



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise with Verizon Business IP Contact Center (IPCC) Services Suite – Issue 1.0

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 Session Border Controller for Enterprise. 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.

Avaya Communication Server 1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon Labs independent certification.

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	9
5.	Configure Avaya Communication Server 1000E	10
5.1.	Node and Key IP Addresses	11
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 Avaya Aura® Session Manager	18
5.4.	Routing of Dialed Numbers to Avaya Aura® Session Manager	24
5.4.1	Route List Block	24
5.4.2	NARS Access Code	26
5.4.3	Numbering Plan Area Codes	27
5.4.4	Other Special Numbers to Route to Session Manager	28
5.5.	Zones	29
5.6.	Codec Parameters, Including Ensuring Annexb=no for G.729	32
5.6.1	Media Gateway Configuration.....	32
5.6.2	Node Voice Gateway and Codec Configuration.....	33
5.7.	Enabling Plug-Ins for Call Transfer Scenarios	36
5.8.	Customer Information	37
5.8.1	Caller ID Related Configuration	37
5.9.	Example Communication Server 1000E Telephone Users.....	40
5.9.1	Example IP UNISim Phone DN 2000, Codec Considerations	40
5.9.2	Example SIP Phone DN 2900, Codec Considerations.....	41
5.9.3	Example Digital Phone DN 2222	42
5.10.	Save Configuration	43
6.	Configure Avaya Aura® Session Manager	44
6.1.	SIP Domain	46
6.2.	Locations	47
6.2.1	Location for Avaya Communication Server 1000E.....	47
6.2.2	Location for Avaya SBCE For Enterprise	48
6.3.	Configure Adaptations	50
6.3.1	Adaptation for Avaya Communication Server 1000E.....	50
6.3.2	Adaptation for Avaya SBC for Enterprise	52
6.4.	SIP Entities.....	53
6.4.1	SIP Entity for Avaya Communication Server 1000E	53
6.4.2	SIP Entity for Avaya SBC for Enterprise	54
6.5.	Entity Links.....	55

6.5.1	Entity Link to Avaya Communication Server 1000E	55
6.5.2	Entity Link to Avaya SBC for Enterprise	56
6.6.	Routing Policies	57
6.6.1	Routing Policy to Avaya Communication Server 1000E	57
6.6.2	Routing Policy to Avaya SBC for Enterprise	57
6.7.	Dial Patterns.....	58
6.7.1	Inbound Verizon Calls to CS1000E Users.....	58
7.	Configure Avaya Session Border Controller for Enterprise	60
7.1.	Access the Management Interface	60
7.2.	Device Specific Settings	62
7.2.1	Define Network Information.....	62
7.2.2	Signaling Interfaces	63
7.2.3	Media Interfaces.....	64
7.3.	Global Profiles	65
7.3.1	Routing Profiles	65
7.3.2	Topology Hiding Profile	66
7.3.3	Server Interworking	68
7.3.4	Signaling Manipulation.....	71
7.3.5	Server Configuration.....	72
7.3.6	Server Configuration for Verizon IPCC	74
7.4.	Domain Policies – Application Rule.....	76
7.5.	Domain Policies – Media Rules.....	77
7.6.	Domain Policies – Signaling Rules.....	79
7.7.	Domain Policies – End Point Policy Groups	80
7.8.	Device Specific Settings – End Point Flows.....	82
8.	Verizon Business IPCC Service Offer Configuration	85
8.1.	Fully Qualified Domain Name (FQDN)s	85
8.2.	DID Numbers Assigned by Verizon	85
9.	Verification Steps.....	86
9.1.	Avaya Communication Server 1000E Verifications.....	86
9.1.1	IP Network Maintenance and Reports Commands	86
9.1.2	System Maintenance Commands.....	91
9.2.	Wireshark Verifications	92
9.2.1	Example Inbound Call	92
9.3.	System Manager and Session Manager Verification	95
9.3.1	Verify SIP Entity Link Status	95
9.4.	Avaya Session Border Controller for Enterprise Verification.....	97
9.4.1	Welcome Screen	97
9.4.2	Alarms.....	97
9.4.3	Incidents.....	98
9.4.4	Tracing	99
10.	Conclusion	100
11.	Additional References.....	101
11.1.	Avaya	101
	Appendix 1: Sigma Script.....	102

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E (CS1000E) Release 7.5, Avaya Aura® Session Manager Release 6.1, and the Avaya Session Border Controller for Enterprise (ASBCE). 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.

Avaya CS1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon Labs independent certification.

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 Session Border Controller for Enterprise (ASBCE) is used as an edge device between the Avaya Customer Premise Equipment(CPE) and Verizon Business. The ASBCE 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 SIP trunk interoperability testing included the following:

- 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, and Avaya digital 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.
- 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 calls with long holding times and call stability
- Long duration calls.
- 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. The following observations were noted:

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.

2.3. Support

2.3.1 Avaya

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

2.3.2 Verizon

For technical support on Verizon Business IPCC service offer, visit 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 Session Border Controller for Enterprise (ASBCE) provides topology hiding and SIP header manipulation. The ASBCE receives traffic from Verizon Business IPCC Services on port 5060 and sends traffic to the Verizon Business IPCC Services using destination port 5071, using the UDP protocol.

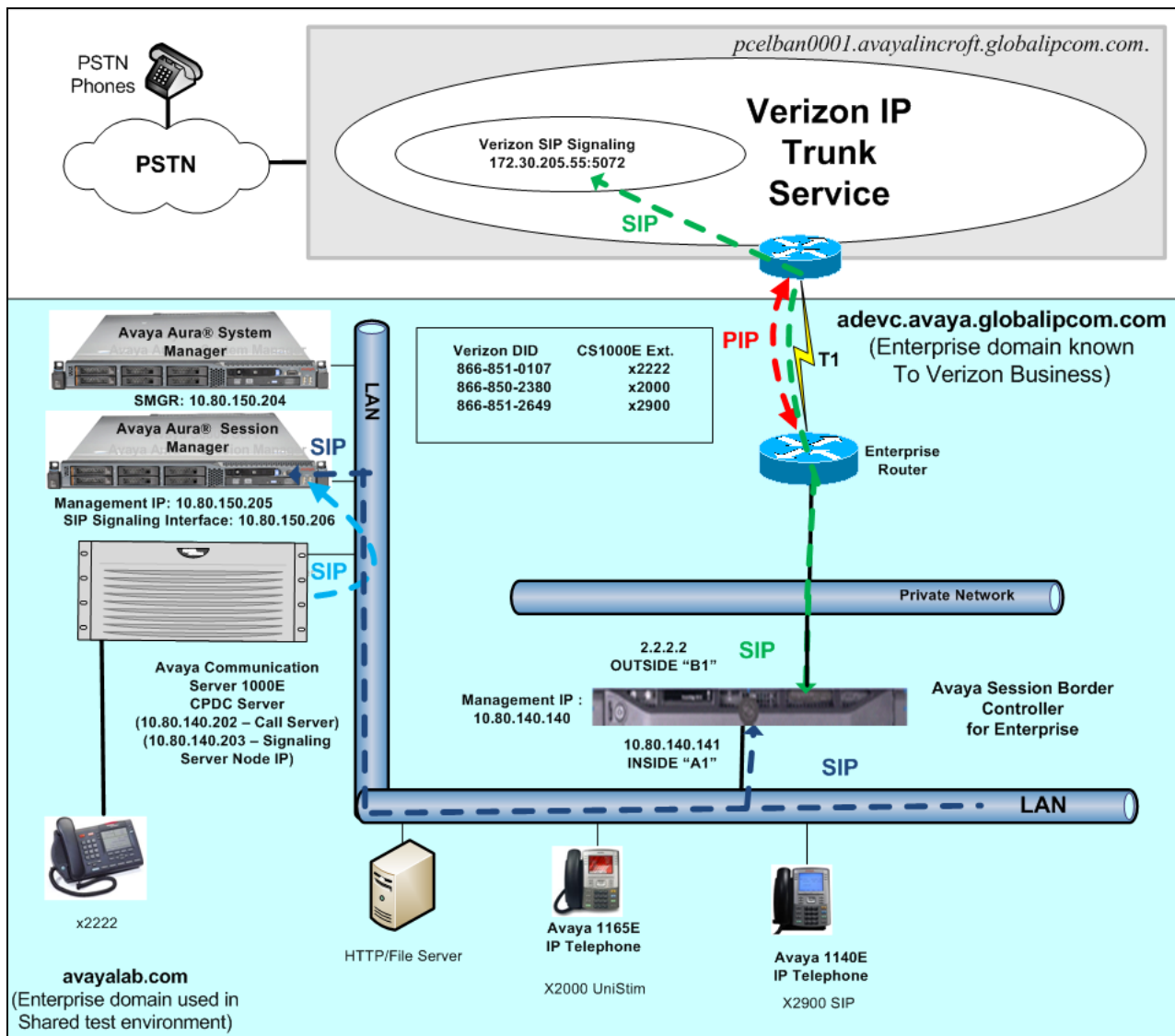


Figure 1: Avaya Interoperability Test Lab Configuration

The Avaya CPE was known to Verizon Business as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya environment utilizing Avaya Aura® 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 “avayalab.com” at the enterprise. Session Manager is used to adapt the “avayalab.com” domain to the domains known to Verizon, defined in **Section 8.1**. 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 Provided Toll-Free	Avaya CS1000E Destination	Notes
866-851-0107	x2222	Avaya M3904 Digital Telephone
866-850-2380	x2000	Avaya 1165E IP Deskphone (UNISim)
866-851-2649	x2900	Avaya 1140E IP Deskphone (SIP)

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

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)
 - *adevc.avaya.globalipcom.com*
- Avaya Session Border Controller for Enterprise(ASBCE) 4.0.5Q09
- Avaya Communication Server 1000E Release 7.5
- Avaya Aura® System Manager Release 6.1
- Avaya Aura® Session Manager Release 6.1
- Avaya 1100-Series IP Deskphones using UNISim software
- Avaya 1140E IP Deskphones using SIP software, registered to the CS1000E
- Avaya M3900-Series Digital phones

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Communication Server 1000E running on CP+DC 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 Aura® System Manager running on HP Common Server	Release 6.1.0 (Build Number 6.1.0.0.7345 Patch 6.1.5.502)
Avaya Aura® Session Manager running on HP Common Server	Release 6.1 (Load 6.1.5.0.615006)
Avaya Session Border Controller for Enterprise running on Dell R210 V2 server	4.0.5Q09
Avaya 1100-Series IP Deskphones (UNISim)	FW 0626C8A
Avaya 1140E IP Deskphones (SIP)	SIP 04.03.09.00

Table 2: Equipment and Software Used in the Sample Configuration

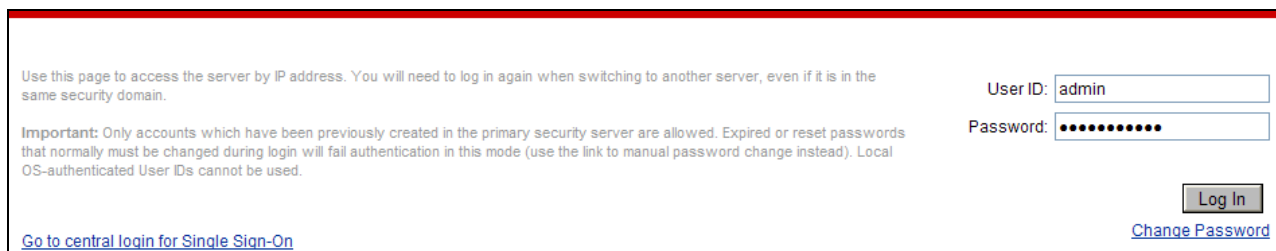
5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to Session Manager over a SIP 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+DC 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.

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, UNISim, and SIP telephones.

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 10.80.140.202. The following screen shows an abridged log-in screen. Log in with appropriate credentials.



The screenshot shows a web-based login interface. On the left, there is instructional text: "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." Below this is an "Important" note: "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." At the bottom left is a link: "Go to central login for Single Sign-On". On the right, there are input fields for "User ID:" (containing "admin") and "Password:" (masked with dots). Below the password field is a "Log In" button. At the bottom right is a link: "Change Password".

Alternatively, if 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 Element Manager may be accessed via System Manager. In this case, access the web based GUI of System Manager by using the URL "**http://<ip-address>/SMGR**", where <ip-address> is the IP address of System Manager. Log in with appropriate credentials. The System Manager Home Page will be displayed. Under the **Services** category on the right side of the page, click the **UCM Services** link (not shown). For more information on configuring System Manager as Primary Security Server, see **Reference [2]**.

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 vz_cs1k”.

Avaya Unified Communications Management
[Help](#) | [Logout](#)

Host Name: 10.80.140.202 **Software Version:** 02.20.0023.00(5197) **User Name** admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

<input type="checkbox"/>	Element Name	Element Type ▲	Release	Address	Description ▲
1 <input type="checkbox"/>	EM on vz_cs1k	CS1000	7.5	10.80.141.202	New element.
2 <input type="checkbox"/>	vz_cs1k.avayalab.com (primary)	Linux Base	7.5	10.80.140.202	Base OS element.
3 <input type="checkbox"/>	10.80.141.201	Media Gateway Controller	7.5	10.80.141.201	New element.
4 <input type="checkbox"/>	NRSRM on vz_cs1k	Network Routing Service	7.5	10.80.141.202	New element.

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 “1004”** was used.

AVAYA
CS1000 Element Manager

Managing: 10.80.141.202 **Username:** admin2
 System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

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

<input type="checkbox"/>	Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/>	1004	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.203		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 **Node IPV4 address** under **Telephony LAN (TLAN)**. In the sample screen below, the **Node IPV4 address** is “10.80.140.203”. This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E.

CS1000 Element Manager

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1004 - SIP Line, LTPS, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: *

Embedded LAN (ELAN)

Telephony LAN (TLAN)

Gateway IP address: *

Node IPv4 address: *

Subnet mask: *

Subnet mask: *

Node IPv6 address:

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

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"/> vz-cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.80.141.202	10.80.140.202	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**. Select the media gateway listed, here **'004 00'**. Click **Next** (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a tree view with 'System' expanded and 'Media Gateways' selected. The main panel displays the 'Media Gateways' configuration page. At the top, it shows 'Managing: 10.80.141.202' and 'Username: admin'. Below this, there are buttons for 'Add...', 'Digital Trunking...', 'Reboot', 'Delete', 'Virtual Terminal', and 'More Actions'. A table lists the media gateways:

	IPMG	IP Address	Zone	Type
○	004 00	10.80.141.201	1	MGS

The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone to the PSTN via Verizon IPCC service, the IP Address in the SDP in the INVITE message will be **"10.80.140.204"** in the sample configuration.

The screenshot shows the 'IPMG 4 0 Media Gateway Survivable(MGS) Configuration' page. The left sidebar is the same as the previous screenshot. The main panel displays the configuration for the selected media gateway. It includes sections for 'Media Gateway (MGS)' and 'DSP Daughterboard'. The 'Media Gateway (MGS)' section contains the following fields:

- Hostname: MGS
- Embedded LAN (ELAN) IP address: 10.80.141.201
- Embedded LAN (ELAN) gateway IP address: 10.80.141.1
- Embedded LAN (ELAN) subnet mask: 255.255.255.0
- Telephony LAN (TLAN) IP address: 10.80.140.201
- Telephony LAN (TLAN) gateway IP address: 10.80.140.1
- Telephony LAN (TLAN) subnet mask: 255.255.255.0

The 'DSP Daughterboard' section contains the following fields:

- Type of the DSP daughterboard: DB128
- Telephony LAN (TLAN) IP address: 10.80.140.204 (highlighted with a red box)
- Telephony LAN (TLAN) gateway IP address: 10.80.140.1

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 15 associated with the Signaling Server.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left navigation pane shows a tree structure with 'Routes and Trunks' expanded, and 'D-Channels' selected. The main content area is titled 'D-Channels' and includes a 'Maintenance' section with links to 'D-Channel Diagnostics (LD 96)', 'Network and Peripheral Equipment (LD 32, Virtual D-Channels)', 'MSDL Diagnostics (LD 96)', 'TMDI Diagnostics (LD 96)', and 'D-Channel Expansion Diagnostics (LD 48)'. Below this is a 'Configuration' section with a form to 'Choose a D-Channel Number' (set to 0) and 'type' (set to DCH), with a 'to Add' button. At the bottom, a table lists the configuration for Channel 15: Type: DCH, Card Type: DCIP, and Description: VtrkNode1004, with an 'Edit' button.

