



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0 with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.1

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Aura® Session Border Controller Release 6.0. The enterprise equipment is integrated with the Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite is comprised of 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. Using the sample configuration, PSTN callers may dial toll-free numbers associated with the IP Toll Free and IP-IVR services to reach Avaya Communication Server 1000E telephone users.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	5
2.3.	Support.....	6
2.3.1	Avaya	6
2.3.2	Verizon.....	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	10
5.	Configure Avaya Communication Server 1000E	11
5.1.	Node and Key IP Addresses	12
5.2.	Virtual D-Channel, Routes and Trunks	14
5.2.1	Virtual D-Channel Configuration	14
5.2.2	Routes and Trunks Configuration.....	15
5.3.	SIP Trunk to Session Manager	17
5.4.	Routing of Dialed Numbers to Session Manager	22
5.4.1	Route List Block	22
5.4.2	NARS Access Code	23
5.4.3	Numbering Plan Area Codes	24
5.5.	Zones	25
5.6.	Codec Parameters, Including Ensuring Annexb=no for G.729	27
5.6.1	Media Gateway Configuration.....	27
5.6.2	Node Voice Gateway and Codec Configuration.....	29
5.7.	Enabling Plug-Ins for Call Transfer Scenarios	31
5.8.	Customer Information	33
5.8.1	Caller ID Related Configuration.....	33
5.9.	Example CS1000 Telephone Users	35
5.9.1	Example IP UNiStim Phone DN 57003, Codec Considerations	35
5.9.2	Example SIP Phone DN 57007, Codec Considerations.....	36
5.9.3	Example Digital Phone DN 57005 with Call Waiting.....	37
5.9.4	Example Analog Port with DN 57021	38
5.10.	Save Configuration	39
6.	Configure Avaya Aura® Session Manager Release 6.1	40
6.1.	SIP Domain	43
6.2.	Locations.....	45
6.2.1	Location for Avaya Communication Server 1000E.....	45
6.2.2	Location for Session Border Controller	46
6.3.	Configure Adaptations	48
6.3.1	Adaptation for Avaya Communication Server 1000E Entity	48
6.3.2	Adaptation for SBC Entity	50
6.3.3	List of Adaptations.....	51
6.4.	SIP Entities.....	51
6.4.1	SIP Entity for Avaya Communication Server 1000E	51
6.4.2	SIP Entity for SBC.....	52

6.5.	Entity Links.....	53
6.5.1	Entity Link to Avaya Communication Server 1000E Entity	54
6.5.2	Entity Link to SBC.....	54
6.6.	Routing Policies	55
6.6.1	Routing Policy to Avaya Communication Server 1000E	55
6.6.2	Routing Policy to SBC.....	56
6.7.	Dial Patterns.....	57
6.7.1	Inbound Verizon Calls to CS1000E Users.....	57
6.7.2	Outbound Calls to Verizon (Optional).....	58
7.	Configure Avaya Aura® Session Border Controller (SBC)	59
7.1.	Avaya Aura® Session Border Controller (SBC) Installation	60
7.2.	Avaya Aura® Session Border Controller (SBC) Licensing	60
7.3.	SBC Element Manager Configuration	60
7.3.1	Adding SIP Gateway to Verizon IP Contact Center Service.....	61
7.3.2	Adding IP Routing for Verizon IP Contact Center Network	66
7.3.3	Configure Dial-Plan	69
7.3.4	Configure OPTIONS ping to Verizon IP Contact Center.....	73
7.3.5	Configure Kernel-Filter for Verizon IPCC	74
7.3.6	Stripping Unnecessary SIP Headers	77
7.3.7	Stripping Unnecessary SIP Message Body Information (Optional)	81
7.3.8	Disable Third Party Call Control	83
7.3.9	Quality Of Service (QoS) Markings for SIP Signaling	84
7.3.10	Quality Of Service (QoS) Markings for Media	85
7.4.	Saving and Activating Configuration Changes.....	86
7.5.	Example Configuration File.....	87
8.	Verizon Business IP Contact Center Configuration	94
8.1.	Service access information	94
8.2.	Numbers Assigned by Verizon	94
9.	Verification Steps.....	94
9.1.	Avaya Communication Server 1000E Verifications.....	94
9.1.1	IP Network Maintenance and Reports Commands	94
9.1.2	System Maintenance Commands.....	96
9.2.	Wireshark Verification.....	97
9.3.	System Manager and Session Manager Verification	100
9.3.1	Verify SIP Entity Link Status	100
9.3.2	Call Routing Test	101
9.4.	Avaya Aura® Session Border Controller Verification	102
9.4.1	Status Tab.....	102
9.4.2	Call Logs	103
10.	Conclusion	105
11.	Additional References.....	105
11.1.	Avaya	105
11.2.	Verizon Business	106

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Aura® Session Border Controller Release 6.0. The enterprise equipment is integrated with the Verizon Business IP Contact Center (IPCC) Services suite. The Verizon Business IPCC Services suite is comprised of 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. Using the sample configuration, PSTN callers may dial toll-free numbers associated with the IP Toll Free and IP-IVR services to reach Avaya Communication Server 1000E telephone users.

Access to the IPCC Services suite may use Internet Dedicated Access (IDA) or Private IP (PIP). The configuration documented in these Application Notes used the Verizon IPCC service terminated via a PIP network connection, but the solution validated in this document can also be applied to IPCC services delivered via IDA service terminations. IP Toll Free 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.

In the sample configuration, an Avaya Aura® Session Border Controller (SBC) is used as an edge device between the Avaya CPE and Verizon Business. The SBC performs SIP header manipulation and topology hiding to convert the private Avaya CPE IP addressing to IP addressing appropriate for the Verizon access method.

Customers using Avaya Communication Server 1000E with the Verizon Business IP Contact Center services are able to receive inbound toll-free calls from the PSTN via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

For more information on the Verizon Business IP Contact Center service, including access alternatives, visit <http://www.verizonbusiness.com/products/contactcenter/ip/>

2. General Test Approach and Test Results

Avaya CS1000E location was connected to the Verizon Business IPCC Service, as depicted in **Figure 1**. Avaya equipment was configured to use the commercially available IP Toll Free VoIP Inbound and IP-IVR services that comprise the Verizon Business IPCC services suite.

2.1. Interoperability Compliance Testing

The testing included executing the test cases detailed in Reference [VZ-Test-Plan]. To summarize, the testing included the following successful compliance testing:

- Incoming calls from the PSTN were routed to the toll-free numbers assigned by Verizon Business to the Avaya CS1000E location. These incoming were answered by Avaya IP-UNISTim telephones, Avaya SIP telephones, Avaya digital telephones, and analog telephones. The display of caller ID on display-equipped Avaya telephones was verified.
- Proper disconnect when the PSTN caller abandons a call before answer.
- Proper disconnect when either party hangs up an active call.
- Proper busy tone heard when a PSTN user calls a toll-free number directed to a busy CS1000E user (i.e., if no redirection is configured for user busy conditions).
- 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 to a CS1000E user while presenting an anonymous display to the CS1000E user.
- SIP OPTIONS monitoring of the health of the SIP trunk was verified. Both Verizon Business and the enterprise SBC can monitor health using SIP OPTIONS. The Avaya Aura® SBC configurable control of SIP OPTIONS timing was exercised successfully.
- Calls using the G.729A (IP Toll Free) and G.711 ULAW (IP-IVR) codecs, and proper protocol procedures related to media
- DTMF transmission using RFC 2833.
- Inbound toll-free call long holding time call stability
- Telephony features such as call waiting, hold, transfer, and conference. Note that CS1000E will not send REFER to the Verizon network.
- Proper DiffServ markings for SIP signaling and RTP media sent to Verizon

2.2. Test Results

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

1. The Verizon IPCC Service does not support fax.
2. Although the Verizon Business IP Contact Center service supports transfer using the SIP REFER method, Avaya CS1000E does not support sending REFER to Verizon.
3. The SIP protocol allows sessions to be refreshed for calls that remain active for some time. In the tested configuration, neither Verizon nor CS1000E send re-INVITE or UPDATE

messages to refresh a session. In the tested configuration, this is transparent to the users that are party to the call in that the media paths remain established.

4. When Avaya Aura® Session Border Controller generates a SIP response (e.g., 180 Ringing or 200 OK for an incoming toll-free call from Verizon), an empty “Request:” header is included. Although this does not have a negative effect on calls (i.e., no user-perceivable problem was observed), product defect **PD00016834** is expected to correct this in a forthcoming SBC service pack.
5. Since the Avaya CPE will respond to an incoming IP-IVR call with 180 Ringing (without SDP), the Verizon IP-IVR service programming must provide pre-answer call treatments (e.g., ring back tone or other network-provided call treatments).

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, visit the online support site at <http://www.verizonbusiness.com/us/customer/>.

3. Reference Configuration

Figure 1 illustrates an example Avaya CS1000E solution connected to the Verizon Business IPCC service. Avaya equipment is located on a private IP network. An enterprise edge router provides access to the Verizon IPCC service network via a T1 circuit provisioned for the Verizon Business Private IP (PIP) service. At the edge of the Avaya CPE location, an Avaya Aura® Session Border Controller (SBC) provides topology hiding and SIP header manipulation. The SBC receives traffic from Verizon Business IPCC Services on port 5060 and sends traffic to the Verizon Business IPCC Services using destination port 5072, using the UDP protocol.

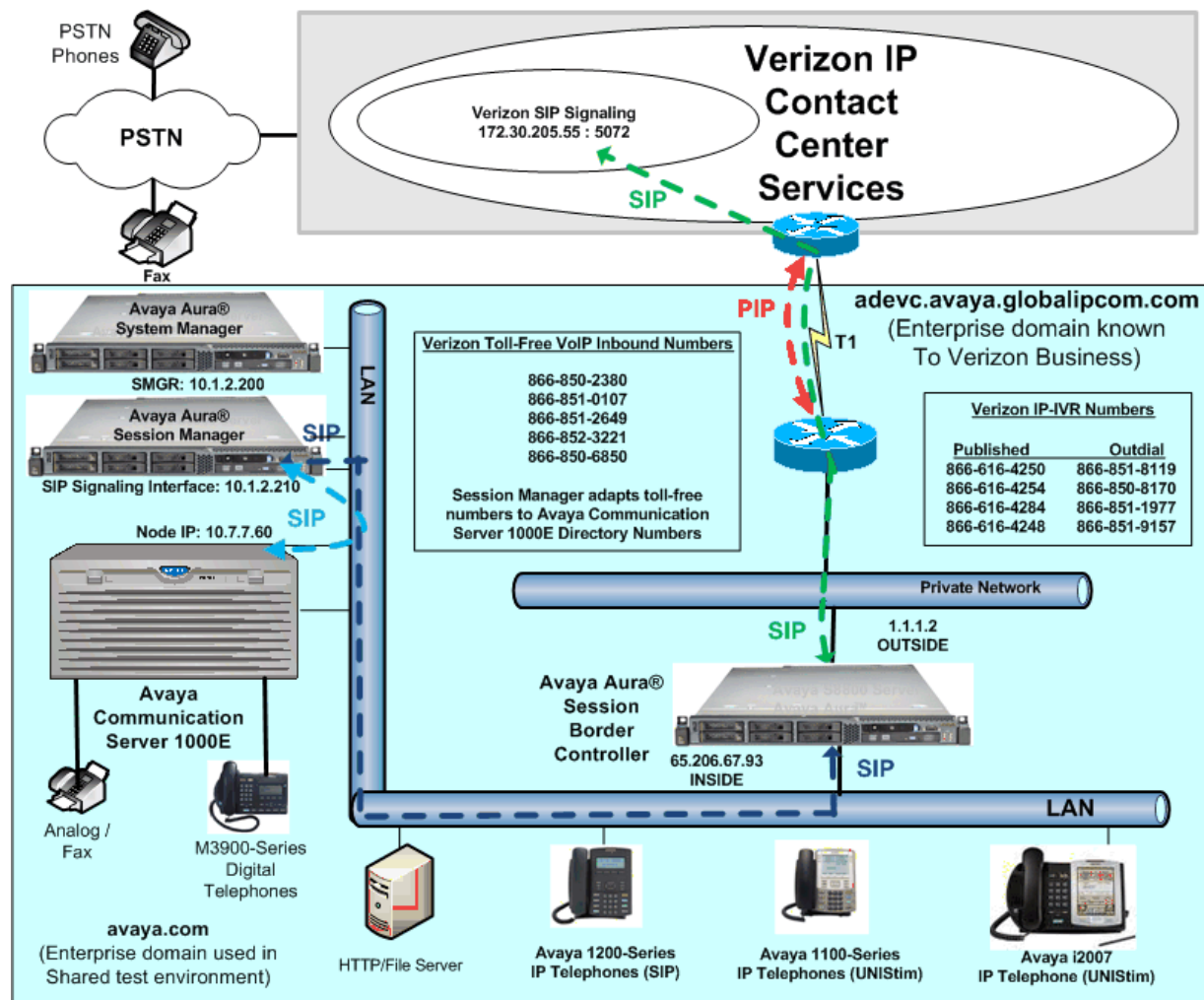


Figure 1: Verizon IP Contact Center Avaya Interoperability Test Lab Configuration

The Avaya CPE was known to Verizon Business as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya environment utilizing Session Manager Release 6.1 and Communication Server 1000E Release 7.5 was shared among many ongoing test efforts at the Avaya Solution and Interoperability Test lab. Access to the Verizon Business IPCC service was added to a configuration that already used domain “avaya.com” at the enterprise. Session Manager is used to adapt the “avaya.com” domain to the domains known to Verizon. These Application Notes indicate the configuration that would not be required in cases where the CPE domain in Communication Server 1000E and Session Manager match the CPE domain known to Verizon.

Table 1 lists a sampling of Verizon Business IP Toll-Free numbers that terminated at the Avaya CS1000E location. These toll-free numbers were mapped to Avaya CS1000E users via an Avaya Aura® Session Manager adaptation.

Verizon IP Toll-Free Number	Avaya CS1000E Destination	Notes
866-850-2380	x57005	Avaya M3903 Digital Telephone
866-850-6850	x57003	Avaya IP Phone 2007 (UNISim)
866-852-3221	x57007	Avaya 1200-Series IP Deskphone (SIP)

Table 1: Sample Verizon IP Toll Free Number to CS1000E Telephone Mappings

Table 2 lists a sampling a sampling of Verizon Business IP-IVR numbers that terminated at the Avaya CS1000E location. The IP-IVR Outdial numbers were mapped to Avaya CS1000E users via an Avaya Aura® Session Manager adaptation.

Verizon IP IVR Published Number	Verizon IP IVR Outdial Number	Avaya CS1000E Destination	Notes
866-616-4250	866-851-8119	x57005	Avaya M3903 Digital Telephone
866-616-4254	866-850-8170	x57007	Avaya 1200-Series IP Deskphone (SIP)
866-616-4284	866-851-1977	x57003	Avaya IP Phone 2007 (UNISim)

Table 2: Sample Verizon IP-IVR Number to CS1000E Telephone Mappings

In the sample configuration, the Verizon Business PIP circuit previously shown in **Figure 1** enabled access to the Verizon IP Trunk Service as well as the Verizon IPCC Service. The companion Application Notes available in Reference [AuraSBC-IP-Trunk] detail the overall configuration for access to the Verizon IP Trunk service. Although Verizon IP Trunk service is not the focus of these Application Notes, the figure below is included because the Verizon IPCC Service configuration builds upon the configuration detailed in Reference [AuraSBC-IP-Trunk], particularly Avaya Aura® Session Border Controller configuration in Section 7.

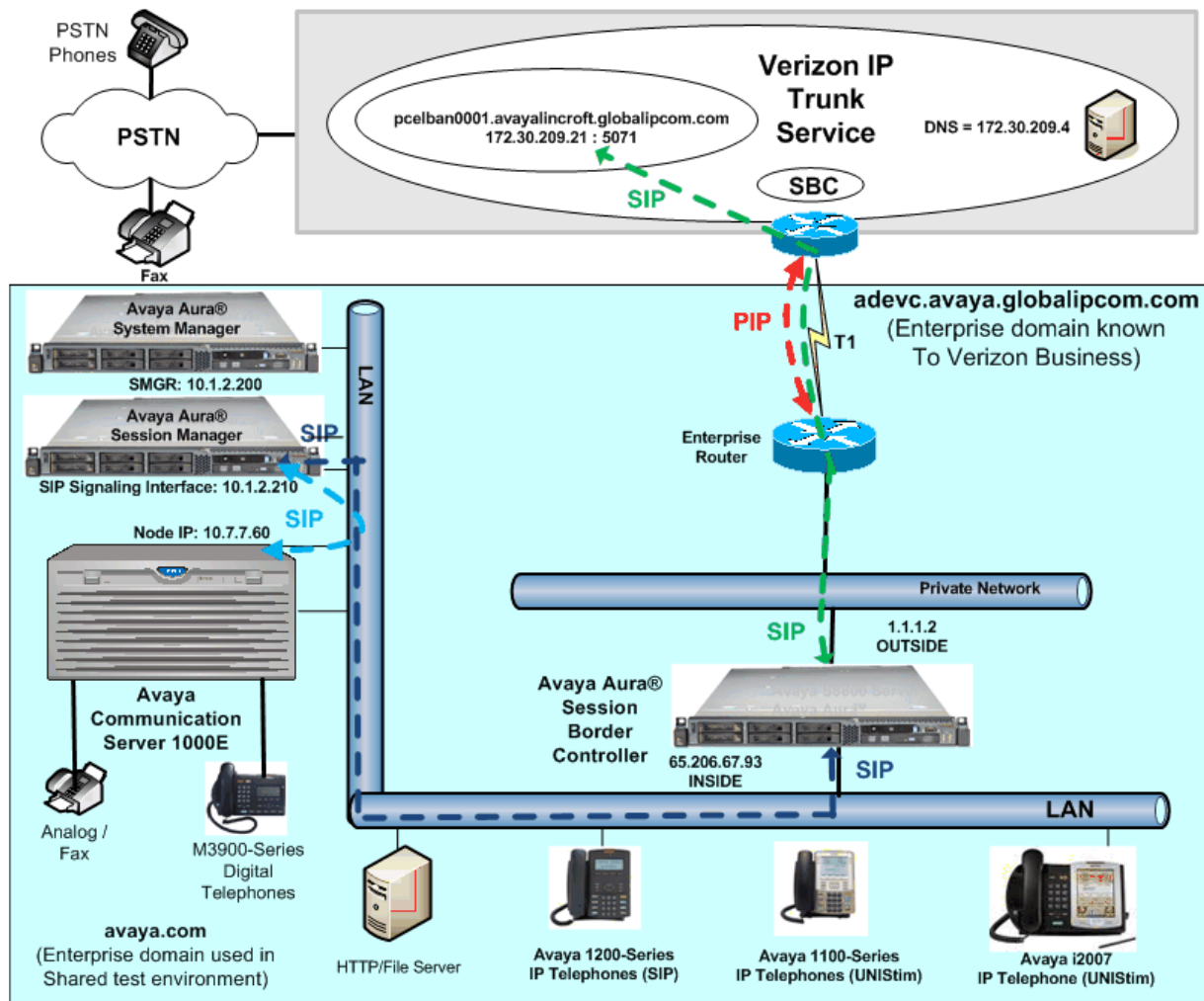


Figure 2: Verizon IP Trunk Avaya Interoperability Test Lab Configuration

The following components were used in the sample configuration:

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

- Avaya CPE Fully Qualified Domain Name (FQDN) known to Verizon
 - *adevc.avaya.globalipcom.com*
- Avaya Aura® Session Border Controller (SBC)
- Avaya Communication Server 1000E Release 7.5
- Avaya Aura® System Manager Release 6.1
- Avaya Aura® Session Manager Release 6.1
- Avaya IP-2007 UNISTim telephones
- Avaya 1100-Series IP Deskphones using UNISTim software
- Avaya 1200-Series IP Deskphones using SIP software, registered to CS1000E
- Avaya M3900-Series Digital phones
- Analog telephones

4. Equipment and Software Validated

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

Equipment	Software
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Release 7.5, Version 7.50.17 (with latest Patches and Deplist) Plug-in 201 Enabled Plug-in 501 Enabled
Avaya S8800 Server (System Manager)	Avaya Aura® System Manager Release 6.1.5.0 (Build Number 6.1.0.0.7345 Patch 6.1.5.7)
Avaya S8800 Server (Session Manager)	Avaya Aura® Session Manager Release 6.1 (Load 6.1.1.0.611023)
Avaya S8800 Server (Session Border Controller)	Avaya Aura® Session Border Controller Release 6.0 SBC Template SBCT 6.0.0.1.5
Avaya 1100-Series IP Deskphones (UNISTim)	FW 0624C8A
Avaya 1200-Series IP Deskphones (SIP)	SIP 04.00.04.00
Avaya IP Phone 2007 (UNISTim)	FW 0621C8A
Avaya M3900-Series Digital Telephone	N/A

Table 3: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the SIP Trunk to Session Manager. As described in Section 3, the same Avaya Communication Server 1000E SIP Trunking configuration was used to test both Verizon IP Trunk Service and Verizon IPCC Service. The configuration for outbound calling using Verizon IP Trunk Service is more fully documented in the companion Application Notes in Reference [AuraSBC-IP-Trunk].

In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server and Call Server applications all running on the same CP-PM server platform.

Avaya Aura® Session Manager Release 6.1 provides all the SIP Proxy Service (SPS) and Network Connect Services (NCS) functions previously provided by the Network Routing Service (NRS). As a result, the NRS application is not required to configure a SIP trunk between Avaya Communication Server 1000E and Session Manager Release 6.1.

This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E is configured to support analog, digital, UNISTim, and SIP telephones. For references on how to administer these functions of Avaya Communication Server 1000E, see Section 11.

Configuration will be shown using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched directly via **https://<ip-address>** where the relevant <ipaddress> in the sample configuration is 10.7.7.61. The following screen shows an abridged log in screen. Log in with appropriate credentials.

Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

[Go to central login for Single Sign-On](#)

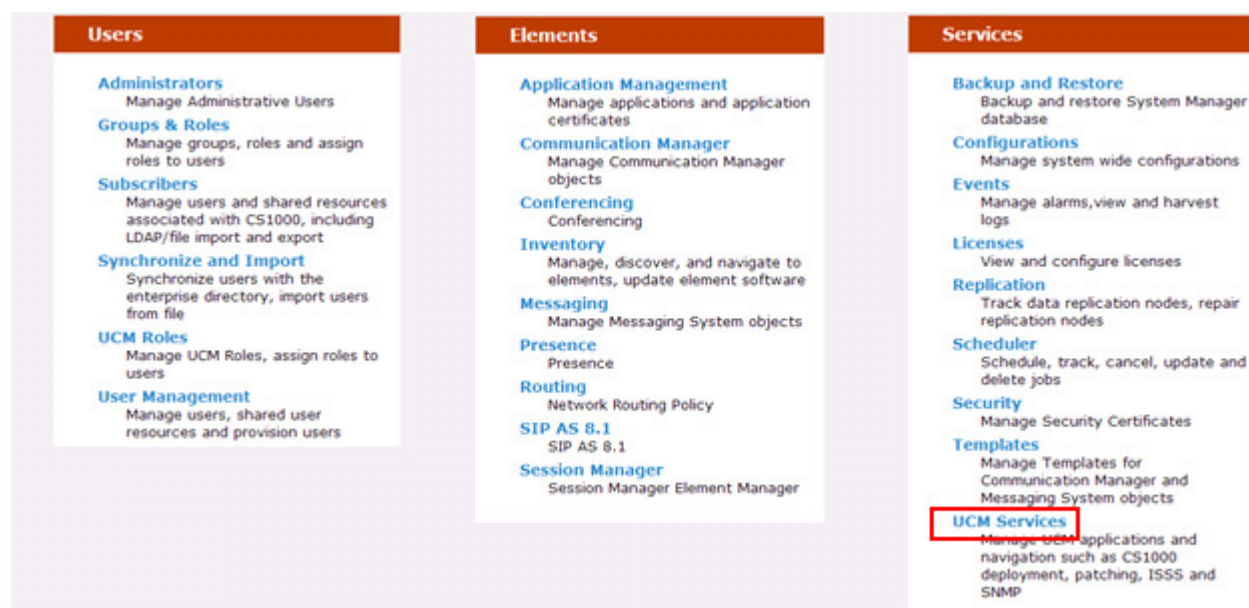
User ID:

Password:

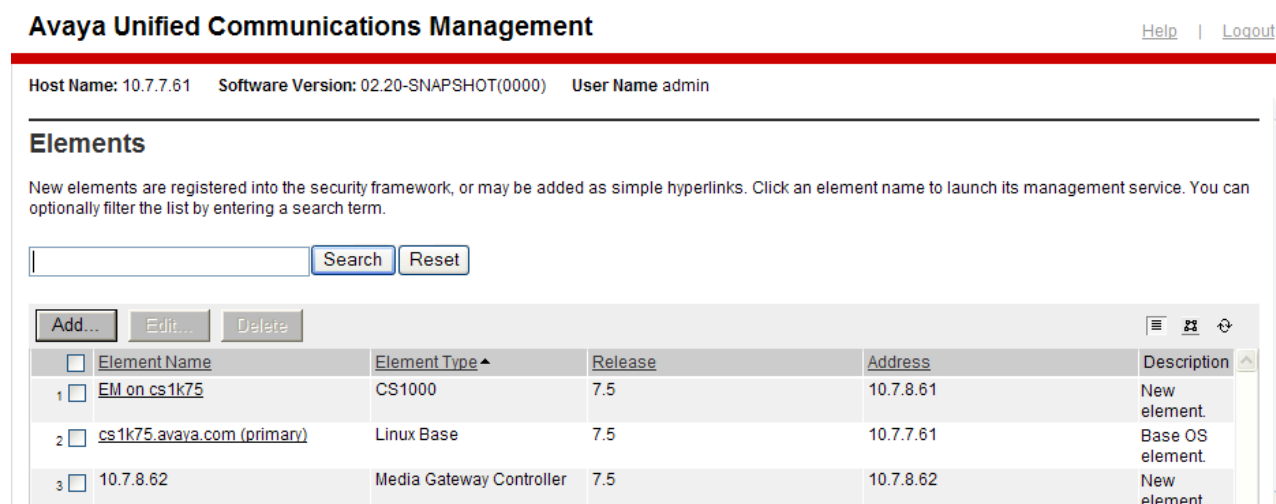
[Change Password](#)

Alternatively, if Avaya Aura® System Manager has been configured as the Primary Security Server for the Avaya Unified Communications Management application and Avaya Communication Server 1000E is registered as a member of the System Manager Security framework, the GUI may be accessed via System Manager. In this case, access the web based GUI of Avaya Aura® System Manager by using the URL “**http://<ip-address>/SMGR**”, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Log in with appropriate credentials.

The Avaya Aura® System Manager Home Page will be displayed. Under the **Services** category on the right side of the page, click the **UCM Services** link.



Whether the CS1000E is accessed directly or via System Manager, the Avaya Unified Communications Management **Elements** page will be used for configuration. Click on the **Element Name** corresponding to “CS1000” in the **Element Type** column. In the abridged screen below, the user would click on the **Element Name** “EM on cs1k75”.



5.1. Node and Key IP Addresses

Expand **System** → **IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Click “<Node id>” in the **Node ID** column to view details of the node. In the sample configuration, **Node ID “2”** was used.

Managing: 10.7.8.61 Username: admin
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

[Add...](#) [Import...](#) [Export...](#) [Delete](#) [Print](#) [Refresh](#)

<input type="checkbox"/> Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 2	1	SIP Line, LTPS, Gateway (SIPGw, H323Gw)	-	10.7.7.60		Synchronized

Show: ☒ Nodes ☐ Component servers and cards ☒ IPv6 address

The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPV4 address**. In the sample screen below, the **Node IPV4 address** is “10.7.7.60”. This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E.

CS1000 Element Manager

Managing: 10.7.8.61 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 2 - SIP Line, LTPS, Gateway (SIPGw, H323Gw))

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: *

Subnet mask: *

Telephony LAN (TLAN)

Node IPv4 address: *

Subnet mask: *

Node IPv6 address:

* Required Value. [Save](#) [Cancel](#)

The following screen shows the **Associated Signaling Servers & Cards** heading at the bottom of the screen, simply to document the configuration.

Associated Signaling Servers & Cards

[Select to add](#) [Add](#) [Remove](#) [Make Leader](#) [Print](#) [Refresh](#)

<input type="checkbox"/> Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.7.8.61	10.7.7.61	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list .

Expand **System** → **IP Network** on the left panel and select **Media Gateways**. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for an inbound Verizon toll-free call to a digital telephone, the IP Address in the SDP in the 200 OK message will be 10.7.7.63 in the sample configuration.

Managing: 10.7.8.61 Username: admin
System » IP Network » Media Gateways » IPMG 4.0 Property Configuration » IPMG 4.0 Media Gateway Controller (MGC) Configuration

IPMG 4.0 Media Gateway Controller (MGC) Configuration

- Media Gateway Controller

Hostname	MGC *
Embedded LAN (ELAN) IP address	10.7.8.62
Embedded LAN (ELAN) gateway IP address	10.7.8.1
Embedded LAN (ELAN) subnet mask	255.255.254.0
Telephony LAN (TLAN) IP address	10.7.7.62
Telephony LAN (TLAN) gateway IP address	10.7.7.1
Telephony LAN (TLAN) subnet mask	255.255.255.0

- DSP Daughterboard 1

Type of the DSP daughterboard	DB96 ▼
Telephony LAN (TLAN) IP address	10.7.7.63
Telephony LAN (TLAN) gateway IP address	10.7.7.1

5.2. Virtual D-Channel, Routes and Trunks

Avaya Communication Server 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server.

5.2.1 Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left navigation panel and select **D-Channels**. In the sample configuration, there is a virtual D-Channel 1 associated with the Signaling Server.

Managing: **10.7.8.61** Username: admin
Routes and Trunks » D-Channels

D-Channels

Maintenance

- [D-Channel Diagnostics](#) (LD 96)
- [Network and Peripheral Equipment](#) (LD 32, Virtual D-Channels)
- [MSDL Diagnostics](#) (LD 96)
- [TMDI Diagnostics](#) (LD 96)
- [D-Channel Expansion Diagnostics](#) (LD 48)

Configuration

Choose a D-Channel Number: and type:

- Channel: 1	Type: DCH	Card Type: DCIP	Description: VirtDchToSS	<input type="button" value="Edit"/>
- Channel: 3	Type: DCH	Card Type: DCIP	Description: ForSIPLineGW	<input type="button" value="Edit"/>

5.2.2 Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left navigation panel and expand the customer number. In the screen that follows, it can be observed that Route 1 has 10 trunks in the sample configuration.

Managing: **10.7.8.61** Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

- Customer: 0	Total routes: 2	Total trunks: 20	<input type="button" value="Add route"/>
- Route: 1	Type: TIE	Description: VTRKTOSS	<input type="button" value="Edit"/> <input type="button" value="Add trunk"/>
+ Trunk: 1 - 10	Total trunks: 10		
+ Route: 2	Type: TIE	Description: SIPLINE	<input type="button" value="Edit"/> <input type="button" value="Add trunk"/>

Select **Edit** to verify the configuration, as shown below. Verify “**SIP (SIP)**” has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** matches the node shown in Section 5.1. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. Recall that the same configuration is used for Verizon IP Trunk Service, which supports outbound dialing to the PSTN. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the

number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy. The **Zone for codec selection and bandwidth management (ZONE)** parameter can be used to associate the route with a zone for configuration of the audio codec preferences sent via the Session Description Protocol (SDP) in SIP messaging.

Customer 0, Route 1 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :	<input type="text" value="RDB"/>
Customer number (CUST) :	<input type="text" value="00"/>
Route number (ROUT) :	<input type="text" value="1"/>
Designator field for trunk (DES) :	<input type="text" value="VTRKTOSS"/>
Trunk type (TKTP) :	<input type="text" value="TIE"/>
Incoming and outgoing trunk (ICOG) :	<input type="text" value="Incoming and Outgoing (IAO)"/>
Access code for the trunk route (ACOD) :	<input type="text" value="5770001"/>
Trunk type M911P (M911P) :	<input type="checkbox"/>
The route is for a virtual trunk route (VTRK) :	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE) :	<input type="text" value="00001"/> (0 - 8000)
- Node ID of signaling server of this route (NODE) :	<input type="text" value="2"/> (0 - 9999)
- Protocol ID for the route (PCID) :	<input type="text" value="SIP (SIP)"/>

Scrolling down, other parameters may be observed. The **D channel number (DCH)** field must match the D-Channel number shown in Section 5.2.1.

Integrated services digital network option (ISDN) :	<input checked="" type="checkbox"/>
- Mode of operation (MODE) :	<input type="text" value="Route uses ISDN Signaling Link (ISLD)"/>
- D channel number (DCH) :	<input type="text" value="1"/> (0 - 254)
- Interface type for route (IFC) :	<input type="text" value="Meridian M1 (SL1)"/>
- Private network identifier (PNI) :	<input type="text" value="00000"/> (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>
- Network call redirection (NCRD) :	<input checked="" type="checkbox"/>

5.3. SIP Trunk to Session Manager

Expand **System** → **IP Network** → **Nodes: Servers, Media Cards**. Click “2” in the **Node ID** column (not shown) to edit configuration settings for the configured node.

Using the scroll bar on the right side of the screen, navigate to the **Applications** section on the screen and select the **Gateway (SIPGw & H323Gw)** link to view or edit the SIP Gateway configuration.

Managing: 10.7.8.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 2 - SIP Line, LTPS, Gateway (SIPGw, H323Gw))

Subnet mask: 255.255.255.0 *	Subnet mask: 255.255.255.0 *
Node IPv6 address: <input type="text"/>	
IP Telephony Node Properties <ul style="list-style-type: none">• Voice Gateway (VGW) and Codecs• Quality of Service (QoS)• LAN• SNTP• Numbering Zones• MCDN Alternative Routing Treatment (MALT) Causes	Applications (click to edit configuration) <ul style="list-style-type: none">• SIP Line• Terminal Proxy Server (TPS)• Gateway (SIPGw & H323Gw)• Personal Directories (PD)• Presence Publisher• IP Media Services
* Required Value.	
<div>Save Cancel</div>	

On the **Node ID: 2 - Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields.

- **SIP domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, “**avaya.com**” was used in the shared Avaya Solution and Interoperability Test lab environment. The SIP domain name for the enterprise known to Verizon is “**adevc.avaya.globalipcom.com**”, and the SIP domain will be adapted by Session Manager for calls to and from the Avaya CS1000E. If no such adaptation is required, enter the domain known to Verizon.
- **Local SIP port:** Enter “**5060**”
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter “**<Node id>**”. In the sample configuration, “**2**” was used, matching the node shown in Section 5.1.

The values defined for the sample configuration are shown below.

Managing: 10.7.8.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2 - Virtual Trunk Gateway Configuration Details

[General](#) | [SIP Gateway Settings](#) | [SIP Gateway Services](#) | [H.323 Gateway Settings](#)

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIPGw and H.323Gw

SIP domain name: avaya.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: CS1KGateway *

Gateway password: *

H.323 ID: CS1KGateway *

Application node ID: 2 * (0-9999)

Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)
Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

Scroll down to the **SIP Gateway Settings → Proxy or Redirect Server:** section.

Under **Proxy Server Route 1**, enter the following and use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration, “**10.1.2.210**” was used.
- **Port:** Enter “**5060**”
- **Transport protocol:** Select “**TCP**”

The values defined for the sample configuration are shown below.

Node ID: 2 - Virtual Trunk Gateway Configuration Details

The screenshot displays the configuration interface for a Virtual Trunk Gateway. The top navigation bar includes tabs for General, SIP Gateway Settings, SIP Gateway Services, and H.323 Gateway Settings. The main content area is titled 'Proxy Or Redirect Server:' and contains a section for 'Proxy Server Route 1:'. Under this section, there are two sets of configuration fields. The first set, for the Primary TLAN IP address, shows the value '10.1.2.210' in a text box, with a note below stating 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"'. Below this is a 'Port' field with the value '5060' and a range '(1 - 65535)', and a 'Transport protocol' dropdown menu set to 'TCP'. There are also two unchecked checkboxes labeled 'Support registration' and 'Primary CDS proxy'. The second set of fields is for the 'Secondary TLAN IP address', showing the value '0.0.0.0' with the same explanatory note, a 'Port' field with '5060' and '(1 - 65535)', and a 'Transport protocol' dropdown menu set to 'TCP'. A vertical scrollbar is visible on the right side of the configuration area.

Scroll down and repeat these steps for the **Proxy Server Route 2**.

Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. In general, the **SIP URI Map** values have been set to blank for call types that may ultimately interact with Verizon. The Avaya CS1000E will put the “string” entered in the **SIP URI Map** in the “phone-context=<string>” parameter in SIP headers such as the P-Asserted-Identity. If the value is configured to blank, the CS1000E will omit the “phone-context=” in the SIP header altogether.

Node ID: 2 - Virtual Trunk Gateway Configuration Details

SIP URI Map:	
Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text"/>
Subscriber: <input type="text"/>	CDP: <input type="text" value="cdp udp"/>
Special number: <input type="text"/>	Special number: <input type="text"/>
Unknown: <input type="text"/>	Vacant number: <input type="text"/>
	Unknown: <input type="text"/>

Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. This will return the interface to the **Node Details** screen. Click **Save** on the **Node Details** screen (not shown).

Select **Transfer Now** on the **Node Saved** page as shown below.

Managing: 10.7.8.61 Username: admin
System » IP Network » IP Telephony Nodes » Node Saved

Node Saved

Node ID: 2 has been saved on the call server.
The new configuration must also be transferred to associated servers and media cards.

Transfer Now... You will be given an option to select individual servers, or transfer to all.

Show Nodes You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed.

Synchronize Configuration Files (Node ID <2>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input type="checkbox"/>	cs1k75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

Enter ☒ associated with the appropriate Hostname and click **Start Sync**. The screen will automatically refresh until the synchronization is finished.

Synchronize Configuration Files (Node ID <2>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

The **Synchronization Status** field will update from **Sync required** (as shown above) to **Synchronized** (as shown below). After synchronization completes, enter ☒ associated with the appropriate Hostname and click **Restart Applications**.

Synchronize Configuration Files (Node ID <2>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

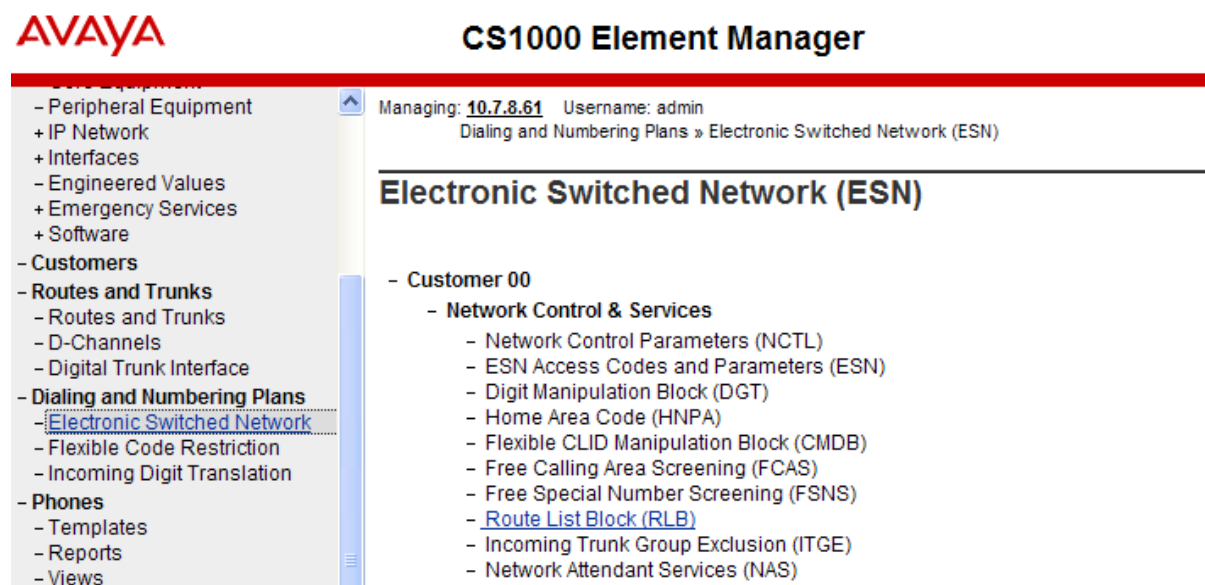
<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

5.4. Routing of Dialed Numbers to Session Manager

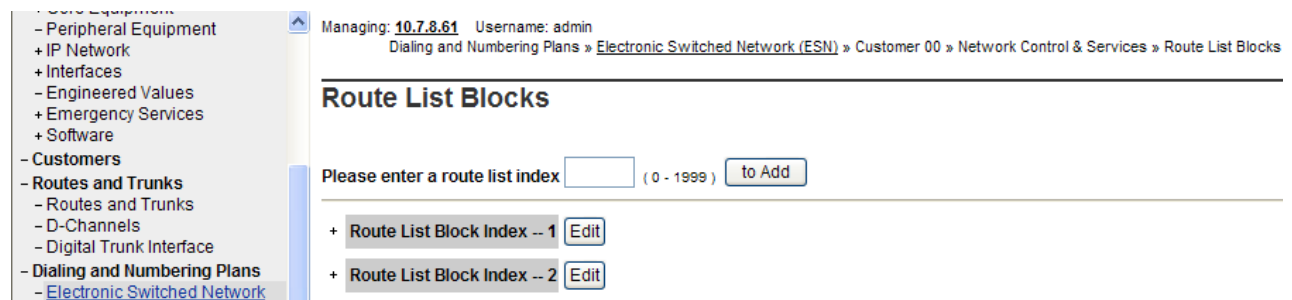
This section illustrates routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the Verizon IP Trunk service, which was available from the same PIP circuit as the Verizon IPCC Service. The routing defined in this section is simply informational, and not intended to be prescriptive.

5.4.1 Route List Block

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.



The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **Add**, or edit an existing entry by clicking the corresponding Edit button. In the sample configuration, route list block index 1 is used.



If adding the route list index anew, scroll down to the **Options** area of the screen. If editing an existing route list block index, select the **Edit** button next to the appropriate **Data Entry Index** as shown below, and scroll down to the **Options** area of the screen.

+ Data Entry Index -- 0 [Edit](#)

Under the **Options** section, select “<Route id>” in the **Route Number** field. In the sample configuration route number 1 was used. Default values may be retained for remaining fields as shown below.

Indexes

Time of Day Schedule:	0	▼
Facility Restriction Level:	0	(0 - 7)
Digit Manipulation Index:	0	▼
ISL D-Channel Down Digit Manipulation Index:	0	(0 - 1999)
Free Calling Area Screening Index:	0	▼
Free Special Number Screening Index:	0	▼
Business Network Extension Route:	<input type="checkbox"/>	
Incoming CLID Table:	0	(0 - 200)

Options

Local Termination entry:	<input type="checkbox"/>
Route Number:	1 ▼
Skip Conventional Signaling:	<input type="checkbox"/>

Click **Save** (not shown) to save the Route List Block definition.

5.4.2 NARS Access Code

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in Section 5.4.1. In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit “9” was used.

