name for the new rule and click **Finish** (not shown).

In the sample configuration, signaling rule “**vz-sig-qos**” is shown with the **DSCP** value “**AF32**” for assured forwarding, changed from the default settings under the **Signaling QoS** tab.



7.10. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section Error! Reference source not found.** Create a separate Endpoint Policy Group for the enterprise and the Verizon IPCC. To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups**. Select the **Add** button.

To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** as shown below. The following screen shows the “**vz-low-remark**” created for Verizon Business IPCC. The details of the non-default rules chosen are shown in previous sections.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows the navigation menu with 'Endpoint Policy Groups' highlighted. The main content area is titled 'Policy Groups: vz-low-remark'. It includes an 'Add' button and a 'Filter By Device' dropdown. Below this, there is a list of policy groups with 'vz-low-remark' selected. The details for the selected policy group are shown in a table with columns: Order, Application, Border, Media, Security, and Signaling. The table contains one row with the following values: 1, vz-trunk, default, vz-low-med-ops, default-low, and vz-ops-ops. There are also buttons for 'Rename', 'Close', and 'Delete' at the top right of the configuration area.

The following screen shows the “**enterprise-low**” created for the enterprise. The details of the non-default rules chosen are shown in previous sections.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows the navigation menu with 'Endpoint Policy Groups' highlighted. The main content area is titled 'Policy Groups: enterprise-low'. It includes an 'Add' button and a 'Filter By Device' dropdown. Below this, there is a list of policy groups with 'enterprise-low' selected. The details for the selected policy group are shown in a table with columns: Order, Application, Border, Media, Security, and Signaling. The table contains one row with the following values: 1, vz-trunk, default, vz-low-med-ops, default-low, and vz-ops-ops. There are also buttons for 'Rename', 'Close', and 'Delete' at the top right of the configuration area.

7.11. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP Media Interface for both the inside and outside IP interfaces.

To create a new Media Interface, navigate to **Device Specific Settings** → **Media Interface** and click **Add Media Interface**. The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces.

The screenshot shows the 'Media Interface: SBC1' configuration page. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of media interfaces:

Name	Media IP Network	Port Range	
int med to enterprise	10.64.91.50 Inside-Enterprise (A1, VLAN 0)	35000 - 40000	Edit Delete
ext med to verizon	1.1.1.2 Outside-Verizon (B1, VLAN 0)	35000 - 40000	Edit Delete
RW int med	10.64.91.49 Inside-Enterprise (A1, VLAN 0)	35000 - 40000	Edit Delete
RW ext med	192.168.80.92 Public RW Access (B2, VLAN 0)	35000 - 40000	Edit Delete

7.12. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings** → **Signaling Interface** and click **Add Signaling Interface**. The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

The screenshot shows the 'Signaling Interface: SBC1' configuration page. A warning message states: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of signaling interfaces:

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
int sig to enterprise	10.64.91.50 Inside-Enterprise (A1, VLAN 0)	5060	—	—	None	Edit Delete
ext sig to verizon	1.1.1.2 Outside-Verizon (B1, VLAN 0)	—	5060	—	None	Edit Delete
RW int sig	10.64.91.49 Inside-Enterprise (A1, VLAN 0)	5060	5060	5061	sbc1RWInternal Server	Edit Delete
RW ext sig	192.168.80.92 Public RW Access (B2, VLAN 0)	—	—	5060	sbc1RWExternal Server	Edit Delete

7.13. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the endpoints are Session Manager and the Verizon IPCC SIP server.

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** as shown in below.



The following screen shows the flow named “**enterprise side**” used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: enterprise side X

Flow Name	enterprise side
Server Configuration	EnterpriseCallServer
URI Group	*/
Transport	*/
Remote Subnet	*/
Received Interface	ext sig to verizon
Signaling Interface	int sig to enterprise
Media Interface	int med to enterprise
End Point Policy Group	enterprise-low
Routing Profile	route to vz ipcc
Topology Hiding Profile	enterprise th profil
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

The following screen shows the flow named “**vz ipcc**” used in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Click **Finish**.