AVAYA CS1000 Element Manager			
Managing: 10.80.141.202 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: 0 and type: DCH to Add			
-	Channel: 15	Type: DCH	Card Type: DCIP Description: VtrkNode1004 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 example screen that follows, it can be observed that **Route 15** has 32 trunks in the sample configuration.

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

D-Channels

Managing: 10.80.141.202 Username: admin2
Routes and Trunks » Routes and Trunks

Routes and Trunks

Customer: 0

Total routes: 2

Total trunks: 64

Add route

Route: 15

Type: TIE

Description: VTKNODE1004SIP

Edit

Add trunk

+ Trunk: 1 - 32

Total trunks: 32

+ Route: 17

Type: TIE

Description: VTK1004SIPLINE

Edit

Add trunk

MEO; Reviewed:
SPOC 10/18/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

15 of 103
VZIPCC1K75ASBCE

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. 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 15 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :

Customer number (CUST) :

Route number (ROUT) :

Designator field for trunk (DES) :

Trunk type (TKTP) :

Incoming and outgoing trunk (ICOG) :

Access code for the trunk route (ACOD) :

Trunk type M911P (M911P) :

The route is for a virtual trunk route (VTRK) :

- Zone for codec selection and bandwidth
management (ZONE) :

- Node ID of signaling server of this route
(NODE) :

- Protocol ID for the route (PCID) :

RDB

00

15

VTKNODE1004SIF

TIE

Incoming and Outgoing (IAO)

7900015

☐

☒

00099

1004

SIP (SIP)

*

(0 - 8000)

(0 - 9999)

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) :	Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) :	15 (0 - 254)
- Interface type for route (IFC) :	Meridian M1 (SL1)
- Private network identifier (PNI) :	00001 (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>
- Network call redirection (NCRD) :	<input checked="" type="checkbox"/>
- Trunk route optimization (TRO) :	<input type="checkbox"/>
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :	<input type="checkbox"/>
- Channel type (CHTY) :	B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) :	Unknown Call type (UKWN)
- Insert ESN access code (INAC) :	<input checked="" type="checkbox"/>
- Integrated service access route (ISAR) :	<input type="checkbox"/>
- Display of access prefix on CLID (DAPC) :	<input type="checkbox"/>
- Mobile extension route (MBXR) :	<input type="checkbox"/>
- Mobile extension outgoing type (MBXOT) :	National number (NPA)
- Mobile extension timer (MBXT) :	0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) :	Unknown (UKWN)

5.3. SIP Trunk to Avaya Aura® Session Manager

Expand **System** → **IP Network** → **Nodes: Servers, Media Cards**. Click “1004” 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)** link to view or edit the SIP Gateway configuration.

The screenshot shows the configuration page for Node 1004. At the top, it displays the management IP (10.80.141.202) and username (admin2). The breadcrumb trail is System » IP Network » IP Telephony Nodes » Node Details. The title is 'Node Details (ID: 1004 - SIP Line, LTPS, Gateway (SIPGw))'. Below this, there are two 'Subnet mask' fields, both containing '255.255.255.0' and marked as required with an asterisk. A 'Node IPv6 address' field is also present. The main content area is divided into two columns: 'IP Telephony Node Properties' and 'Applications (click to edit configuration)'. The first column lists links for Voice Gateway (VGW) and Codecs, Quality of Service (QoS), LAN, SNTP, Numbering Zones, and MCDN Alternative Routing Treatment (MALT) Causes. The second column lists links for SIP Line, Terminal Proxy Server (TPS), Gateway (SIPGw), Personal Directories (PD), Presence Publisher, and IP Media Services. A vertical scrollbar is on the right. At the bottom, there is a note '* Required Value.' and 'Save' and 'Cancel' buttons.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1004 - SIP Line, LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.0 * Subnet mask: 255.255.255.0 *

Node IPv6 address:

IP Telephony Node Properties

- [Voice Gateway \(VGW\) and Codecs](#)
- [Quality of Service \(QoS\)](#)
- [LAN](#)
- [SNTP](#)
- [Numbering Zones](#)
- [MCDN Alternative Routing Treatment \(MALT\) Causes](#)

Applications (click to edit configuration)

- [SIP Line](#)
- [Terminal Proxy Server \(TPS\)](#)
- [Gateway \(SIPGw\)](#)
- [Personal Directories \(PD\)](#)
- [Presence Publisher](#)
- [IP Media Services](#)

* Required Value. Save Cancel

On the **Node ID: 1004 - 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, “**avayalab.com**” was used in the shared Avaya Solution and Interoperability Test lab environment. Note: The SIP domain name for the enterprise known to Verizon is “*adevc.avaya.globalipcom.com*”, and the SIP domain will be adapted by the ASBCE for calls to and from the Avaya CS1000E.
- **Local SIP port:** Enter “**5060**”
- **Gateway endpoint name:** Enter a descriptive name
- **Application node ID:** Enter “<Node id>”. In the sample configuration, Node “**1004**” was used matching the node shown in **Section 5.1**.

The values defined for the sample configuration are shown below.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1004 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: avayalab.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: node1004 *

Gateway password: *

Application node ID: 1004 * (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: Add

Monitor addresses:

Remove

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, “10.80.150.206” was used.
- **Port:** Enter “5060”.
- **Transport protocol:** Select “TCP”.

The values defined for the sample configuration are shown below.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1004 - Virtual Trunk Gateway Configuration Details

[General](#) | [SIP Gateway Settings](#) | [SIP Gateway Services](#)

Proxy Server Route 1:

Primary TLAN IP address:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: (1 - 65535)

Transport protocol:

Options: ☐ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: (1 - 65535)

Transport protocol:

Scroll down and repeat these steps for the **Proxy Server Route 2** (not shown).

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 calls that may ultimately be routed to the Verizon IPCC service. The 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: 1004 - Virtual Trunk Gateway Configuration Details	
General <u>SIP Gateway Settings</u> SIP Gateway Services	
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"/>
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: 10.80.141.202 Username: admin2	
System » IP Network » <u>IP Telephony Nodes</u> » Node Saved	
Node Saved	
Node ID: 1004 has been saved on the call server.	
The new configuration must also be transferred to associated servers and media cards.	
<input type="button" value="Transfer Now..."/>	You will be given an option to select individual servers, or transfer to all.
<input type="button" value="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.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1004>)

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"/>	vz-cs1k	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.

Select the check box associated with the appropriate Hostname and click **Start Sync**.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1004>)

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"/>	vz-cs1k	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 screen will automatically refresh until the synchronization is finished. The **Synchronization Status** field will update from **Sync required** (as shown in the previous screen) to **Synchronized** (as shown below). After synchronization completes, select the check box associated with the appropriate Hostname and click **Restart Applications**.

Managing: 10.80.141.202 Username: admin2
 System » IP Network » [IP Telephony Nodes](#) » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1004>)

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"/>	vz-cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

* 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.

5.4. Routing of Dialed Numbers to Avaya Aura® Session Manager

This section provides the configuration of the 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 IPCC service. The routing defined in this section is simply an example and not intended to be prescriptive. The example will focus on the configuration enabling a CS1000E telephone user to dial 9-1-303-538-7022 to reach a PSTN telephone using the Verizon IPCC service. Other routing policies may be appropriate for different customer networks.

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.

Managing: **10.80.141.202** Username: admin2
Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - **Route List Block (RLB)**
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)

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 to **Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, route list block index “15” is used.

Managing: **10.80.141.202** Username: admin2
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index (0 - 1999)

⌘ **Route List Block Index -- 15**

If adding the route list index as new, 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**>” defined in **Section 5.2.2** in the **Route Number** field. In the sample configuration route number “**15**” 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 - 1)
Options	
Local Termination entry:	<input type="checkbox"/>
Route Number:	15 ▼
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: ☒

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: 6 (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

- Maximum number of Steering Codes: 2000 (1 - 64000)

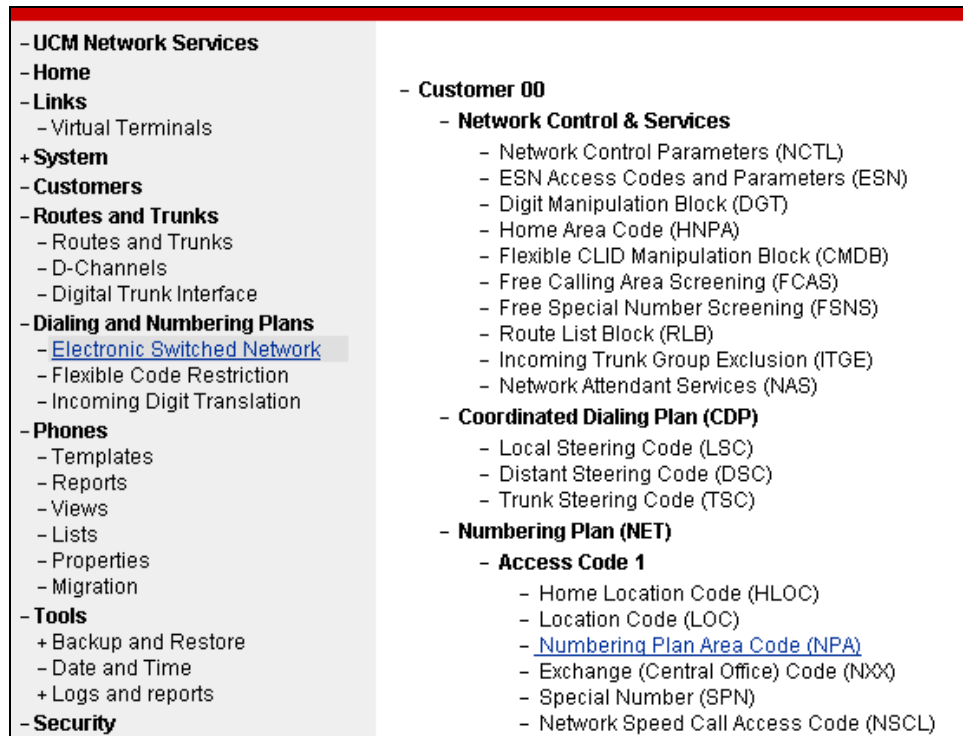
- Number of digits in CDP DN (DSC + DN or LSC + DN): 4 (3 - 10)

Routing Controls: ☐

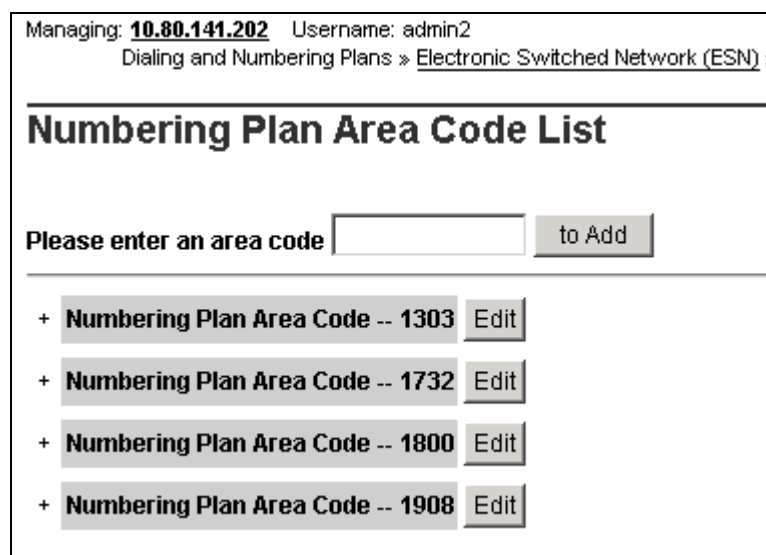
Check for Trunk Group Access Restrictions: ☐

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 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 “1303” are configured.



In the screen below, the entry for “**1303**” is displayed. In the Route List Index, “**15**” is selected to use the route list associated with the SIP Trunk to Session Manager defined in **Section 5.4.1**. 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:

5.4.4 Other Special Numbers to Route to Session Manager

In the testing associated with these Application Notes, non-emergency service numbers such as x11, 1x11, international calls, and operator assisted calls were also routed to Session Manager and ultimately to the Verizon IPCC service. Although not intended to be prescriptive, one approach to such routing is summarized in this section.

Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.4.3**).

Add a new number by entering it in the **Please enter a Special Number** box and click to **Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as “0”, “011”, and non-emergency x11 calls are listed. In each case, **Route list index “15”** has been selected in the same manner as shown for the NPAs in the prior section. For special numbers, the **Flexible length** field can also be configured as appropriate for the number. For example, for 511, the **Flexible length** field can be set to “3”.

Managing: **10.80.141.202** Username: admin2
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) »

Special Number List

Please enter a Special Number

+ **Special Number -- 0**
+ **Special Number -- 011**
+ **Special Number -- 0144**
+ **Special Number -- 1411**
+ **Special Number -- 311**
+ **Special Number -- 411**
+ **Special Number -- 511**
+ **Special Number -- 711**

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: **10.80.141.202** Username: admin2
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 lab 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 “99”.

Managing: **10.80.141.202** Username: admin
System » IP Network » Zones » Bandwidth Zones

Bandwidth Zones

Add... Edit... Import... Export Maintenance... Delete Refresh

	Zone ▲	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	<input type="radio"/> 1	1000000	BQ	1000000	BQ	SHARED	MO	IPSETS
2	<input type="radio"/> 99	1000000	BB	1000000	BB	SHARED	VTRK	VTRUNK

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

Managing: **10.80.141.202** Username: admin2
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 99 » Edit Bandwidth Zone

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 99 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 IPCC service.

Managing: **10.80.141.202** Username: admin2
 System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 99 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	99 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB) ▼
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	VTRK (VTRK) ▼
Description (ZDES):	VTRUNK

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 determines whether 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 a Media Gateway (MGS). On the left is a navigation tree under 'UCM Network Services' with categories like Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, and Phones. The 'Media Gateways' link under 'System' is selected. The main panel is titled '- Media Gateway (MGS)' and contains several configuration fields:

- Hostname:** MGS
- Embedded LAN (ELAN) IP address:** 10.80.141.201
- Embedded LAN (ELAN) gateway IP address:** 10.80.141.1
- Embedded LAN (ELAN) subnet mask:** 255.255.255.0
- Telephony LAN (TLAN) IP address:** 10.80.140.201
- Telephony LAN (TLAN) gateway IP address:** 10.80.140.1
- Telephony LAN (TLAN) subnet mask:** 255.255.255.0

Below these is the '- DSP Daughterboard' section:

- Type of the DSP daughterboard:** DB128
- Telephony LAN (TLAN) IP address:** 10.80.140.204
- Telephony LAN (TLAN) gateway IP address:** 10.80.140.1
- Telephony LAN (TLAN) IPv6 address:** (empty field)
- Telephony LAN (TLAN) subnet mask:** 255.255.255.0
- Hostname:** DB1

At the bottom, there are expandable sections: 'VGW and IP phone codec profile' (expanded), '+ QoS', '+ Media Based CLID', and '- Call Server LAN'.

