



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and Acme Packet Net-Net Session Border Controller 6.2 with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E, Avaya Aura® Session Manager Release 6.1, and Acme Packet Net-Net Session Border Controller Release 6.2, with the Verizon Business Private IP (PIP) IP Trunk service. The optional Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Acme Packet Net-Net Session Border Controllers.

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.

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

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

Table of Contents

1.	Introduction	4
2.	General Test Approach and Test Results	4
2.1.	Interoperability Compliance Testing	5
2.2.	Test Results	6
2.3.	Support	6
2.3.1	Avaya	6
2.3.2	Verizon	7
3.	Reference Configuration	7
3.1.	History-Info and Diversion Headers	9
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	13
5.2.1	Virtual D-Channel Configuration	13
5.2.2	Routes and Trunks Configuration	14
5.3.	SIP Trunk to Session Manager	16
5.4.	Routing of Dialed Numbers to Session Manager	21
5.4.1	Route List Block	21
5.4.2	NARS Access Code	22
5.4.3	Numbering Plan Area Codes	23
5.4.4	Other Special Numbers to Route to Session Manager	24
5.5.	Zones	25
5.6.	Codec Parameters, Including Ensuring Annexb=no for G.729	27
5.6.1	Media Gateway Configuration	27
5.6.2	Node Voice Gateway and Codec Configuration	28
5.7.	Enabling Plug-Ins for Call Transfer Scenarios	30
5.8.	Customer Information	32
5.8.1	Caller ID Related Configuration	32
5.9.	Example CS1000 Telephone Users	34
5.9.1	Example IP UNISTim Phone DN 57003, Codec Considerations	34
5.9.2	Example SIP Phone DN 57007, Codec Considerations	35
5.9.3	Example Digital Phone DN 57005 with Call Waiting	36
5.9.4	Example Analog Port with DN 57021, Fax	37
5.10.	Save Configuration	38
6.	Configure Avaya Aura® Session Manager Release 6.1	39
6.1.	SIP Domain	42
6.2.	Locations	44
6.2.1	Location for Avaya Communication Server 1000E	44
6.2.2	Location for Session Border Controller	45
6.3.	Configure Adaptations	47
6.3.1	Adaptation for Avaya Communication Server 1000E Entity	47
6.3.2	Adaptation for SBC Entity	49
6.3.3	List of Adaptations	50
6.4.	SIP Entities	50

6.4.1	SIP Entity for Avaya Communication Server 1000E	50
6.4.2	SIP Entity for SBC	51
6.5.	Entity Links	53
6.5.1	Entity Link to Avaya Communication Server 1000E Entity	53
6.5.2	Entity Link to SBC	53
6.6.	Routing Policies	54
6.6.1	Routing Policy to Avaya Communication Server 1000E	54
6.6.2	Routing Policy to SBC	55
6.7.	Dial Patterns	57
6.7.1	Inbound Verizon Calls to CS1000E Users	57
6.7.2	Outbound Calls to Verizon	58
7.	Configure Acme Packet Net-Net SBC	60
7.1.	Acme Packet Command Line Interface Summary	60
7.2.	System Configuration, Physical, and Network Interfaces	61
7.3.	Realms	63
7.4.	SIP Configuration	65
7.5.	SIP Interface	65
7.6.	Session Agent	67
7.7.	Session Agent Groups (SAG)	69
7.8.	SIP Manipulation	70
7.8.1	Header Modification for Topology Hiding or Domain Adaptation	70
7.8.2	Stripping Unnecessary SIP Headers and Message Body Information	74
7.9.	Quality Of Service (QoS) Markings for SIP Signaling and RTP Media	76
7.10.	Steering Pools	77
7.11.	Local Policies	77
7.12.	Access Control	79
7.13.	Host Routes	79
8.	Verizon Business IP Trunk Service Offer Configuration	79
8.1.	Fully Qualified Domain Name (FQDN)s	80
8.2.	DID Numbers Assigned by Verizon	80
9.	Verification Steps	80
9.1.	Avaya Communication Server 1000E Verifications	80
9.1.1	IP Network Maintenance and Reports Commands	80
9.1.2	System Maintenance Commands	85
9.2.	Wireshark Verifications	86
9.2.1	Example Outbound Call	86
9.2.2	Example Inbound Call	89
9.3.	System Manager and Session Manager Verification	91
9.3.1	Verify SIP Entity Link Status	91
9.3.2	Call Routing Test	93
9.4.	Acme Packet Net-Net Session Border Controller Verification	95
10.	Conclusion	95
11.	Additional References	95
11.1.	Avaya	95
11.2.	Verizon Business	96
11.3.	Acme Packet	96

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000E (CS1000E), Avaya Aura® Session Manager Release 6.1, and Acme Packet Net-Net Session Border Controller Release 6.2, with the Verizon Business Private IP (PIP) IP Trunk service.

The optional Verizon Business SIP trunk redundant architecture (2-CPE) is supported by dual Acme Packet Net-Net Session Border Controllers (SBCs). The Verizon Business SIP Trunk redundant (2-CPE) architecture provides for redundant SIP trunk access between the Verizon Business IP Trunk service offer and the customer premises equipment (CPE). SIP trunk calls can be automatically re-routed to bypass SIP trunk failures due to network or component outages. The 2-CPE architecture described in these Application Notes is based on a customer location having two Acme Packet Net-Net SBCs.

Avaya Aura® Session Manager can be provisioned for fail-over of outbound calls from one Acme Packet Net-Net SBC to the other, if there is a failure (e.g., timeout, or error response) associated with the first choice. Similarly, the Verizon Business IP Trunk service node will send inbound calls to an Acme Packet Net-Net SBC. If there is a failure (e.g., timeout, or error response), then the call will be sent to the other Acme Packet Net-Net SBC automatically.

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.