Edit Flow: vz ipcc

Flow Name

vz ipcc

Server Configuration

Vz IPCC Server

URI Group

*

Transport

*

Remote Subnet

*

Received Interface

int sig to enterprise

Signaling Interface

ext sig to verizon

Media Interface

ext med to verizon

End Point Policy Group

vz-low-remark

Routing Profile

route to sm

Topology Hiding Profile

vz ipcc th profile

Signaling Manipulation Script

None

Remote Branch Office

Any

Finish

8. Verizon Business IPCC Services Suite Configuration

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

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

8.1. Service Access Information

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

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i> <i>UDP port 5060</i>	<i>172.30.205.55</i> <i>UDP Port 5072</i>

Toll Free Numbers
866-850-2380
866-851-0107
866-851-2649
866-852-3221
866-850-6850

9. Verification Steps

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

9.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

9.1.1 Example Incoming Call from PSTN via Verizon IPCC to Telephone

Incoming PSTN calls arrive from Verizon at Avaya SBCE, which sends the call to Session Manager. Session Manager sends the call to Communication Manager. On Communication Manager, the incoming call arrives via signaling group 2 and trunk group 2.

The following edited Communication Manager *list trace tac* trace output shows a call incoming on trunk group 2. The PSTN telephone dialed 866-850-6850. Session Manager mapped the number received from Verizon to the extension of a Communication Manager telephone (x12003). Extension 12003 is an IP Telephone with IP address 10.64.91.32 in Region 1. Initially, the G450 Media Gateway (10.64.91.81) is used, but as can be seen in the final trace output, once the call is answered, the final RTP media path is “ip-direct” from the IP Telephone (10.64.91.32) to the “inside” of the Avaya SBCE (10.64.91.50) in Region 2.

```
LIST TRACE
time      data
/* Incoming call arrives to Communication Manager for x12003 */
14:27:54 TRACE STARTED 09/14/2015 CM Release String cold-00.0.441.0-22477
14:27:57 SIP<INVITE sip:12003@avayalab.com;user=phone SIP/2.0
14:27:57      Call-ID: 9e118c5b1533b9650a291357d8984426
/* Communication Manager sends 183 with SDP as a result of TG 2 configuration */
14:27:57 SIP>SIP/2.0 183 Session Progress
14:27:57      Call-ID: 9e118c5b1533b9650a291357d8984426
14:27:57      dial 12003
14:27:57      ring station      12003 cid 0x551
/* G450 Gateway at 10.64.91.81, ringback tone heard by caller */
14:27:57      G711MU ss:off ps:20
              rgn:1 [10.64.91.32]:2838
              rgn:10 [10.64.91.81]:2058
14:27:57      G711MU ss:off ps:20
              rgn:2 [10.64.91.50]:35724
              rgn:10 [10.64.91.81]:2054
14:27:57      xoip options: fax:PT modem:off tty:US uid:0x5000b
              xoip ip: [10.64.19.61]:2054
/* User Answers call, Communication Manager sends 200 OK */
14:27:58 SIP>SIP/2.0 200 OK
14:27:58      Call-ID: 9e118c5b1533b9650a291357d8984426
14:27:58      active station      12003 cid 0x551
/* Communication Manager receives ACK to 200 OK */
14:27:58 SIP<ACK sip:+17329450233@10.64.91.65:5071;transport=tls SIP
14:27:58 SIP</2.0
14:27:58      Call-ID: 9e118c5b1533b9650a291357d8984426

<continued on next page>
```

```

/* Communication Manager sends re-INVITE to begin shuffle to ip-direct */
14:27:58 SIP>INVITE sip:+13035382177@10.64.91.50:5060;transport=tcp;
14:27:58 SIP>sipappsessionid=app-lna3oxt2pkd2k;gsid=ee9c10e0-5b1e-11
14:27:58 SIP>e5-8d7d-000c292d062f SIP/2.0
14:27:58 Call-ID: 9e118c5b1533b9650a291357d8984426
/* Communication Manager receives 200 OK with SDP, sends ACK with SDP */
14:27:59 SIP>ACK sip:+13035382177@10.64.91.50:5060;transport=tcp;wls
14:27:59 SIP>scid=-270f46a416660660;sipappsessionid=app-lna3oxt2pkd2
14:27:59 SIP>k;gsid=ee9c10e0-5b1e-11e5-8d7d-000c292d062f SIP/2.0
14:27:59 Call-ID: 9e118c5b1533b9650a291357d8984426
/* Final media path is ip-direct from answering IP (10.64.91.32) to inside of
SBC (10.64.91.50) */
14:27:59 G729A ss:off ps:20
          rgn:2 [10.64.91.50]:35724
          rgn:1 [10.64.91.32]:2838
14:27:59 G729 ss:off ps:20
          rgn:1 [10.64.91.32]:2838
          rgn:2 [10.64.91.50]:35724
14:28:00 SIP>BYE sip:+13035382177@10.64.91.50:5060;transport=tcp;wls
14:28:00 SIP>scid=-270f46a416660660;sipappsessionid=app-lna3oxt2pkd2
14:28:00 SIP>k;gsid=ee9c10e0-5b1e-11e5-8d7d-000c292d062f SIP/2.0
14:28:00 Call-ID: 9e118c5b1533b9650a291357d8984426
14:28:00 idle station 12003 cid 0x551