Expand **VGW and IP phone codec profile**. To use G.729A with Verizon IPCC service, 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** of “20” can be used with Verizon IPCC service for both G.729A and G.711. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. The following screen shows the parameters used.

The screenshot displays two codec configuration sections. The top section is for **Codec G711**, which has its **Select** checkbox checked. Below it, the **Voice payload size** is set to 20 (ms/frame), **Voice playout (jitter buffer) nominal delay** is 40, and **Voice playout (jitter buffer) maximum delay** is 80. A red warning message states: "Modifications may cause changes to dependent settings". The **VAD** checkbox is unchecked. The bottom section is for **Codec G729A**, which also has its **Select** checkbox checked (circled in orange). Its **Voice payload size** is 20 (ms/frame), **Voice playout (jitter buffer) nominal delay** is 40, and **Voice playout (jitter buffer) maximum delay** is 80. A red warning message states: "Modifications may cause changes to dependent settings". The **VAD** checkbox is unchecked (circled in orange).

5.6.2 Node Voice Gateway and Codec Configuration

Expand **System → IP Network** and select **Node, Server, Media Cards**. Select the appropriate **Node Id** which is “1004” for sample configuration as shown below.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

Buttons: Add... Import... Export... Delete Print | Refresh

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1004	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.203		Synchronized

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

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.

Managing: 10.80.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1004 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

General

Echo cancellation: ☒ Use canceller, with tail delay: 128
☒ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection
☐ Low latency mode
☒ Remove DTMF delay (squelch DTMF from TDM to IP)
☒ Modem/Fax pass-through
☒ V.21 Fax tone detection
☐ 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.

Voice Codecs

Codec G711: ☒ Enabled (required)

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)

For the **Codec G.729**, ensure that the **Enabled** box is checked, and the **Voice Activity Detection (VAD)** box is un-checked, as shown below. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order.

Managing: 10.60.141.202 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1004 - Voice Gateway (VGW) and Codecs

General | **Voice Codes** | 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)

Note: click **Save** (not shown) to save changes and follow the procedure described in **Section 5.3** to transfer and synchronize changes between Node and associated Signaling Server.

5.7. Enabling Plug-Ins for Call Transfer Scenarios

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 IPCC 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.

<div>  CS1000 Element Manager </div>				
<ul style="list-style-type: none"> - System <ul style="list-style-type: none"> + Alarms - Maintenance + Core Equipment <ul style="list-style-type: none"> - Peripheral Equipment - IP Network <ul style="list-style-type: none"> - Nodes: Servers, Media Cards - Maintenance and Reports - Media Gateways - Zones - Host and Route Tables - Network Address Translation (N - QoS Thresholds - Personal Directories - Unicode Name Directory + Interfaces <ul style="list-style-type: none"> - Engineered Values + Emergency Services - Software <ul style="list-style-type: none"> - Call Server PEPs - Loadware PEPs - File Upload - IP Phone Firmware - Voice Gateway Media Card - Media Cards PEPs - Plug-ins - Customers 	<input type="checkbox"/> Enable <input type="checkbox"/> Disable			
	<input type="checkbox"/>	Number	Description	MPLR Number Status
	86 <input type="checkbox"/>	223	PI:HICOM REJECTS QSIG CCBS REQUEST WITH NO CALLING NUMBER	MPLR12290 Disabled
	87 <input type="checkbox"/>	224	PI:No busy treatment on external transfer through application if OUT_T306 > 0	MPLR24676 Disabled
	88 <input type="checkbox"/>	225	PI:PKG 179, Taurus, electronic look, Mail and CallPilot softkeys	MPLR22389 Disabled
	89 <input type="checkbox"/>	226	PI:ACLD should display more than 10 digits	MPLR15783 Disabled
	90 <input type="checkbox"/>	228	PI: TTY 0 on CPU card (8/1/N) causes cursor to go up on VDU	MPLR07613 Disabled
	91 <input type="checkbox"/>	230	PI: Unplugged telset disables after midnight routines.	MPLR11700 Disabled
	92 <input type="checkbox"/>	231	PI: BRI 64K data not possible over DTI2. With mix of spans (both DTI and DTI2) THIS is not supported.	MPLR10878 Disabled
	93 <input type="checkbox"/>	232	PI: QSIG GF: No diverting and originally called number in DLI2 APDU on calls from MCDN TRO-BA.	MPLR24273 Disabled
	94 <input type="checkbox"/>	233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506 Disabled
	95 <input type="checkbox"/>	235	Restrict Hands-free functionality for all IP set types.	MPLR29100 Disabled
	96 <input type="checkbox"/>	500	NO DESCRIPTION	MPLR21979 Disabled
	97 <input type="checkbox"/>	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070 Enabled
	98 <input type="checkbox"/>	504	PRI232 BUG253 from PI 10 Delay in Response at Called IFC	MPLR24744 Disabled
	99 <input type="checkbox"/>	505	UM2K integration problem with S100 Interface	MPLR30004 Disabled

The same procedure may be used to enable Plug-in 201 if desired (not shown). Plug-in 201 will allow a CS1000E user to make a call to the PSTN using the Verizon IPCC service, and then subsequently perform an attended transfer of the call to another PSTN destination via the Verizon IPCC service.

5.8. Customer Information

This section documents basic Customer 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: **10.80.141.202** Username: admin2
Customers » Customer 00 » Customer Details » ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code: (0 - 9999)
Code for processing the called number

National access code:

International access code:

Options: ☒ Transfer on ringing of supervised external trunks
☒ Connection of supervised external trunks
Network option: ☒ Coordinated dialing plan routing
Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-DID users: ☐ Coordinated dialing plan
☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

Size: (0 - 4000)

Country code: (0 - 9999)
Code displayed as part of calling number

[Calling Line Identification Entries](#)

5.8.1 Caller ID Related Configuration

Although not intended to be prescriptive, in the sample configuration the CS1000E would send the user's four-digit directory number in SIP headers such as the From and PAI headers. Session Manager would adapt the user's directory number to an appropriate Verizon IPCC toll-free number before passing the message to the ASBCE towards Verizon.

Scroll down from the screen shown in **Section 5.8**, click the **Calling Line Identification Entries** link (not shown), and search for the **Calling Line Identification Entries** by **Entry ID**. As shown below, the **Use DN as DID** parameter was set to “NO” and an entry ID was created for every DID used in the sample configuration. The local DID will be replaced with the **Local Code** and the **Entry ID** will be configured on the individual extensions in **Section 5.9**.

Managing: **10.80.141.202** Username: admin
 Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries

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	Emergency Local Code
1 <input type="checkbox"/>	0		8668502380			NO	
2 <input type="checkbox"/>	1		8668510107			NO	
3 <input type="checkbox"/>	2		8668512649			NO	

Click on **Entry Id “0”** to view or change further details as shown below.

Managing: **10.80.141.202** Username: admin
 Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 0

Edit Calling Line Identification 0

General Properties

National Code: (0 - 999999)
Code for national home number

Local Code: (1-12 digits)
Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID :

Emergency Services Access

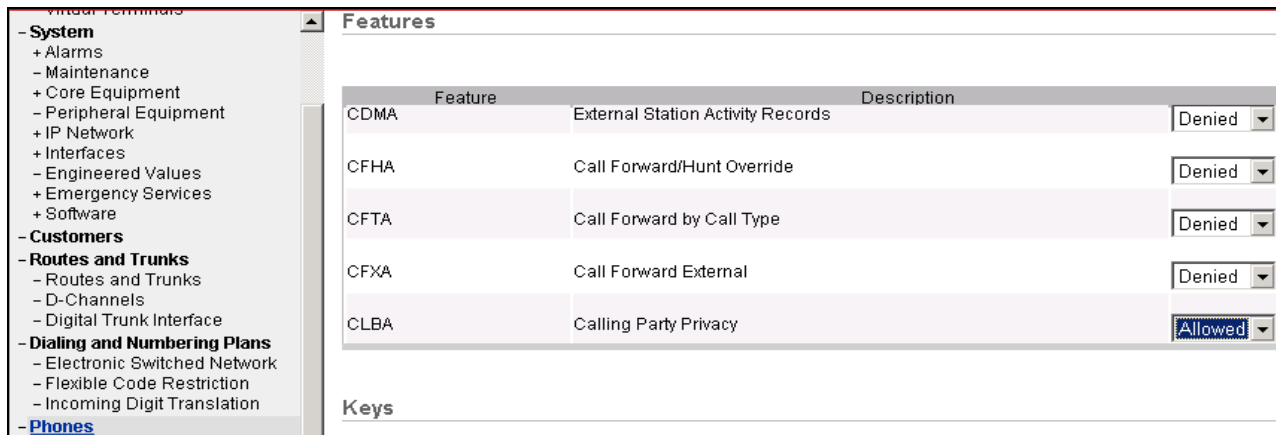
Emergency Local Code: (1-12 digits)
Code for home local number during Emergency calls

Emergency Options: ☐ Home national number for emergency services access calls
☒ Append the originating directory number for emergency services access calls

5.8.1.1 Requesting Privacy

One means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IPCC service is to configure each phone with the appropriate option. Expand **Phones** on the left navigation panel and enter **Search Criteria** to display a list of stations. Select a specific station for editing (not shown).

In the **Features** table, scroll to **CLBA Calling Party Privacy** feature and select “**Allowed**” as shown below.



The screenshot shows the 'Features' table in the Element Manager. The left navigation pane is expanded to 'Phones'. The 'Features' table has columns for 'Feature', 'Description', and a status dropdown. The 'CLBA' feature, described as 'Calling Party Privacy', is highlighted with its status set to 'Allowed'. Other features like 'CDMA External Station Activity Records', 'CFHA Call Forward/Hunt Override', 'CFTA Call Forward by Call Type', and 'CFXA Call Forward External' are listed above it with status 'Denied'. A 'Keys' section is visible below the table.

Feature	Description	Status
CDMA	External Station Activity Records	Denied
CFHA	Call Forward/Hunt Override	Denied
CFTA	Call Forward by Call Type	Denied
CFXA	Call Forward External	Denied
CLBA	Calling Party Privacy	Allowed

Another means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IPCC service is to set **DDGA Present/Restrict Calling Number** feature to “**Denied**” via the Phone **Features** table in Element Manager (not shown).

5.9. Example Communication Server 1000E Telephone Users


This section is not intended to be prescriptive, but simply illustrates a sampling of the telephone users in the sample configuration.

5.9.1 Example IP UNISTim Phone DN 2000, Codec Considerations

The following screen shows basic information for an IP UNISTim phone in the configuration. The telephone is configured as Directory Number 2000. Note that the telephone is in Zone 1. A call between this telephone and another telephone in Zone 1 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 IPCC service, the call would use a “best bandwidth” strategy, and the call would use G.729A.

Managing: EM on vz-cs1k(10.80.141.202)
[Phones»Phone Details](#)

Phone Details

 System: EM on vz-cs1k
Phone Type: 1165
Sync Status: TRN

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

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

Zone: *

Scrolling down to the **Keys** section. The **First** and **Last Name**, the **Directory Number** as well as the **Calling Lined ID (CLID)** is configured. The **CLID** entry is defined in **Section 5.8.1**.

AVAYA CS1000 Element Manager

Help | Log Out

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
 - 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

ADAY Alternate Redirection by Day Option

ADV Data Port Verification Denied

Keys

Key No	Key Type	Key Value
0	SCR - Single Call Ringing	<p>Directory Number: 2000</p> <p><input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)</p> <p>First Name: 1165 Last Name: UNISTIM Display Format: First, Last Language: Roman</p> <p>CLID Entry (Numeric or D): 0</p> <p>ANIE Entry:</p>

5.9.2 Example SIP Phone DN 2900, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 2900. Note that the telephone is in Zone 1 and is associated with Node 1004 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 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 IPCC service, the call would use a “best bandwidth” strategy, and the call would use G.729A.

Virtual Terminals

- 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
 - Date and Time
 - + Logs and reports

System: EM on vz-cs1k

Phone Type: UEXT-SIPL

Sync Status: TRN

General Properties | Features | Keys | User Fields

General Properties

Customer Number: 0 *

Terminal Number: 252 0 09 00

Designation: SIPN * (1-6 characters)

Zone: 1 *

SIP User Name: 2900 * (1-16 characters)

Node Id: 1004 *


5.9.3 Example Digital Phone DN 2222

The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 2222.

The screenshot shows a web-based configuration interface. On the left is a navigation tree with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Phones' category is selected. The main content area is titled 'Phone Details' and shows information for a phone managed by 'EM on vz-cs1k(10.80.141.202)'. It includes a phone icon, system details (System: EM on vz-cs1k, Phone Type: M3904, Sync Status: TRN), and 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 (DIG).

Managing: **EM on vz-cs1k(10.80.141.202)**
[Phones»Phone Details](#)

Phone Details

 System: EM on vz-cs1k
Phone Type: M3904
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 1 (Section 5.8.1)**. 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 configured with 'SCR - Single Call Ringing' as the key type. The key value section includes a 'Directory Number' field set to 2222, a checked 'Multiple Appearance Redirection Prime(MARP)' checkbox, and a table for appearance information with fields for First Name, Last Name, Display Format, and Language. Below this are fields for 'CLID Entry (Numeric or D)' set to 1 and an empty 'ANIE Entry' field. At the bottom, there is a dropdown menu for 'CWT - Call Waiting'.

Keys

Key No.	Key Type	Key Value								
0	SCR - Single Call Ringing	<p>Directory Number: <input type="text" value="2222"/></p> <p><input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP)</p> <table border="1"><tr><td>First Name</td><td>Last Name</td><td>Display Format</td><td>Language</td></tr><tr><td><input type="text" value="Digital"/></td><td><input type="text" value="-3904"/></td><td><input type="text" value="First, Last"/></td><td><input type="text" value="Roman"/></td></tr></table> <p>CLID Entry (Numeric or D): <input type="text" value="1"/></p> <p>ANIE Entry: <input type="text"/></p> <p><input type="text" value="CWT - Call Waiting"/></p>	First Name	Last Name	Display Format	Language	<input type="text" value="Digital"/>	<input type="text" value="-3904"/>	<input type="text" value="First, Last"/>	<input type="text" value="Roman"/>
First Name	Last Name	Display Format	Language							
<input type="text" value="Digital"/>	<input type="text" value="-3904"/>	<input type="text" value="First, Last"/>	<input type="text" value="Roman"/>							

5.10. Save Configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** for **Action** and click **Submit** to save configuration changes as shown below.

The screenshot shows a web interface for managing a system. On the left is a navigation menu with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Tools' category is expanded, showing 'Backup and Restore', 'Call Server' (highlighted), and 'Personal Directories'. The main content area is titled 'Call Server Backup'. At the top of this area, it says 'Managing: 10.80.141.202 Username: admin2' and 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. Below this is a form with an 'Action' dropdown menu set to 'Backup', and 'Submit' and 'Cancel' buttons.