Customers using Avaya CS1000E with the Verizon Business IP Trunk SIP Trunk service are able to place and receive PSTN calls via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

Verizon Business IP Trunk service offer can be delivered to the customer premise via either a Private IP (PIP) or Internet Dedicated Access (IDA) IP network terminations. Although the configuration documented in these Application Notes used Verizon's IP Trunk service terminated via a PIP network connection, the solution validated in this document also applies to IP Trunk services delivered via IDA service terminations.

For more information on the Verizon Business IP Trunking service, including access alternatives, visit <http://www.verizonbusiness.com/us/products/voip/trunking/>

2. General Test Approach and Test Results

The Avaya CS1000E location was connected to the Verizon Business IP Trunk Service, as depicted in **Figure 1**. The Avaya equipment was configured to use the commercially available SIP Trunking solution provided by the Verizon Business IP Trunk SIP Trunk Service. This allowed Avaya CS1000E users to make calls to the PSTN and receive calls from the PSTN via the Verizon Business IP Trunk SIP Trunk Service.

2.1. Interoperability Compliance Testing

The testing included executing the test cases detailed in Reference [VZ-Test-Plan], which contains the Verizon Test Suite for VoIP Interoperability for IP Trunking. In the summary below, the relevant test case numbers from [VZ-Test-Plan] are shown parenthetically. The testing included the following successful SIP trunk interoperability compliance testing:

- DNS SRV (TC2) to determine the Verizon IP Trunk SIP signaling information, using UDP for SIP signaling (TC46) and full SIP headers (TC49). The use of DNS SRV is optional, and the configuration was tested with static configuration of the Verizon SIP signaling IP Address and port as well as with the DNS SRV configuration.
- Incoming calls (TC3, TC13) from the PSTN were routed to the DID numbers assigned by Verizon Business to the Avaya CS1000E location. These incoming PSTN calls arrived via the SIP Trunk and were answered by Avaya SIP telephones, Avaya IP UNISTim telephones, Avaya digital telephones, and analog telephones and fax machines. The display of caller ID (TC8) on display-equipped Avaya CS1000E telephones was verified. Avaya CS1000E sends 180 Ringing (without SDP) for calls ringing to an Avaya CS1000E telephone user (TC50).
- Outgoing calls (TC17, TC18, and TC20) from the Avaya CS1000E location to the PSTN were routed via the SIP Trunk to Verizon Business. These outgoing PSTN calls were originated from Avaya SIP telephones, Avaya IP UNISTim telephones, Avaya digital telephones, and analog telephones and fax machines. The display of caller ID (TC36) on display-equipped PSTN telephones was verified. Outbound calls using “fast answer” (Verizon 200 OK without a preceding 18x, TC37) were also tested successfully.
- Proper disconnect when the caller abandoned a call before answer for both inbound (TC6) and outbound (TC19) calls.
- Proper disconnect when the Avaya CS1000E party (TC5, TC17) or the PSTN party (TC4, TC18) terminated an active call.
- Proper busy tone heard when an Avaya CS1000E user called a busy PSTN user (TC43), or a PSTN user (TC7, TC12) called a busy Avaya CS1000E user (i.e., if no redirection was configured for user busy conditions)
- Various outbound PSTN call types were tested including long distance (TC20), international (TC21), toll-free (TC29), operator assisted (TC30-TC34), directory assistance (TC23-TC25), and non-emergency x11 (TC22, TC26, TC28) calls.
- Requests for privacy (i.e., caller anonymity) for Avaya CS1000E outbound calls (TC38) to the PSTN were verified. That is, when privacy is requested by Avaya CS1000E, outbound PSTN calls were successfully completed while withholding the caller ID from the displays of display-equipped PSTN telephones.
- Privacy requests for inbound calls from the PSTN to Avaya CS1000E users were verified. That is, when privacy is requested by a PSTN caller (TC11), the inbound PSTN call was successfully completed to an Avaya CS1000E user while presenting an “anonymous” display to the Avaya CS1000E user.
- SIP OPTIONS monitoring (TC93) of the health of the SIP trunk was verified. Both Verizon Business and the Acme Packet Net-Net Session Border Controller (SBC) were able to monitor health using SIP OPTIONS. .

- Incoming and outgoing voice calls using the G.729(a) (TC60) and G.711 ULAW (TC59) codecs, and proper protocol procedures related to media (TC47, TC48, TC55, TC61).
- DTMF transmission (RFC 2833) for incoming (TC54) and outgoing (TC53) calls
- Inbound (TC14) and outbound (TC42) long holding time call stability.
- Telephony features such as call waiting (TC9), hold (TC56), transfer using re-INVITE (TC65-TC76), and conference (TC89-TC92). Note that CS1000E will not send REFER to the Verizon network.
- Inbound calls from Verizon IP Trunk Service that were call forwarded (TC52) back to PSTN destinations via Verizon IP Trunk Service, presenting true calling party information to the destination PSTN telephone.
- Proper DiffServ markings for SIP signaling (TC64) and RTP (TC63) media.
- Inbound fax (TC10) and outbound fax (TC35) calls. See the following section for fax considerations.
- Inbound (TC98) and outbound G.729a voice calls (TC97) for which intentionally induced ambient fax tone “noise” played to the voice call causes Verizon to issue a re-INVITE to G.711.
- Automatic failover to secondary paths for calls encountering failures of the primary path (TC95). Automatic recovery to full service on restoration from failures (TC95, TC96).

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results. The following observations were noted:

1. At time of writing, T.38 fax was not available on the production Verizon circuit used in the verification of these Application Notes. Fax calls were completed using fax over G.711.
2. Avaya CS1000E does not support sending REFER to Verizon. Incoming Verizon IP Trunk calls that are transferred back out to the PSTN via the Verizon IP Trunk service will continue to traverse the enterprise site (i.e., will not be released via a REFER-based transfer).
3. Assume a call is active between a CS1000E telephone user and a PSTN user “A”. To allow the CS1000E user to transfer the call using the Verizon IP Trunk service to another PSTN user B before user B has answered the call, CS1000E plug-in 501 must be enabled as shown in Section 5.7. While plug-in 501 will allow the CS1000E user to complete the transfer operation, user A will not hear ring back tone while user B is ringing in this case. PSTN users A and B will have two-way talk path once user B answers.