```

The following screen shows **Page 2** of the output of the *status trunk* command pertaining to this same call. Note the signaling using port 5071 between Communication Manager and Session Manager. Note the media is “**ip-direct**” from the IP Telephone (10.64.91.32) to the inside IP address of Avaya SBCE (10.64.91.50) using codec G.729.

```

status trunk 2/1                                     Page 2 of 3
CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling IP Address Port
  Near-end: 10.64.91.65 : 5071
  Far-end: 10.64.91.61 : 5071
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: 10.64.91.32 : 2838
  Far-end: 10.64.91.50 : 35726

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

```

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

status trunk 2/1

Page 3 of 3

SRC PORT TO DEST PORT TALKPATH

src port: T00011

T00011:TX:10.64.91.50:35726/g729/20ms

S00003:RX:10.64.91.32:2838/g729a/20ms

9.1.2 Example Incoming Call Referred via Call Vector to PSTN Destination

The following edited and annotated Communication Manager *list trace tac* trace output shows a call incoming on trunk group 2. The call was routed to a Communication Manager vector directory number (VDN 10001) associated with a call vector (call vector 1). The vector answers the call, plays an announcement to the caller, and then uses a “route-to” step to cause a REFER message to be sent with a Refer-To header containing the number configured in the vector “route-to” step. The PSTN telephone dialed 866-852-3221. Session Manager can map the number received from Verizon to the VDN extension (x10001), or the incoming call handling table for trunk group 1 can do the same. In the trace below, Session Manager had already mapped the Verizon number to the Communication Manager VDN extension. The annotations in the edited trace highlight key behaviors. At the conclusion, the PSTN caller that dialed the Verizon toll-free number is talking to the Referred-to PSTN destination, and no trunks (i.e., from trunk 1 handling the call) are in use.

Page 1

```

list trace tac *02
/* Session Manager has adapted the dialed number 8668523221 to VDN 10001 */
14:21:06 SIP<INVITE sip:10001@avayalab.com SIP/2.0
14:21:06      Call-ID: 2036505164-1723268874@10.10.20.23
14:21:06      active trunk-group 1 member 1      cid 0x18dd
14:21:06      0 0 ENTERING TRACE cid 6365
14:21:06      2 1 vdn e10001 bsr appl 0 strategy 1st-found override n
14:21:06      2 1 wait 2 secs hearing ringback
14:21:06 SIP>SIP/2.0 183 Session Progress
14:21:06      Call-ID: 2036505164-1723268874@10.10.20.23
14:21:06      dial 10001
14:21:06      ring vector 2      cid 0x18dd
/* Vector step plays ringback. A 183 with SDP is sent*/
14:21:06      G729 ss:off ps:20
14:21:06      rgn:2 [10.64.91.50]:35002
14:21:06      rgn:1 [10.64.91.81]:2062
14:21:06      xoip options: fax:T38 modem:off tty:US uid:0x50009
14:21:06      xoip ip: [10.64.91.81]:2062
14:21:08      2 2 # Play announcement to caller i...
14:21:08      2 3 announcement 11006
14:21:08 SIP>SIP/2.0 183 Session Progress
14:21:08      Call-ID: 2036505164-1723268874@10.10.20.23
14:21:08      2 3      announcement: board 001V9 ann ext: 11006
/* Vector step answers call with announcement. 200 OK is sent */
14:21:08 SIP>SIP/2.0 200 OK
14:21:08      Call-ID: 2036505164-1723268874@10.10.20.23
14:21:08      active announcement      11006 cid 0x18dd
14:21:08      hear annc board 001V9 ext 11006 cid 0x18dd
14:21:08 SIP<ACK sip:8668523221@10.64.91.63:5071;transport=tls SIP/
14:21:08 SIP<2.0
14:21:08      Call-ID: 2036505164-1723268874@10.10.20.23
/* Caller hears pre-REFER announcement, announcement completes, REFER sent */
14:21:11      idle announcement      cid 0x18dd
14:21:11      2 4 # Refer the call to PSTN Destin...
14:21:11      2 5 route-to number ~r+13035387024 cov n if unconditionally
14:21:11 SIP>REFER sip:+13035387006@10.64.91.50:5060;transport=tcp;
14:21:11 SIP>gsid=a5787640-b753-11e2-b83f-9c8e992b0a68 SIP/2.0
14:21:11      Call-ID: 2036505164-1723268874@10.10.20.23
/* Communication Manager receives 202 Accepted sent by Verizon IPCC */
14:21:11 SIP<SIP/2.0 202 Accepted
14:21:11      Call-ID: 2036505164-1723268874@10.10.20.23

<continued on next page>