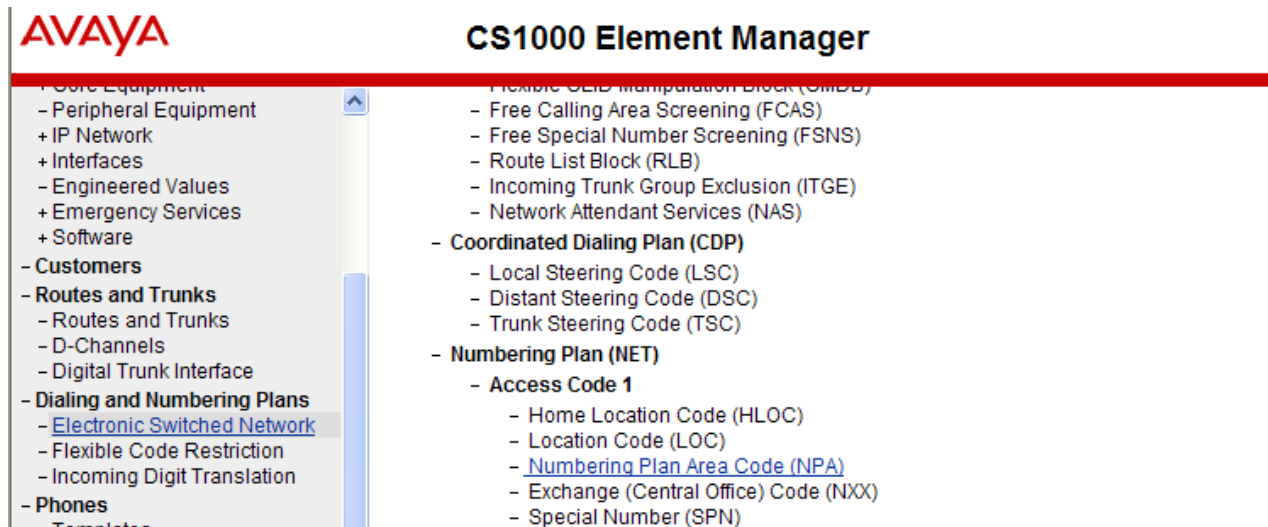
ESN Access Codes and Basic Parameters

General Properties

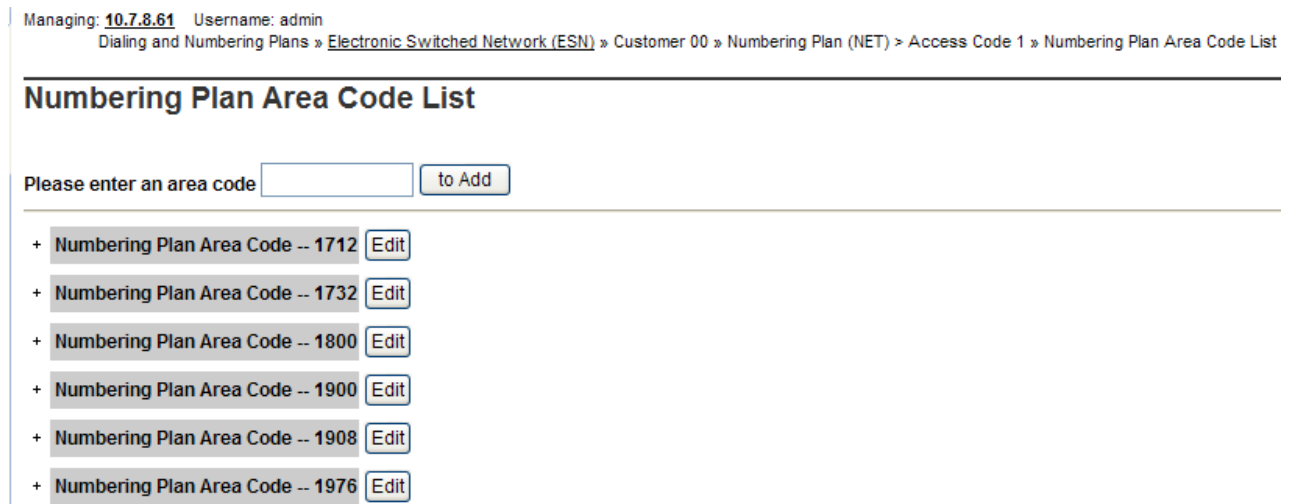
NARS/BARS Access Code 1:	9
NARS Access Code 2:	
NARS/BARS Dial Tone after dialing AC1 or AC2 access codes:	<input checked="" type="checkbox"/>
Expensive Route Warning Tone:	<input checked="" type="checkbox"/>
- Expensive Route Delay Time:	6 (0 - 10)
Coordinated Dialing Plan feature for this customer:	<input checked="" type="checkbox"/>
- Maximum number of Steering Codes:	5000 (1 - 64000)
- Number of digits in CDP DN (DSC + DN or LSC + DN):	5 (3 - 10)

5.4.3 Numbering Plan Area Codes

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Scroll down and select **Numbering Plan Area Code (NPA)** under the appropriate access code heading. In the sample configuration, this is **Access Code 1**, as shown in below.



Add a new NPA by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured. In the screen below, it can be observed that various dial strings such as 1800 and 1908 are configured.



In the screen below, the entry for “1908” is displayed. In the Route List Index, “1” is selected to use the route list associated with the SIP Trunk to Session Manager. Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to Session Manager.

Numbering Plan Area Code

General Properties

Numbering Plan Area code translation:

Route List Index:

Incoming Trunk group Exclusion Index:

5.5. Zones

Zone configuration can be used to control codec selection and for bandwidth management. To configure, expand **System** → **IP Network** and select **Zones** as shown below.

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - **Zones**

Managing: **10.7.8.61** Username: admin
System » IP Network » Zones

Zones

Zones are used to group related information for either bandwidth or dial plan numbering purposes.

Bandwidth Zones
Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones
Numbering zones are used to route calls through a centralized call server.

Select **Bandwidth Zones**. In the sample configuration, two zones are configured as shown below. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration, this is Zone number 1.

Managing: **10.7.8.61** Username: admin
System » IP Network » **Zones** » Bandwidth Zones

Bandwidth Zones

<div>Add... Edit... Import... Export Maintenance... Delete</div>								
	Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	1000000	BB	1000000	BB	SHARED	VTRK	VTRKZONE
2	2	1000000	BQ	1000000	BQ	SHARED	MO	IPPHONE

In the resultant screen shown below, select **Zone Basic Property** and **Bandwidth Management**.

Edit Bandwidth Zone

[Zone Basic Property and Bandwidth Management](#)

[Adaptive Network Bandwidth Management and CAC](#)

[Alternate Routing for Calls between IP Stations](#)

[Branch Office Dialing Plan and Access Codes](#)

[Branch Office Time Difference and Daylight Saving Time Property](#)

[Media Services Zone Properties](#)

The following screen shows the Zone 1 configuration. Note that “Best Bandwidth (BB)” is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with Verizon. Using the production circuit, inbound Verizon IP Toll Free calls preferred and used G.729A while Verizon offered only G.711MU for inbound IP-IVR calls.

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	<input type="text" value="1"/> * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	<input type="text" value="1000000"/> (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB) ▼
Interzone Bandwidth (INTER_BW):	<input type="text" value="1000000"/> (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	VTRK (VTRK) ▼
Description (ZDES):	<input type="text" value="VTRKZONE"/>

5.6. Codec Parameters, Including Ensuring Annexb=no for G.729

Verizon IPCC Service does not support G.729 Annex B, and Verizon requires that SDP offers and SDP answers in SIP messages include the “annexb=no” attribute when G.729 is used. This section includes the configuration that ensures that the “annexb=no” attribute is included.

5.6.1 Media Gateway Configuration

To ensure that the “annexb=no” attribute is included, expand **System → IP Network** on the left panel and select **Media Gateways**. Select the appropriate media gateway (not shown), and scroll down to the area of the screen containing **VGW and IP phone codec profile** as shown below.

The screenshot displays the configuration interface for Media Gateways. On the left is a navigation tree under 'UCM Network Services' with 'Media Gateways' selected. The main area shows two sections: 'DSP Daughterboard 1' and 'DSP Daughterboard 2'. Each section contains fields for 'Type of the DSP daughterboard', 'Telephony LAN (TLAN) IP address', 'Telephony LAN (TLAN) gateway IP address', 'Telephony LAN (TLAN) IPv6 address', 'Telephony LAN (TLAN) subnet mask', and 'Hostname'. Below these is a section for 'VGW and IP phone codec profile'.

Section	Type of the DSP daughterboard	Telephony LAN (TLAN) IP address	Telephony LAN (TLAN) gateway IP address	Telephony LAN (TLAN) IPv6 address	Telephony LAN (TLAN) subnet mask	Hostname
DSP Daughterboard 1	DB96	10.7.7.63	10.7.7.1		255.255.255.0	CS1KR7DSP1 *
DSP Daughterboard 2	NODB	0.0.0.0	10.7.7.1		255.255.255.0	DB2 *

+ VGW and IP phone codec profile

Expand **VGW and IP phone codec profile**. To use G.729A, ensure that the **Select** box is checked for **Codec G729A**, and the **VAD** (Voice Activity Detection) box is un-checked.

Note that **Codec G.711** is enabled by default. **Voice payload size** “20” can be used with Verizon for both G.729A and G.711. The following screen shows the parameters used.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Interfaces, Customers, and Routes and Trunks. The 'Media Gateways' link is highlighted. The main content area shows two sections for codec configuration. The first section is for 'Codec G711', which is selected with a checked box. It lists settings: Codec name G711, Voice payload size 20 (ms/frame), Voice playout (jitter buffer) nominal delay 40, and Voice playout (jitter buffer) maximum delay 80. A red warning message states 'Modifications may cause changes to dependent settings'. The VAD checkbox is unchecked. The second section is for 'Codec G729A', also selected with a checked box. It lists the same settings: Codec name G729A, Voice payload size 20 (ms/frame), Voice playout (jitter buffer) nominal delay 40, and Voice playout (jitter buffer) maximum delay 80. A red warning message is also present. The VAD checkbox is unchecked.

AVAYA **CS1000 Element Manager**

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks

- Codec G711 Select ☒

Codec name G711

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

- Codec G729A Select ☒

Codec name G729A

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

5.6.2 Node Voice Gateway and Codec Configuration

Expand **System** → **IP Network** and select **Node, Server, Media Cards**. Select the appropriate **Node Id** “2” as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'System' expanded and 'Nodes: Servers, Media Cards' selected. The main content area is titled 'IP Telephony Nodes' and shows a table of nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. Node 2 is selected, showing 1 component and SIP Line, LTPS, Gateway (SIPGw, H323Gw) as the enabled application. The status is 'Synchronized'.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
2	1	SIP Line, LTPS, Gateway (SIPGw, H323Gw)	-	10.7.7.60		Synchronized

In the resultant screen (not shown) use the scroll bar on the right to select **Voice Gateway (VGW) and Codecs**. The following screen shows the **General** parameters used in the sample configuration.

The screenshot shows the 'Node ID: 2 - Voice Gateway (VGW) and Codecs' configuration page. The 'General' tab is selected. The configuration includes: Echo cancellation (checked, Use canceller, with tail delay: 128), Dynamic attenuation (checked), Voice activity detection threshold: -17 (-20 - +10 DBM), Idle noise level: -65 (-327 - +327 DBM), Signaling options (checked: DTMF tone detection, Remove DTMF delay (squelch DTMF from TDM to IP), Modem/Fax pass-through, V.21 Fax tone detection; unchecked: Low latency mode, R factor calculation).

Use the scroll bar on the right to find the area with heading **Voice Codecs**. Note that **Codec G.711** is enabled by default. The following screen shows the G.711 parameters used in the sample configuration.

The screenshot shows the 'Voice Codecs' configuration page. The 'Codec G711' is checked and 'Enabled (required)'. The 'Voice payload size' is 20 (milliseconds per frame). The 'Voice playout (jitter buffer) delay' is 40 (Nominal) and 80 (Maximum) milliseconds. The 'Voice Activity Detection (VAD)' is unchecked.

To allow the use of G.729, ensure that the **Enabled** box is checked for the **Codec G.729**, and the **Voice Activity Detection (VAD)** box is un-checked, as shown below.

AVAYA **CS1000 Element Manager**

Managing: 10.7.8.61 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 2 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

5.7. Enabling Plug-Ins for Call Transfer Scenarios

The procedures in this section are optional for Verizon IPCC deployments, but are included for completeness, since the same Avaya CS1000E configuration was used in testing both Verizon IP Trunk Service and Verizon IPCC Service. Plug-ins allow specific CS1000E software feature behaviors to be changed. In the testing associated with these Application Notes, two plug-ins were enabled as shown in this section.

To view or enable a plug-in, from the left navigation menu, expand **System** → **Software**, and select **Plug-ins**. In the right side screen, a list of available plug-ins will be displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-in 501 is displayed as shown in the screen below. If the **Status** is “Disabled”, select the check-box next to Number 501 and click the **Enable** button at the top, if it is desirable to allow CS1000E users to complete call transfer to PSTN destinations via the Verizon IP Trunk service before the call has been answered by the PSTN user. Note that enabling plug-in 501 will allow the user to complete the transfer while the call is in a ringing state, but no audible ring back tone will be heard after the transfer is completed.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like Maintenance, Core Equipment, Peripheral Equipment, IP Network, Zones, Host and Route Tables, Network Address Translation, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Software, Call Server PEPs, Loadware PEPs, File Upload, IP Phone Firmware, Voice Gateway Media Card, Media Cards PEPs, Plug-ins, Customers, Routes and Trunks, Routes and Trunks, and D-Channels. The 'Plug-ins' item is selected. The main area shows a table of plug-ins with columns for Number, Description, MPLR Number, and Status. Plug-in 501 is selected with a checkmark in the first column.

Number	Description	MPLR Number	Status
223	PL:ICOM REJECTS QSIG CCBS REQUEST WITH NO CALLING NUMBER	MPLR12290	Disabled
224	PI:No busy treatment on external transfer through application if OUT_T306 > 0	MPLR24676	Disabled
225	PI:PKG 179, Taurus, elektronick look, Mail and CallPilot softkeys	MPLR22389	Disabled
226	PI:ACLD should display more than 10 digits	MPLR15783	Disabled
228	PI: TTY 0 on CPU card (8/1/N) causes cursor to go up on VDU	MPLR07613	Disabled
230	PI: Unplugged telset disables after midnight routines.	MPLR11700	Disabled
231	PI: BRI 64K data not possible over DTI2. With mix of spans (both DTI and DTI2) THIS is not supported.	MPLR10878	Disabled
232	PI: QSIG GF: No diverting and originally called number in DLI2 APDU on calls from MCDN TRO-BA.	MPLR24273	Disabled
233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506	Disabled
235	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
500	NO DESCRIPTION	MPLR21979	Disabled
501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Disabled

The following screen shows the relevant portion of this same screen after plug-in 501 has been enabled.

97	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Enabled
98	504	PRI232 BUG253 from PI 10 Delay in Response at Called IFC	MPLR24744	Disabled
99	505	UM2K integration problem with S100 Interface	MPLR30004	Disabled

The same procedure may be used to enable plug-in 201 if desired. Plug-in 201 will allow a CS1000E user to make a call to the PSTN using the Verizon IP Trunk service, and then

subsequently perform an attended transfer of the call to another PSTN destination via the Verizon IP Trunk service.

Expand **System** → **Software**, and select **Plug-ins**. Use the scroll bar to scroll down so that Plug-in 201 is displayed as shown in the screen below. If the **Status** is “Disabled”, and it is desirable to allow attended transfer of an outbound trunk call to another outbound trunk, select the check-box next to Number 201 and click the **Enable** button at the top.

Managing: Username: System » Software » Plug-ins

Plug-ins

[Enable](#) [Disable](#) [Print](#)

<input type="checkbox"/>	Number	Description	MPLR Number	Status
<input type="checkbox"/>	61 70	SPN 411 WITH NON ZERO FLEN DISCARDS TAIL DIGITS	MPLR12554	Disabled
<input type="checkbox"/>	62 72	DAPC DIGIT INSERTION DOESNT WORK OVER DPNSS LINK	MPLR15741	Disabled
<input type="checkbox"/>	63 73	"MU-LAW" to "A-LAW" conversion cannot be administered on BRI	MPLR07113	Disabled
<input type="checkbox"/>	64 74	Support of "Time of day display" on DECT handsets	MPLR16079	Disabled
<input checked="" type="checkbox"/>	65 201	Pl:Cant XFER OUTG TRK TO OUTG TRK	MPLR08139	Disabled
<input type="checkbox"/>	66 202	Pl:Allow DNIS and INST prompt to work together	MPLR18286	Disabled
<input type="checkbox"/>	67 203	Pl:Allow Loop Start to Loop start Trunk Transfer	MPLR20783	Disabled
<input type="checkbox"/>	68 205	Unable to configure NI2-TIE with CBCR set to NO	MPLR21073	Disabled
<input type="checkbox"/>	69 206	Pl:Connected party number inserted at the tandem node	MPLR19491	Disabled
<input type="checkbox"/>	70 207	Pl:Ability to Ignore/Release or Dynamically divert calls without answering	MPLR23784	Disabled

The following screen shows the relevant portion of this same screen after plug-in 201 has been enabled.

63	<input type="checkbox"/>	73	"MU-LAW" to "A-LAW" conversion cannot be administered on BRI	MPLR07113	Disabled
64	<input type="checkbox"/>	74	Support of "Time of day display" on DECT handsets	MPLR16079	Disabled
65	<input type="checkbox"/>	201	Pl:Cant XFER OUTG TRK TO OUTG TRK	MPLR08139	Enabled

5.8. Customer Information

This section documents basic configuration relevant to the sample configuration. This section is not intended to be prescriptive. Select **Customers** from the left navigation menu, click on the appropriate **Customer Number** and select **ISDN and ESN Networking** (not shown). The following screen shows the **General Properties** used in the sample configuration.

Managing: [10.7.8.61](#) Username: admin
[Customers](#) » Customer 00 » [Customer Details](#) » ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:	<input type="text" value="Connections restricted"/>
Flexible orbiting prevention timer:	<input type="text" value="6"/>
Country code:	<input type="text" value="1"/> (0 - 9999)
National access code:	<input type="text" value="1"/>
International access code:	<input type="text" value="011"/>
Options:	<input checked="" type="checkbox"/> Transfer on ringing of supervised external trunks <input checked="" type="checkbox"/> Connection of supervised external trunks
Network option:	<input checked="" type="checkbox"/> Coordinated dialing plan routing
Integrated services digital network:	<input checked="" type="checkbox"/>
Microsoft converged office dialing plan:	<input type="text" value="Private dialing plan"/>

Calling Line Identification

Information for incoming/outgoing calls:	<input type="text" value="No manipulation is done"/>
--	--

5.8.1 Caller ID Related Configuration

Although not intended to be prescriptive, in the sample configuration, the CS1000E would send the user's five-digit directory number in SIP headers such as the From and PAI headers. Avaya Aura® Session Manager would adapt the user's directory number to an appropriate number before passing the message to the Avaya Aura® SBC towards Verizon.

Scroll down from the screen shown in Section 5.8, click the **Calling Line Identification Entries** link (now shown), and search for the **Calling Line Identification Entries** by **Entry ID**. As shown below, the **Use DN as DID** parameter was set to "YES" for the **Entry ID** "0" used in the sample configuration.

Calling Line Identification Entries

Search for CLID

Start range :

End range :

'End range' should not exceed the CLID size specified

Calling Line Identification Entries

<input type="checkbox"/>	Entry Id ▲	National Code	Local Code	Home location code	Local steering code	Use DN as DID
1	<input type="checkbox"/> 0					YES

Click on **Entry Id 0** to view or change further details. The following shows the **Calling Party Name Display** configuration used in the sample configuration.

Calling Party Name Display

Roman characters: ☒

CPND Name: *

first name, last name

Expected Length: 13

Display Format: ▼

5.9. Example CS1000 Telephone Users

This section is not intended to be prescriptive, but simply illustrates a sampling of the telephone users in the sample configuration. These telephone directory numbers can be observed in the Session Manager configuration, since Session Manager is used to adapt the Verizon IP toll free numbers to Avaya CS1000E user telephone numbers.

5.9.1 Example IP UNISTim Phone DN 57003, Codec Considerations

The following screen shows basic information for an IP UNISTim phone in the configuration. The telephone is configured as Directory Number 57003. Note that the telephone is in Zone 2. A call between this telephone and another telephone in Zone 2 will use a “best quality” strategy (see Section 5.5) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the Verizon IP Trunk service or receives an inbound Verizon IP Toll Free call, the call would use a “best bandwidth” strategy, and the call would use G.729A.

The screenshot displays the Avaya Session Manager configuration interface. On the left is a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System (with sub-items: + Alarms, - Maintenance, + Core Equipment, - Peripheral Equipment, + IP Network, + Interfaces, - Engineered Values, + Emergency Services, + Software), - Customers, - Routes and Trunks (with sub-items: - Routes and Trunks, - D-Channels, - Digital Trunk Interface), - Dialing and Numbering Plans (with sub-items: - Electronic Switched Network, - Flexible Code Restriction, - Incoming Digit Translation), - Phones (highlighted, with sub-items: - Templates, - Reports, - Views, - Lists, - Properties, - Migration), and - Tools. The main content area shows the configuration for a phone managed by 'EM on cs1k75(10.7.8.61)'. The breadcrumb is 'Phones»Phone Details'. The section is titled 'Phone Details' and includes an image of a telephone. To the right of the image, the following information is displayed: System: EM on cs1k75, Phone Type: 2007, and Sync Status: TRN. Below this is a tabbed interface with 'General Properties' selected, and other tabs for 'Features', 'Keys', and 'User Fields'. The 'General Properties' section contains the following fields: Customer Number (a dropdown menu showing '0' with an asterisk), Terminal Number (a text box containing '096 0 00 12'), Designation (a text box containing 'IP2007' with an asterisk and '(1-6 characters)' to its right), and Zone (a text box containing '2' with an asterisk).

Managing: EM on cs1k75(10.7.8.61)
Phones»Phone Details

Phone Details

System: EM on cs1k75
Phone Type: 2007
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

General Properties

Customer Number: 0 *

Terminal Number: 096 0 00 12

Designation: IP2007 * (1-6 characters)

Zone: 2 *

5.9.2 Example SIP Phone DN 57007, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 57007. Note that the telephone is in Zone 2 and is associated with Node 2 (see Section 5.1). A call between this telephone and another telephone in Zone 2 will use a “best quality” strategy (see Section 5.5) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the Verizon IP Trunk service, the call would use a “best bandwidth” strategy, and the call would use G.729A. Similarly, if the user receives a call from Verizon IP Toll Free service, the call will use G.729A.