Managing: **10.80.141.202** Username: admin2
Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup

Call Server Backup

Action

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
Starting database backup
to local Removable Media Device
USB mass storage device found available
.
Backing up reten.bkp to "/var/opt/nortel/cs/fs/usb/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

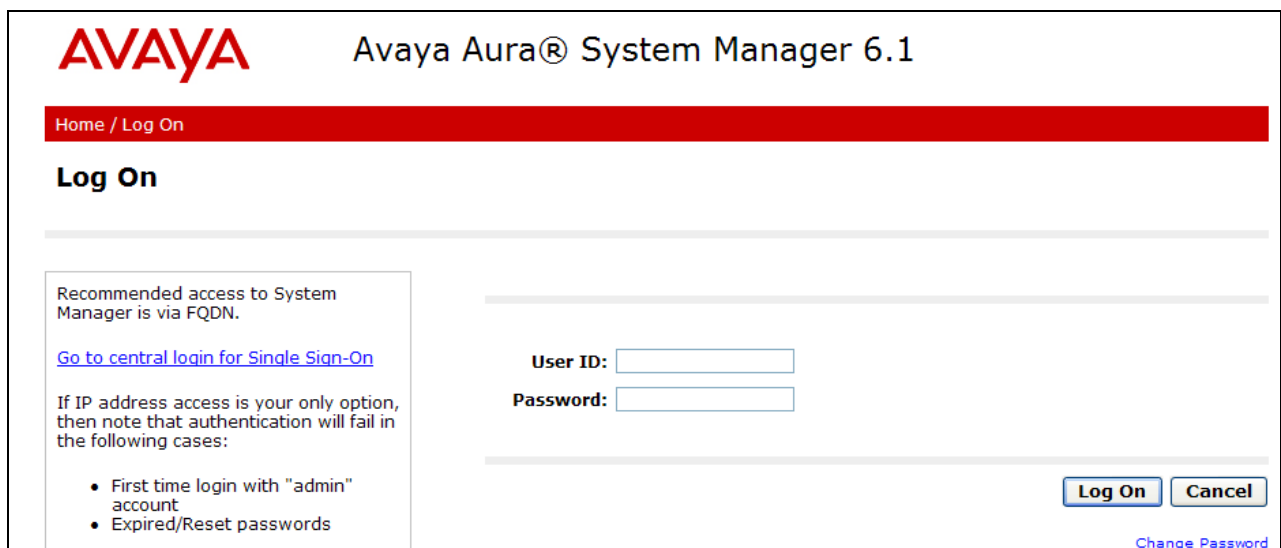
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

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**.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Avaya Communication Server 1000E and Session Manager, and the SIP trunk between Session Manager and the ASBCE.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “<http://<ip-address>/SMGR>”, where <ip-address> is the IP address of 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.



The screenshot shows the Avaya Aura® System Manager 6.1 Log On interface. At the top, the Avaya logo is on the left and the title "Avaya Aura® System Manager 6.1" is on the right. Below the title is a red navigation bar with the text "Home / Log On". The main heading "Log On" is displayed. On the left, a box contains the text "Recommended access to System Manager is via FQDN." followed by a blue link "Go to central login for Single Sign-On". Below this, it states "If IP address access is your only option, then note that authentication will fail in the following cases:" and lists two bullet points: "First time login with 'admin' account" and "Expired/Reset passwords". To the right of this box are two input fields labeled "User ID:" and "Password:". At the bottom right, there are two buttons: "Log On" and "Cancel". A blue link "Change Password" is located at the bottom right of the page.

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.

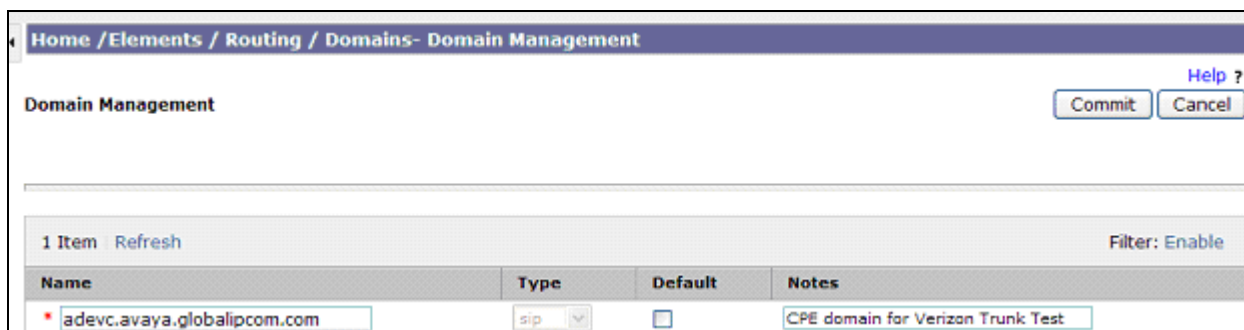
▼ Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

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. In the shared environment of the Avaya Solution and Interoperability Test lab, a domain “**avayalab.com**” is also defined and used by the shared 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].



Home / Elements / Routing / Domains- Domain Management

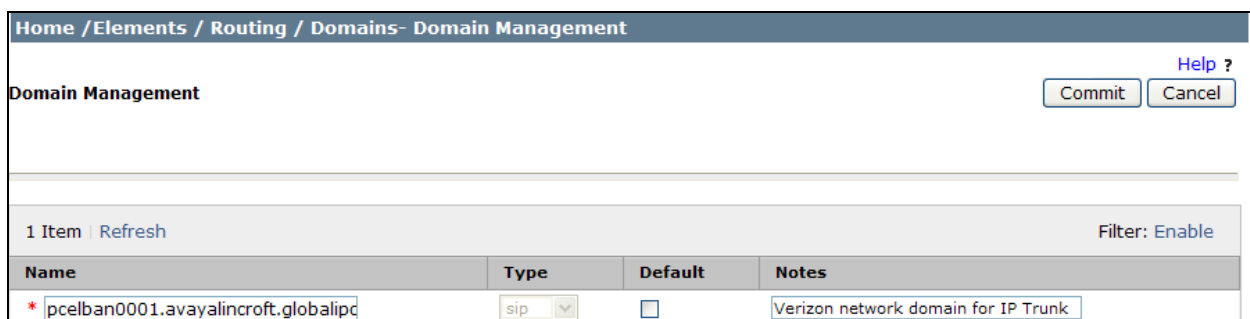
Domain Management [Help ?](#)

1 Item Refresh Filter: Enable

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

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

- **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 ?](#)

1 Item Refresh Filter: Enable

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

Click **Commit** to save.

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

Home / Elements / Routing / Domains - Domain Management

Domain Management

1 Item Refresh

Name	Type	Default	Notes
* avayalab.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.

Home / Elements / Routing / Domains - Domain Management

Domain Management

Edit New Duplicate Delete More Actions ▾

7 Items Refresh

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Test Trunk
<input type="checkbox"/>	attaep60.com	sip	<input type="checkbox"/>	Testing with AEP6.0
<input type="checkbox"/>	attavaya.com	sip	<input type="checkbox"/>	Testing ATT VP
<input type="checkbox"/>	avayalab.com	sip	<input type="checkbox"/>	Shared Avaya SIL network
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk
<input type="checkbox"/>	qwest.com	sip	<input type="checkbox"/>	Qwest SIP Trunk
<input type="checkbox"/>	sip.avaya.com	sip	<input type="checkbox"/>	

Select : All, None

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].

Click **Commit** to save. **Note:** No IP Address is added in the **Location Pattern** section.

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

Home / Elements / Routing / Locations - Location Details

Location Details [Help ?](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

Location Pattern

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

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

* Input Required

6.2.2 Location for Avaya SBCE For Enterprise

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].

Click **Commit** to save.

The screen below shows the Location defined for the ASBCE.

[Home](#) / [Elements](#) / [Routing](#) / [Locations - Location Details](#)

[Help ?](#)

Location Details

Commit

Cancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name:

ASBCE_1_Loc_140

Notes:

10.80.140.140

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

80

Kbit/sec

Location Pattern

Add

Remove

0 Items

[Refresh](#)

Filter: [Enable](#)

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

* Input Required

Commit

Cancel

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 to Avaya Communication Server 1000E to the format used by other Avaya products and endpoints.

6.3.1 Adaptation for Avaya Communication Server 1000E

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., “Vz_CS1K7.5”).
- **Module Name:** Select “CS1000Adapter” from drop-down menu (or add an adapter with name “CS1000Adapter” if not previously defined).

Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details [Help ?](#)

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

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Scrolling down, in the **Digit Conversion for Outgoing Calls from SM** section, click **Add** to configure entries for calls from Verizon to CS1000E users. The text below and the screen example that follows explain how to use Session Manager to convert between Verizon inbound toll-free numbers and corresponding CS1000E directory numbers. **Digit Conversion for Incoming Calls to SM** could be used, however the extensions will be adapted by the CLID entries on the individual extensions (**Section 5.9**).

- **Matching Pattern** Enter Verizon inbound toll-free numbers (or number ranges via wildcard pattern matching). For other entries, enter the dialed prefix for any SIP endpoints registered to Session Manager (if any).
- **Min** Enter minimum number of digits (e.g., 10).
- **Max** Enter maximum number of digits (e.g., 10).
- **Delete Digits** Enter “10”, the number of digits to be removed from dialed toll-free number before routing by Session Manager. For Verizon DID conversion to the corresponding CS1000E extension, remove all digits in the toll-free number.
- **Insert Digits** Enter the CS1000E extension corresponding to the toll-free number.
- **Address to modify** Select “both”.

Digit Conversion for Incoming Calls to SM

0 Items |
Filter: Enable

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

Digit Conversion for Outgoing Calls from SM

3 Items |
Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 8668510107	* 10	* 10		* 10	2222	both	
<input type="checkbox"/>	* 8668502380	* 10	* 10		* 10	2000	both	
<input type="checkbox"/>	* 8668512649	* 10	* 10		* 10	2900	both	

Select : All, None

Click **Commit** (not shown).

6.3.2 Adaptation for Avaya SBC for Enterprise

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 “**MIME=no**” to strip the CS1000E MIME information from the SDP sent to Verizon.

[Home](#) / [Elements](#) / [Routing](#) / [Adaptations - Adaptation Details](#)

[Help ?](#)

Adaptation Details

Commit

Cancel

General

* Adaptation name:

History Diversion IPT

Module name:

VerizonAdapter

Module parameter:

MIME=no

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add

Remove

0 Items

[Refresh](#)

Filter: [Enable](#)

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

Digit Conversion for Outgoing Calls from SM

Add

Remove

0 Items

[Refresh](#)

Filter: [Enable](#)

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

* Input Required

Commit

Cancel

Click **Commit**.

MEO; Reviewed:
SPOC 10/18/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

52 of 103
VZIPCC1K75ASBCE

6.4. SIP Entities

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

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 CS1000E created in **Section 6.3.1**.
- **Location:** Select the Location for 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** 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.

The screenshot displays the 'SIP Entity Details' configuration window. The breadcrumb trail at the top reads 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. The window title is 'SIP Entity Details'. In the top right corner, there are 'Commit', 'Cancel', and 'Help ?' buttons. The 'General' section is active, showing the following fields:

- Name:** Vz_CS1K_7.5
- FQDN or IP Address:** 10.80.140.203
- Type:** SIP Trunk (dropdown menu)
- Notes:** CS1000E 7.5
- Adaptation:** Vz_CS1K7.5 (dropdown menu)
- Location:** Vz_CS1K (dropdown menu)
- Time Zone:** America/Denver (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown menu)

The 'SIP Link Monitoring' section is also visible, with the 'SIP Link Monitoring' dropdown set to 'Use Session Manager Configuration'.

6.4.2 SIP Entity for Avaya SBC for Enterprise

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 ASBCE created in **Section 6.3.2**.
- **Location:** Select the Location for the ASBCE.

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 ASBCE in the sample configuration.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities - SIP Entity Details". The page title is "SIP Entity Details". In the top right corner, there are "Commit" and "Cancel" buttons, and a "Help ?" link. The "General" section contains the following fields: "Name" (Vz_ASBCE-1), "FQDN or IP Address" (10.80.140.141), "Type" (Other), "Notes" (empty), "Adaptation" (History Diversion IPT), "Location" (ASBCE_1_Loc_140), "Time Zone" (America/Denver), "Override Port & Transport with DNS" (unchecked), "SRV" (unchecked), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), "Call Detail Recording" (none), and "SIP Link Monitoring" (Link Monitoring Disabled). The "SIP Link Monitoring" section contains "Proactive Monitoring Interval (in seconds)" (60), "Reactive Monitoring Interval (in seconds)" (120), and "Number of Retries" (5).

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

SIP Entity Details [Help ?](#)

General

* Name: Vz_ASBCE-1

* FQDN or IP Address: 10.80.140.141

Type: Other

Notes:

Adaptation: History Diversion IPT

Location: ASBCE_1_Loc_140

Time Zone: America/Denver

Override Port & Transport with DNS ☐

SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 5

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 ASBCE.

6.5.1 Entity Link to Avaya Communication Server 1000E

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.
- **Protocol:** Select protocol to use “TCP”.
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is “5060”.
- **SIP Entity 2:** Select the SIP Entity defined for CS1000E.
- **Port:** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is “5060”.
- **Trusted** Check this option box.
- **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.

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item [Refresh](#) Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Vz_CS100075-Link	* ASM	TCP	* 5060	* Vz_CS1K_7.5	* 5060	Trusted	

6.5.2 Entity Link to Avaya SBC for Enterprise

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 ASBCE.
- **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:** Check this option box.
- **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 ASBCE.

Home / Elements / Routing / Entity Links - Entity Links

Entity Links Help ? Commit Cancel

1 Item [Refresh](#) Filter: Enable

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

6.6. Routing Policies

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

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 CS1000E and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page (not shown).

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 Policy Details [Help ?](#)

General

* Name: Vz_CS1K-R75_RP

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Vz_CS1K_7.5	10.80.140.203	SIP Trunk	CS1000E 7.5

6.6.2 Routing Policy to Avaya SBC for Enterprise

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 ASBCE and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page (not shown).

Click **Commit** to save the Routing Policy definition.

The following screen shows the Routing Policy for the ASBCE.

The screenshot shows the 'Routing Policy Details' page for 'Vz_ASBCE-1_RP'. The page has a breadcrumb trail: 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. There are 'Commit', 'Cancel', and 'Help' buttons in the top right. The 'General' section contains fields for 'Name' (Vz_ASBCE-1_RP), 'Disabled' (checkbox), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button. Below these sections is a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one entry: Vz_ASBCE-1, 10.80.140.141, Other.

Name	FQDN or IP Address	Type	Notes
Vz_ASBCE-1	10.80.140.141	Other	

6.7. Dial Patterns

Dial Patterns are used to route calls to the appropriate Routing Policies, and ultimately to the appropriate SIP Entities. Dial Patterns will be configured to route outbound calls from CS1000E users to the PSTN via the Verizon IPCC Service. Other dial patterns will be configured to route inbound calls from Verizon IPCC Service to CS1000E users.

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 inbound 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 (e.g. “**ASBCE_1_Loc_140**”). In the example below, the ASBCE Location was selected as the originating Location.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya Communication Server 1000E (“**Vz_CS1K_7.5**”).
- 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 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

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

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	ASBCE_1_Loc_140	10.80.140.140	Vz_CS1K-R75_RP	0	<input type="checkbox"/>	Vz_CS1K_7.5	

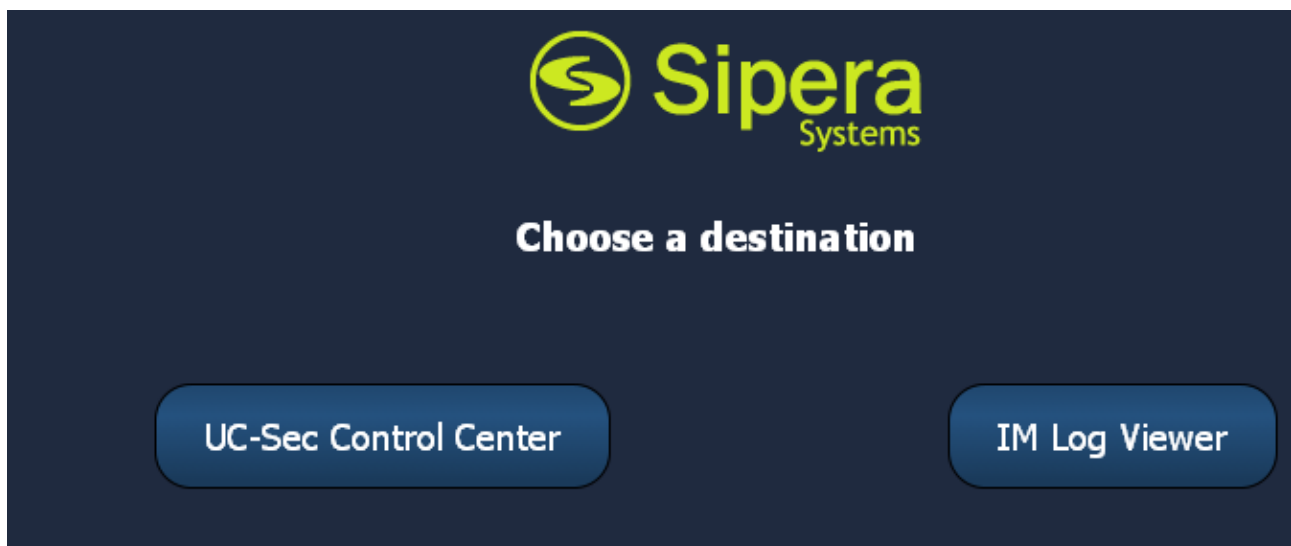
7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya Session Border Controller for Enterprise is used as the edge device between the Avaya CPE and Verizon Business.