```

```

/* Verizon IPCC sends re-INVITE with c=0.0.0.0 SDP and 200 OK/ACK occur */
14:21:11 SIP<INVITE sip:8668523221@10.64.91.63:5071;transport=tls S
14:21:11 SIP<IP/2.0
14:21:11 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP>SIP/2.0 100 Trying
14:21:11 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP>SIP/2.0 200 OK
14:21:11 Call-ID: 2036505164-1723268874@10.10.20.23
/* Verizon IPCC sends NOTIFY with sipfrag 100 Trying,CM sends 200 OK */
14:21:11 SIP<NOTIFY sip:8668523221@10.64.91.63:5071;transport=tls S
14:21:11 SIP<IP/2.0
14:21:11 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP>SIP/2.0 200 OK
14:21:11 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:11 SIP<ACK sip:8668523221@10.64.91.63:5071;transport=tls SIP/
14:21:11 SIP<2.0
14:21:11 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16 SIP<NOTIFY sip:8668523221@10.64.91.63:5071;transport=tls S
14:21:16 SIP<IP/2.0
14:21:16 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16 SIP>SIP/2.0 200 OK
* Note that caller does not hear ringback or any audible feedback until answer
*/
/* Verizon IPCC sends NOTIFY with sipfrag 200 OK and CM sends 200 OK and BYE */
14:21:16 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16 2 5 LEAVING VECTOR PROCESSING cid 6365
14:21:16 SIP>BYE sip:+13035387006@10.64.91.50:5060;transport=tcp;gs
14:21:16 SIP>id=a5787640-b753-11e2-b83f-9c8e992b0a68 SIP/2.0
14:21:16 Call-ID: 2036505164-1723268874@10.10.20.23
14:21:16 idle vector 0 cid 0x18dd
/* Trunks are now idle. Caller and refer-to target are connected by Verizon */

```

When the initial call arrived from Verizon, it used trunk member 1 from trunk group 2. In the final state when the PSTN caller is speaking with the answering agent at the Refer-To target, trunk member 1 is idle, reflecting the successful REFER.

```

status trunk 2

```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports
			Busy
0077/001	T00041	in-service/idle	no
0077/002	T00042	in-service/idle	no
0077/003	T00043	in-service/idle	no
0077/004	T00044	in-service/idle	no
0077/005	T00045	in-service/idle	no
0077/006	T00046	in-service/idle	no
0077/007	T00047	in-service/idle	no
0077/008	T00048	in-service/idle	no
0077/009	T00049	in-service/idle	no
0077/010	T00050	in-service/idle	no

9.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager. Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. A screen such as the following is displayed.