The screenshot displays the configuration page for a SIP phone in the UCM Network Services interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, and Phones. The 'Phones' section is selected. The main area shows the 'General Properties' tab for a phone with a handset icon. System information at the top right indicates 'System: EM on cs1k75', 'Phone Type: UEXT-SIPL', and 'Sync Status: TRN'. Below this are tabs for 'General Properties', 'Features', 'Keys', and 'User Fields'. The 'General Properties' section contains several fields: 'Customer Number' (0), 'Terminal Number' (096 0 00 10), 'Designation' (1230SI), 'Zone' (2), 'SIP User Name' (57007), 'Node Id' (2), and 'Super User' (checkbox). Each field has a required field indicator (*).

System: EM on cs1k75
Phone Type: UEXT-SIPL
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

General Properties

Customer Number: 0 *

Terminal Number: 096 0 00 10

Designation: 1230SI * (1-6 characters)

Zone: 2 *

SIP User Name: 57007 * (1-16 characters)

Node Id: 2 *

Super User: ☐


5.9.3 Example Digital Phone DN 57005 with Call Waiting

The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 57005.

The screenshot shows the 'Phone Details' configuration page for a digital phone. On the left is a navigation menu with options like 'UCM Network Services', 'Home', 'Links', 'System', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', and 'Phones'. The main content area shows the phone's details for 'EM on cs1k75(10.7.8.61)'. It includes a photo of the phone, the system name, phone type (M3903), and sync status (TRN). Below this are tabs for 'General Properties', 'Features', 'Keys', and 'User Fields'. The 'General Properties' tab is active, showing fields for 'Customer Number' (0), 'Terminal Number' (004 0 02 00), and 'Designation' (R7DIG).

Managing: [EM on cs1k75\(10.7.8.61\)](#)
[Phones»Phone Details](#)

Phone Details

 System: EM on cs1k75
Phone Type: M3903
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#)

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone, and uses CLID Entry 0 (see Section 5.8). Although not shown in detail below, to use call waiting with tone, assign a key “CWT – Call Waiting”, set the feature “SWA – Call waiting from a Station” to “Allowed”, and set the feature “WTA – Warning Tone” to “Allowed”.

The screenshot shows the 'Keys' configuration page. It has a table with columns 'Key No.', 'Key Type', and 'Key Value'. Key 0 is 'SCR - Single Call Ringing' with a directory number of 57005. Key 1 is 'CWT - Call Waiting'. To the right of the table are fields for 'Directory Number' (57005), 'Multiple Appearance Redirection Prime(MARP)' (checked), 'First Name' (CS1KR7), 'Last Name' (Digital), 'Display Format' (First, Last), 'Language' (Roman), 'CLID Entry (Numeric or D)' (0), and 'ANIE Entry'.

Keys

Key No.	Key Type	Key Value
0	SCR - Single Call Ringing	Directory Number: <input type="text" value="57005"/> <input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP) First Name: <input type="text" value="CS1KR7"/> Last Name: <input type="text" value="Digital"/> Display Format: <input type="text" value="First, Last"/> Language: <input type="text" value="Roman"/>
1	CWT - Call Waiting	CLID Entry (Numeric or D): <input type="text" value="0"/> ANIE Entry: <input type="text"/>


5.9.4 Example Analog Port with DN 57021

The following screen shows basic information for an analog port in the configuration that may be used with a basic analog telephone. The port is configured as Directory Number 57021.

The screenshot displays the Avaya configuration interface. On the left is a navigation tree with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The 'Phones' category is selected. The main area shows 'Managing: EM on cs1k75(10.7.8.61)' and a breadcrumb 'Phones»Phone Details'. The 'Phone Details' section includes a phone icon and system information: System: EM on cs1k75, Phone Type: 2500, and Sync Status: TRN. Below this is a tabbed interface with 'General Properties' selected. The 'General Properties' section contains fields for Customer Number (0), Terminal Number (004 0 03 00), Designation (ANLG1), and Directory Number (57021).

Managing: [EM on cs1k75\(10.7.8.61\)](#)
[Phones»Phone Details](#)

Phone Details

 System: EM on cs1k75
Phone Type: 2500
Sync Status: TRN

[General Properties](#) | [Features](#) | [Single Line Features](#) | [User Fields](#)

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

Directory Number: 🔍

5.10. Save Configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** (not shown) and click **Submit** to save configuration changes as shown below.

The screenshot shows the Avaya Communication Server 1000E web interface. On the left is a navigation tree with the following structure:

- System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
- Tools
 - Backup and Restore
 - Call Server

The main content area shows the 'Call Server Backup' page. At the top, it displays 'Managing: 10.7.8.61 Username: admin' and a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The page title is 'Call Server Backup'. Below the title, there is an 'Action' label followed by a dropdown menu set to 'Backup', and two buttons: 'Submit' and 'Cancel'.