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 IP Trunk 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 IP Trunk SIP Trunk service. The Avaya equipment is located on a private IP network. An enterprise edge router provides access to the Verizon Business IP Trunk service network via a Verizon Business T1 circuit. This circuit is provisioned for the Verizon Business Private IP (PIP) service. The optional Verizon “unscreened ANI” feature is not provisioned on the production circuit used for testing.

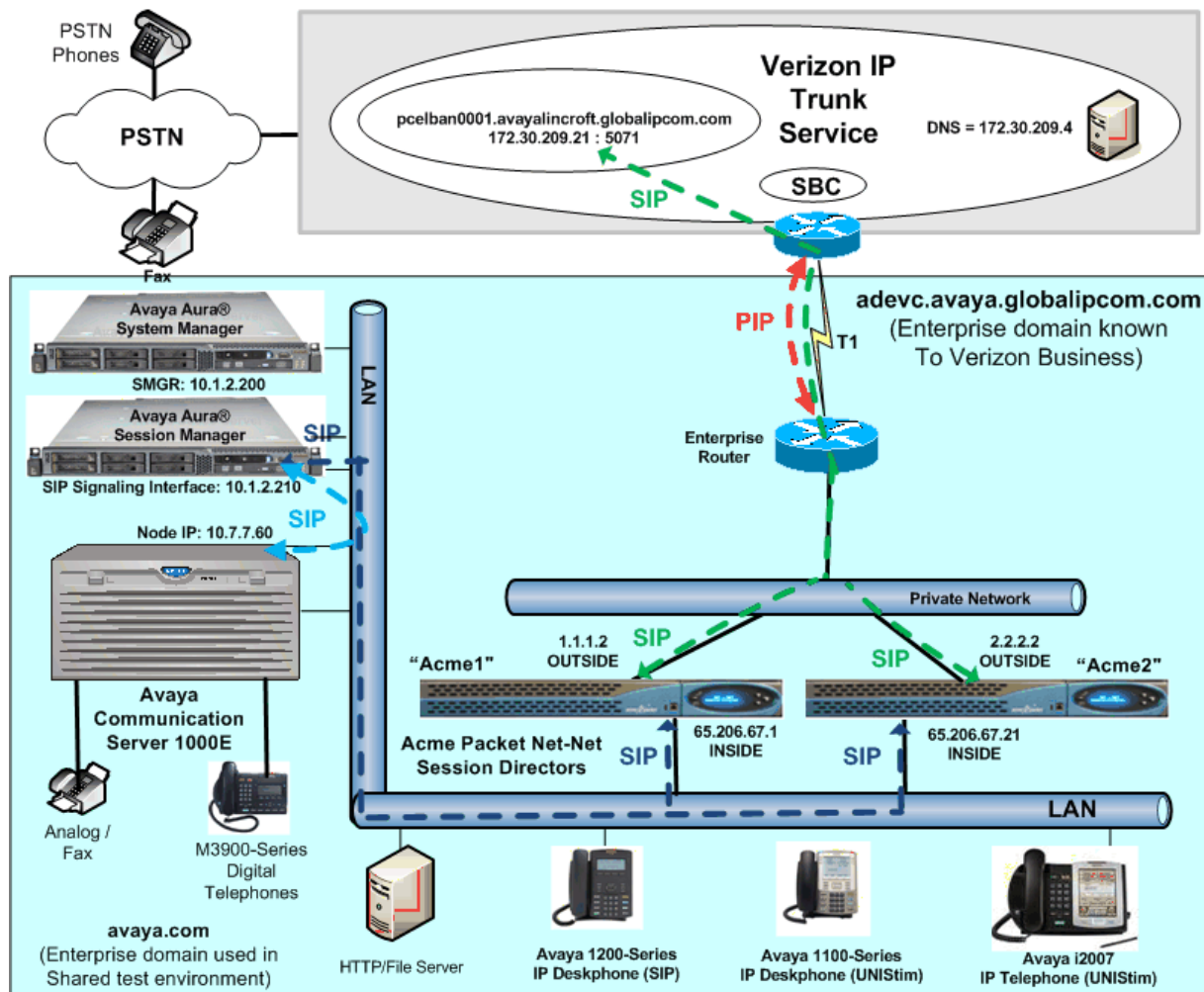


Figure 1: Avaya Interoperability Test Lab Configuration

In the sample configuration, the two Acme Packet Net-Net SBCs labeled “Acme1” and “Acme2” receive traffic from the Verizon Business IP Trunk service on port 5060. The SBCs may be

configured with a static Verizon SIP signaling IP address and port. Alternatively, if DNS SRV is preferred, the SBC can be configured to use DNS SRV to determine the IP Address and port to be used to send SIP signaling to Verizon. In the sample configuration, the DNS process will result in SIP signaling being sent using UDP to IP Address 172.30.209.21 and port 5071.

The Verizon Business IP Trunk service used FQDN *pcelban0001.avayalincroft.globalipcom.com*. The Avaya CPE environment was known to Verizon Business IP Trunk Service as FQDN *adevc.avaya.globalipcom.com*. For efficiency, the Avaya environment utilizing Session Manager Release 6.1 and Communication Server 1000E Release 7.5 was shared among many ongoing test efforts at the Avaya Solution and Interoperability Test lab. Access to the Verizon Business IP Trunk service was added to a configuration that already used domain “avaya.com” at the enterprise. Session Manager is used to adapt the “avaya.com” domain to the domains known to Verizon.