SIP Entity Link Monitoring Status Summary

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

SIP Entities Status for All Monitoring Session Manager Instances

1 Items | Refresh

Session Manager	Type	Down	Partially Up	Up	Not Monitored	Deny	Total
SessionManager	Core	0	0	6	0	0	6

Select: All Items

All Monitored SIP Entities

6 Items | Refresh

SIP Entity Name
Vz-SBC-2
CM-TG2
Aura Messaging
Vz-SBC-1
CM-TG3
CM-TG1

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

All Entity Links to SIP Entity: Vz-SBC-1

Summary View

Status Details for the selected Session Manager:

1 Items | Refresh

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SessionManager	10.64.91.50	5060	TCP	FALSE	UP	200 OK	UP

9.3. Avaya Session Border Controller for Enterprise Verification

9.3.1 Welcome Screen

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

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main content area is divided into several sections: a left sidebar with a 'Dashboard' menu, a central 'Dashboard' section with system information, and two right-hand sections for 'Installed Devices' and 'Alarms/Incidents (past 24 hours)'. The system information includes System Time (03:56:03 PM MDT), Version (7.0.0-21-6602), Build Date (Wed Jun 24 21:19:29 EDT 2015), License State (OK), and various licensing and login statistics. The installed devices list shows 'EMS' and 'SBC1'. Both the alarms and incidents sections show 'None found'.

Information	
System Time	03:56:03 PM MDT
Version	7.0.0-21-6602
Build Date	Wed Jun 24 21:19:29 EDT 2015
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	-
Failed Login Attempts	1

Installed Devices	
EMS	
SBC1	

Alarms (past 24 hours)	
None found.	

Incidents (past 24 hours)	
None found.	

9.3.2 Alarms

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

This screenshot shows the 'Alarms' tab selected in the top navigation bar. The page title is 'Session Border Controller for Enterprise'. The 'Alarms' tab is highlighted in the left sidebar.

Alarm Viewer.

The screenshot shows the 'Alarm Viewer' interface. The left sidebar has a 'Devices' menu with 'EMS' and 'SBC1' listed. The main content area is titled 'Alarms' and contains a table with columns: ID, Details, State, Time, and Device. The table is currently empty, displaying the message 'No alarms found for this device.' Below the table are 'Clear Selected' and 'Clear All' buttons.

ID	Details	State	Time	Device
No alarms found for this device.				

9.3.3 Incidents

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

Incident Viewer:

Incident Viewer						
Device All Category All Clear Filters Refresh Generate Report						
Displaying results 1 to 15 out of 850.						
Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	719101247191465	7/29/15	2:41 PM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	71909946311171	7/29/15	1:58 PM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719096161307487	7/29/15	12:58 PM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719096376321364	7/29/15	11:59 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719094591304372	7/29/15	10:59 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719092606303055	7/29/15	10:00 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719091021302164	7/29/15	9:00 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719089236300524	7/29/15	8:01 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719087451298995	7/29/15	7:01 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719085666296473	7/29/15	6:02 AM	Policy	SBC1	Heartbeat Successful, Server is UP
Server Heartbeat	719083681299167	7/29/15	5:02 AM	Policy	SBC1	Heartbeat Successful, Server is UP

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

Incident Information				X
General Information				
Incident Type	Server Heartbeat		Category	Policy
Timestamp	July 29, 2015 2:41:34 PM MDT		Device	SBC1
Cause	Heartbeat Successful, Server is UP			
Message Data				
Response Code	200	Transport	UDP	
Call ID	f1c1073a39b6750b9dd8e1469906b5e52eeebdf9382a7f9d40de512517d85e		From	sip:ping@adevc.avaya.glob
To	sip:ping@pcelban0001.avayalincroft.globalipcom.com		Source IP	1.1.1.2
Destination IP	172.30.209.21			
Server Configuration	Verizon Server			
Direct Access to this page: https://10.64.90.50:443/ehc/incident?id=719101247191465				

9.3.4 Diagnostics

The full diagnostics check will verify the link of each interface, and ping the configured next-hop gateways and DNS servers.

Click on Diagnostics on the top bar, select the Avaya SBCE from the list of devices and then click “Start Diagnostics”

The screenshot shows the 'Full Diagnostic' tab selected. A 'Start Diagnostic' button is in the top right. Below is a table with two columns: 'Task Description' and 'Status'. All tasks have a red status icon (a circle with a red 'x').

Task Description	Status
EMS Link Check	
SBC Link Check: A1	
SBC Link Check: B1	
SBC Link Check: B2	
Ping: SBC (10.64.91.49 [A1]) to Gateway (10.64.91.1)	
Ping: SBC (10.64.91.49 [A1]) to Primary DNS (10.64.19.201)	
Ping: SBC (10.64.91.50 [A1]) to Gateway (10.64.91.1)	
Ping: SBC (10.64.91.50 [A1]) to Primary DNS (10.64.19.201)	
Ping: SBC (1.1.1.2 [B1]) to Gateway (1.1.1.1)	
Ping: SBC (1.1.1.2 [B1]) to Primary DNS (10.64.19.201)	

A green check mark or a red x will indicate success or failure.