The backup process may take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
.  
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"  
Database backup Complete!  
TEMU207  
Backup process to local Removable Media Device ended successfully.
```

The configuration of Avaya Communication Server 1000E is complete.

6. Configure Avaya Aura® Session Manager Release 6.1

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 the two. For more information, consult the references in Section 11.

As described in Section 3, the same Session Manager configuration was used for testing both Verizon IP Trunk Service and Verizon IPCC Service. Although not the focus of these Application Notes, Verizon IP Trunk Service supports outbound dialing to the PSTN, and this section includes the procedures to allow outbound routing, for completeness. Consult Reference [AuraSBC-IP-Trunk] for more information on connecting to Verizon IP Trunk Service.

The following administration activities will be described:

- Define SIP Domain
- Define Locations for Avaya Communication Server 1000E and for the SBC
- Configure the Adaptation Modules that will be associated with the SIP Entities for Avaya Communication Server 1000E and the SBC
- Define SIP Entities corresponding to Avaya Communication Server 1000E and the SBC
- Define Entity Links describing the SIP trunk between Avaya Communication Server 1000E and Session Manager, and the SIP Trunk between Session Manager and the SBC.
- Define Routing Policies associated with the Avaya Communication Server 1000E and the SBC.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL “<http://<ip-address>/SMGR>”, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown).



Avaya Aura® System Manager 6.1

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

Log On

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

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

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

User ID:

Password:

[Log On](#)

[Cancel](#)

[Change Password](#)

Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.

Users	Elements	Services
Administrators Manage Administrative Users Groups & Roles Manage groups, roles and assign roles to users Subscribers Manage users and shared resources associated with CS1000, including LDAP/file import and export Synchronize and Import Synchronize users with the enterprise directory, import users from file UCM Roles Manage UCM Roles, assign roles to users User Management Manage users, shared user resources and provision users	Application Management Manage applications and application certificates Communication Manager Manage Communication Manager objects Conferencing Conferencing Inventory Manage, discover, and navigate to elements, update element software Messaging Manage Messaging System objects Presence Presence Routing Network Routing Policy Session Manager Session Manager Element Manager SIP AS 8.1 SIP AS 8.1	Backup and Restore Backup and restore System Manager database Configurations Manage system wide configurations Events Manage alarms, view and harvest logs Licenses View and configure licenses Replication Track data replication nodes, repair replication nodes Scheduler Schedule, track, cancel, update and delete jobs Security Manage Security Certificates Templates Manage Templates for Communication Manager and Messaging System objects UCM Services Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.

▼ Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

6.1. SIP Domain

Select **Domains** from the left navigation menu. Two domains can be added, one for the enterprise SIP domain, and one for the Verizon network SIP domain, if needed. In the shared environment of the Avaya Solution and Interoperability Test lab, a domain “avaya.com” is also defined and used by the shared Avaya equipment.

Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter the enterprise SIP Domain Name. In the sample screen below, “adevc.avaya.globalipcom.com” is shown, the CPE domain known to Verizon.
- **Type** Verify “SIP” is selected.
- **Notes** Add a brief description. [Optional]

The screenshot shows the 'Domain Management' interface. At the top, there is a breadcrumb trail: Home / Elements / Routing / Domains- Domain Management. Below this, the title 'Domain Management' is displayed. On the right, there are buttons for 'Commit', 'Cancel', and 'Help ?'. Below the title bar, there is a table with the following data:

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

At the top left of the table, it says '1 Item Refresh'. At the top right, it says 'Filter: Enable'.

Click **New** (not shown). Enter the following values and use default values for remaining fields. The domain shown below is associated with the Verizon IP Trunk Service available from the same PIP access circuit. This domain can be omitted if configuring only the Verizon IPCC Service.

- **Name** Enter the Domain Name used for the Verizon network. In the sample screen below, “pcelban0001.avayalincroft.globalipcom.com” is shown.
- **Type** Verify “SIP” is selected.
- **Notes** Add a brief description. [Optional]

Home / Elements / Routing / Domains- Domain Management

Domain Management Help ? Commit Cancel

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

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

Click **Commit** to save.

The following screen shows the “avaya.com” SIP domain that was already configured in the shared laboratory network.

Home / Elements / Routing / Domains- Domain Management

Domain Management Help ? Commit Cancel

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

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	Shared Avaya SIL Network

The screen below shows an example SIP Domain list after SIP Domains are configured. Many SIP Domains can be configured, distinguished, and adapted by the same Session Manager as needed.

Domain Management

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

8 Items Refresh				Filter: Enable
<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avaya.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Trunk Test
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	Shared Avaya SIL Network
<input type="checkbox"/>	avocs.contoso.com	sip	<input type="checkbox"/>	Microsoft OCS Test Environment
<input type="checkbox"/>	contosomed1.avocs.contoso.com	sip	<input type="checkbox"/>	Mediation server inserts this
<input type="checkbox"/>	cust2-tor.vtac.bell.ca	sip	<input type="checkbox"/>	CPE domain for Bell Canada SIP Trunking
<input type="checkbox"/>	devconn.com	sip	<input type="checkbox"/>	ACE/ICP James L
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk
<input type="checkbox"/>	siptrunking.bell.ca	sip	<input type="checkbox"/>	SP domain for Bell Canada SIP Trunk

6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be used for bandwidth management or location-based routing.

6.2.1 Location for Avaya Communication Server 1000E

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the IP Address or IP Address pattern used to identify the location.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows the top portion of the screen for the Location defined for Avaya Communication Server 1000E.

Location Details

General

* Name: CS1K75-Location

Notes: CS1000 7.5

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec ▼

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Scrolling down, the following screen shows the lower portion of the Location for the CS1000E.

Location Pattern

Add

Remove

1 Item | Refresh

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.7.7.60	CS1000 7.5 TLAN

6.2.2 Location for Session Border Controller

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the IP Address or IP Address pattern used to identify the location.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows the top portion of the screen for the Location defined for the SBC.

Location Details

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Scrolling down, the following screen shows the lower portion of the Location for the SBC.

Location Pattern

1 Item [Refresh](#)

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

6.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module designed for Avaya Communication Server 1000E to convert SIP headers in messages sent by Avaya Communication Server to the format used by other Avaya products and endpoints.

6.3.1 Adaptation for Avaya Communication Server 1000E Entity

Select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., “CS1000”)
- **Module Name:** Select “CS1000Adapter” from drop-down menu (or add an adapter with name “CS1000Adapter” if not previously defined)
- **Module Parameter:** Enter “osrcd=<cs1000-domain>.com” and “odstd=<cs1000-domain>.com” where <cs1000-domain> is the SIP domain configured in the CS1000E system. Enter “fromto=true” to allow the From and To headers to be modified by Session Manager (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers).

Home / Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

* **Adaptation name:**

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Scroll down to the **Digit Conversion for Incoming Calls to SM** section. Click **Add** to configure entries for calls from CS1000E users to Verizon, a necessary step for outbound calls to the Verizon IP Trunk service, but an optional step if only inbound calls from the Verizon IPCC services will be configured. If only Verizon IPCC service is used, this area of the screen need not be configured, but may optionally be used to map the CS1000 DN to a Verizon IP Toll Free number in the PAI header sent to Verizon in 180 Ringing and 200 OK for an inbound toll-free call.

- **Matching Pattern** Enter Avaya CS1000E extensions (or extension ranges via wildcard pattern matching).
- **Min** Enter minimum number of digits (e.g., 5)
- **Max** Enter maximum number of digits (e.g., 5)
- **Phone Context** Enter value of **Private CDP domain name** defined in the CS1000E for any patterns matching SIP endpoints registered to Session Manager (if any).
- **Delete Digits** Enter “0”, unless digits should be removed before routing by Session Manager. For CS1000E extension conversion to the corresponding Verizon number, enter the number of digits in the extension to remove all digits.
- **Insert Digits** Enter the Verizon number corresponding to the matched extension. The numbers shown below are Verizon IP Trunk DID numbers. For inbound IPCC calls, it is not imperative that the PAI in responses contain a Verizon IPCC number. If only IPCC service is used, an IP Toll Free number or IP-IVR number may be used.
- **Address to modify** Select “both”

Notes:

Digit Conversion for Incoming Calls to SM

<input type="button" value="Add"/> <input type="button" value="Remove"/>								
5 Items <input type="button" value="Refresh"/>		Filter: Enabled						
<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 3	* 5	* 5	cdp.udp	* 0		both ▼	3xxxx on CM/SM
<input type="checkbox"/>	* 57003	* 5	* 5		* 5	7329450235	both ▼	CS1K IP-Unistim to Verizon IPCC
<input type="checkbox"/>	* 57005	* 5	* 5		* 5	7329450231	both ▼	CS1K Digital to Verizon IPCC
<input type="checkbox"/>	* 57007	* 5	* 5		* 5	7329450236	both ▼	CS1K SIP phone to Verizon IPCC
<input type="checkbox"/>	* 57021	* 5	* 5		* 5	7329450288	both ▼	CS1K Analog port (fax)

Scroll down to the **Digit Conversion for Outgoing Calls from SM** section, corresponding to inbound Verizon toll-free calls to CS1000E. In the **Matching Pattern**, enter a Verizon toll-free number, with **Min** and **Max** set to 10, the length of the number to match. In the **Delete Digits** field, enter the number of digits to delete. In the sample configuration, the entire 10 digit toll-free number is deleted and replaced by the desired CS1000E Directory Number.

Digit Conversion for Outgoing Calls from SM

11 Items [Refresh](#)

Filter: Enabled

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7329450231	* 10	* 10		* 10	57005	both ▼	Verizon DID to CS1K Digital
<input type="checkbox"/>	* 7329450232	* 10	* 10		* 10	57001	both ▼	Verizon DID to CS1K IP-Unis
<input type="checkbox"/>	* 7329450235	* 10	* 10		* 10	57003	both ▼	Verizon DID to CS1K IP-Unis
<input type="checkbox"/>	* 7329450236	* 10	* 10		* 10	57007	both ▼	Verizon DID to CS1K SIP ph
<input type="checkbox"/>	* 7329450288	* 10	* 10		* 10	57021	both ▼	Verizon DID to CS1K analog
<input type="checkbox"/>	* 8668502380	* 10	* 10		* 10	57005	both ▼	Verizon IPTF to CS1K Digital
<input type="checkbox"/>	* 8668506850	* 10	* 10		* 10	57003	both ▼	Verizon IPTF to CS1K IP-Uni
<input type="checkbox"/>	* 8668508170	* 10	* 10		* 10	57007	both ▼	Verizon IP-IVR to CS1K SIP
<input type="checkbox"/>	* 8668511977	* 10	* 10		* 10	57003	both ▼	Verizon IP-IVR to CS1K IP-U
<input type="checkbox"/>	* 8668518119	* 10	* 10		* 10	57005	both ▼	Verizon IP-IVR to CS1K Digi
<input type="checkbox"/>	* 8668523221	* 10	* 10		* 10	57007	both ▼	Verizon IPTF to CS1K SIP

As an example, using these screens, if a PSTN user dials Verizon IP Toll Free number 866-850-6850, and the call is routed to the CS1000E, then this adapter will change the number sent to the CS1000E to directory number 57003. Other mappings of IP Toll Free and IP-IVR numbers from **Table 1** and **Table 2** in Section 3 can also be observed.

Click **Commit** (not shown).

6.3.2 Adaptation for SBC Entity

Select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select “**VerizonAdapter**” from drop-down menu (or add an adapter with name “VerizonAdapter” if not previously defined)
- **Module Parameter:** Enter “osrcd=<CPE-domain-known-to-Verizon>.com” and (optionally) “odstd=<Verizon-domain>.com”. The <CPE-domain-known-to-Verizon> is the SIP domain for the CPE configured in the Verizon network (i.e., the SIP domain Verizon would include in the Request-URI for an inbound toll-free call). <Verizon-domain> is the Verizon network SIP domain (i.e., the SIP domain Verizon would expect in the Request-URI for an INVITE sent from the CPE to the PSTN for the Verizon IP Trunk Service, if used). Enter “fromto=true” to allow the From and To headers to be modified by Session Manager (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers).

Adaptation Details

General

* **Adaptation name:**

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Click **Commit** (not shown).

6.3.3 List of Adaptations

Select **Adaptations** from the left navigational menu. A partial list of the Adaptation Modules defined for the sample configuration is shown below. In list form, the module parameters assigned to the adapters named “CS1000” and “History_Diversion_IPT” are more evident than the screens presented in the prior sections.

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	AcmeAdapt	DigitConversionAdapter odstd=138.210.71.242		Change RURI To Dest IP
<input type="checkbox"/>	Avaya-R6.0	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	BC AA-SBC	DigitConversionAdapter osrcd=cust2-tor.vsac.bell.ca odstd=siptrunking.bell.ca		convert to BC's domains
<input type="checkbox"/>	BC CM-ES	DigitConversionAdapter odstd=avaya.com		avaya.com for shared SIL ntwk
<input type="checkbox"/>	BCM Adapter	DigitConversionAdapter avaya.com		Delete prefix
<input type="checkbox"/>	Cisco-UCM513	CiscoAdapter 192.45.130.105		
<input type="checkbox"/>	Cisco-UCM6	CiscoAdapter avaya.com		
<input type="checkbox"/>	Cisco-UCM7	CiscoAdapter avaya.com		
<input type="checkbox"/>	CiscoUCME	CiscoAdapter iosrcd=avaya.com odstd=192.45.131.1		
<input type="checkbox"/>	CM5-2-1 Adapt	DigitConversionAdapter osrcd=avaya.com		Tim For CLink Testing
<input type="checkbox"/>	CM-ES Inbound	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	CM-ES-VZ Inbound	DigitConversionAdapter odstd=avaya.com		Avaya.com for shared SIL ntwk
<input type="checkbox"/>	CS1000	CS1000Adapter osrcd=avaya.com odstd=avaya.com fromto=true		CS1000 7.5
<input type="checkbox"/>	Digit Conversion VZ	DigitConversionAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com		Verizon DID to CM Extn map, param above should be on VZ-adapter
<input type="checkbox"/>	History_Diversion_IPT	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com fromto=true		

6.4. SIP Entities

SIP Entities must be added for the Avaya Communication Server 1000E and for the SBC.

6.4.1 SIP Entity for Avaya Communication Server 1000E

Select **SIP Entities** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter the TLAN IP address of the CS1000E Node.
- **Type:** Select “**SIP Trunk**”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module for the CS1000E
- **Location:** Select the Location for the CS1000E

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “Use Session Manager Configuration” (or choose an alternate Link Monitoring approach for this entity, if desired).

Click **Commit** (not shown) to save the definition of the new SIP Entity.

The following screen shows the SIP Entity defined for Avaya Communication Server 1000E in the sample configuration.

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities- SIP Entity Details](#)

SIP Entity Details

General

*

Name:

*

FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV:

☐

*

SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring:

6.4.2 SIP Entity for SBC

Select **SIP Entities** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter the private side IP Address of the SBC.
- **Type:** Select “**Other**”
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module for the SBC
- **Location:** Select the Location for the SBC

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “Use Session Manager Configuration” (or choose an alternate Link Monitoring approach for this entity, if desired).

The following screen shows the SIP Entity defined for the SBC in the sample configuration.

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name:

AuraSBC

* FQDN or IP Address:

65.206.67.93

Type:

Other

Notes:

Avaya Aura SBC Inside IP

Adaptation:

History_Diversion_IPT

Location:

Aura-SBC

Time Zone:

America/New_York

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

SIP Link Monitoring:

Use Session Manager Configuration

6.5. Entity Links

The SIP trunk between Session Manager and Avaya Communication Server 1000E is described by an Entity Link, as is the SIP trunk between Session Manager and the SBC.

6.5.1 Entity Link to Avaya Communication Server 1000E Entity

Select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link.
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **SIP Entity 2** Select the SIP Entity defined for the CS1000E
- **Protocol** After selecting both SIP Entities, select “**TCP**”.
- **Port** Verify **Port** for both SIP entities is the default listen port.
For the sample configuration, default listen port is “**5060**”.
- **Trusted** Enter ☒
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save the **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and Avaya Communication Server 1000E.

The screenshot shows a web interface for configuring Entity Links. The breadcrumb navigation at the top reads: Home / Elements / Routing / Entity Links- Entity Links. Below the navigation, the title 'Entity Links' is displayed on the left, and 'Commit' and 'Cancel' buttons are on the right, along with a 'Help ?' link. The main content area shows a table with one item. Above the table, there is a '1 Item Refresh' link and a 'Filter: Enable' dropdown. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The single row contains the following data: Name: * CS100075-Link, SIP Entity 1: * SM1 (dropdown), Protocol: TCP (dropdown), Port: * 5060, SIP Entity 2: * CS1000-R75 (dropdown), Port: * 5060, Trusted: ☒, Notes: CS1000 R7.5.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CS100075-Link	* SM1	TCP	* 5060	* CS1000-R75	* 5060	<input checked="" type="checkbox"/>	CS1000 R7.5

6.5.2 Entity Link to SBC

Select **Entity Links** from the left navigation menu. Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link.
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **SIP Entity 2** Select the SIP Entity defined for the SBC.
- **Protocol** After selecting both SIP Entities, select “**TCP**”.
- **Port** Verify **Port** for both SIP entities is the default listen port.
For the sample configuration, default listen port is “**5060**”.
- **Trusted** Enter ☒
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save the **Entity Link** definition.

The following screen shows the entity link defined for the SIP trunk between Session Manager and the SBC.

Home / Elements / Routing / Entity Links- Entity Links

Entity Links [Help ?](#)

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* AuraSBC	* SM1	TCP	* 5060	* AuraSBC	* 5060	<input checked="" type="checkbox"/>	

6.6. Routing Policies

Routing policies describe the conditions under which calls will be routed to the Avaya Communication Server 1000E or SBC.

6.6.1 Routing Policy to Avaya Communication Server 1000E

To add a new routing policy, select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with the CS1000E and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

In the **Time of Day** section, add an appropriate time of day. In the sample configuration, time of day was not a relevant routing criteria, so the “24/7” range was chosen. Use default values for remaining fields. Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for Avaya Communication Server 1000E.

Home / Elements / Routing / Routing Policies- Routing Policy Details

routing
Help ?

Routing Policy Details

CommitCancel

General

* Name: CS1K-R75-RP

Disabled: ☐

Notes: CS1000 R7.5

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1000-R75	10.7.7.60	SIP Trunk	CS1000 7.5

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

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

6.6.2 Routing Policy to SBC

The configuration in this section is not required if only inbound toll-free calls will be configured for the Verizon IPCC Services. In the sample configuration, Verizon IP Trunk service, which supports outbound dialing to the PSTN, was also available.

To add a new routing policy, select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional]

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the SIP Entity associated with the SBC and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

In the **Time of Day** section, add an appropriate time of day. In the sample configuration, time of day was not a relevant routing criteria, so the “24/7” range was chosen. Use default values for remaining fields. Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for the SBC.

Routing Policy Details

Commit

Cancel

General

* Name: To-Aura-SBC

Disabled: ☐

Notes: Avaya Aura SBC for Verizon test

SIP Entity as Destination

Select

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

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item | [Refresh](#)

Filter: [Enable](#)

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

6.7. Dial Patterns

Dial patterns are used to route calls to the appropriate routing policies, and ultimately to the appropriate SIP Entities.

6.7.1 Inbound Verizon Calls to CS1000E Users

To define a dial pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Avaya Communication Server 1000E (e.g., a Verizon toll-free number)
- **Min:** Enter the minimum number of digits.
- **Max:** Enter the maximum number of digits.
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select “**Apply the Selected Routing Policies to All Originating Locations**” or alternatively, select a specific location. In the example below, the SBC location was selected as the originating location.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya Communication Server 1000E.
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows an example Dial Pattern. In the screen, Verizon IP Toll Free number 866-850-2380 is routed to the Avaya CS1000E. The adapter assigned to the Avaya CS1000E (in Section 6.3) will map the toll-free number to the desired CS1000E Directory Number. Repeat this procedure as needed to allow additional Verizon toll-free numbers to be routed to the CS1000E. Wildcards may be used in the **Pattern** field so that blocks of matching numbers are routed based on a single dial pattern.

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details Help ?

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Aura-SBC	Location for Avaya Aura SBC Verizon testing	CS1K-R75-RP	0	<input type="checkbox"/>	CS1000-R75	CS1000 R7.5

6.7.2 Outbound Calls to Verizon (Optional)

The configuration in this section is not required if only inbound toll-free calls will be configured for the Verizon IPCC Services. In the sample configuration, Verizon IP Trunk service, which supports outbound dialing to the PSTN, was also available.

To define a dial pattern, select **Dial Patterns** from the navigation menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls destined for the Verizon network
- **Min:** Enter the minimum number of digits.
- **Max:** Enter the maximum number of digits.
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route outgoing calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In the **Originating Location** list, select “Apply the Selected Routing Policies to All Originating Locations” or alternatively, select a specific originating location. In the **Routing Policies** table, select the Routing Policy defined for the SBC.

- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional PSTN numbers to be routed to the Verizon network via the SBC. Wildcards may be used in the **Pattern** field so that blocks of matching numbers are routed based on a single dial pattern.

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

[Help ?](#)

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To-Aura-SBC	0	<input type="checkbox"/>	AuraSBC	Avaya Aura SBC for Verizon test

7. Configure Avaya Aura® Session Border Controller (SBC)

This section illustrates an example configuration of the Avaya Aura® SBC. In the sample configuration, the Avaya Aura® SBC runs on its own S8800 Server as an application template using System Platform. The installation of the System Platform is assumed to have been previously completed. The Avaya Aura® Session Border Controller includes a configuration wizard that can be used as part of the installation of the SBC template on System Platform. The wizard pre-configures the underlying SBC for much of the required provisioning.

Reference [AuraSBC-IP-Trunk] is a companion Application Notes document that illustrates the initial installation, licensing, and wizard configuration of the SBC that formed the starting point for the SBC configuration shown in these Application Notes. In Section 7 of reference [AuraSBC-IP-Trunk], the installation, licensing, and initial wizard configuration of the SBC are detailed. These procedures will not be repeated here.

The configuration shown in this section assumes that the configuration of the connection to the Verizon IP Contact Center Service is being added to the SBC configuration previously documented in reference [AuraSBC-IP-Trunk]. As an alternative, if only the Verizon IPCC Service is necessary, the procedures that use the installation wizard from reference [AuraSBC-IP-Trunk] can be used to connect to the Verizon IPCC Service only, using the appropriate Verizon-

provided IPCC Service IP Address and port information. The wizard can be used for one SIP Service Provider service connection only.

After the SBC has been installed, any subsequent changes to the network configuration (e.g., IP address, network mask, hostname) for the SBC eth0 or eth2 interfaces must be done via the System Platform webconsole Network Configuration page. Any backup and restore actions should also use System Platform. Configuration of specific SBC behaviors (e.g., header manipulations) can be performed through the element manager GUI as shown in Section 7.3.

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

7.1. Avaya Aura® Session Border Controller (SBC) Installation

For the installation procedures used in the sample configuration, please refer to Section 7.1 of reference [AuraSBC-IP-Trunk].


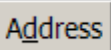
7.2. Avaya Aura® Session Border Controller (SBC) Licensing

For the licensing procedures used in the sample configuration, please refer to Section 7.2 of reference [AuraSBC-IP-Trunk].

7.3. SBC Element Manager Configuration

This section presents the incremental configuration using the element manager of the SBC. It is assumed that the installation, licensing, and configuration shown in Section 7.1 – Section 7.3 of reference [AuraSBC-IP-Trunk] has already been completed. In the screens below, it can also be observed that Section 12 (an optional procedure covering use of DNS-SRV with Verizon) from reference [AuraSBC-IP-Trunk] has also already been completed.

The configuration screens will be familiar to the reader experienced with the Acme Packet Net-Net

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

Acme Packet Net-Net OS-E

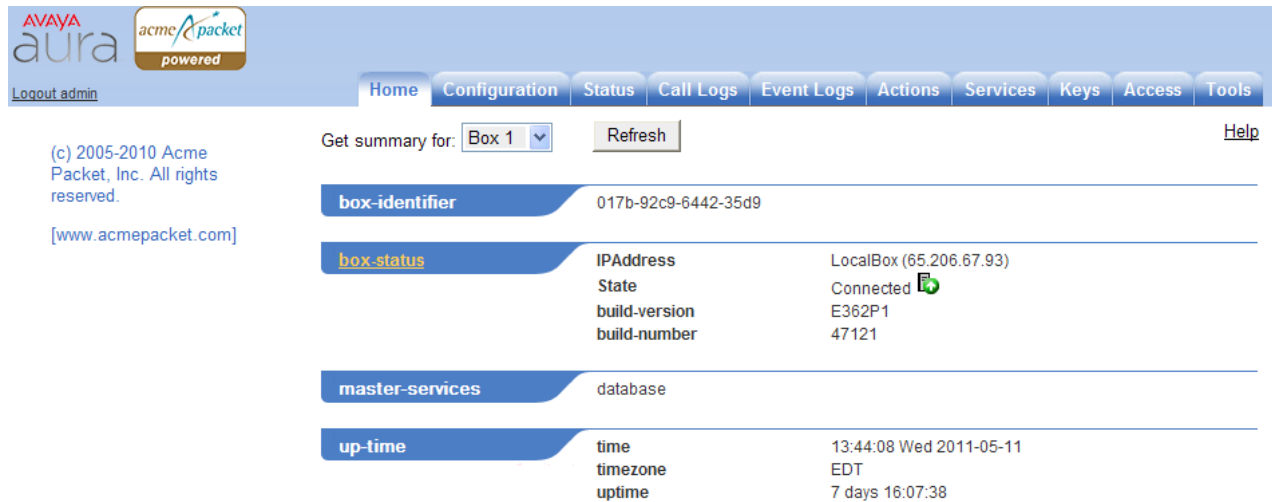
To access the NNOS-E management interface, you must first log in. Please provide your user name

Username:

Password:

Login

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



AVAYA aura acme packet powered

Logout admin

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

Get summary for: Refresh Help

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

box-identifier 017b-92c9-6442-35d9

box-status

IPAddress	LocalBox (65.206.67.93)
State	Connected
build-version	E362P1
build-number	47121

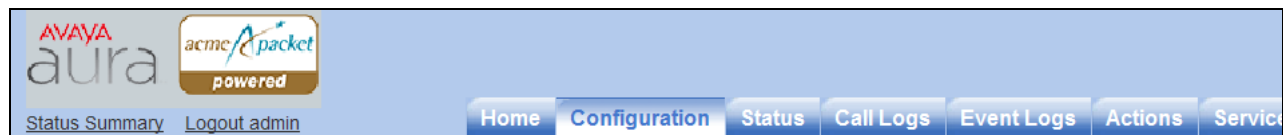
master-services database

up-time

time	13:44:08 Wed 2011-05-11
timezone	EDT
uptime	7 days 16:07:38

7.3.1 Adding SIP Gateway to Verizon IP Contact Center Service

After logging in, select the **Configuration** tab.



AVAYA aura acme packet powered

Status Summary Logout admin

Home Configuration Status Call Logs Event Logs Actions Services

Configuration: all

Configuration Setup View

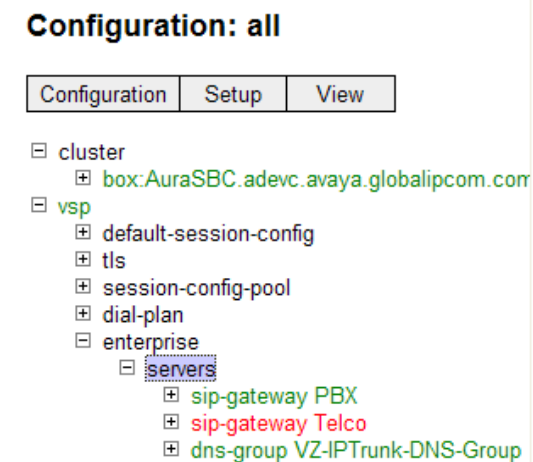
cluster

- box:AuraSBC.adevc.avaya.globalipcom.com

vsp

- default-session-config
- tls
- session-config-pool
- dial-plan
- enterprise
- servers
 - sip-gateway PBX
 - sip-gateway Telco
 - dns-group VZ-IPTrunk-DNS-Group

Using the menu on the left hand side, expand **vsp** → **enterprise** → **servers** as shown below.



Configuration: all

Configuration Setup View

cluster

- box:AuraSBC.adevc.avaya.globalipcom.com

vsp

- default-session-config
- tls
- session-config-pool
- dial-plan
- enterprise
- servers
 - sip-gateway PBX
 - sip-gateway Telco
 - dns-group VZ-IPTrunk-DNS-Group

On the right hand side, the following screen shows the foundational configuration of “sip-gateways” already in place from reference [AuraSBC-IP-Trunk]. Note that there is already a “sip-gateway PBX” that will be used for connectivity towards Session Manager. There is also a “sip-gateway Telco” previously configured for connectivity to the Verizon IP Trunk Service, and an optional “DNS Group” illustrated in Section 12 of reference [AuraSBC-IP-Trunk]. Although not the focus of these Application Notes, the connectivity to the Verizon IP Trunk Service will remain

in place, and connectivity to the Verizon IP Contact Center service will be added. Click **Add sip-gateway** as shown below.

server

	server	admin	domain	failover-detection	carrier	routing-tag	inbound-session-config-pool-entry
Edit Delete	sip-gateway PBX	enabled	adevc.avaya.globalipcom.com	ping	default		Edit
Edit Delete	sip-gateway Telco	disabled		ping	default		Edit
Edit Delete	dns-group VZ-IPTrunk-DNS-Group	enabled	pcelban0001.avayalincroft.globalipcom.com	ping	default		Edit

[Add h323-server](#)
[Add sip-gateway](#)

Add sip-gateway

In the resultant screen shown below, enter an appropriate **name** for the new sip-gateway to the Verizon IP Contact Center service and click **Create**.

Create vsplenterprise\servers\sip-gateway - Step 1 of 1: Edit sip-gateway [Help](#) [Index](#)

Please provide some basic information for sip-gateway. Then press "Create".

general:

* name

In the resultant screen, click **Configure** under the “servers: server-pool” heading, as shown below.

Configure vspl\enterprise\servers\sip-gateway VZ-IPCC Show advanced [Help](#) [Index](#)

Set Reset Back Copy Delete

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

general:

* name	<input type="text" value="VZ-IPCC"/>
admin	enabled ▼ (Resource is active)
domain	<input type="text"/>
failover-detection	none ▼ (No server failover detection)

servers:

server-pool	Configure
-------------	------------------------

Configure server-pool

In the resultant screen, click **Add server** as shown below.

Configure vsp\enterprise\servers\sip-gateway VZ-IPCC\server-pool
Index

server	Add server
handle-response	<input type="button" value="Add server"/> Add handle-response