The Verizon Business IP Trunk service provided Direct Inward Dial (DID) numbers that terminated at the Avaya CS1000E location. These DID numbers were mapped to Avaya CS1000E users via an Avaya Aura® Session Manager adaptation. **Table 1** shows a sample mapping of Verizon-provided DID numbers to CS1000E telephone users.

Verizon Provided DID	Avaya CS1000E Destination	Notes
732-945-0231	x57005	Avaya M3903 Digital Telephone
732-945-0235	x57003	Avaya IP Phone 2007 (UNISim)
732-945-0232	x57001	Avaya 1100-Series IP Deskphone (UNISim)
732-945-0236	x57007	Avaya 1200-Series IP Deskphone (SIP)
732-945-0288	x57021	Analog telephone / fax

Table 1: Sample Verizon DID 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.

- Verizon Business IP Trunk network Fully Qualified Domain Name (FQDN)
 - *pcelban0001.avayalincroft.globalipcom.com*
- Avaya CPE Fully Qualified Domain Name (FQDN)
 - *adevc.avaya.globalipcom.com*
- Acme Packet Net-Net 4250 Session Border Controller (SBC)
- Avaya Communication Server 1000E Release 7.5
- Avaya Aura® System Manager Release 6.1
- Avaya Aura® Session Manager Release 6.1

- Avaya IP-2007 UNISTim telephones
- Avaya 1100-Series IP Deskphones using UNISTim software
- Avaya 1200-Series IP Deskphones using SIP software, registered to CS1000E
- Avaya M3900-Series Digital phones
- Analog telephones and fax machines

3.1. History-Info and Diversion Headers

The Verizon Business IP Trunk service does not support SIP History-Info Headers. Instead, the Verizon Business IP Trunk service requires that SIP Diversion Header be sent for redirected calls. The Avaya Communication Server 1000E includes History-Info header in messaging sent to Avaya Aura® Session Manager. Avaya Aura® Session Manager can convert the History Info header into the Diversion Header required by Verizon. This is performed by specifying the “*VerizonAdapter*” adaptation in Avaya Aura® Session Manager. See Section 6.3.

The Avaya Communication Server 1000E call forwarding feature may be used for call scenarios testing Diversion Header.

4. Equipment and Software Validated

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

Equipment	Software
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Release 7.5, Version 7.50.17 (with latest Patches and Deplst) Plug-in 201 Enabled Plug-in 501 Enabled
Avaya S8800 Server (System Manager)	Avaya Aura® System Manager Release 6.1.5.0 (Build Number 6.1.0.0.7345 Patch 6.1.5.7)
Avaya S8800 Server (Session Manager)	Avaya Aura® Session Manager Release 6.1 (Load 6.1.1.0.611023)
Avaya 1100-Series IP Deskphones (UNISTim)	FW 0624C8A
Avaya 1200-Series IP Deskphones (SIP)	SIP 04.00.04.00
Avaya IP Phone 2007 (UNISTim)	FW 0621C8A
Avaya M3900-Series Digital Telephone	N/A
Brother Intellifax 1360	N/A
Acme Packet 4250 ¹ (Session Border Controller)	Release 6.2.0 (SC6.2.0 MR-3 Patch 5 Build 687)

Table 2: Equipment and Software Used in the Sample Configuration

¹ Although an Acme Net-Net 4250 was used in the sample configuration, the 3800, 4500, and 9200 platforms are also supported.

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+PM server platform.

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

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

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

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

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

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

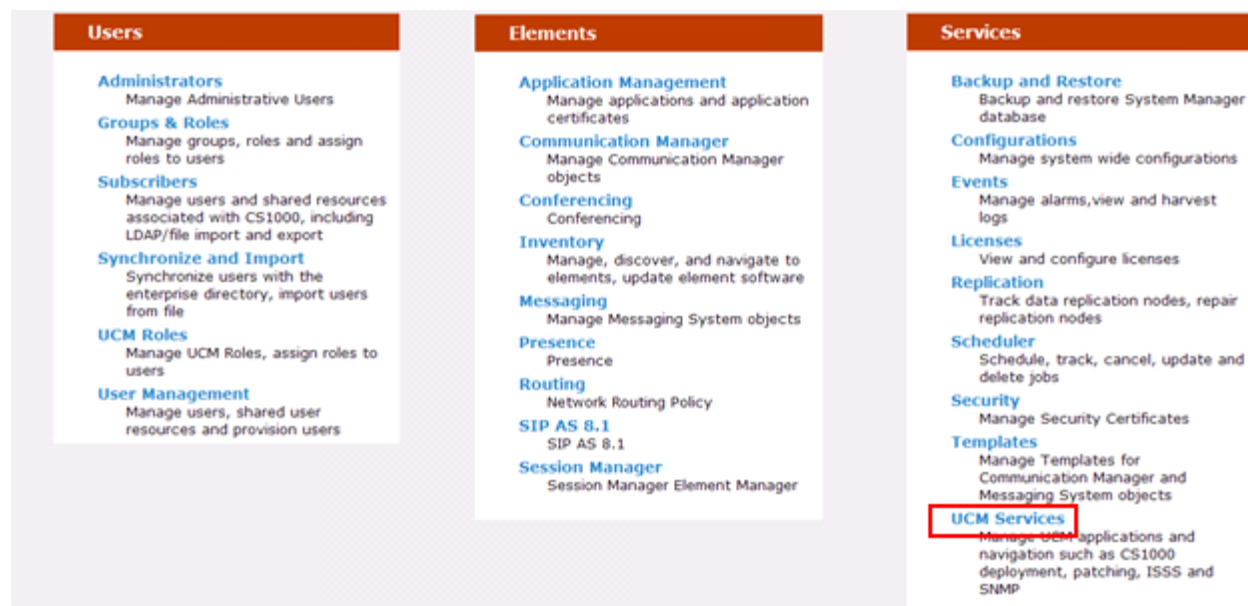
User ID:

Password:

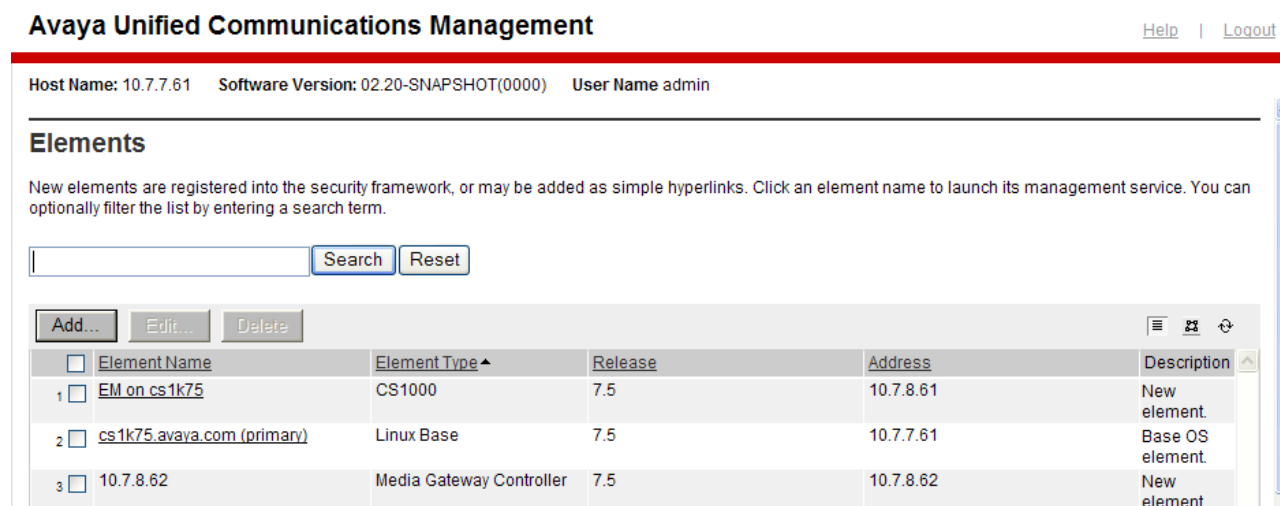
[Change Password](#)

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

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



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



5.1. Node and Key IP Addresses

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

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

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

IP Telephony Nodes

Click the Node ID to view or edit its properties.

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

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

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

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

CS1000 Element Manager

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

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

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Telephony LAN (TLAN)

Gateway IP address: *

Node IPv4 address: *

Subnet mask: *

Subnet mask: *

Node IPv6 address:

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

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

Associated Signaling Servers & Cards

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

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

Show: ☐ IPv6 address

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

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

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

IPMG 4.0 Media Gateway Controller (MGC) Configuration

- Media Gateway Controller	
Hostname	MGC *
Embedded LAN (ELAN) IP address	10.7.8.62
Embedded LAN (ELAN) gateway IP address	10.7.8.1
Embedded LAN (ELAN) subnet mask	255.255.254.0
Telephony LAN (TLAN) IP address	10.7.7.62
Telephony LAN (TLAN) gateway IP address	10.7.7.1
Telephony LAN (TLAN) subnet mask	255.255.255.0
- DSP Daughterboard 1	
Type of the DSP daughterboard	DB96 ▼
Telephony LAN (TLAN) IP address	10.7.7.63
Telephony LAN (TLAN) gateway IP address	10.7.7.1

5.2. Virtual D-Channel, Routes and Trunks

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

5.2.1 Virtual D-Channel Configuration

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

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

D-Channels

Maintenance

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

Configuration

Choose a D-Channel Number: and type:

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

5.2.2 Routes and Trunks Configuration

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

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

Routes and Trunks

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

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

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

Customer 0, Route 1 Property Configuration

- Basic Configuration

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

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

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

5.3. SIP Trunk to Session Manager

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

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

Managing: 10.7.8.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

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

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

- **SIP domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, “**avaya.com**” was used in the shared Avaya Solution and Interoperability Test lab environment. The SIP domain name for the enterprise known to Verizon is “**adevc.avaya.globalipcom.com**”, and the SIP domain will be adapted by Session Manager for calls to and from the Avaya CS1000E.
- **Local SIP port:** Enter “**5060**”
- **Gateway endpoint name:** Enter descriptive name
- **Application node ID:** Enter “**<Node id>**”. In the sample configuration, Node “**2**” was used matching the node shown in Section 5.1.

The values defined for the sample configuration are shown below.

Managing: 10.7.8.61 Username: admin

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

Node ID: 2 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIPGw and H.323Gw
SIP domain name: avaya.com *
Local SIP port: 5060 * (1 - 65535)
Gateway endpoint name: CS1KGateway *
Gateway password: *
H.323 ID: CS1KGateway *
Application node ID: 2 * (0-9999)
Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

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

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

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

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

The values defined for the sample configuration are shown below.

Node ID: 2 - Virtual Trunk Gateway Configuration Details

The screenshot shows the 'SIP Gateway Settings' tab selected in a configuration interface. Under the 'Proxy Or Redirect Server:' section, 'Proxy Server Route 1:' is expanded. It contains fields for 'Primary TLAN IP address' (10.1.2.210), 'Port' (5060), and 'Transport protocol' (TCP). Below these are two unchecked checkboxes: 'Support registration' and 'Primary CDS proxy'. A 'Secondary TLAN IP address' field is also present, set to 0.0.0.0, with its own 'Port' (5060) and 'Transport protocol' (TCP) fields. A vertical scrollbar is visible on the right side of the configuration area.

General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.1.2.210
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

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

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

Node ID: 2 - Virtual Trunk Gateway Configuration Details

General SIP Gateway Settings SIP Gateway Services H.323 Gateway Settings	
SIP URI Map:	
Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text"/>
Subscriber: <input type="text"/>	CDP: <input type="text" value="cdp udp"/>
Special number: <input type="text"/>	Special number: <input type="text"/>
Unknown: <input type="text"/>	Vacant number: <input type="text"/>
	Unknown: <input type="text"/>

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

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

Managing: 10.7.8.61 Username: admin System » IP Network » IP Telephony Nodes » Node Saved	
Node Saved	
Node ID: 2 has been saved on the call server.	
The new configuration must also be transferred to associated servers and media cards.	
<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.