These Application Notes assume that the installation of the ASBCE and the assignment of a management IP Address have already been completed.

7.1. Access the Management Interface

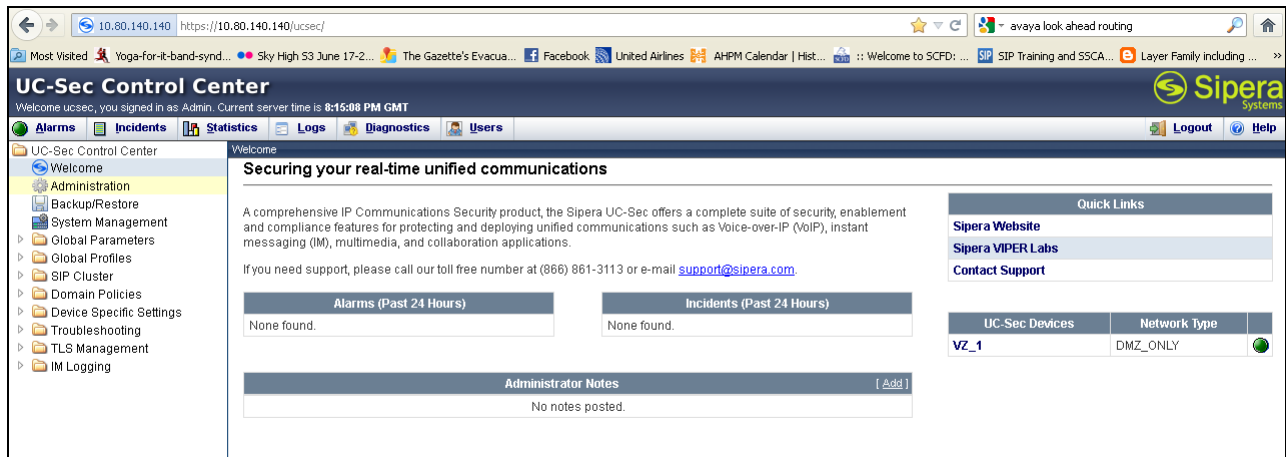
Access the web management interface by entering the URL `https://<ip-address>` where `<ip-address>` is the management IP address assigned during installation. Select **UC-Sec Control Center**.



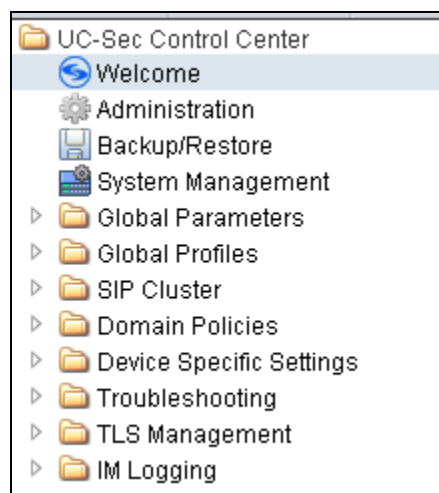
A log-in screen is presented. Enter an appropriate **Login ID** and **Password**.

The image shows the Sipera Systems login form. On the left, there is a banner with the Sipera Systems logo and the tagline "LEARN - VERIFY - PROTECT". Below the banner, there is a paragraph of text describing the UC-Sec family of products. To the right of the banner is a "Sign in" form. The form has a title "Sign in" and a message "Session expired, please login again". It contains two input fields: "Login ID" with the value "ucsec" and "Password" with masked characters "*****". Below the password field is a "Sign in" button. At the bottom of the form, there is a "NOTICE TO USERS" section with a warning about unauthorized use and a link to the Sipera Systems website.

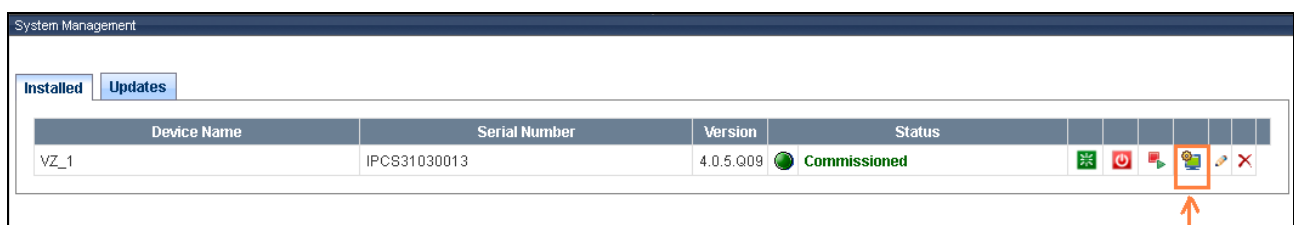
Once logged in, the main page of the UC-Sec Control Center will appear.



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



To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named “VZ_1” is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).



The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to “SIP” and the **Deployment Mode** was set to “Proxy”.

System Information: VZ_1				
Network Configuration				
General Settings		Device Settings		
Appliance Name	VZ_1	HA Mode	No	
Box Type	SIP	Secure Channel Mode	None	
Deployment Mode	Proxy	Two Bypass Mode	No	
Network Settings				
IP	Public IP	Netmask	Gateway	Interface
10.80.140.141	10.80.140.141	255.255.255.0	10.80.140.1	A1
2.2.2.2	2.2.2.2	255.255.255.0	2.2.2.1	B1
DNS Configuration		Management IP(s)		
Primary DNS	172.30.209.4	IP	10.80.140.140	
Secondary DNS				
DNS Location	DMZ			
DNS Client IP	2.2.2.2			

7.2. Device Specific Settings

7.2.1 Define Network Information

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

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

Click **Save Changes**. Repeat the process for external interfaces using **B1**.

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

Device Specific Settings > Network Management: VZ_1

UC-Sec Devices
VZ_1

Network Configuration Interface Configuration

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.0 B2 Netmask

Add IP Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface
10.80.140.141		10.80.140.1	A1 <input type="button" value="X"/>
2.2.2.2		2.2.2.1	B1 <input type="button" value="X"/>

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

Device Specific Settings > Network Management: VZ_1

UC-Sec Devices
VZ_1

Network Configuration Interface Configuration

Name	Administrative Status	
A1	Enabled	<input type="button" value="Toggle State"/>
A2	Disabled	<input type="button" value="Toggle State"/>
B1	Enabled	<input type="button" value="Toggle State"/>
B2	Disabled	<input type="button" value="Toggle State"/>

7.2.2 Signaling Interfaces

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

Define a signaling interface for Verizon:

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

Click **Finish** (not shown).

Repeat the process for the internal Avaya network.

The screen below shows the configured internal and external signaling interfaces used in the sample configuration.

Device Specific Settings > Signaling Interface: VZ_1

UC-Sec Devices
VZ_1

Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Inside_to_CPE	10.80.140.141	5060	5060	---	None		
Sig_Outside_to_Vz	2.2.2.2	---	5060	---	None		

7.2.3 Media Interfaces

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

Define a media interface for Verizon:

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

Repeat the process for the internal Avaya network.

The screen below shows the configured internal and external media interfaces used in the sample configuration.

Device Specific Settings > Media Interface: VZ_1

UC-Sec Devices
VZ_1

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add Media Interface

Name	Media IP	Port Range		
Int_Media_to_CPE	10.80.140.141	35000 - 40000		
Ext_Media_to_Vz	2.2.2.2	35000 - 40000		

7.3. Global Profiles

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

7.3.1 Routing Profiles

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

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

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

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

Click **Finish** (not shown).

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

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.80.150.206:5060	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to Verizon. In the **Next Hop Server 1** field enter the IP address that Verizon uses for the Verizon IPCC with a colon and then the port number. Check the **Next Hop Priority**. Enter “UDP” for the **Outgoing Transport** field.

NOTE: If the outside port is something other than 5060 the **Next Hop Server 1** and **Next Hop Server 2** fields must contain a colon and the port number after the IP address or domain name. If these are not entered, then the OPTIONS messages from Session Manager will be proxied to the service provider with a port of 5060 and may not get a response. This will cause ASBCE to respond to the Session Manager OPTIONS with a 408 Request Timeout, which will cause the Session Manager to mark the entity link as down.

Global Profiles > Routing: Vz_IPCC

[Add Profile](#) [Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

Routing Profiles

- default
- Route to SM6.1
- Vz_IPCC**
- Route to SM6.2
- Vz_IPT

Click here to add a description.

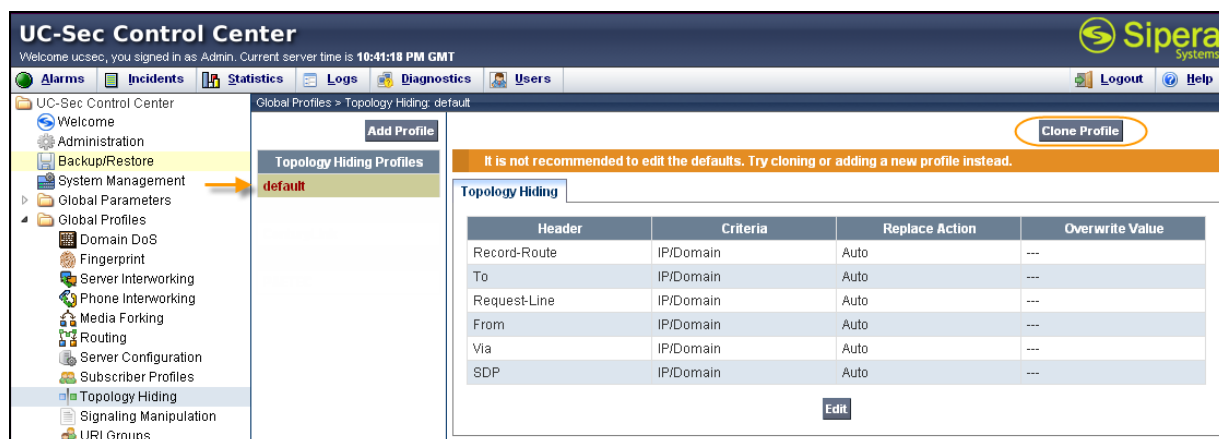
Routing Profile [Add Routing Rule](#)

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	172.30.205.55:5072	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

7.3.2 Topology Hiding Profile

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

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



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

The 'Clone Profile' dialog box shows the 'Profile Name' as 'default' and the 'Clone Name' as 'Avaya'. The 'Finish' button is located at the bottom right.

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

The 'Edit Topology Hiding Profile' dialog box shows a table with the following data:

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

The 'Finish' button is located at the bottom right.

It is not necessary to modify the **Verizon** profile from the default values if IP addresses are used. The following screen shows the Topology Hiding Policy **Verizon** created for Verizon with the domain names overwritten in the appropriate fields:

Global Profiles > Topology Hiding: IPCC_Topology_Hiding

[Add Profile](#) [Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

Topology Hiding Profiles

- default
- cisco_th_profile
- Avaya
- Verizon_IPT
- IPCC_Topology_Hiding**

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	adevc.avaya.globalipcom.com
To	IP/Domain	Overwrite	pcelban0001.avayalincroft.globalipcom.com
SDP	IP/Domain	Auto	---

[Edit](#)

7.3.3 Server Interworking

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

Interworking Profile

Profile Name

[Next](#)

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

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

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

Interworking Profile

Privacy

Privacy Enabled ☐

User Name

P-Asserted-Identity ☐

P-Preferred-Identity ☐

Privacy Header

DTMF

DTMF Support ☒ None ☐ SIP NOTIFY ☐ SIP INFO

Back **Next**

Interworking Profile

Configuration is not required. All fields are optional.

SIP Timers

Min-SE seconds, [90 - 86400]

Init Timer milliseconds, [50 - 1000]

Max Timer milliseconds, [200 - 8000]

Trans Expire seconds, [1 - 64]

Invite Expire seconds, [180 - 300]

Transport Timers

TCP Connection Inactive Timer seconds, [600 - 3600]

Back **Next**

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

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

Click **Finish** to save changes.

Interworking Profile

Advanced Settings

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

Back

Finish

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

Global Profiles > Server Interworking: Verizon-IPCC

Add Profile

Rename Profile

Clone Profile

Delete Profile

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

Sipera-Halo

OCS-FrontEnd-Server

Avaya

Verizon-IPCC

Verizon_IPT

Click here to add a description.

General

Timers

URI Manipulation

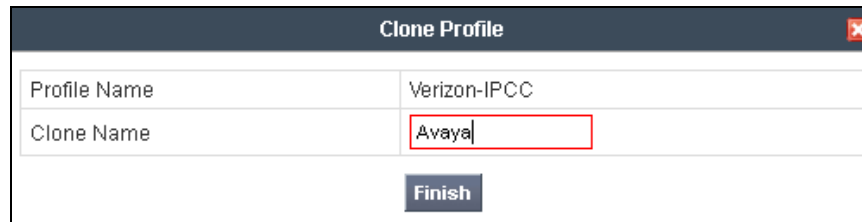
Header Manipulation

Advanced

General

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

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



Clone Profile	
Profile Name	Verizon-IPCC
Clone Name	Avaya
Finish	

7.3.4 Signaling Manipulation

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

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

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

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown). A new blank SigMa Editor window will pop up. Enter Appropriate script and click **Save**.

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

- **within session “All”** Transformations applied to all SIP sessions.
Actions to be taken to any SIP message.
- **act on message %DIRECTION=“OUTBOUND”** Applied to a message leaving ASBCE.
- **%ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has routed through ASBCE.
- **remove(%HEADERS[“P-Location”][1]);** Used to remove an entire header (like P-Location). The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message.

With this script Endpoint-View, Alert-Info, User-Agent, Server, and P-Location headers will be removed. These items are being removed for general security purposes and because the SIP Service provider has no need of these items. These are optional inclusions to any SigMa Script.

The screenshot shows the SigMa Editor window. At the top, there's a title bar 'SigMa Editor'. Below it, an 'Options' section contains a 'Title' field with the text 'Example_for_IPCC'. The main area is a code editor with a line number column on the left (1-14). The script content is as follows:

```

1 within session "ALL"
2 {
3   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4   {
5     // Topology Hiding of P-Location header for subsequent re-INVITES
6
7     remove(%HEADERS["Endpoint-View"][1]);
8     remove(%HEADERS["Alert-Info"][1]);
9     remove(%HEADERS["User-Agent"][1]);
10    remove(%HEADERS["Server"][1]);
11    remove(%HEADERS["P-Location"][1]);
12
13  }
14 }

```

The following screen shows the finished Signaling Manipulation Script **"Example_for_IPCC"**. This script will later be applied to the Verizon Server Configuration in **Section 7.3.6**. The details of these script elements can be found in **Appendix A**.