In the resultant screen, enter an appropriate **server-name** and **host** for the Verizon IP Contact Center service. In the screen shown below, the IP Address 172.30.205.55 was provided by Verizon as the SIP signaling IP Address of the IP Contact Center service. Click **Create**.

Create vsp\enterprise\servers\sip-gateway VZ-IPCC\server-pool\server - Step 1 of 1: Edit server
Help Index

Please provide some basic information for server. Then press "Create".

General:

* server-name	<input type="text" value="VZ-IPCC-network"/>
* host	<input type="text" value="172.30.205.55"/> (host name or n.n.n.n)

In the resultant screen, select UDP as the **transport** and enter an appropriate **port**. In the sample configuration, Verizon IP Contact Center service expected the enterprise to send SIP signaling to IP Address 172.30.205.55 and port 5072, as shown below. Click **Set**.

Configure vsplenterprise\servers\sip-gateway VZ-IPCC\server-pool\server VZ-IPCC-network

[Show advanced](#) [Help](#) [Index](#)

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

General:

* server-name	<input type="text" value="VZ-IPCC-network"/>
admin	<input type="text" value="enabled"/> (Resource is active)
* host	<input type="text" value="172.30.205.55"/> (host name or n.n.n.n)
transport	transport <input type="text" value="UDP"/> (User Datagram Protocol)
port	<input type="text" value="5072"/> (at minimum 1,default=5060)

After clicking **Set**, a screen such as the following is displayed.

Configure vsplenterprise\servers\sip-gateway VZ-IPCC\server-pool [Show advanced](#) [Help](#)

[Index](#)

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

server	server	admin	host	transport	port	outbound-normalization	inbound-normalization
Edit Delete	server VZ-IPCC-network	enabled	172.30.205.55	UDP	5072	Configure	Configure

[Add server](#)

Using the left-side menu, navigate to **vsp** → **enterprise** → **servers** → **sip-gateway** and select the newly created “VZ-IPCC” entry. Scroll down to the policy heading. Using the **outbound-session-config-pool-entry** drop-down menu, select the entry “vsp\session-config-pool\entry To-Telco” as shown in the screen below. This session-config-pool entry was created by the wizard configuration shown in reference [AuraSBC-IP-Trunk]. Using the **failover-detection** drop-down, select “ping” to cause the SBC to periodically send SIP OPTIONS messages to the Verizon IPCC Service to verify the health of the connection.

general:	
* name	VZ-IPCC
admin	enabled (Resource is active)
domain	
failover-detection	ping (Use OPTIONS to detect failures)

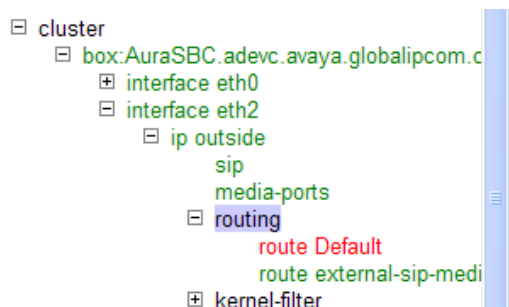
servers:	
server-pool	[Delete]

policy:	
inbound-session-config-pool-entry	
outbound-session-config-pool-entry	vsp\session-config-pool\entry ToTelco

other properties:	

7.3.2 Adding IP Routing for Verizon IP Contact Center Network

From the left-side menu, select **routing** for the interface to the outside network, which is interface virtual “eth2” in the sample configuration, as shown in the navigation screen below.



In the right-side, a screen such as the following is displayed. The screen below shows the IP route established from reference [AuraSBC-IP-Trunk]. The Verizon IP Trunk Service on network 172.30.209.0/24 used gateway 1.1.1.1. A new route will be added for the Verizon IP Contact

Center service using the same gateway. In the sample configuration, Verizon IP Trunk service and Verizon IP Contact Center service shared the same PIP access circuit. Click **Add route**.

Configure cluster\box:AuraSBC.adevc.avaya.globalipcom.com\interface eth2\ip outside\routing

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

route		route	admin	destination	gateway	metric
	Edit Delete	route Default	disabled	default	0.0.0.0	1
	Edit Delete	route external-sip-media-1	enabled	network 172.30.209.0/24	1.1.1.1	1
Add route						

In the resultant screen shown below, enter an appropriate **route-name**. Using the **type** drop-down, select “network”. In the **address/mask** field, enter the IP address and network mask associated with the Verizon IP Contact Center service. In the sample configuration, the Verizon IP Contact Center service uses 172.30.205.0/24 as shown below. In the **gateway** field, enter the IP address that is the gateway for the public side of the SBC to Verizon. In the sample configuration, the gateway is 1.1.1.1, the same gateway used with the Verizon IP Trunk service, since both share the same PIP access circuit. Click **Create**.

Create cluster\box 1\interface eth2\ip outside\routing\route - Step 1 of 1: Edit route

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

Please provide some basic information for route. Then press "Create".

* route-name	<input type="text" value="VZ-IPCC-network"/>		
* destination	* type	<input type="text" value="network"/> (network route)	
	* address/mask	<input type="text" value="172.30.205.0/24"/>	
* gateway	<input type="text" value="1.1.1.1"/> (n.n.n.n)		

[Create](#) [Reset](#) [Cancel](#)

In the resultant screen shown below, click the **Set** button.

Configure cluster\box:AuraSBC\interface eth2\ip outside\routing\route VZ-IPCC-network [Help](#) [Index](#)

admin	enabled <input type="button" value="v"/> (Resource is active)
* route-name	VZ-IPCC-network
* destination	<div> * type network <input type="button" value="v"/> (network route) </div> <div> * address/mask 172.30.205.0/24 </div>
* gateway	1.1.1.1 (n.n.n.n)
metric	1 (from 0 to 1,000,default=1)

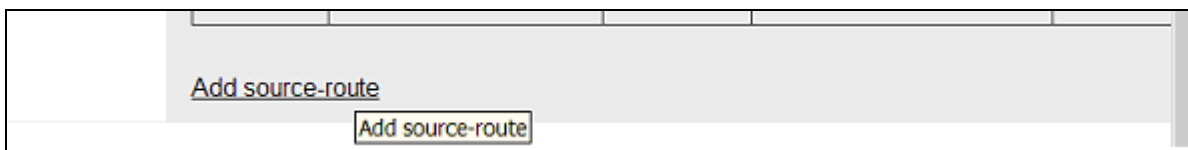
The following screen summarizes the updated routing configuration.

Configure cluster\box:AuraSBC.adevc.avaya.globalipcom.com\interface eth2\ip outside\routing

route						
		route	admin	destination	gateway	metric
	Edit Delete	route Default	disabled	default	0.0.0.0	1
	Edit Delete	route external-sip-media-1	enabled	network 172.30.209.0/24	1.1.1.1	1
	Edit Delete	route VZ-IPCC-network	enabled	network 172.30.205.0/24	1.1.1.1	1

7.3.3 Configure Dial-Plan

From the left-side menu, select **vsp** → **dial-plan**. In the right-hand side, scroll down and click **Add source-route** as shown below.



In the resultant screen, enter an appropriate name in the **name** field. In the **type** field drop-down menu, select “server”, and in the **source-server** drop-down menu, select the sip-gateway entry previously created in **Section 7.3.1**, as shown below. Click **Create**.

Create vsp\dial-plan\source-route - Step 1 of 1: Edit source-route [Help](#) [Index](#)

Please provide some basic information for source-route. Then press "Create".

general:	
* name	<input type="text" value="FromVZIPCC"/>
* source-match	<div><div>* type</div><div>server</div></div>
	<div><div>* source-server</div><div>vsp\enterprise\servers\sip-gateway VZ-IPCC</div><div>Edit Create</div></div>

In the resultant screen, in the **peer** area, select “server” from the **type** drop-down. In the **server** drop-down, select the sip-gateway representing the enterprise SIP equipment. In the sample configuration, “vsp\enterprise\servers\sip-gateway PBX” already existed from the wizard configuration in reference [AuraSBC-IP-Trunk]. Incoming toll-free calls from the Verizon IP Contact Center service will route to Avaya Aura® Session Manager. Click **Set**.

Configure vsp\dial-plan\source-route FromVZIPCC		Show advanced	Help
Index			
<div> <div>Set</div> <div>Reset</div> <div>Back</div> <div>Copy</div> <div>Delete</div> </div>			
general:			
* name	FromVZIPCC		
description			
* source-match	<div> <div>* type</div> <div>server</div> </div> <div> <div>* source-server</div> <div>vsp\enterprise\servers\sip-gateway VZ-IPCC</div> <div> <a>Edit <a>Create </div> </div>		
peer	<div> <div>type</div> <div>server</div> <div>(Peer is a SIP server)</div> </div> <div> <div>server</div> <div>vsp\enterprise\servers\sip-gateway PBX</div> <div> <a>Edit <a>Create </div> </div>		
location-match-preferred	<div> <div>up-to-outbound-peer</div> <div>(Outbound peer determines whether preferred)</div> </div>		

These same procedures can be repeated to create another source-route. Scroll down in the source-route area and click **Add source route** as shown below.

Edit Delete	source-route FromVZIPCC		server vsp\enterprise\servers\sip-gateway VZ-IPCC	server vsp\ent gatewa
---	---	--	--	-----------------------------

[Add source-route](#)

[Add source-route](#)

In the resultant screen, enter an appropriate name in the **name** field. Using the **type** drop-down menu, select “server”. Using the **source-server** drop-down, select the sip-gateway corresponding to the Avaya enterprise equipment. In the sample configuration, “vsp\enterprise\servers\sip-gateway PBX” is selected, which represents the connection to Session Manager. Click **Create**.

Create vsp\dial-plan\source-route - Step 1 of 1: Edit source-route
[Help](#)
[Index](#)

Please provide some basic information for source-route. Then press "Create".

general:

* name	<input type="text" value="FromPBXtoVZIPCC"/>		
* source-match	* type	<input type="text" value="server"/>	
	* source-server	<input type="text" value="vsp\enterprise\servers\sip-gateway PBX"/>	
		Create	

In the **peer** area, select “server” from the **type** drop-down. From the **server** drop-down, select the sip-gateway corresponding to the Verizon IP Contact Center service created in **Section 7.3.1**. Click **Set** (not shown).

general:	
* name	<input type="text" value="FromPBXtoVZIPCC"/>
description	<input type="text"/>
* source-match	<div><div>* type</div><div>server</div></div> <div><div>* source-server</div><div>vsp\enterprise\servers\sip-gateway PBX</div><div>Edit Create</div></div>
peer	<div><div>type</div><div>server</div><div>(Peer is a SIP server)</div></div> <div><div>server</div><div>vsp\enterprise\servers\sip-gateway VZ-IPCC</div><div>Edit Create</div></div>
location-match-preferred	<div><div>up-to-outbound-peer</div><div>(Outbound peer determines whether preferred)</div></div>

7.3.4 Configure OPTIONS ping to Verizon IP Contact Center

From the left-side menu, select **vsp** → **enterprise** → **servers** → **sip-gateway**. Select the sip-gateway to the Verizon IP Contact Center service added in Section 7.3.1. Click the **Show Advanced** button (not shown). In general, clicking this button reveals additional configuration parameters, and a **Show basic** button is presented, as shown below.

In the **failover-detection** drop-down, verify “ping” as selected as shown below.

Configure vsp\enterprise\servers\sip-gateway VZ-IPCC Show basic

Set Reset Back Copy Delete

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

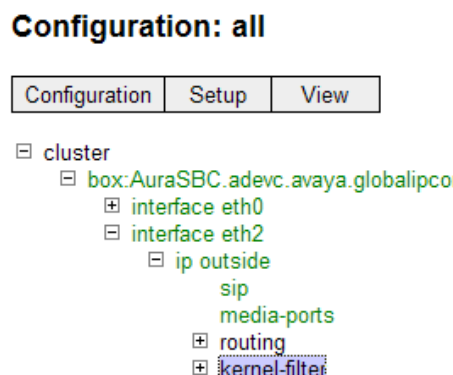
general:	
* name	<input type="text" value="VZ-IPCC"/>
peer-identity	<input type="text"/>
admin	<input type="text" value="enabled"/> (Resource is active)
domain	<input type="text"/>
directory	<input type="text"/> Create
user	<input type="text"/>
password-tag	<input type="text"/> Manage Password
failover-detection	<input type="text" value="ping"/> (Use OPTIONS to detect failures)

Scroll down and locate the **ping-interval** parameter, which is considered an “advanced” parameter (i.e., only available after the **Show Advanced** button has been clicked). Enter the desired period, in seconds, that the SBC will use to source SIP OPTIONS messages towards the Verizon IP Contact Center service. In the sample configuration shown below, the SBC will send OPTIONS every 30 seconds. This is not intended to be prescriptive; other intervals may be used.

routing:	
routing-setting	<div> <div>normalization</div> <div>auto-tag-match</div> <div>auto-domain-match</div> <div>pstn-backup</div> </div> <div> <div>Select All</div> <div>Unselect All</div> </div>
domain-alias	Edit domain-alias
domain-subnet	Edit domain-subnet
loop-detection	<div>tight</div> <div>(Compare source and destination address/port/transport)</div>
service-type	<div>provider</div> <div>(Provider peer)</div>
ping-interval	<div>30</div> <div>seconds</div>

7.3.5 Configure Kernel-Filter for Verizon IPCC

Using the left-hand side navigation menu, select **kernel-filter** as shown in the menu tree below.



On the right, the kernel-filters that were established by the wizard configuration at installation time can be observed. In the sample configuration, the wizard configuration in reference [AuraSBC-IP-Trunk] has established an “allow-rule” that permits traffic from the Verizon IP Trunk service network 172.30.209.0/24, as shown below. Had the wizard been run for Verizon IPCC service, an allow-rule would already exist for the Verizon IPCC network, and this step would not be required.

Configure cluster\box:AuraSBC.adevc.avaya.globalipcom.com\interface eth2\ip outside\kernel-filter [Help](#)
[Index](#)

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

allow-rule		allow-rule	admin	destination-port	source-address/mask	source-port	protocol
	Edit Delete	allow-rule allow-sip-udp-from-peer-1	enabled	5060	172.30.209.0/24	0	udp
Add allow-rule							
deny-rule		deny-rule	admin	destination-port	source-address/mask	source-port	protocol
	Edit Delete	deny-rule deny-all-sip	enabled	5060	0.0.0.0/0	0	all

Click **Add allow-rule**. Enter an appropriate **name**. In the **source-address/mask** field, enter the network information corresponding to the Verizon IPCC Service network. In the sample configuration, “172.30.205.0/24” was entered. Click **Create**.

Create cluster\box 1\interface eth2\ip outside\kernel-filter\allow-rule - Step 1 of 1: Edit allow-rule

Please provide some basic information for allow-rule. Then press "Create".

* name	<input type="text" value="allow-sip-udp-from-peer-2"/>
* source-address/mask	<input type="text" value="172.30.205.0/24"/> (n.n.n.n/n)

[Create](#) [Reset](#) [Cancel](#)

In the resultant screen, enter “5060” in the **destination-port** field. Verizon IPCC will signal to port 5060. In the **protocol** field, select “udp”. In the source-port field, the default “0” may be retained to mimic the configuration that would be performed by the wizard. Alternatively, a more specific port may be entered, such as source-port “5072” used in the sample configuration. Both approaches were tested successfully. Click **Set**.

Configure cluster\box:AuraSBC.adevc.avaya.globalipcom.com\interface eth2\ip outside\kernel-filter\allow-rule [Help](#) [Index](#)
allow-sip-udp-from-peer-2

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

* name	<input type="text" value="allow-sip-udp-from-peer-2"/>
admin	<input type="button" value="enabled"/> (Resource is active)
destination-port	<input type="text" value="5060"/> (from 0 to 65,535)
* source-address/mask	<input type="text" value="172.30.205.0/24"/> (n.n.n.n/n)
source-port	<input type="text" value="5072"/> (from 0 to 65,535)
protocol	<input type="button" value="udp"/> (User Datagram Protocol)

The following screen shows the resulting kernel-filter, which allows SIP traffic from both the Verizon IP Trunk service (from the wizard configuration shown in Reference [AuraSBC-IP-Trunk]) and the Verizon IPCC service (from the manual configuration in this section).

Configure clusterbox:AuraSBC.adevc.avaya.globalipcom.com\interface eth2\ip outside\kernel-filter [Help](#)
[Index](#)

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

allow-rule		allow-rule	admin	destination-port	source-address/mask	source-port	protocol
	Edit Delete	allow-rule allow-sip-udp-from-peer-1	enabled	5060	172.30.209.0/24	0	udp
	Edit Delete	allow-rule allow-sip-udp-from-peer-2	enabled	5060	172.30.205.0/24	5072	udp
Add allow-rule							
deny-rule		deny-rule	admin	destination-port	source-address/mask	source-port	protocol
	Edit Delete	deny-rule deny-all-sip	enabled	5060	0.0.0.0/0	0	all
Add deny-rule							

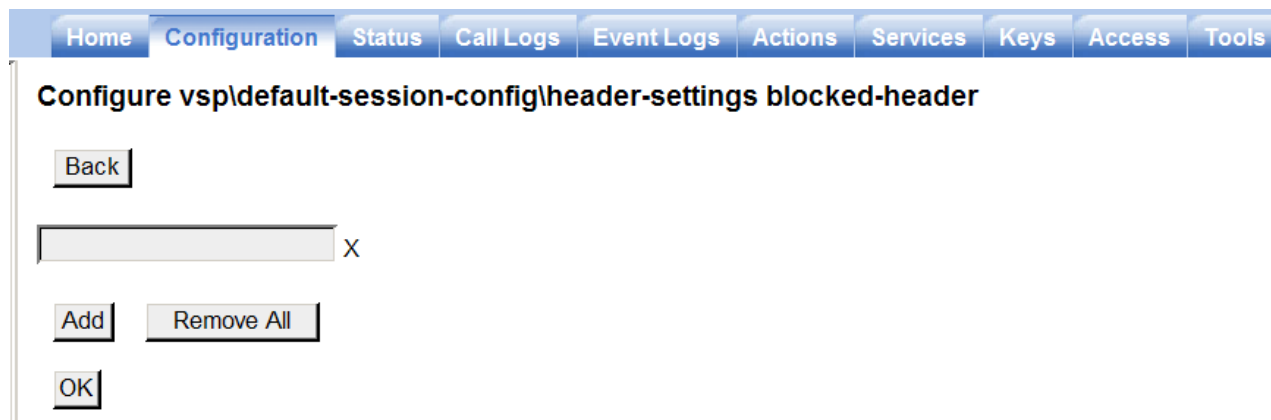
Proceed to save and activate the configuration as described in Section 7.4.

7.3.6 Stripping Unnecessary SIP Headers

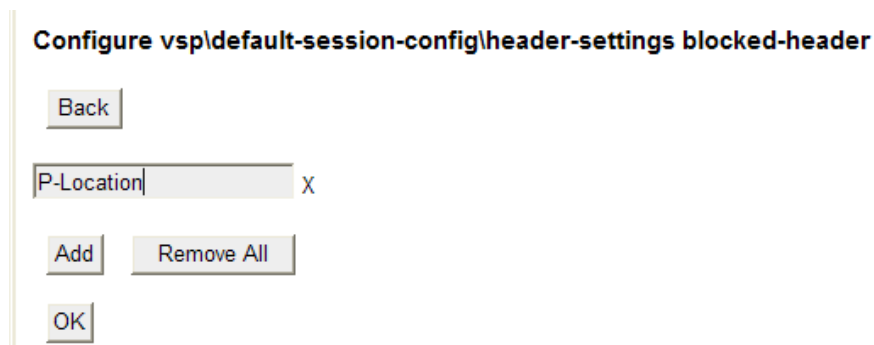
The SBC can be used to strip SIP headers that are not required or expected by Verizon. For headers that have relevance only within the enterprise, it may be desirable to prevent the header from being sent to the public SIP Service Provider. For example, Session Manager Release 6.1 may insert the P-Location header. The Avaya CS1000E may send the “x-nt-e164-clid”, “x-nt-corr-id”, and “Alert-Info” headers. While allowing these headers to be sent to Verizon does not cause any user-perceivable problem, the following procedures may be used to strip such headers that Verizon does not require.

Select the **Configuration** tab. Using the menu on the left hand side, select **vsp** → **default-session-config**. Scroll down on the right and select **header-settings** or expand **default-session-config** and click on **header-settings**. Select the **blocked-header** link on the right.

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



To block the P-Location header, enter “P-Location” and click **OK**, or click **Add** to configure more blocked headers.



The following screen shows the screen after the **Add** button was clicked and the addition blocked-header “x-nt-e164-clid” was entered.

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

X

X

Continue to add the desired blocked-headers in this fashion. When finished, click **OK** and **Set**. The following screen shows the blocked-headers used in the sample configuration.

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

allowed-header	Edit allowed-header
blocked-header	<div> <input type="text" value="P-Location"/> <input type="text" value="x-nt-e164-clid"/> <input type="text" value="x-nt-corr-id"/> <input type="text" value="Alert-Info"/> </div> Edit blocked-header

If the default-session-config does not apply, similar procedures can be used to strip headers in a more specific session-config-pool. For example, to strip the P-Location header in the session-config-pool “To-Telco”, navigate to **vsp → session-config-pool → entry ToTelco → header-settings**. In the resultant screen, click **Edit blocked-header** and proceed to add the P-Location and other blocked headers as described in this section.

Proceed to save and activate the configuration as described in Section 7.4.

7.3.6.1 Stripping Diversion for IP Contact Center Only

The Verizon IP Contact Center service does not support receiving Diversion header. However, the Verizon IP Trunk service does support Diversion header and expects to receive Diversion header in specific scenarios, such as call forwarding to Verizon IP Trunk service. To ensure that a Diversion header is never sent to Verizon IP Contact Center, the following procedure may be followed. On the production circuit used for testing, this procedure was not required.

Navigate to **vsp** → **session-config-pool** as shown below on the left. In the right-hand side, enter a **name** for a new session-config-pool entry that will later be assigned for use by Verizon IPCC. Click **Create**.

Configuration: all

Configuration Setup View

- cluster
 - box:AuraSBC.adevc.avaya.globalipcom.co
- vsp
 - default-session-config
 - tls
 - session-config-pool

Create vsp\session-config-pool\entry - Step 1 of 1: Edit entry

Please provide some basic information for entry. Then press "Create".

basic:

* name To-VZIPCC

Create Reset Cancel

Navigate to the newly created “To-VZIPCC” session-config-pool entry, and scroll down on the right to the “header” area. Select **Configure** next to **header-settings** as shown below.

Configuration: all

Configuration Setup View

- cluster
 - box:AuraSBC.adevc.avaya.globalipcom.co
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelco
 - entry ToPBX
 - entry Discard
 - entry To-VZIPCC

media-scanner-settings [Configure](#)

dtmf:

in-dtmf-translation [Configure](#)

out-dtmf-translation [Configure](#)

header:

header-settings [Configure](#)

inbound-header-settings [Configure](#)

Configure header-settings

Select **Edit blocked-header** as shown below.

Configure vsp\session-config-pool\entry To-VZIPCC\header-settings [Show advanced](#)

Set Reset Back Delete

allowed-header	Edit allowed-header
blocked-header	Edit blocked-header
altered-header	Add altered-header Edit blocked-header

In the resultant screen, type in “Diversion” and click **Add**. Since this session-config-pool entry will be used instead of the default session-config-pool entry, any blocked-headers previously assigned to the default session-config-pool entry should also be added, as shown earlier in this section. After completing data entry for all blocked headers, click **OK** and **Set**.

Configure vsp\session-config-pool\entry To-VZIPCC\header-settings blocked-header

Back

Diversion X

Add Remove All

OK

The following screen shows the list of blocked-headers assigned to the session-config-pool entry To-VZIPCC at the end of the procedure.

The screenshot shows a configuration window with a left-hand menu and a main content area. The left-hand menu is expanded to show the path: **enterprise** → **servers** → **sip-gateway VZ-IPCC**. The main content area is titled **header-settings** and contains a table with two columns: **allowed-header** and **blocked-header**. The **blocked-header** column contains a list of headers: **Diversion**, **P-Location**, **x-nt-e164-clid**, **x-nt-corr-id**, and **Alert-Info**. There are links for **Edit allowed-header** and **Edit blocked-header** at the top and bottom of the table respectively.

On the left menu, navigate to **vsp** → **enterprise** → **servers** and select the sip-gateway “VZ-IPCC” for the Verizon IP Contact Center service, as shown in the abridged screen below.

The screenshot shows the left-hand menu with the following structure: **enterprise** (expanded) → **servers** (expanded) → **sip-gateway PBX** (highlighted in green) → **sip-gateway Telco** (highlighted in red) → **dns-group VZ-IPTrunk-DNS-Group** (highlighted in green) → **vsp\session-config-pool\entry ToTelco** (highlighted in blue) → **sip-gateway VZ-IPCC** (highlighted in blue).

On the right, scroll down to the **policy** area. In the inbound-session-config-pool-entry, select the newly created session-config-pool that blocks Diversion header, as shown below.

general:	
* name	VZ-IPCC
admin	enabled (Resource is active)
domain	
failover-detection	ping (Use OPTIONS to detect failures)

servers:	
+	server-pool
	[Delete]

policy:	
inbound-session-config-pool-entry	vsp\session-config-pool\entry To-VZIPCC Edit Create
outbound-session-config-pool-entry	vsp\session-config-pool\entry ToTelco Edit Create

Proceed to save and activate the configuration as described in Section 7.4.

7.3.7 Stripping Unnecessary SIP Message Body Information (Optional)

The procedures in this section are optional.

The SBC can be used to strip information from the message body that is not required or expected by Verizon. For example, if Verizon IP Trunk service will be used for outbound calls, the message body of an INVITE message sent from the Avaya CS1000E will contain a MIME Multipart message body containing the SDP information expected by Verizon, but also containing “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” application parts that are not processed by Verizon. On the production circuit used for testing, Verizon was able to properly parse the Multipart MIME message body, and outgoing calls from the CS1000E to Verizon IP Trunk Service could be completed successfully without the configuration in this section. Nevertheless, since Verizon has no use for this information, the following procedures may be used to strip out unnecessary information and send only SDP in the message body to Verizon.

Two alternative approaches were tested successfully. In one approach, the SBC is used to specifically block the “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” parts. In another approach, the SBC is used to block any body part that is not SDP.

7.3.7.1 Block Any body part but SDP Approach

To block any body part but SDP, navigate to **vsp → default-session-config → bodypart-type**. Click **Add allowed-body-part**. In the **bodypart-type** drop-down menu, select “application”. In the application-sub-type menu, select “sdp” as shown in the screen below. Click **Create**.

Create vsp\default-session-config\bodypart-type\allowed-body-part - Step 1 of 1: Edit allowed-body-part

Please provide some basic information for allowed-body-part. Then press "Create".

* bodypart-type	application
* application-sub-type	sdp
<div>Create Reset Cancel</div>	

Then navigate to **vsp → default-session-config → bodypart-type**. Click **Add blocked-body-part**. In the **bodypart-type** drop-down menu, select "application". In the application-sub-type menu, select "any" as shown in the screen below. Click **Create**.

Create vsp\default-session-config\bodypart-type\blocked-body-part - Step 1 of 1: Edit blocked-body-part

Please provide some basic information for blocked-body-part. Then press "Create".

* bodypart-type	application
* application-sub-type	any
<div>Create Reset Cancel</div>	

The following screen shows the resulting configuration, where any application except SDP is blocked. Click **Set**.

Configuration: all

Configuration Setup View

cluster

box:AuraSBC.adevc.avaya.globalipcom.com

vsp

default-session-config

sip-settings

media

bodypart-type

sdp-regeneration

sip-directive

log-alert

header-settings

third-party-call-control

codec-specific-parameters

tls

session-config-pool

dial-plan

enterprise

dns

...

Configure vsp\default-session-config\bodypart-type

Set Reset Back Delete

allowed-body-part

bodypart-type

Edit Delete application sdp

Add allowed-body-part

blocked-body-part

bodypart-type

Edit Delete application any

Add blocked-body-part

move-bp-headers

disabled (Resource is inactive)

Set Reset Back

Proceed to save and activate the configuration as described in Section 7.4.

7.3.7.2 Block Specific Body Part Approach

This is an alternative to the approach documented in the previous sub-section. That is, it is shown as if the procedures in the prior section were not followed. In this section, the specific body parts that the CS1000E inserts in the message body are blocked rather than blocking anything but SDP.

Navigate to **vsp → default-session-config → bodypart-type**. Click **Add blocked-body-part**. In the **bodypart-type** drop-down menu, select “application”. In the application-sub-type menu, type in or select “x-nt-mcdn-frag-hex”. Click **Create**.

Again click **Add blocked-body-part**. In the **bodypart-type** drop-down menu, select “application”. In the application-sub-type menu, type in or select “x-nt-epid-frag-hex”. Click **Create**.

The following screen shows the resulting configuration. Click **Set**.

Configure vsp\default-session-config\bodypart-type [Help](#) [Index](#)

Set	Reset	Back	Delete
------------	--------------	-------------	---------------

allowed-body-part	Add allowed-body-part									
blocked-body-part	<table border="1"><thead><tr><th></th><th></th><th>bodypart-type</th></tr></thead><tbody><tr><td>▼</td><td>Edit Delete</td><td>application x-nt-mcdn-frag-hex</td></tr><tr><td>▲</td><td>Edit Delete</td><td>application x-nt-epid-frag-hex</td></tr></tbody></table> Add blocked-body-part			bodypart-type	▼	Edit Delete	application x-nt-mcdn-frag-hex	▲	Edit Delete	application x-nt-epid-frag-hex
		bodypart-type								
▼	Edit Delete	application x-nt-mcdn-frag-hex								
▲	Edit Delete	application x-nt-epid-frag-hex								

Proceed to save and activate the configuration as described in Section 7.4.

7.3.8 Disable Third Party Call Control

The installation wizard for the Avaya Aura® SBC in the release documented in these Application Notes will enable the **admin** field for third party call control. However, with third party call control enabled, the SBC is not able to properly reformat the message body with only the SDP information as described in the previous section. See Section 2.2 of Reference [AuraSBC-IP-Trunk].

To disable third party call control, navigate to **vsp → default-session-config → third-party-call-control**. To disable third-party-call-control, select disabled from the **admin** drop-down and click **Set** as shown below.

Set

Reset

Back

Delete

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

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

Configuration: all

Configuration Setup View

- cluster
 - box:AuraSBC.adevc.avaya.globalipcom.co
- vsp
 - default-session-config
 - sip-settings
 - media
 - bodypart-type
 - sdp-regeneration
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control

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

Show advanced

Set Reset Back Delete

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

Proceed to save and activate the configuration as described in Section 7.4.

7.3.9 Quality Of Service (QoS) Markings for SIP Signaling

The procedure in this section is optional. The procedure can be used to achieve SIP signaling re-marking using the Avaya Aura® SBC.

The default QoS behavior after using the installation wizard will be to preserve the TOS values. That is, the TOS value received from the private side of the SBC will be transmitted to Verizon on the public side of the SBC. For example, if Session Manager sends a SIP message to the SBC with a Differentiated Services Code Point (DSCP) value of 46, then the SBC will send the SIP message to Verizon with a DSCP of 46. To change this behavior, navigate to **vsp** → **session-config-pool** → **entry default-session-config** → **sip-settings** and scroll down to the **message-options** heading. The following portion of the screen shows the settings configured by the installation wizard, where the **inleg-tos** and **outleg-tos** are set to “preserve”.

inleg-tos	mode preserve
outleg-tos	mode preserve

If it is desired to have the SBC re-mark SIP signaling to a different DSCP, the **inleg-tos** and **outleg-tos** parameters can be changed to desired DSCP values. For example, select “overwrite” from the **outleg-tos mode** drop-down menu.

outleg-tos	mode	overwrite ▼
	value	104 (from 0 to 255)

In the **value** field that appears after selecting “overwrite”, enter the decimal value corresponding to the byte containing the ToS field. For example, if the value is set to 104 (0x68) as shown above, the DSCP value 26 (0x1A) will be sent to Verizon (decoded by Wireshark as “Assured Forwarding 31”).

outleg-tos	mode	overwrite ▼
	value	104 (from 0 to 255)

If desired, make the same change for the **inleg-tos**. Click the **Set** button. If DSCP value 28 (0x1C) is desired (decoded by Wireshark as “Assured Forwarding 32”), then the **value** field can be set to 112 instead.

inleg-tos	mode	overwrite ▼
	value	104 (from 0 to 255)
outleg-tos	mode	overwrite ▼
	value	104 (from 0 to 255)

Proceed to save and activate the configuration as described in Section 7.4.

7.3.10 Quality Of Service (QoS) Markings for Media

The procedure in this section is optional. If it is desired to have the SBC re-mark the DSCP in RTP media packets, navigate to **vsp → default-session-config → media**. Scroll down on the right until the **packet-marking** section is visible. The following screen shows the relevant area.

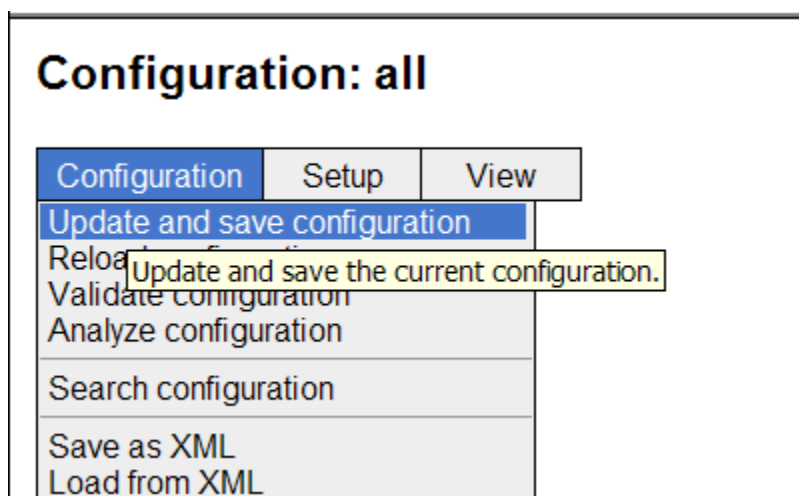
Set the **packet-marking mode** to “tos”. In the **value** field, enter the desired value of the ToS byte. The following screen uses the **value** “0xb8”. With this configuration, RTP packets flowing to Verizon will contain DSCP 0x2e (decoded by Wireshark as “Expedited Forwarding”).

inactivity-style	<div>session</div> <div>(inactivity is determined across the entire session)</div>
monitor	<div>▼</div> <div>Create</div>
media-verify-config	<div>Configure</div>
packet-marking	<div>* mode</div> <div>tos</div> <div>(Specify TOS value to mark packets with)</div> <div>value</div> <div>0xb8</div> <div>(from 0 to 255)</div>
rtp-stats	<div>enabled</div> <div>(Resource is active)</div>

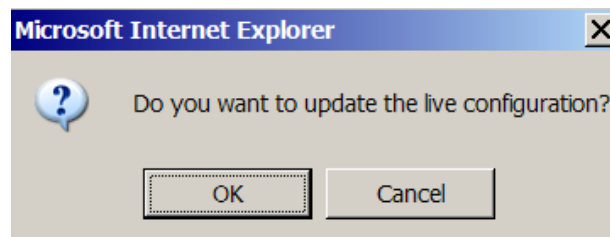
Proceed to save and activate the configuration as described in Section 7.4.

7.4. Saving and Activating Configuration Changes

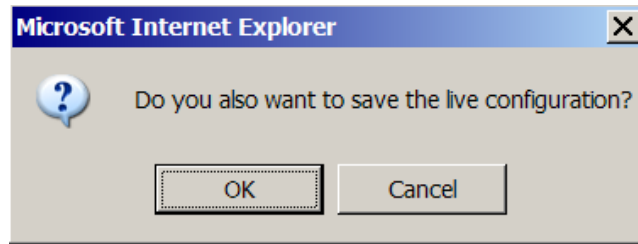
To save and activate configuration changes, select **Configuration → Update and save configuration** from the upper left hand side of the user interface, as shown below.



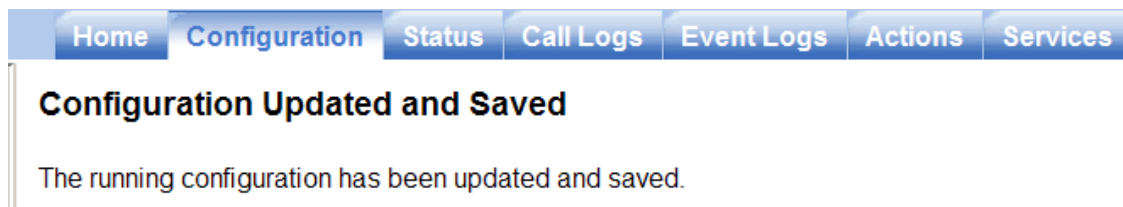
Click **OK** to update the live configuration.



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



A screen that includes the following should appear.



7.5. Example Configuration File

The configuration changes made by the installation wizard and the element manager OS-E GUI result in a text configuration file. A copy of the configuration file can be retrieved from the SBC by selecting the **Tools** tab and selecting **Download saved configuration file** from the left-side menu. An example configuration file resulting from the configuration in Section 7 is included below. This file includes configuration for Verizon IP Trunk service (from Reference [AuraSBC-IP-Trunk]) as well as configuration for Verizon IPCC service.