Synchronize Configuration Files (Node ID <2>)

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

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

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

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

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

Synchronize Configuration Files (Node ID <2>)

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

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

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

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

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

Synchronize Configuration Files (Node ID <2>)

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

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

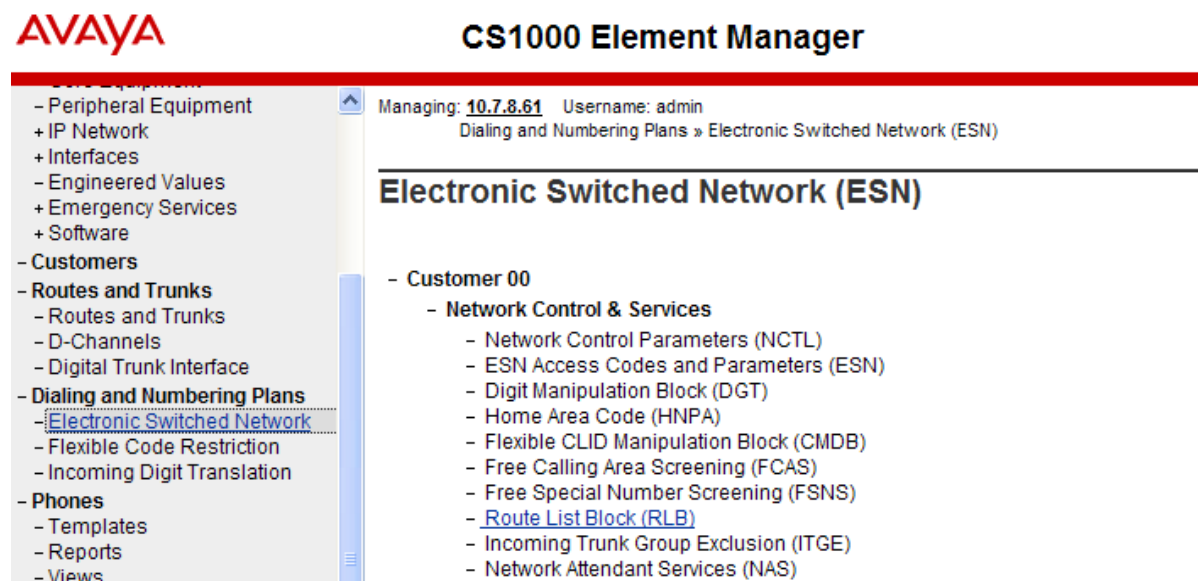
<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k75	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

5.4. Routing of Dialed Numbers to Session Manager

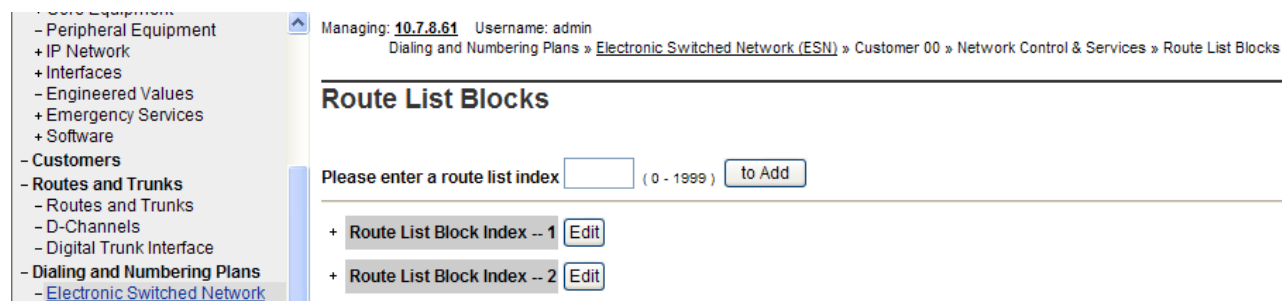
This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the Verizon IP Trunk service. The routing defined in this section is simply an example and not intended to be prescriptive. The example will focus on the configuration enabling a CS1000E telephone user to dial 9-1-908-848-5704 to reach a PSTN telephone using the Verizon IP Trunk 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.



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 1 is used.



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

+ **Data Entry Index -- 0** **Edit**

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

Indexes

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

Options

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

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

5.4.2 NARS Access Code

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

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1:

NARS Access Code 2:

NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☒

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

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

5.4.3 Numbering Plan Area Codes

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

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with the following items: Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Software, Customers, Routes and Trunks, D-Channels, Digital Trunk Interface, Dialing and Numbering Plans (selected), Electronic Switched Network (selected), Flexible Code Restriction, Incoming Digit Translation, Phones, and Templates. The main panel displays the configuration for Access Code 1 under the Numbering Plan (NET) section. The configuration includes: Flexible CLID Manipulation Block (CLMB), Free Calling Area Screening (FCAS), Free Special Number Screening (FSNS), Route List Block (RLB), Incoming Trunk Group Exclusion (ITGE), Network Attendant Services (NAS), Coordinated Dialing Plan (CDP), Local Steering Code (LSC), Distant Steering Code (DSC), Trunk Steering Code (TSC), and Access Code 1. Under Access Code 1, the following options are listed: Home Location Code (HLOC), Location Code (LOC), Numbering Plan Area Code (NPA) (selected), Exchange (Central Office) Code (NXX), and Special Number (SPN).