The screenshot shows the 'Global Profiles > Signaling Manipulation: Example_for_IPCC' window. It has a sidebar on the left with a list of scripts: 'Example', 'CS1K_Sigma_Script', 'Example2', 'CS1K_Combined', 'Example22', 'Example_for_IPCC' (highlighted in green), and 'IPCC Test'. The main area has buttons at the top: 'Upload Script', 'Add Script', 'Download Script', 'Clone Script', and 'Delete Script'. Below these is a yellow bar with the text 'Click here to add a description.' and a tab labeled 'Signaling Manipulation'. The script content is displayed in a text area, matching the code from the previous screenshot. An 'Edit' button is at the bottom right of the script area.

7.3.5 Server Configuration

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

Add Server Configuration Profile

Profile Name: Avaya_SM6.1

Next

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

- **Server Type:** Select “**Call Server**” from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module.
- **Supported Transports:** Select **TCP** and **UDP**. This is the transport protocol used in the ASBCE Entity Link on Session Manager configured in **Section 6.5**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the ASBCE Entity Link on Session Manager configured in **Section 6.5**.

Click **Next** to continue.

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

Add Server Configuration Profile - General

Server Type: Call Server

IP Addresses / Supported FQDNs: 10.80.150.206

Supported Transports: ☒ TCP, ☒ UDP, ☐ TLS

TCP Port: 5060

UDP Port: 5060

TLS Port:

Back Next

Add Server Configuration Profile - Authentication

Enable Authentication: ☐

User Name:

Realm:

Password:

Confirm Password:

Back Next

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

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

Click **Next** to continue.

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

The image shows two side-by-side screenshots of configuration windows. The left window is titled "Edit Server Configuration Profile - Heartbeat" and contains the following fields: "Enable Heartbeat" (checked), "Method" (OPTIONS), "Frequency" (60 seconds), "From URI" (ping@10.80.140.141), "To URI" (ping@10.80.150.206), "TCP Probe" (unchecked), and "TCP Probe Frequency" (empty). The right window is titled "Edit Server Configuration Profile - Advanced" and contains the following fields: "Enable DoS Protection" (unchecked), "Enable Grooming" (unchecked), "Interworking Profile" (Avaya), "Signaling Manipulation Script" (None), and "TCP Connection Type" (SUBID selected, PORTID and MAPPING unselected). Both windows have a "Finish" button at the bottom.

7.3.6 Server Configuration for Verizon IPCC

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

The image shows a screenshot of the "Add Server Configuration Profile" window. It has a title bar with a close button. The main area contains a "Profile Name" label and a text input field containing "IPCC_Service". Below the input field is a "Next" button.

The screen below shows the General parameter settings for the “**IPCC_Service**” server configured as **Trunk Server**, with Verizon IP Address, transport, and port:

Global Profiles > Server Configuration: IPCC_Service	
<div> Add Profile </div> <div> Profile </div> <div> Avaya_SM6.2 </div> <div> Vz_IPT </div> <div> Avaya_SM6.1 </div> <div> default </div> <div> IPCC_Service </div>	<div> <div> General Authentication Heartbeat Advanced </div> <div> General </div> <div> Server Type Trunk Server </div> <div> IP Addresses / FQDNs 172.30.205.55 </div> <div> Supported Transports UDP </div> <div> UDP Port 5072 </div> <div> Edit </div> </div>

The following screens show the settings in the **Authentication** and the **Heartbeat** tabs (note that external OPTIONS to Verizon are not enabled in this configuration):

Authentication		Heartbeat	
<div> General Authentication Heartbeat Advanced </div> <div> Authentication </div> <div> Enable Authentication <input type="checkbox"/> </div> <div> Edit </div>	<div> General Authentication Heartbeat Advanced </div> <div> Heartbeat </div> <div> Enable Heartbeat <input type="checkbox"/> </div> <div> TCP Probe <input type="checkbox"/> </div> <div> Edit </div>		

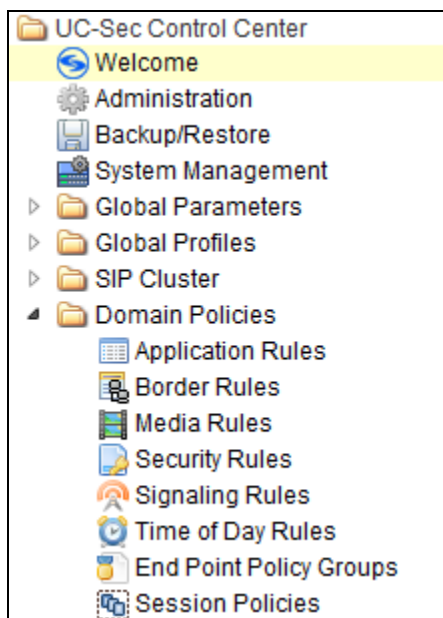
In the **Advanced Tab**, select “**Verizon-IPCC**” for **Interworking Profile** and “**Example_for_IPCC**” as the **Signaling Manipulation Script** as shown below:

Global Profiles > Server Configuration: IPCC_Service	
<div> Add Profile </div> <div> Profile </div> <div> Avaya_SM6.2 </div> <div> Vz_IPT </div> <div> Avaya_SM6.1 </div> <div> default </div> <div> IPCC_Service </div>	<div> <div> General Authentication Heartbeat Advanced </div> <div> Advanced </div> <div> Enable DoS Protection <input type="checkbox"/> </div> <div> Enable Grooming <input type="checkbox"/> </div> <div> Interworking Profile Verizon-IPCC </div> <div> Signaling Manipulation Script Example_for_IPCC </div> <div> UDP Connection Type SUBID </div> <div> Edit </div> </div>

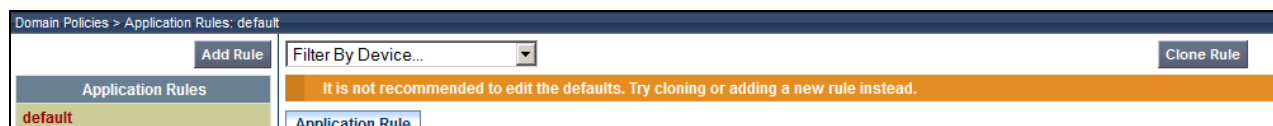
Click **Finish** to save changes (not shown).

7.4. Domain Policies – Application Rule

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



In the sample configuration, a single application rule was created by cloning the default rule called “**default**”. Select the default rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “**Vz_App_Rule**” as shown below. Click **Finish**.

Clone Rule	
Rule Name	default
Clone Name	<input type="text" value="Vz_App_Rule"/>
<input type="button" value="Finish"/>	

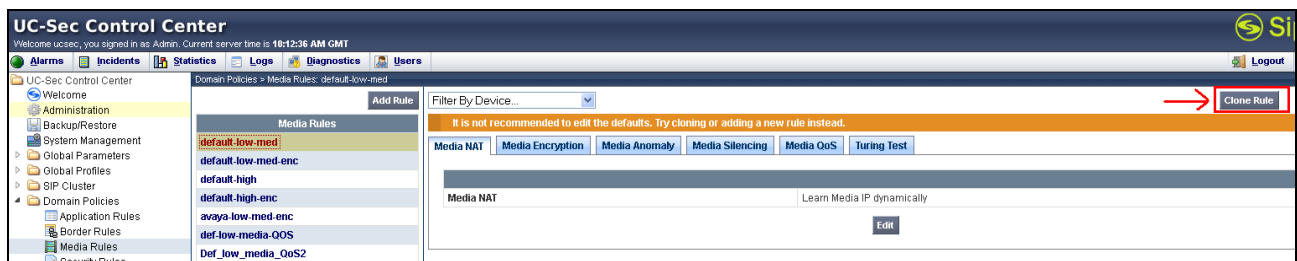
Select the newly created rule and click the **Edit** button (not shown). In the resulting screen, change the default **Maximum Concurrent Sessions** to 2000, the **Maximum Session per Endpoint** to 2000. Click **Finish**.

Application Rule				
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		
Miscellaneous				
CDR Support	None			
IM Logging	No			
RTCP Keep-Alive	No			

7.5. Domain Policies – Media Rules

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

In the sample configuration, a single media rule was created by cloning the default rule called “**default-low-med**”. Select the default-low-med rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “**def-low-med-QoS**” as shown below. Click **Finish**.

Media Rule

Rule Name

def-low-media-QoS

Next

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

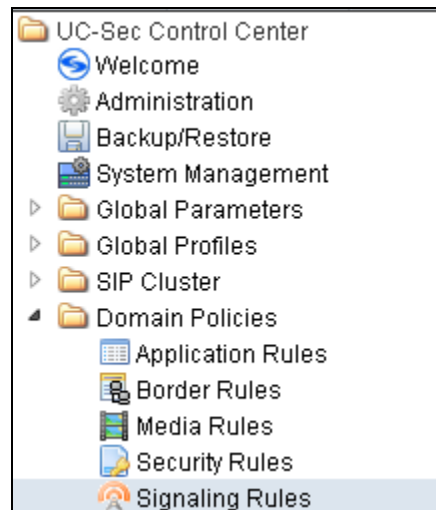
Media QoS			
Media QoS Reporting			
RTCP Enabled	<input type="checkbox"/>		
Media QoS Marking			
Enabled	<input checked="" type="checkbox"/>		
<input type="radio"/> ToS			
Audio Precedence	Routine		000
Audio ToS	Minimize Delay		1000
Video Precedence	Routine		000
Video ToS	Minimize Delay		1000
<input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

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

Domain Policies > Media Rules: def-low-media-QoS	
<div> <div>Add Rule</div> <div>Filter By Device...</div> </div> <div> <div>Media Rules</div> <ul style="list-style-type: none"> default-low-med default-low-med-enc default-high default-high-enc avaya-low-med-enc def-low-media-QoS def_low_media_QoS2 </div>	<div> <div>Click here to add a description.</div> <div> <div>Media NAT</div> <div>Media Encryption</div> <div>Media Anomaly</div> <div>Media Silencing</div> <div>Media QoS</div> <div>Turing Test</div> </div> <div> <div>Media QoS Reporting</div> <div>RTCP Enabled <input type="checkbox"/></div> </div> <div> <div>Media QoS Marking</div> <div>Enabled <input checked="" type="checkbox"/></div> <div>QoS Type DSCP</div> </div> <div> <div>Audio QoS</div> <div>Audio DSCP EF</div> </div> <div> <div>Video QoS</div> <div>Video DSCP EF</div> </div> <div>Edit</div> </div>

7.6. Domain Policies – Signaling Rules

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



Click the **Add Rule** button (not shown) to add a new signaling rule. In the **Rule Name** field, enter an appropriate name, such as “**Block_Hdr_Remark**”. Click **Next**.

Signaling Rule	
Rule Name	Block_Hdr_Remark
Next	

In the subsequent screen (not shown), click **Next** to accept defaults. In the **Signaling QoS** screen, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down menu. In the sample configuration, “**AF32**” was selected for “Assured Forwarding 32.” Click **Finish** (not shown).

Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
	Precedence	Routine	000
	ToS	Minimize Delay	1000
<input checked="" type="radio"/> DSCP			
	Value	AF32	011100

After this configuration, the new “**Block_Hdr_Remark**” rule will appear as follows.

The screenshot shows the configuration page for the 'Block_Hdr_Remark' rule under 'Domain Policies > Signaling Rules'. The left sidebar lists 'Signaling Rules' with options: default, No-Content-Type-Checks, HideP-Loc, signal-QoS, and Block_Hdr_Remark (highlighted). The main area has tabs: General, Requests, Responses, Request Headers, Response Headers, and Signaling QoS (selected). A yellow banner says 'Click here to add a description.' Below the tabs, a table shows the 'Signaling QoS' configuration:

Signaling QoS	
QoS Type	DSCP
DSCP	AF32

7.7. Domain Policies – End Point Policy Groups

Select **Domain Policies** → **End Point Policy Groups** from the left-side menu as shown below.

Select the **Add Group** button.

The screenshot shows the 'Add Group' page under 'Domain Policies > End Point Policy Groups: default-low'. The left sidebar has 'Policy Groups' selected. The main area has a 'Filter By Device...' dropdown and a blue 'Add Group' button. An orange banner at the bottom states: 'It is not recommended to edit the defaults. Try adding a new group instead.'

Enter a name in the **Group Name** field, such as “**def_low_remark**” as shown below. Click **Next**.

The screenshot shows the 'Policy Group' form. It has a title bar 'Policy Group' with a close button. Below is a 'Group Name' field containing the text 'def_low_remark', which is highlighted with a red box. At the bottom is a blue 'Next' button.

In the sample configuration, defaults were selected for all fields, with the exception of **Application Rule** which was set to “**Vz_App_Rule**”, **Media Rule** which was set to “**def-low-med-QoS**”, and **Signaling Rule**, which was set to “**Block_Hdr_Remark**” as shown below. The selected application rule, non-default media rule and signaling rule were created in previous sections. Click **Finish**.

Edit Policy Set	
Application Rule	Vz_App_Rule
Border Rule	default
Media Rule	def-low-media-QOS
Security Rule	default-low
Signaling Rule	Block_Hdr_Remark
Time of Day Rule	default
<input type="button" value="Finish"/>	

Once configuration is completed, the “**def_low_remark**” policy group will appear as follows.

Domain Policies > End Point Policy Groups: def_low_remark

Add Group

Filter By Device...

Rename Group

Delete Group

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

OCS-default-high

avaya-def-low-enc

def_low_remark

Click here to add a description.

Hover over a row to see its description.

Policy Group

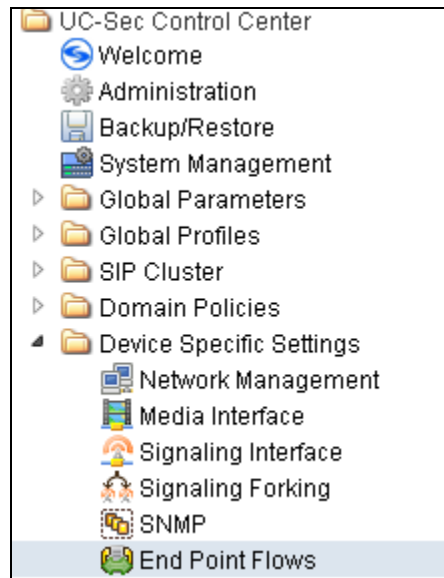
View Summary

Add Policy Set

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	Vz_App_Rule	default	def-low-media-QOS	default-low	Block_Hdr_Remark	default		

7.8. Device Specific Settings – End Point Flows

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



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



The following screen shows the flow named “**Avaya_SM6.1**” being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections and uses defaults for **URI Group**, **Transport** and **Remote Subnet**.. Click **Finish**.