```
#
# Copyright (c) 2004-2010 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 10:11:00 Wed 2011-05-18
#
config cluster
config box 1
set hostname AuraSBC.adevc.avaya.globalipcom.com
set timezone America/New_York
set name AuraSBC.adevc.avaya.globalipcom.com
set identifier 00:ca:fe:69:46:13
config interface eth0
config ip inside
set ip-address static 65.206.67.93/24
config ssh
return
config snmp
set trap-target 65.206.67.92 162
set trap-filter generic
set trap-filter dos
set trap-filter sip
set trap-filter system
return
config web
```

```

return
config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
return
config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
return
config icmp
return
config media-ports
return
config routing
    config route Default
        set gateway 65.206.67.254
    return
    config route Static0
        set destination network 192.11.13.4/30
        set gateway 65.206.67.91
    return
    config route Static1
        set admin disabled
    return
    config route Static2
        set admin disabled
    return
    config route Static3
        set admin disabled
    return
    config route Static4
        set admin disabled
    return
    config route Static5
        set admin disabled
    return
    config route Static6
        set admin disabled
    return
    config route Static7
        set admin disabled
    return
return
config dns-server
return
return
config interface eth2
    config ip outside
        set ip-address static 1.1.1.2/24
    config sip
        set udp-port 5060 "" "" any 0
    return
    config media-ports
    return
    config routing

```



```

config route Default
    set admin disabled
return
config route external-sip-media-1
    set destination network 172.30.209.0/24
    set gateway 1.1.1.1
return
config route VZ-IPCC-network
    set destination network 172.30.205.0/24
    set gateway 1.1.1.1
return
return
config kernel-filter
    config allow-rule allow-sip-udp-from-peer-2
        set destination-port 5060
        set source-address/mask 172.30.205.0/24
        set source-port 5072
        set protocol udp
    return
    config allow-rule allow-sip-udp-from-peer-1
        set destination-port 5060
        set source-address/mask 172.30.209.0/24
        set protocol udp
    return
    config deny-rule deny-all-sip
        set destination-port 5060
    return
return
return
return
config cli
    set prompt AuraSBC.adevc.avaya.globalipcom.com
return
return
return

config services
config event-log
    config file access
        set filter access info
        set count 3
    return
    config file system
        set filter system info
        set count 3
    return
    config file errorlog
        set filter all error
        set count 3
    return
    config file db
        set filter db debug
        set filter dosDatabase info
        set count 3
    return
    config file management
        set filter management info

```

```

    set count 3
return
config file peer
    set filter sipSvr info
    set count 3
return
config file dos
    set filter dos alert
    set filter dosSip alert
    set filter dosTransport alert
    set filter dosUrl alert
    set count 3
return
config file krnlsys
    set filter krnlsys debug
    set count 3
return
return
return

config master-services
    config database
    set media enabled
    return
return

config vsp
    set admin enabled
    config default-session-config
    config sip-settings
        set inleg-tos overwrite 104
        set outleg-tos overwrite 104
    return
    config media
        set anchor enabled
        set packet-marking tos 0xb8
        set rtp-stats enabled
    return
    config bodypart-type
        set allowed-body-part application sdp
        set blocked-body-part application any
    return
    config sdp-regeneration
        set regenerate disabled
        set name Aura-SBC
    return
    config sip-directive
        set directive allow
    return
    config log-alert
        set apply-to-methods-for-filtered-logs
    return
    config header-settings
        set blocked-header P-Location
        set blocked-header x-nt-e164-clid
        set blocked-header x-nt-corr-id
        set blocked-header Alert-Info

```

```

return
config third-party-call-control
    set handle-refer-locally disabled
return
config codec-specific-parameters
return
return
config tls
config default-ca
    set ca-file /cxc/certs/sipca.pem
return
config certificate ws-cert
    set certificate-file /cxc/certs/ws.cert
return
config certificate aasbc.pl2
    set certificate-file /cxc/certs/aasbc.pl2
    set passphrase-tag aasbc-cert-tag
return
return
config session-config-pool
config entry ToTelco
return
config entry ToPBX
    config to-uri-specification
        set host next-hop-domain
    return
    config request-uri-specification
        set host next-hop-domain
    return
return
config entry Discard
    config sip-directive
return
return
config entry To-VZIPCC
    config header-settings
        set blocked-header Diversion
        set blocked-header P-Location
        set blocked-header x-nt-e164-clid
        set blocked-header x-nt-corr-id
        set blocked-header Alert-Info
    return
return
return
config dial-plan
config route Default
    set priority 500
    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
return
config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\dns-group VZ-IPTrunk-DNS-
Group"
return
config source-route FromPBX
    set peer server "vsp\enterprise\servers\dns-group VZ-IPTrunk-DNS-Group"

```

```

    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
return
config source-route FromVZIPCC
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway VZ-IPCC"
return
config source-route FromPBXtoVZIPCC
    set peer server "vsp\enterprise\servers\sip-gateway VZ-IPCC"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
return
return
config enterprise
    config servers
        config sip-gateway PBX
            set domain adevc.avaya.globalipcom.com
            set failover-detection ping
            set outbound-session-config-pool-entry vsp\session-config-pool\entry ToPBX
        config server-pool
            config server PBX1
                set host 10.1.2.210
                set transport TCP
            return
        return
    return
    config sip-gateway Telco
        set admin disabled
        set failover-detection ping
        set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
        config server-pool
            config server Telco1
                set host 172.30.209.21
                set port 5071
            return
        return
    return
    config dns-group VZ-IPTrunk-DNS-Group
        set domain pcelban0001.avayalincroft.globalipcom.com
        set failover-detection ping
        set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
        return
        config sip-gateway VZ-IPCC
            set failover-detection ping
            set ping-interval 30
            set inbound-session-config-pool-entry vsp\session-config-pool\entry To-
VZIPCC
            set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
        config server-pool
            config server VZ-IPCC-network
                set host 172.30.205.55
                set port 5072
            return
        return
    return
return

```

```

return
config dns
  config resolver
    config server 172.30.209.4
    set name VZ-IPTrunk-DNS
  return
return
return
config settings
  set read-header-max 8191
return
return

config external-services
return

config preferences
  config gui-preferences
  return
return

config access
  config permissions superuser
    set cli advanced
  return
  config permissions read-only
    set config view
    set actions disabled
  return
  config users
    config user admin
      set password 0x00e9a8385c963a64b97c9efd745dca47a89d67a2ff039b08cefbbe8c6b
      set permissions access\permissions superuser
    return
    config user cust
      set password 0x0077cc723ccd18d052a3ce58a8f47712d1c49d99963a7b8086a554d15e
      set permissions access\permissions read-only
    return
    config user init
      set password 0x00527bc64d625298d3d82aecb06b5b82d74e6c74a212e7d7783276bd46
      set permissions access\permissions superuser
    return
    config user craft
      set password 0x00623332bf3f6d7069f443dcdc98b8d4aa67bb3d4e3bebed35fd2f09f8
      set permissions access\permissions superuser
    return
    config user dadmin
      set password 0x00f6240b8d3a025fdf273432b58036947f461243c56717ec8379432867
      set permissions access\permissions read-only
    return
  return
return