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

Numbering Plan Area Code List

Please enter an area code

- + Numbering Plan Area Code -- 1712
- + Numbering Plan Area Code -- 1732
- + Numbering Plan Area Code -- 1800
- + Numbering Plan Area Code -- 1900
- + Numbering Plan Area Code -- 1908
- + Numbering Plan Area Code -- 1976

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

Numbering Plan Area Code

General Properties

Numbering Plan Area code translation:

Route List Index:

Incoming Trunk group Exclusion Index:

5.4.4 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 IP Trunk 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** “1” 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.

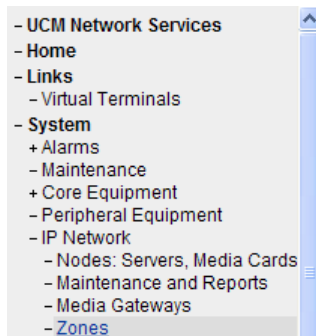
Special Number List

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.

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

Zones

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

Bandwidth Zones

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

Numbering Zones

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

Select **Bandwidth Zones**. In the sample configuration, two zones are configured as shown below.

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

Managing: 10.7.8.61 Username: admin
System » IP Network » [Zones](#) » Bandwidth Zones

Bandwidth Zones

<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Import..."/> <input type="button" value="Export"/> <input type="button" value="Maintenance..."/> <input type="button" value="Delete"/>								
	Zone *	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	1000000	BB	1000000	BB	SHARED	VTRK	VTRKZONE
2	2	1000000	BQ	1000000	BQ	SHARED	MO	IPPHONES

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

Managing: **10.7.8.61** Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 1 » 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 1 configuration. Note that “Best Bandwidth (BB)” is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with Verizon IP Trunk service.

Managing: **10.7.8.61** Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 1 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	1 (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):	VTRKZONE

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

Verizon IP Trunk 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 a web-based configuration interface for media gateways. On the left is a navigation tree with the following structure:

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
 - + Alarms
 - Maintenance
 - Core Equipment
 - Loops
 - Superloops
 - MSDL/MISP Cards
 - Conference/TDS/Multifrequen
 - Tone Senders and Detectors
 - 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
 - Application Module Link

The main content area is divided into two sections for DSP Daughterboards:

- DSP Daughterboard 1

- Type of the DSP daughterboard: DB96
- Telephony LAN (TLAN) IP address: 10.7.7.63
- Telephony LAN (TLAN) gateway IP address: 10.7.7.1
- Telephony LAN (TLAN) IPv6 address: (empty field)
- Telephony LAN (TLAN) subnet mask: 255.255.255.0
- Hostname: CS1KR7DSP1 *

- DSP Daughterboard 2

- Type of the DSP daughterboard: NODB
- Telephony LAN (TLAN) IP address: 0.0.0.0
- Telephony LAN (TLAN) gateway IP address: 10.7.7.1
- Telephony LAN (TLAN) IPv6 address: (empty field)
- Telephony LAN (TLAN) subnet mask: 255.255.255.0
- Hostname: DB2 *

At the bottom, there is a section labeled **+ VGW and IP phone codec profile**.

Expand **VGW and IP phone codec profile**. To use G.729A with Verizon IP Trunk 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** “20” can be used with Verizon IP Trunk 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, as shown in the example Wireshark trace illustration in Section 9.2.1. The following screen shows the parameters used.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, and Customers. The main area displays configuration for two codecs: G711 and G729A. For each codec, there are settings for Codec name, Voice payload size (set to 20 ms/frame), Voice playback (jitter buffer) nominal delay (set to 40), and Voice playback (jitter buffer) maximum delay (set to 80). A red warning message states 'Modifications may cause changes to dependent settings'. The VAD checkbox is unchecked for both codecs.

5.6.2 Node Voice Gateway and Codec Configuration

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

The screenshot shows the AVAYA CS1000 Element Manager interface with the 'IP Telephony Nodes' section selected. The table below lists the configured nodes.

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

Below the table, there are filters: 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.

Node ID: 2 - 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, as shown in the example Wireshark trace illustration in Section 9.2.1.

AVAYA **CS1000 Element Manager**

Managing: 10.7.8.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

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

General | Voice Codecs | Fax

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

5.7. Enabling Plug-Ins for Call Transfer Scenarios

Plug-ins allow specific CS1000E software feature behaviors to be changed. In the testing associated with these Application Notes, two plug-ins were enabled as shown in this section.

To view or enable a plug-in, from the left navigation menu, expand **System** → **Software**, and select **Plug-ins**. In the right side screen, a list of available plug-ins will be displayed along with the associated MPLR Number and Status. Use the scroll bar on the right to scroll down so that Plug-in 501 is displayed as shown in the screen below. If the **Status** is “Disabled”, select the check-box next to Number 501 and click the **Enable** button at the top, if it is desirable to allow CS1000E users to complete call transfer to PSTN destinations via the Verizon IP Trunk service before the call has been answered by the PSTN user. This scenario corresponds to test cases 70 and 72 from reference [VZ-Test-Plan]. 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.

Managing: Username: System » Software » Plug-ins

Plug-ins

Enable Disable [Print](#)

<input type="checkbox"/>	Number	Description	MPLR Number	Status
86	223	PLACUM REJECTS QSIG CCBS REQUEST WITH NO CALLING NUMBER	MPLR12290	Disabled
87	224	PI: No busy treatment on external transfer through application if OUT_T306 > 0	MPLR24676	Disabled
88	225	PI: PKG 179, Taurus, electronic look, Mail and CallPilot softkeys	MPLR22389	Disabled
89	226	PI: ACLID should display more than 10 digits	MPLR15783	Disabled
90	228	PI: TTY 0 on CPU card (8/1/N) causes cursor to go up on VDU	MPLR07613	Disabled
91	230	PI: Unplugged telset disables after midnight routines.	MPLR11700	Disabled
92	231	PI: BRI 64K data not possible over DTI2. With mix of spans (both DTI and DTI2) THIS is not supported.	MPLR10878	Disabled
93	232	PI: QSIG GF: No diverting and originally called number in DLI2 APDU on calls from MCDN TRO-BA.	MPLR24273	Disabled
94	233	MWI (High Voltage) Support for CLASS set with CLS LPA	MPLR16506	Disabled
95	235	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
96	500	NO DESCRIPTION	MPLR21979	Disabled
97	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Disabled

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

97	<input checked="" 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	PR1232 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. Plug-in 201 will allow a CS1000E user to make a call to the PSTN using the Verizon IP Trunk service, and then

subsequently perform an attended transfer of the call to another PSTN destination via the Verizon IP Trunk service. This scenario corresponds to test case 66 from reference [VZ-Test-Plan].