Criteria	
Flow Name	Avaya_SM6.1
Server Configuration	Avaya_SM6.1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Slg_Outside_to_Vz
Signaling Interface	Sig_Inside_to_CPE
Media Interface	Int_Media_to_CPE
End Point Policy Group	def_low_remark
Routing Profile	Vz_IPCC
Topology Hiding Profile	Avaya
File Transfer Profile	None
<input type="button" value="Finish"/>	

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

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

Edit Flow: SIP Trunk ✕

Criteria	
Flow Name	<input style="width: 100%;" type="text" value="IPCC_Trunk"/>
Server Configuration	<input style="width: 100%;" type="text" value="IPCC_Service"/>
URI Group	<input style="width: 100%;" type="text" value="*/"/>
Transport	<input style="width: 100%;" type="text" value="*/"/>
Remote Subnet	<input style="width: 100%;" type="text" value="*/"/>
Received Interface	<input style="width: 100%;" type="text" value="Sig_Inside_to_CPE"/>
Signaling Interface	<input style="width: 100%;" type="text" value="Sig_Outside_to_Vz"/>
Media Interface	<input style="width: 100%;" type="text" value="Ext_Media_to_Vz"/>
End Point Policy Group	<input style="width: 100%;" type="text" value="def_low_remark"/>
Routing Profile	<input style="width: 100%;" type="text" value="Route to SM6.1"/>
Topology Hiding Profile	<input style="width: 100%;" type="text" value="IPCC_Topology_Hiding"/>
File Transfer Profile	<input style="width: 100%;" type="text" value="None"/>

Finish

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

Device Specific Settings > End Point Flows: VZ_1

UC-Sec
Devices
VZ_1

Subscriber Flows

Server Flows

Add Flow

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

Server Configuration: Avaya_SM6.1

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Avaya_SM6.1	*	*	*	Sig_Outside_to_Vz	Sig_Inside_to_CPE	Int_Media_to_CPE	def_low_remark	Vz_IPCC	Avaya	None			

Server Configuration: IPCC_Service

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	IPCC_Trunk	*	*	*	Sig_Inside_to_CPE	Sig_Outside_to_Vz	Ext_Media_to_Vz	def_low_remark	Route to SM6.1	IPCC_Topology_Hiding	None			

Update Order

8. Verizon Business IPCC Service Offer Configuration

Information regarding Verizon Business IPCC service offer can be found at <http://www.verizonbusiness.com/us/Products/communications/contact-center/inbound-transport/> or by contacting a Verizon Business sales representative.

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

8.1. Fully Qualified Domain Name (FQDN)s

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

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

8.2. DID Numbers Assigned by Verizon

Verizon provided inbound toll-free numbers that could be called from the PSTN. These Verizon-provided toll-free numbers terminated to the Avaya CS1000E location via the Verizon IPCC Service. **Table 1 in Section 3** shows example Verizon toll-free numbers and the configurable association of the Verizon toll-free numbers with Avaya CS1000E users.

9. Verification Steps

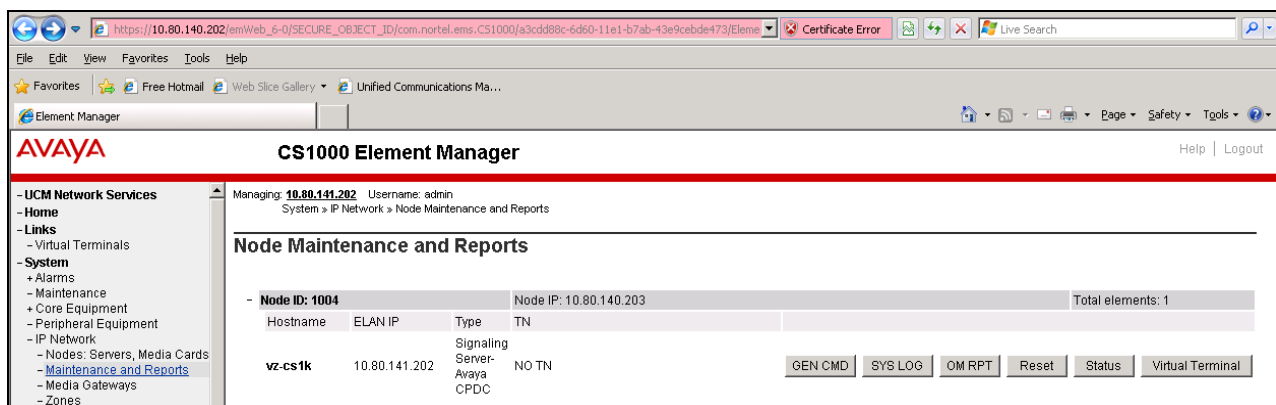
This section provides example verifications of the Avaya configuration with Verizon Business IPCC service.

9.1. Avaya Communication Server 1000E Verifications

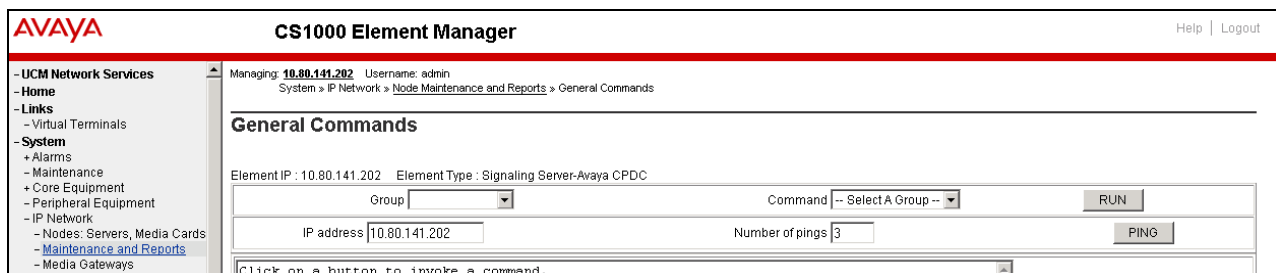
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

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.



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



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 (10.80.150.206, port 5060, TCP) has SIPNPM Status “Active”.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation menu with categories like UCM Network Services, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main content area is titled 'General Commands' and shows the command 'SIPGwShow' being executed for the 'Sip' group on IP address 10.80.141.202. The output displays the SIPNPM Status as 'Active' and lists various proxy IP addresses and ports.

Parameter	Value
SIPNPM Status	Active
Primary Proxy IP address	10.80.150.206
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	10.80.150.206
Primary Proxy2 port	5060
Primary Proxy2 Transport	TCP
Active Proxy	Primary : Register Not Supported
Time To Next Registration	0 Seconds
Channels Busy / Idle / Total	0 / 32 / 32
Stack version	5.5.0.13
TLS Security Policy	Security Disabled

As another example, the following screen shows the results of the “vtrkShow” Command from the “Vtrk” Group. The command was run with an active incoming call from the Verizon IPCC to an IP/Unistim telephone. Therefore, one channel is busy, and 63 idle.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation menu. The main content area is titled 'General Commands' and shows the command 'vtrkShow' being executed for the 'Vtrk' group on IP address 10.80.141.202. The output displays the VTRK Summary, including status, master status, registration node, protocol, and channel counts.

Parameter	Value
VTRK status	Active
Master status	On
VTRK REG Node	1004
Protocol	SIP SIPL
D-Channel	15
Customer	0
Channels Idle	63
Channels Busy	1
Channels Mbsy	0
Channels Pend	0
Channels Dsbl	0
Channels Ukwn	0

Below is the same call placed to a SIP extension. Notice that the Channels Busy is now 2 instead of 1.

AVAYA CS1000 Element Manager

Managing: 10.80.141.202 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: Vtrk Command: vtrkShow Protocol: Start: Range: RUN

IP address: 10.80.141.202 Number of pings: 3 PING

```

-----
VTRK Summary
-----
VTRK status : Active
Master status : On
VTRK REG Node : 1004
Protocol : SIP SIPL
D-Channel : 15
Customer : 0
Channels Idle : 62
Channels Busy : 2
Channels Misy : 0
Channels Pend : 0
Channels Dsbl : 0
Channels Ukwn : 0
  
```

The next screen capture shows the output of the Command “SIPGWShowch” in Group “Sip” for channel 1, while an incoming call was active (using channel 1) from the Verizon IPCC Service to an IP-UNISim phone. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was “G_729A_20MS”. Note that the Remote IP (10.80.140.141) is the IP Address of the inside private interface of ASBCE.

Managing: 10.80.141.202 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: Sip Command: SIPGWShowch Sip: 1 RUN

IP address: 10.80.141.202 Number of pings: 3 PING

```

Stack version : 5.5.0.13
TLS Security Policy : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used : RPT
Channel tracing : -1
Handle Chan Type Direction CallState SIPState RxState TxState
-----
0xb7e0f418 1 VTRK Terminate BUSY Ringing Sent Connected Connected
Codec AirTime FS MS Fax DestNum RemoteIP URI Scheme
-----
G_729A_20MS 9 yes m no 2000 10.80.140.141 :: SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```


The next screen capture shows an alternate way to view similar information, but in this case, by searching for calls involving a specific directory number. The screen shows the output of the **Command “SIPGWShownum”** in **Group “Sip”** where DN 2000 was specified. An incoming call was active from the Verizon IPCC Service to the IP-UNISTim phone with DN 2000. In the output below, the scroll bar was used to scroll down to the area showing that the codec in use was “G_729A_20MS”. Note that the Remote IP (10.80.140.141) is the IP Address of the inside private interface of the ASBCE.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, and Customers. The main panel is titled 'General Commands' and shows the command 'SIPGWShownum' being executed in the 'Sip' group for directory number '2000'. The output displays various system parameters and a call log entry for a call from 10.80.140.141 to 2000 using the G_729A_20MS codec.

```

Managing: 10.80.141.202 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: Sip Command: SIPGWShownum SIP: 2000 RUN
IP address: 10.80.141.202 Number of pings: 3 PING

TLS Security Policy : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used : RPT
Channel tracing : -1
Calling/Called Party Number: 2000
Numbering Plan Indicator: Undefined
Type Of Number: Undefined

Handle Chan Type Direction CallState SIPState RxState TxState
-----
0xb7e0f418 1 VTRK Terminate BUSY Ringing Sent Connected Connected
Codec AirTime FS MS Fax DestNum RemoteIP URI Scheme
-----
G_729A_20MS 309 yes m no 2000 10.80.140.141 :: SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```

The following screen shows the output of the **Command “SIPGWShowch”** in **Group “Sip”** for channel 1, when an incoming call was active (using channel 1) to an IP UNISTim telephone via the Verizon IPCC Service. Again, the use of G.729A to the inside IP Address (10.80.140.141) of the SBC can be observed.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar is the same as the previous screenshot. The main panel shows the command 'SIPGWShowch' being executed in the 'Sip' group for channel '1'. The output displays system parameters and a call log entry for a call from 10.80.140.141 to 2000 using the G_729A_20MS codec.

```

Managing: 10.80.141.202 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group: Sip Command: SIPGWShowch SIP: 1 RUN
IP address: 10.80.141.202 Number of pings: 3 PING

Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 1 / 31 / 32
Stack version : 5.5.0.13
TLS Security Policy : Security Disabled
SIP Gw Registration Trace : OFF
Output Type Used : RPT
Channel tracing : -1
Handle Chan Type Direction CallState SIPState RxState TxState
-----
0xb7e0f418 1 VTRK Terminate BUSY Ringing Sent Connected Connected
Codec AirTime FS MS Fax DestNum RemoteIP URI Scheme
-----
G_729A_20MS 396 yes m no 2000 10.80.140.141 :: SIP
nearEnd Msec policy = 0
farEnd Msec policy = 0
  
```

The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command “slgSetShowAll”** in **Group “SipLine”**. At the time this screen was captured, the SIP telephone with DN 2900 was involved in an active call with the Verizon IPCC service.

Managing: **10.80.141.202** Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group **SipLine** Command **slgSetShowAll** **RUN**

IP address **10.80.141.202** Number of pings **3** **PING**

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPv4 Endpoints -----							
2900	2900	252-00-09-00	1	0	0x9709da0		SIP Lines
Total User Registered = 1 V4 Registered = 1 V6 Registered = 0							

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 “1165E IP Deskphone” UNISim telephone was involved in an active call with the Verizon IPCC service.

Managing: **10.80.141.202** Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 10.80.141.202 Element Type : Signaling Server-Avaya CPDC

Group **Iset** Command **isetShow** Range **0** **500** **RUN**

IP address **10.80.141.202** Number of pings **3** **PING**

Set Information						
IP Address	NAT	Model Name	Type	RegType	State	Up
10.80.140.135		1165E IP Deskphone	1165	Regular	busy	2
Total sets = 1						

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: 10.80.141.202 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.

Managing: 10.80.141.202 Username: admin
System » Maintenance

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 15, which is used in the sample configuration, is established “**EST**” and active “**ACTV**”.

Managing: **10.80.141.202** Username: admin
System » Maintenance » D-Channel Diagnostics

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_RECV PDCH BDCH

☐ 015 VtrkNode1004 OPER EST ACTV AUTO

9.2. Wireshark Verifications

This section illustrates Wireshark traces for sample outbound and inbound calls using the sample configuration.

9.2.1 Example Inbound Call

This section illustrates an inbound call from PSTN telephone 303-538-7022 to Verizon IPCC toll free 866-851-2649.

The following screen shows a Wireshark trace filtered on SIP messages to and from the Verizon IP Address and taken from the outside of the ASBCE. The INVITE from Verizon in frame “1787” is selected and expanded to illustrate the contents of the message header and message body. Note that Verizon sends the calling party number 3035387022 in the From header, and does not include a PAI header. The Request-URI and To header both contain the dialed Verizon DID 8668502380. In the message body, note that the Verizon SDP offer lists G.729A (18) and G.711MU (0) and G.711A (8). In frame 24, a 180 Ringing (without SDP) response is sent to Verizon.

Filter: sip && ip.addr==172.30.205.55					
Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
1787	8.794966	172.30.205.55	1.1.1.2	SIP/SDP	Request: INVITE sip:8668502380@1.1.1.2:5060;transport=udp;user=phone, in-
1789	8.796120	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
1795	8.806877	1.1.1.2	172.30.205.55	SIP/SDP	Status: 200 OK, with session description

<ul style="list-style-type: none"> Frame 1787: 919 bytes on wire (7352 bits), 919 bytes captured (7352 bits) Ethernet II, Src: Cisco_5c:21:41 (00:04:9a:5c:21:41), Dst: IntelCor_cc:23:11 (00:1b:21:cc:23:11) Internet Protocol Version 4, 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 <ul style="list-style-type: none"> Request-Line: INVITE sip:8668502380@1.1.1.2:5060;transport=udp;user=phone SIP/2.0 Message Header <ul style="list-style-type: none"> Via: SIP/2.0/UDP 172.30.205.55:5072;branch=z9hG4bkh27eup30dgl0hsgcg300cb0000010.1 Call-ID: -1810058258723244228010.10.20.33 From: <3035387022@199.173.94.24;user=phone>;tag=-643550697.7.kakaebbc0efk0kmlj0ieagdb To: <3035387022@1.1.1.2>;tag=46fcf90-cb8c500a-13c4-55013-585d0-5c01dfe2-585d0 CSeq: 2 INVITE Contact: <3035387022@172.30.205.55:5072;transport=udp> Allow: INVITE, ACK, BYE, OPTIONS, CANCEL, SUBSCRIBE, REFER Accept: application/sdp Content-Type: application/sdp Content-Length: 215 Max-Forwards: 69 Route: <3035387022@1.1.1.2:5060;ipcs-line=2607;lr;transport=udp> Message Body <ul style="list-style-type: none"> Session Description Protocol <ul style="list-style-type: none"> Session Description Protocol version (v): 0 Owner/Creator, Session Id (o): - 1348866057551 1 IN IP4 172.30.205.164 Session Name (s): - Connection Information (c): IN IP4 0.0.0.0 Time Description, active time (t): 0 0 Media Description, name and address (m): audio 12112 RTP/AVP 18 0 8 101 Connection Information (c): IN IP4 0.0.0.0 Media Attribute (a): rtpmap:101 telephone-event/8000 Media Attribute (a): fmtp:101 0-15 Media Attribute (a):ptime:20 Media Attribute (a): fmtp:18 annexb=no
--

The following screen shows the 200 OK in frame 1795 expanded to show the contents of the SDP answer containing G.729A returned to Verizon. The use of the value 101 for any transmission of DTMF telephone events via RFC 2833 can also be observed.