The screenshot shows the 'Full Diagnostic' tab. A 'Stop Diagnostic' button is in the top right. The table below shows all tasks completed successfully, indicated by green checkmarks. The 'Status' column provides detailed information for each task.

Task Description	Status
EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
SBC Link Check: B2	B2 is operating within normal parameters with a full duplex connection at 1Gb/s.
Ping: SBC (10.64.91.49 [A1]) to Gateway (10.64.91.1)	Average ping from 10.64.91.49 [A1] to 10.64.91.1 is 0.571ms.
Ping: SBC (10.64.91.49 [A1]) to Primary DNS (10.64.19.201)	Average ping from 10.64.91.49 [A1] to 10.64.19.201 is 0.219ms.
Ping: SBC (10.64.91.50 [A1]) to Gateway (10.64.91.1)	Average ping from 10.64.91.50 [A1] to 10.64.91.1 is 0.236ms.
Ping: SBC (10.64.91.50 [A1]) to Primary DNS (10.64.19.201)	Average ping from 10.64.91.50 [A1] to 10.64.19.201 is 0.208ms.

9.3.5 Tracing

To take a call trace, Select **Device Specific Settings → Troubleshooting → Tracing** from the left-side menu (not shown).

Select the Packet Capture tab and set the desired configuration for a call trace and click **Start Capture**.

The screenshot shows the 'Packet Capture' tab selected at the top. Below it is the 'Captures' tab. The main area is titled 'Packet Capture Configuration'. It contains the following fields:

Status	Ready
Interface	B1
Local Address IP[:Port]	All :
Remote Address *, *:Port, IP, IP:Port	*
Protocol	All
Maximum Number of Packets to Capture	1000
Capture Filename Using the name of an existing capture will overwrite it.	Test-Trace.pcap

At the bottom right of the configuration area are two buttons: 'Start Capture' and 'Clear'.

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

This screenshot is similar to the previous one, but it includes a blue status bar at the top with a circular arrow icon and the text: 'Please wait while your settings are saved and the capture is started...'. The configuration fields below remain the same: Status (Ready), Interface (B1), Local Address (All), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (1000), and Capture Filename (Test-Trace.pcap).

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

Packet Capture		Captures		
				Refresh
File Name	File Size (bytes)	Last Modified		
Test-Trace_20150807161226.pcap	0	August 7, 2015 4:12:27 PM MDT		
		Delete		

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.0, Avaya Aura® Session Manager 7.0, and Avaya Session Border Controller for Enterprise 7.0 can be configured to interoperate successfully with Verizon Business IP Contact Center Services suite. This solution enables inbound toll free calls over a Verizon Business VoIP Inbound SIP trunk service connection. In addition, these Application Notes further demonstrate that the Avaya Aura® Communication Manager implementation of SIP Network Call Redirection (SIP-NCR) can work in conjunction with Verizon's Business IP Contact Center services implementation of SIP-NCR to support call redirection over SIP trunks inclusive of passing User-User Information (UUI).

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

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

11. Additional References

11.1. Avaya

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

- [1] *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 7.0
- [2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, Release 7.0
- [3] *Deploying Avaya Aura® Session Manager on VMware®*, Release 7.0
- [4] *Installing Service Packs for Avaya Aura® Session Manager*, Release 7.0
- [5] *Upgrading Avaya Aura® Session Manager*, Release 7.0
- [6] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 7.0
- [7] *Deploying Avaya Aura® System Manager*, Release 7.0
- [8] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0
- [9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0
- [10] *Administering 9608,9808G,9611G,9621G,9641G IP Deskphones Edition H.323*, Document Number 16-300698, Issue 19, June 2014.
- [11] *Administering 9608,9808G,9611G,9621G,9641G IP Deskphones Edition SIP*, Document Number 16-601944, Issue 1, January 2015.
- [12] *Administering Avaya one-X® Communicator*, April 2015.

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

The following Application Notes cover Session Manager 6.3 with Verizon Business IP Contact Center Services.

[VZ-IPCC] – Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2 with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.1

11.2. Verizon Business

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

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

©2015 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.