config features
return

```

8. Verizon Business IP Contact Center 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 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 IPCC Network
<i>adevc.avaya.globalipcom.com</i> <i>UDP port 5060</i>	<i>172.30.205.55</i> <i>UDP Port 5072</i>

8.2. Numbers Assigned by Verizon

Verizon will provide IP Toll Free VoIP Inbound numbers and/or Verizon IP-IVR numbers as part of service provisioning. **Table 2** and **Table 3** in Section 3 show the Verizon-provided IP Toll Free and IP-IVR numbers used in the sample configuration.

9. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business IP Contact Center service.

9.1. Avaya Communication Server 1000E Verifications

This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI. Additional commands are illustrated in Section 9.1 of [AuraSBC-IP-Trunk].

9.1.1 IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below. In the resultant screen on the right, click the **Gen CMD** button.

Managing: 10.7.8.61 Username: admin
System » IP Network » Node Maintenance and Reports

Node Maintenance and Reports

Node ID: 2		Node IP: 10.7.7.60		
Hostname	ELAN IP	Type	TN	
cs1k75	10.7.8.61	Signaling Server-Avaya CPPMv1	NO TN	

GEN CMD SYS LOG OI

The **General Commands** page is displayed as shown below.

General Commands

Element IP : 10.7.8.61 Element Type : Signaling Server-Avaya CPPMv1

Group

Command

-- Select A Group --

RUN

IP address

10.7.8.61

Number of pings

3

PING

Click on a button to invoke a command.

A variety of commands are available by selecting an appropriate **Group** and **Command** from the drop-down menus, and selecting **Run**.

To check the status of the SIP Gateway to Session Manager in the sample configuration, select “Sip” from the **Group** menu and “SIPGwShow” from the **Command** menu. Click **Run**. The example output below shows that the Session Manager (10.1.2.210, port 5060, TCP) has “SIPNPM Status” Active.

General Commands

Element IP : 10.7.8.61 Element Type : Signaling Server-Avaya CPPMv1

Group

Sip

Command

SIPGwShow

Sip

RUN

IP address

10.7.8.61

Number of pings

3

PING

SIPNPM Status : Active

Primary Proxy IP address : 10.1.2.210

Primary Proxy port : 5060

Primary Proxy Transport : TCP

Secondary Proxy IP address : 0.0.0.0

Secondary Proxy port : 5060

Secondary Proxy Transport : TCP

Primary Proxy2 IP address : 10.1.2.210

Primary Proxy2 port : 5060

Primary Proxy2 Transport : TCP

The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command** “sigSetShowAll” in **Group** “SipLine”. At the time this screen was captured, the SIP telephone with DN 57007 was involved in an active call.

General Commands

Element IP : 10.7.8.61 Element Type : Signaling Server-Avaya CPPMv1

Group

SipLine

Command

sigSetShowAll

RUN

IP address

10.7.8.61

Number of pings

3

PING

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
IPV4 Endpoints							
57004	57004	096-00-00-00	1	0	0xa94fb80		SIP Lines
57007	57007	096-00-00-10	1	1	0xa955cc8		SIP Lines

The following screen shows a means to view IP UNISim telephones. The screen shows the output of the **Command** “isetShow” in **Group** “Iset”. At the time this screen was captured, the “2007 Phase 2 IP Deskphone” UNISim telephone was involved in an active call.

General Commands

Element IP : 10.7.8.61 Element Type : Signaling Server-Avaya CPPMV1

Group	Iset	Command	isetShow	Range	0	
IP address		10.7.8.61				
		Number of pings				3

Set Information

IP Address	NAT	Model Name	Type	RegType	State	Up
10.7.7.121		1120E IP Deskphone	1120	Regular	online	
10.7.7.122		1140E IP Deskphone	1140	Regular	online	
10.7.7.123		2007 Phase 2 IP Deskphone	2007	Regular	busy	

9.1.2 System Maintenance Commands

A variety of system maintenance commands are available by navigating to **System** → **Maintenance** using Element Manager. The user can navigate the maintenance commands using either the “Select by Overlay” approach or the “Select by Functionality” approach.

Managing: 10.7.8.61 Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay

☐ Select by Functionality

The following screen shows an example where “Select by Overlay” has been chosen. The various overlays are listed, and the “LD 96 – D-Channel” is selected.

Maintenance

☒ Select by Overlay

☐ Select by Functionality

<Select by Overlay>
LD 30 - Network and Signaling
LD 32 - Network and Peripheral Equipment
LD 34 - Tone and Digit Switch
LD 36 - Trunk
LD 37 - Input/Output
LD 38 - Conference Circuit
LD 39 - Intergroup Switch and System Clock
LD 45 - Background Signaling and Switching
LD 46 - Multifrequency Sender
LD 48 - Link
LD 54 - Multifrequency Signaling
LD 60 - Digital Trunk Interface and Primary Rate Interface
LD 75 - Digital Trunk
LD 80 - Call Trace
LD 96 - D-Channel
LD 117 - Ethernet and Alarm Management
LD 135 - Core Common Equipment
LD 137 - Core Input/Output
LD 143 - Centralized Software Upgrade

<Select Group>
D-Channel Diagnostics
MSDL Diagnostics
TMDI Diagnostics

On the preceding screen, if **D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 1, which is used in the sample configuration, is established “EST” and active “ACTV”.

D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	<input type="button" value="Submit"/>
Test Interrupt Generation (TEST 100)		<input type="button" value="Submit"/>
Establish D-Channel (EST DCH)		<input type="button" value="Submit"/>

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_REC	PDCH	BDCH
-----	-----	-------------	-------------	----------	------	------

☐ 001 VirtDchToSS OPER EST ACTV AUTO

9.2. Wireshark Verification

This section illustrates Wireshark traces for an inbound IP Toll-Free VoIP Inbound call using the sample configuration. The PSTN telephone 908-848-5704 dials the IP Toll Free number 866-850-6850.

The following screen shows a Wireshark trace taken from the outside of the SBC. The use of UDP and port 5072 can be observed. The INVITE from Verizon in frame 9 is selected and expanded to illustrate the contents of the message header. The Request-URI contains the dialed IP Toll Free number 8668506850. Note that Verizon prefixes the calling party number 9088485704 in the From and PAI headers with +1. The overall flow for an incoming call can be observed. In frame 11, a 180 Ringing (without SDP) response is sent to Verizon. In frame 13, the 200 OK with SDP answering the inbound call is sent to Verizon.

Filter: sip && ip.addr == 172.30.205.55

No.	Time	Source	Destination	Protocol	Info
9	5.907405	172.30.205.55	1.1.1.2	SIP/SD	Request: INVITE sip:8668506850@adecv.avaya.globalipcom.c
10	5.910727	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
11	6.031796	1.1.1.2	172.30.205.55	SIP	Status: 180 Ringing
13	7.991757	1.1.1.2	172.30.205.55	SIP/SD	Status: 200 OK, with session description

Expanded details for Frame 9:

- Internet Protocol, Src: 172.30.205.55 (172.30.205.55), Dst: 1.1.1.2 (1.1.1.2)
- User Datagram Protocol, Src Port: ayiya (5072), Dst Port: sip (5060)
- Session Initiation Protocol
 - Request-Line: INVITE sip:8668506850@adecv.avaya.globalipcom.com:5060 SIP/2.0
 - Message Header
 - Via: SIP/2.0/UDP 172.30.205.55:5072;branch=z9hG4bKncms5n209gn0ntk7g4b1.1
 - Call-ID: -1427917342892969055@63.78.210.214
 - From: <sip:+19088485704@199.173.95.16:5060;user=phone>;tag=-643550759.10.pdoecnf1ofkchicckfcmn1
 - To: sip:18668506850@1.1.1.2
 - CSeq: 1 INVITE
 - Contact: <sip:+19088485704@172.30.205.55:5072;transport=udp>
 - Allow: INVITE, ACK, BYE, OPTIONS, CANCEL, SUBSCRIBE, REFER
 - P-Asserted-Identity: <sip:+19088485704@199.173.95.16;user=phone>
 - Accept: application/sdp
 - Content-Type: application/sdp
 - Content-Length: 204
 - Max-Forwards: 69
 - Message Body

The following screen shows the same Wireshark trace and message, focusing on the message body of the INVITE in frame 9. Note that the Verizon SDP offer lists G.729 first, followed by G.711. The value “101” is specified for “DTMF” using RFC 2833.

No. ↓	Time	Source	Destination	Protocol	Info
9	5.907405	172.30.205.55	1.1.1.2	SIP/SD	Request: INVITE sip:8668506850@adevc.avaya.globalipcom.com
Internet Protocol, Src: 172.30.205.55 (172.30.205.55), Dst: 1.1.1.2 (1.1.1.2)					
User Datagram Protocol, Src Port: ayiya (5072), Dst Port: sip (5060)					
Session Initiation Protocol					
Request-Line: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060 SIP/2.0					
Message Header					
Message Body					
Session Description Protocol					
Session Description Protocol Version (v): 0					
Owner/Creator, Session Id (o): - 1304436057580 0 IN IP4 172.30.205.164					
Session Name (s): -					
Connection Information (c): IN IP4 172.30.205.164					
Time Description, active time (t): 0 0					
Media Description, name and address (m): audio 10026 RTP/AVP 18 0 8 101					
Media Attribute (a): rtpmap:101 telephone-event/8000					
Media Attribute (a): fmtp:101 0-15					
Media Attribute (a): ptm:20					
Media Attribute (a): fmtp:18 annexb=no					

The following screen shows a filtered Wireshark trace taken from the inside of the SBC. The INVITE sent from the SBC to Session Manager in frame 367 is selected and expanded to illustrate the message headers. The toll-free number 8668506850 can be observed in the Request-URI along with the domain “adevc.avaya.globalipcom.com”. Session Manager will use the Request-URI for routing. The From and PAI headers contain the calling PSTN telephone number 908-848-5704, prefixed with “+1”. This screen also shows the SIP messaging through answer. In frame 379, the CS1000E sends 180 Ringing (without SDP) when alerting the telephone, and in frame 432, the CS1000E sends the 200 OK with SDP when the call is answered.

Filter: (sip && ip.addr == 10.7.7.60) (sip && ip.addr == 65.206.67.93) Expression... Clear Apply					
No. ↓	Time	Source	Destination	Protocol	Info
367	10.842085	65.206.67.93	10.1.2.210	SIP/SDP	Request: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060, with session description
368	10.843968	10.1.2.210	65.206.67.93	SIP	Status: 100 Trying
372	10.887489	10.1.2.210	10.7.7.60	SIP/SDP	Request: INVITE sip:57003@avaya.com:5060, with session description
375	10.910207	10.7.7.60	10.1.2.210	SIP	Status: 100 Trying
379	10.956954	10.7.7.60	10.1.2.210	SIP	Status: 180 Ringing
381	10.959148	10.1.2.210	65.206.67.93	SIP	Status: 180 Ringing
432	12.914132	10.7.7.60	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
435	12.917757	10.1.2.210	65.206.67.93	SIP/SDP	Status: 200 OK, with session description
446	13.142521	65.206.67.93	10.1.2.210	SIP	Request: ACK sip:57003@avaya.com:5060;maddr=10.7.7.60;transport=tcp;user=phone
447	13.145070	10.1.2.210	10.7.7.60	SIP	Request: ACK sip:57003@avaya.com:5060;maddr=10.7.7.60;transport=tcp;user=phone
Session Initiation Protocol					
Request-Line: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060 SIP/2.0					
Message Header					
From: <+19088485704@199.173.95.16:5060>;tag=5d43ce41-13c4-4dc01f00-6b8eb27f-28862b0b					
To: <+18668506850@adevc.avaya.globalipcom.com>					
Call-ID: CXC-108-5c412e70-5d43ce41-13c4-4dc01f00-6b8eb27f-199d7c85@199.173.95.16					
CSeq: 1 INVITE					
Via: SIP/2.0/TCP 65.206.67.93:5060;branch=z9hG4bK-2590-4dc01f00-6b8eb27f-37bfdde8					
Allow: INVITE,ACK,BYE,OPTIONS,CANCEL,SUBSCRIBE,REFER					
P-Asserted-Identity: <+19088485704@199.173.95.16>					
Accept: application/sdp					
Max-Forwards: 68					
Contact: <+19088485704@199.173.95.16:5060;maddr=65.206.67.93;transport=tcp>					
Content-Type: application/sdp					
Content-Length: 200					

The following screen shows the same filtered Wireshark trace. The INVITE sent from Session Manager to the CS1000E in Frame 372 is selected and expanded to illustrate select message headers. From the selected frame (in blue), it can be observed that the toll-free number 8668506850 in the original Request-URI has been adapted by Session Manager to the CS1000E Directory Number 57003. The original domain “adevc.avaya.globalipcom.com” has been adapted to “avaya.com” in the Request-URI, From, and To headers by this same Session Manager adapter.

Filter: (sip && ip.addr == 10.7.7.60) (sip && ip.addr == 65.206.67.93) Expression... Clear Apply					
No. .	Time	Source	Destination	Protocol	Info
367	10.842085	65.206.67.93	10.1.2.210	SIP/SDP	Request: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060, with session description
368	10.843968	10.1.2.210	65.206.67.93	SIP	Status: 100 Trying
372	10.887489	10.1.2.210	10.7.7.60	SIP/SDP	Request: INVITE sip:57003@avaya.com:5060, with session description
P-Asserted-Identity: <sip:+19088485704@avaya.com> From: <sip:+19088485704@avaya.com:5060>;tag=5d43ce41-13c4-4dc01f00-6b8eb27f-28862b0b Route: <sip:10.7.7.60;transport=tcp;lr;phase=terminating> P-Location: SM;origlocname="Aura-SBC";termlocname="CS1K75-Location" Max-Forwards: 64 User-Agent: AVAYA-SM-6.1.1.0.611023					

The following screens show the same Wireshark trace, focused on the message bodies. The SDP offer in the INVITE in frame 367 is expanded in the screen below. Note that inbound IP Toll-Free VoIP Inbound calls prefer G.729A (18, annexb=no) and allow G.711 (0). For “DTMF” events, the value “101” is used. The IP Address (65.206.67.93) is the inside private IP address of the SBC.

Filter: (sip && ip.addr == 10.7.7.60) (sip && ip.addr == 65.206.67.93) Expression... Clear Apply					
No. .	Time	Source	Destination	Protocol	Info
367	10.842085	65.206.67.93	10.1.2.210	SIP/SDP	Request: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060, with session description
368	10.843968	10.1.2.210	65.206.67.93	SIP	Status: 100 Trying
372	10.887489	10.1.2.210	10.7.7.60	SIP/SDP	Request: INVITE sip:57003@avaya.com:5060, with session description
375	10.910207	10.7.7.60	10.1.2.210	SIP	Status: 100 Trying
379	10.956954	10.7.7.60	10.1.2.210	SIP	Status: 180 Ringing
381	10.959148	10.1.2.210	65.206.67.93	SIP	Status: 180 Ringing
432	12.914132	10.7.7.60	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
435	12.917757	10.1.2.210	65.206.67.93	SIP/SDP	Status: 200 OK, with session description
Session Initiation Protocol Request-Line: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060 SIP/2.0 Message Header Message Body Session Description Protocol Session Description Protocol Version (v): 0 Owner/Creator, Session Id (o): - 1304436057580 0 IN IP4 65.206.67.93 Session Name (s): - Connection Information (c): IN IP4 65.206.67.93 Time Description, active time (t): 0 0 Media Description, name and address (m): audio 22350 RTP/AVP 18 0 8 101 Media Attribute (a): rtpmap:101 telephone-event/8000 Media Attribute (a): fmtp:101 0-15 Media Attribute (a): ptm:20 Media Attribute (a): fmtp:18 annexb=no					

In the next screen, the 200 OK sent by the CS1000E in frame 432 is expanded to illustrate the SDP answer. The CS1000E answers with G.729A (18, annexb=no), and the IP Address (10.7.7.123) is the IP Address of the answering IP UNISTim telephone. The use of RFC 2833 value 101 for “DTMF” can be observed.

Filter: (sip && ip.addr == 10.7.7.60) (sip && ip.addr == 65.206.67.93) Expression... Clear Apply					
No. .	Time	Source	Destination	Protocol	Info
367	10.842085	65.206.67.93	10.1.2.210	SIP/SDP	Request: INVITE sip:8668506850@adevc.avaya.globalipcom.com:5060, w
368	10.843968	10.1.2.210	65.206.67.93	SIP	Status: 100 Trying
372	10.887489	10.1.2.210	10.7.7.60	SIP/SDP	Request: INVITE sip:57003@avaya.com:5060, with session description
375	10.910207	10.7.7.60	10.1.2.210	SIP	Status: 100 Trying
379	10.956954	10.7.7.60	10.1.2.210	SIP	Status: 180 Ringing
381	10.959148	10.1.2.210	65.206.67.93	SIP	Status: 180 Ringing
432	12.914132	10.7.7.60	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
435	12.917757	10.1.2.210	65.206.67.93	SIP/SDP	Status: 200 OK, with session description
Message Body Session Description Protocol Session Description Protocol Version (v): 0 Owner/Creator, Session Id (o): - 586 1 IN IP4 10.7.7.60 Session Name (s): - Connection Information (c): IN IP4 10.7.7.123 Time Description, active time (t): 0 0 Media Description, name and address (m): audio 5200 RTP/AVP 18 101 111 Connection Information (c): IN IP4 10.7.7.123 Media Attribute (a): ptm:20 Media Attribute (a): fmtp:18 annexb=no Media Attribute (a): rtpmap:101 telephone-event/8000 Media Attribute (a): fmtp:101 0-15 Media Attribute (a): rtpmap:111 X-nt-inforeq/8000 Media Attribute (a): sendrecv					

The following screen shows a portion of the 200 OK sent to Verizon from the outside of the SBC, focusing on the SDP in the message body. The mapping of the IP Address in the connection information to the outside IP address of the SBC (1.1.1.2) can be observed. The SDP answer contains G.729A (i.e., 18, with annexb=no) and uses “101” for “DTMF” telephone events using RFC2833.

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
9	5.907405	172.30.205.55	1.1.1.2	SIP/SD	Request: INVITE sip:8668506850@adevc.avaya.globalipcom.
10	5.910727	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
11	6.031796	1.1.1.2	172.30.205.55	SIP	Status: 180 Ringing
13	7.991757	1.1.1.2	172.30.205.55	SIP/SD	Status: 200 OK, with session description

Message Body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): - 586 1 IN IP4 1.1.1.2

Session Name (s): -

Connection Information (c): IN IP4 1.1.1.2

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 21014 RTP/AVP 18 101 111

Connection Information (c): IN IP4 1.1.1.2

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): rtpmap:111 X-nt-infomreq/8000

Media Attribute (a):ptime:20

Media Attribute (a):fmtp:18 annexb=no

Media Attribute (a):fmtp:101 0-15

Media Attribute (a):sendrecv

9.3. System Manager and Session Manager Verification

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

9.3.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**.

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

Home / Elements / Session Manager / System Status / SIP Entity Monitoring- SIP Entity Monitoring [Help ?](#)

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: AuraSBC

[Summary View](#)

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

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SM1	65.206.67.93	5060	TCP	Up	404 Not found	Up

Return to the list of monitored entities, and select another entity of interest, such as “CS1000-R75”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. In this case, “Show” under Details was selected to view additional information.

All Entity Links to SIP Entity: CS1000-R75							
Summary View							
1 Item Refresh				Filter: Ena			
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM1	10.7.7.60	5060	TCP	Up	200 OK	Up
Time Last Down		Time Last Up		Last Message Sent		Last Message Response	Last Response Latency (ms)
May 12, 2011 3:24:13 PM EDT		May 12, 2011 3:25:41 PM EDT		May 16, 2011 12:16:22 PM EDT			8

9.3.2 Call Routing Test

The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. A screen such as the following is displayed.

Call Routing Test

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

SIP INVITE Parameters

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

As an example, the following screen shows a call routing test for an inbound IP Toll Free call from the PSTN to the enterprise, arriving via the Avaya Aura® SBC. Under **Routing Decisions**, observe that the call will route to the CS1000E (10.7.7.60) using the SIP entity named “CS1000-R75”. The user part of the Request-URI is adapted from the Verizon IP Toll Free number “8668506850” to the CS1000E Directory Number 57003. The host part of the Request-URI is adapted from the enterprise domain known to Verizon “adevc.avaya.globalipcom.com” to the domain “avaya.com” configured for the shared Avaya Solution and Interoperability Lab test network. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Call Routing Test

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

SIP INVITE Parameters

Called Party URI 8668506850@adevc.avaya.globalipcom.com	Calling Party Address 65.206.67.93
Calling Party URI anyuser@anyhost.com	Session Manager Listen Port 5060
Day Of Week Wednesday ▼	Time (UTC) 11:04
Called Session Manager Instance SM1 ▼	Transport Protocol TCP ▼
<input type="button" value="Execute Test"/>	

Routing Decisions

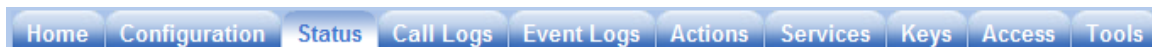
Route < sip:57003@avaya.com > to SIP Entity CS1000-R75 (10.7.7.60). Terminating Location is CS1K75-Location.

9.4. Avaya Aura® Session Border Controller Verification

This section contains verification steps that may be performed using the Avaya Aura® Session Border Controller. Section 9.4 of reference [AuraSBC-IP-Trunk] contains additional methods of verification.

9.4.1 Status Tab

A wealth of status information is available via the **Status** tab. This section provides several examples of status information that may be obtained. Select the **Status** tab as shown below.



There is a **SIP** heading on the left that can be expanded as shown in the abridged screen below.

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

In the example screen below, **active-calls** was selected from the left, revealing details about an active incoming call on the right. A scroll bar allows viewing of information about the active call. The following screen was captured when an incoming Verizon IP Toll Free call was active.

active-calls - currently active calls

View: Basic Search

session-id	from	to	state	previous-hop-ip
0x04C2D405F816E193	<sip:+19088485704@199.173.94.16:5060;user=phone>;tag=643550759.10.pdoecfnpbgnicpjbmadmobk	<sip:18668506850@1.1.1.2>	B2B_CONNECTED	172.30.205.55

Additional information about the call is available by continuing to scroll right, as shown below.

seconds Refresh

previous-hop-ip	next-hop-domain	duration (seconds)	inbound-connection	outbound-connection	header-value	subject-to-CAC	contact
172.30.205.55	avaya.com	128		65.206.67.93:4868-10.1.2.210:5060 TCP	true	<sip:+19088485704@172.30.205.55:5072;transport=udp>	
Taken May 25, 2011 8:46:39 AM XML							

The following screen shows an example screen output when **sdp-session-stats** was selected from the navigation menu on the left (not shown), and “Verbose” was selected for the **View**. This screen was captured when the same inbound Verizon IP Toll Free call was active. Observe that media is anchored at the SBC, and the codec in use is G.729.

sdp-session-stats - Active SDP session information

View: Verbose Search

seconds Refresh

session-id	stream	stream-type	anchor-setting	anchor-state	num-answers	associated-session	sdp-state	on-hold	codecs
0x04C2D405F816E193	1	audio	enabled	anchored	1	0x00	answered	false	g729, telephone-event, inforeq

The following screen shows an example screen output when **media → media-ports-sessions** was selected from the navigation menu on the left (not shown) and “Verbose” was selected for the **View**. This screen was captured when the same inbound Verizon IP Toll Free call was active.

media-ports-sessions - Addresses used by media stream sessions

View: Verbose Search

seconds Refresh

ip-address	port	session-id	call-leg	anchor-state
1.1.1.2	22124	0x04C2D405F816E193	1	anchored
65.206.67.93	21190	0x04C2D405F816E193	2	anchored

9.4.2 Call Logs

The **Call Logs** tab can provide useful diagnostic or troubleshooting information. The following screen shows a portion of the **Call Logs** tab selected after making an inbound Verizon IP Toll Free call.

Sessions

Search Type: All Sessions

View All Sessions

Search

Page 1 of 1 showing 30 items

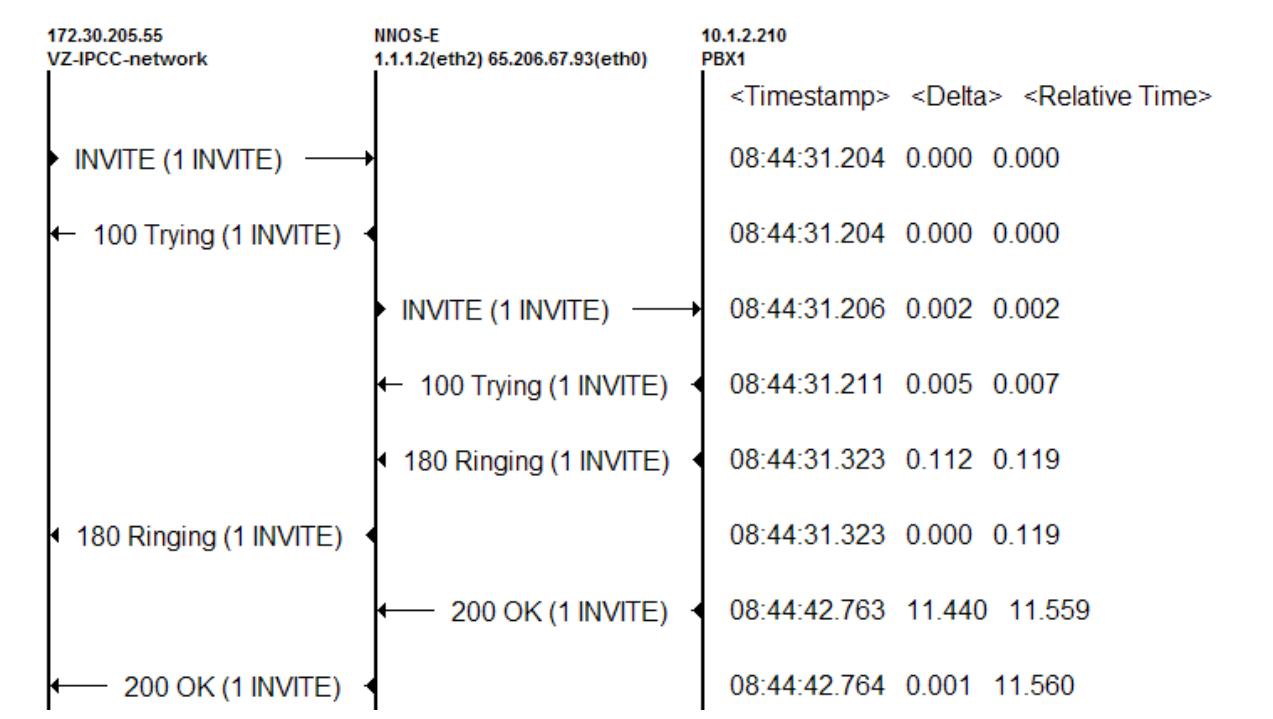
View: Us

Created		Method	Result	From			To			Call ID				Session ID
Detail	Call Diagram	Session Diagram		Call Record	Delete Media	Disconnect	Play	Call-out	Files	IM Archive	Statistics	Audit	Archive	
08:44:31.204 Wed 2011-05-25		INVITE		sip:+19088485704@199.173.94.16:5060			sip:18668506850@1.1.1.2			-1353623405- 884563291@63.78.210.214				0x04C2D405F81

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

Created	Method	Result	From	To	Call ID							
Detail	Call Diagram	Session Diagram	Call Record	Delete Media	Disconnect	Play	Call-out	Files	IM Archive	Statistics	Audit	Archive
08:44:31.204 Wed 2011-05-25	INVITE	<div>Show Event Sequence Diagram For Session Only</div>	sip:+19088485704@199.173.94.16:5060	sip:18668506850@1.1.1.2	-1353623405- 884563291@63.78.210.214							

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



Select the **Back** button (not shown). At the top right of the screen, the session may be saved as a text or XML file. If the session is saved as an XML file, using the **Save as XML** link, the xml file

can be provided to support personnel that can open the session on another Avaya Aura® SBC for analysis.

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

Session 0x04C2D405F816E193

[Add Session](#)

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server Release 7.5, Avaya Aura® Session Manager 6.1, and the Avaya Aura® Session Border Controller Release 6 can be configured to interoperate successfully with Verizon Business IP Contact Center service. This solution enables callers on the PSTN to dial Verizon toll-free numbers to reach the Avaya Communication Server 1000E via the SIP protocol.

11. Additional References

This section references documentation relevant to these Applications.

11.1. Avaya

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

- [1] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Issue 4, Feb 2011 available at <http://support.avaya.com/css/P8/documents/100082630>
- [2] *Installing and Configuring Avaya Aura™ Session Manager*, Doc ID 03-603473 Issue 2, November 2010 available at <http://support.avaya.com/css/P8/documents/100089152>
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, Issue 3.1, March 2011 available at <http://support.avaya.com/css/P8/documents/100089154>
- [4] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, June 2010 available at <http://support.avaya.com/css/P8/documents/100089681>

Avaya Communication Server 1000E

- 1) IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313
- 2) Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116
- 3) Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02
- 4) Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509
- 5) Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125

A variety of Avaya Application Notes on Verizon solutions tested via Avaya DevConnect are available at the following link:

<http://devconnect.avaya.com/dc/Public/WebListings/v2/CompanyWebListing.aspx?CompanyId=1236>

Reference [AuraSBC-IP-Trunk] below is a companion to these Application Notes. The document is among those available at the above link.

[AuraSBC-IP-Trunk] Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Aura® Session Border Controller 6.0 with Verizon Business IP Trunk SIP Trunk Service
<https://devconnect.avaya.com/public/download/dyn/CS1K75-VZIPT.pdf>

11.2. Verizon Business

Information in the following Verizon documents was also used for these Application Notes. Contact a Verizon Business Account Representative for additional information.

- [VZ-Test-Plan] Verizon Business IPCC Interoperability Lab Test Plan, Revision 1.7
- [VZ-Spec] Verizon Business IPCC Trunk Interface Network Interface Specification, Document Version 2.2.1.9

©2013 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.