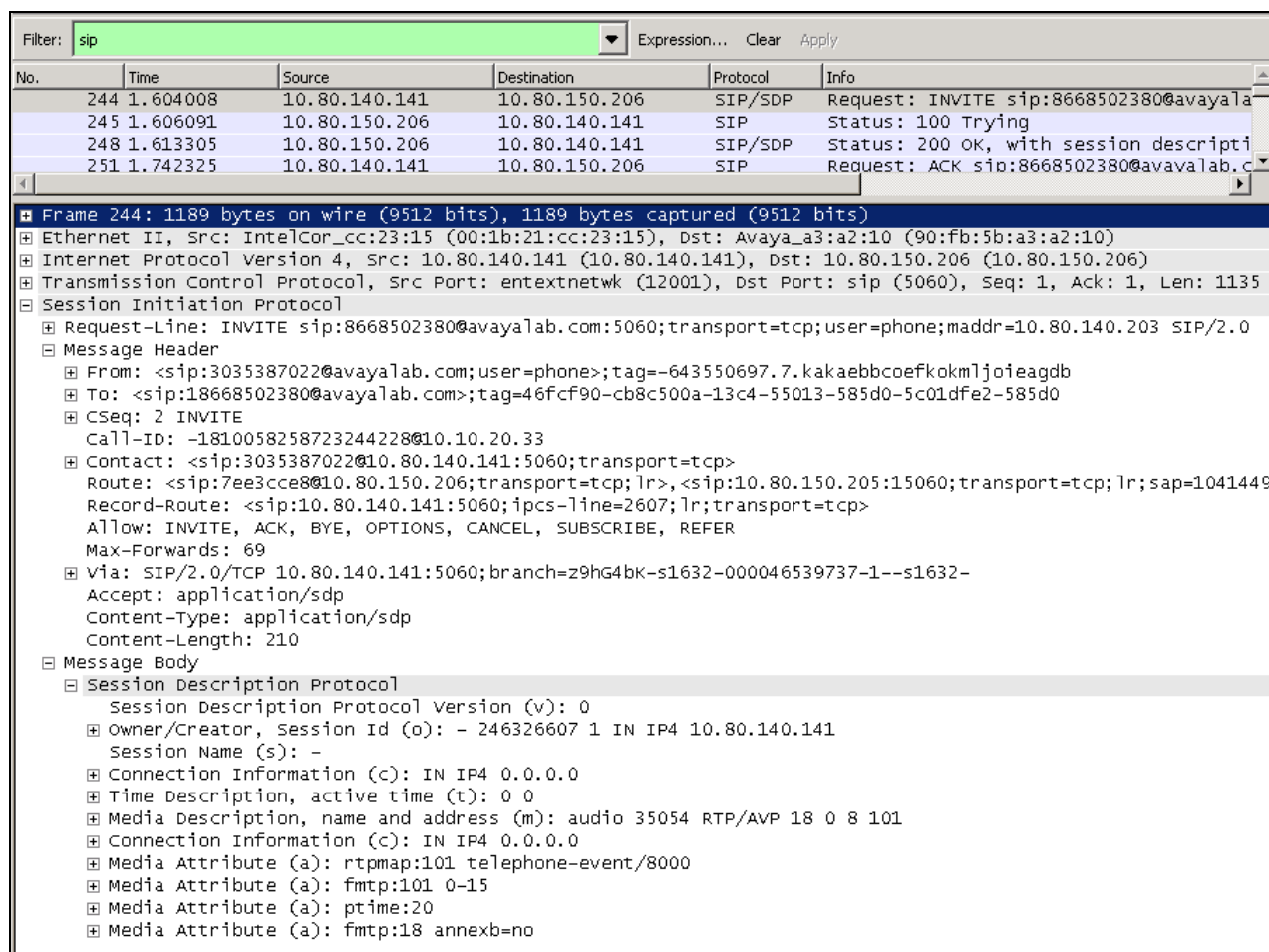
Filter: sip && ip.addr==172.30.205.55 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1787	8.794966	172.30.205.55	1.1.1.2	SIP/SDP	Request: INVITE sip:8668502380@1.1.1.2:5060;transport=udp;user=phone, in
1789	8.796120	1.1.1.2	172.30.205.55	SIP	Status: 100 Trying
1795	8.806877	1.1.1.2	172.30.205.55	SIP/SDP	Status: 200 OK, with session description

Frame 1795: 1028 bytes on wire (8224 bits), 1028 bytes captured (8224 bits)

- Ethernet II, Src: IntelCor_cc:23:11 (00:1b:21:cc:23:11), Dst: Cisco_5c:21:41 (00:04:9a:5c:21:41)
- Internet Protocol Version 4, Src: 1.1.1.2 (1.1.1.2), Dst: 172.30.205.55 (172.30.205.55)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: ayiya (5072)
- Session Initiation Protocol
 - Status-Line: SIP/2.0 200 OK
 - Message Header
 - From: <sip:3035387022@199.173.94.24;user=phone>;tag=-643550697.7.kakaebbc0efk0kmlj0feagdb
 - To: <sip:18668502380@1.1.1.2>;tag=46fcf90-cb8c500a-13c4-55013-585d0-5c01dfe2-585d0
 - CSeq: 2 INVITE
 - Call-ID: -1810058258723244228@10.10.20.33
 - Contact: <sip:8668502380@1.1.1.2:5060;transport=udp;user=phone>
 - Record-Route: <sip:1.1.1.2:5060;ipcs-line=2607;lr;transport=udp>
 - Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
 - Supported: 100rel, x-nortel-sipvc, replaces
 - Via: SIP/2.0/UDP 172.30.205.55:5072;branch=z9hg4bkh27eup30dg10hsgcg300cb0000010.1
 - Privacy: none
 - P-Asserted-Identity: "1165 UNISTIM" <sip:8668502380@avaya1ab.com;user=phone>
 - Content-Type: application/sdp
 - Content-Length: 242
 - Message Body
 - Session Description Protocol
 - Session Description Protocol version (v): 0
 - Owner/Creator, Session Id (o): - 177 2 IN IP4 1.1.1.2
 - Session Name (s): -
 - Connection Information (c): IN IP4 0.0.0.0
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 35022 RTP/AVP 18 101 111
 - Connection Information (c): IN IP4 0.0.0.0
 - 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):ptime:20
 - Media Attribute (a): inactive

The following screen capture shows a Wireshark trace filtered on SIP messages. The INVITE message from the ASBCE is selected and the message header is expanded for visibility. The message headers in the Request-URI, To and From now contain avayalab.com, the internal shared lab domain. Session Manager will adapt 866-850-2380 such that the call rings the IP UNISim telephone with Directory Number 2000, an IP UNISim telephone.



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 “Vz_ASBCE-1”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below.

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: Vz_ASBCE-1

Summary View

1 Item Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	ASM	10.80.140.141	5060	TCP	Up	200 OK	Up

Return to the list of monitored entities, and select another entity of interest, such as “Vz_CS1K_7.5”. 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.

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

hide navigation tree

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: Vz_CS1K_7.5

Summary View

1 Item Refresh Filter: Enable

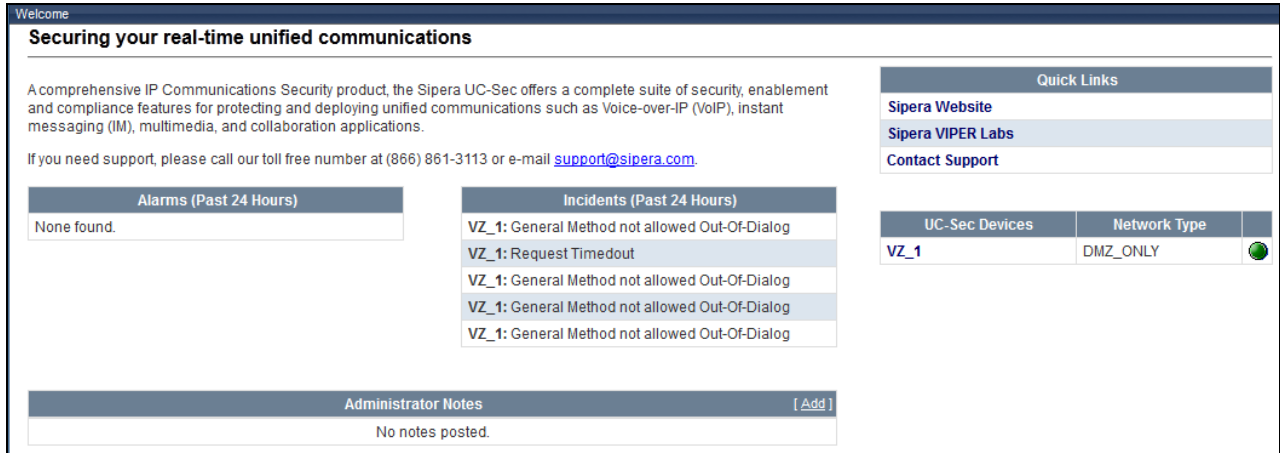
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	ASM	10.80.140.203	5060	TCP	Up	200 OK	Up

Time Last Down	Time Last Up	Last Message Sent	Last Message Response	Last Response Latency (ms)
Aug 23, 2012 3:19:06 PM MDT	Aug 23, 2012 3:21:23 PM MDT	Sep 13, 2012 11:06:01 AM MDT		9


9.4. Avaya Session Border Controller for Enterprise Verification

9.4.1 Welcome Screen

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



The screenshot shows the 'Welcome' page of the UC-Sec interface. The main heading is 'Securing your real-time unified communications'. Below this, a paragraph describes the product as a comprehensive IP Communications Security product. A support contact link is provided. The page is divided into three main sections: Alarms (Past 24 Hours), Incidents (Past 24 Hours), and Administrator Notes. The Alarms section shows 'None found'. The Incidents section lists five incidents, all with the message 'VZ_1: General Method not allowed Out-Of-Dialog'. The Administrator Notes section shows 'No notes posted'. On the right side, there is a 'Quick Links' section with links to 'Sipera Website', 'Sipera VIPER Labs', and 'Contact Support'. Below this is a table showing 'UC-Sec Devices' and 'Network Type'.

UC-Sec Devices	Network Type	Status
VZ_1	DMZ_ONLY	

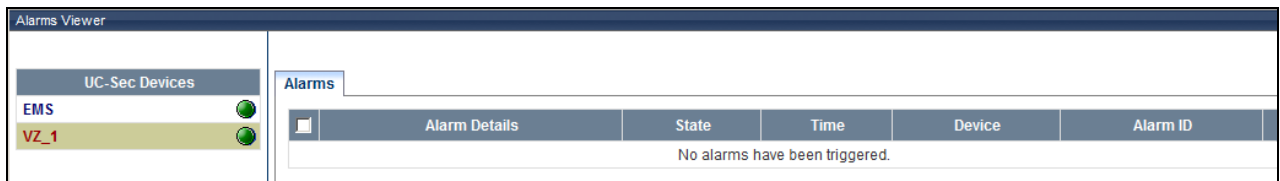
9.4.2 Alarms

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



The screenshot shows the top bar of the UC-Sec Control Center. It features a dark blue header with the text 'UC-Sec Control Center' and 'Welcome ucsec, you signed in as Admin. Current server time is 3:45:21 PM GMT'. Below the header is a navigation bar with icons and labels for 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'.

Alarms Viewer:



The screenshot shows the 'Alarms Viewer' interface. On the left side, there is a sidebar with a 'UC-Sec Devices' section containing 'EMS' and 'VZ_1', both with green status icons. The main area is titled 'Alarms' and contains a table with columns: 'Alarm Details', 'State', 'Time', 'Device', and 'Alarm ID'. The table is currently empty, with the message 'No alarms have been triggered.' displayed below the header.

9.4.3 Incidents

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

Incidents Viewer:

Incident Viewer

Device

All

Category

All

Clear Filters

Refresh

Show Chart

Generate Report

Displaying results 1 to 15 out of 712.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
BYE Message Out of Dialog	665258355113357	2/29/12	11:58 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665258344177160	2/29/12	11:58 AM	Policy	VZ_1	Request Timeout
BYE Message Out of Dialog	665258321513229	2/29/12	11:57 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
ACK Message Out of Dialog	665255354911409	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
REINVITE Message Out of Dialog	665255354909959	2/29/12	10:18 AM	Protocol Discrepancy	VZ_1	General Method not allowed Out-Of-Dialog
Routing Failure	665254922012124	2/29/12	10:04 AM	Policy	VZ_1	Request Timeout
Server Heartbeat	665000194930633	2/23/12	12:33 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	66500000924145	2/23/12	12:26 PM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664988030831612	2/23/12	5:47 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938207935094	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938196326749	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664938193902637	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664938182323645	2/22/12	2:06 AM	Policy	VZ_1	Server Heartbeat is failed
Server Heartbeat	664916847577761	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is UP
Server Heartbeat	664916833545584	2/21/12	2:14 PM	Policy	VZ_1	Server Heartbeat is failed

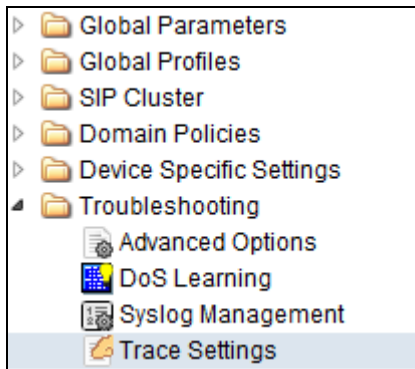
<< < 1 2 3 4 5 > >>

Further Information can be obtained by clicking on an incident in the **Incidents** viewer:

Incident Information				
General Information				
Incident Type	Server Heartbeat		Category	Policy
Timestamp	September 28, 2012 11:14:52 AM GMT		Device	VZ_1
Cause	Server Heartbeat is failed			
Message Data				
Response Code	408		Transport	TCP
Call ID	4bd3324effa6ec46c330fe5cb23cb50eshiepaerrtab		From	sip:ping@10.80.140.141
To	sip:ping@10.80.150.206		Source IP	10.80.150.206
Destination IP	10.80.140.141			

9.4.4 Tracing

To take a call trace, Select **Troubleshooting → Trace Settings** from the left-side menu as shown below.



Select the **Packet Capture** tab and set the desired configuration for a call trace, then press **Start Capture**. Only one interface can be selected at once, so only an inside or only an outside trace is possible.

Packet Trace	Call Trace	Packet Capture	Captures
Packet Capture Configuration			
Currently capturing	No		
Interface	A1		
Local Address (ip:port)	All :		
Remote Address (*, *.port, ip, ip:port)	*		
Protocol	All		
Maximum Number of Packets to Capture	1000		
Capture Filename	Test_trace.pcap		
Existing captures with the same name will be overwritten			
Start Capture Clear			

When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, press the **Stop Capture** button at the bottom (not shown).

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

Packet Trace	Call Trace	Packet Capture	Captures	
				Refresh
File Name		File Size (bytes)	Last Modified	
Test trace_20120229160214.pcap		49,152	February 29, 2012 4:02:26 PM GMT	X

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise Release 4.0.5 can be configured to interoperate successfully with Verizon Business IPCC service.

Avaya Communication Server 1000E Release 7.5 has not been independently certified by Verizon labs. These Application Notes can be used to facilitate customer engagements via the Verizon field trial process, pending Verizon Labs independent certification.

11. Additional References

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 2.2, April 2011 available at <https://downloads.avaya.com/css/P8/documents/100120934>
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, Issue 4.2, November 2011 available at <https://downloads.avaya.com/css/P8/documents/100120937>
- [4] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, November 2010 available at <https://downloads.avaya.com/css/P8/documents/100120857>

Avaya Communication Server 1000E

- [1] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, Issue 05.09
- [2] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, Issue 05.17
- [3] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.10
- [4] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, Issue 03.05
- [5] Signaling Server and IP Line Applications Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, Issue 03.12

Appendix 1: Sigma Script

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

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

  }
}
```

©2012 Avaya Inc. All Rights Reserved.

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

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