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

Managing: Username: System » Software » Plug-ins

Plug-ins

[Print](#)

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

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

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

5.8. Customer Information

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

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

ISDN and ESN Networking

General Properties

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

Calling Line Identification

Information for incoming/outgoing calls:

5.8.1 Caller ID Related Configuration

In the sample configuration, the CS1000E would send the user's five-digit directory number in SIP headers such as the From and PAI headers. Avaya Aura® Session Manager would adapt the user's directory number to an appropriate Verizon IP Trunk DID number before passing the message to the Acme Packet Net-Net SBC towards Verizon.

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

Calling Line Identification Entries

Search for CLID

Start range :

End range :

'End range' should not exceed the CLID size specified

Calling Line Identification Entries

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

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

Calling Party Name Display

Roman characters: ☒

CPND Name:

first name, last name

Expected Length: 13

Display Format:

5.8.1.1 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 IP Trunk service (i.e., test cast 38 from reference [VZ-Test-Plan]) is to set **CLBA Calling Party Privacy** to “Allowed” via the Phone **Features** in Element Manager as shown below.

Feature	Description	
CFTA	Call Forward by Call Type	<input type="button" value="Allowed"/>
CFXA	Call Forward External	<input type="button" value="Allowed"/>
CLBA	Calling Party Privacy	<input type="button" value="Denied"/>
CLRO	Calling Number Restriction Override	<input type="button" value="Allowed"/> <input type="button" value="Denied"/>

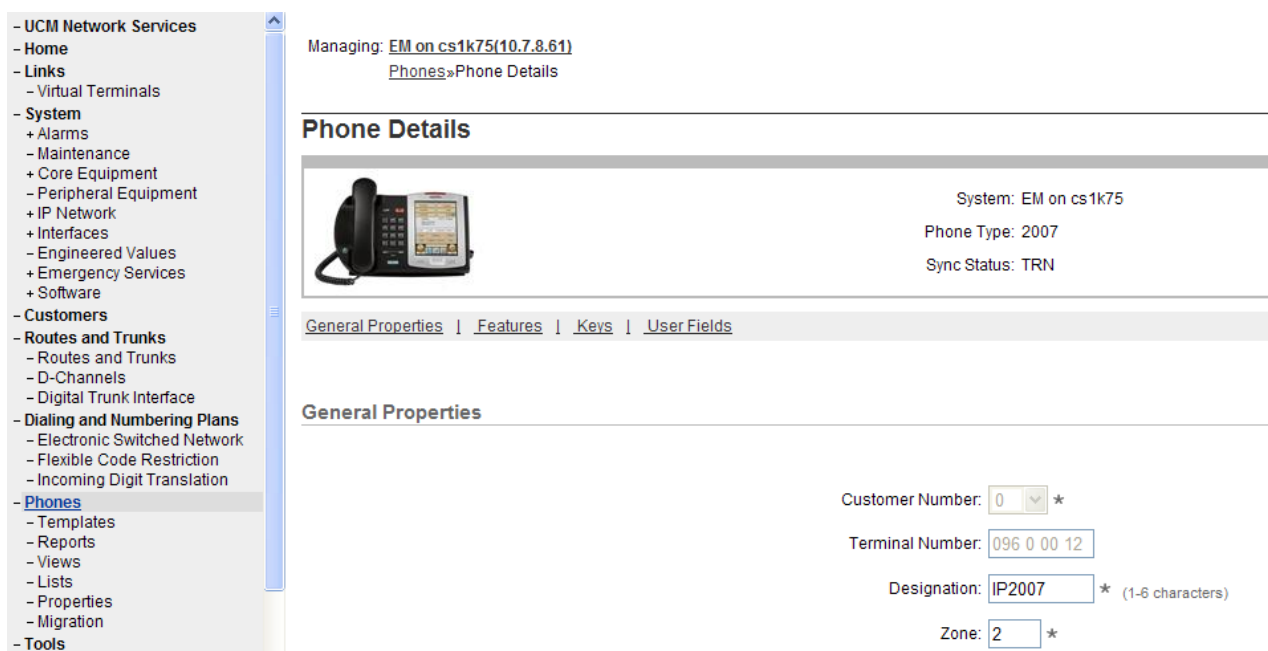
Another means to have the CS1000E request privacy (i.e., Privacy: id in SIP INVITE) for an outbound call from a specific phone to the Verizon IP Trunk service is to set **DDGA Present/Restrict Calling Number** to “Denied” via the Phone **Features** in Element Manager (not shown).

5.9. Example CS1000 Telephone Users

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

5.9.1 Example IP UNISTim Phone DN 57003, Codec Considerations


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



The screenshot displays the Avaya Session Manager configuration interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Phones' category is selected. The main area shows the configuration for a phone managed by 'EM on cs1k75(10.7.8.61)'. The 'Phone Details' section includes a photo of a phone and metadata: System: EM on cs1k75, Phone Type: 2007, and Sync Status: TRN. Below this is a tabbed interface with 'General Properties' selected. The 'General Properties' section contains fields for Customer Number (0), Terminal Number (096 0 00 12), Designation (IP2007), and Zone (2), each with an asterisk indicating a required field. A note next to the Designation field specifies '(1-6 characters)'.

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

Phone Details

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

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

General Properties

Customer Number: *

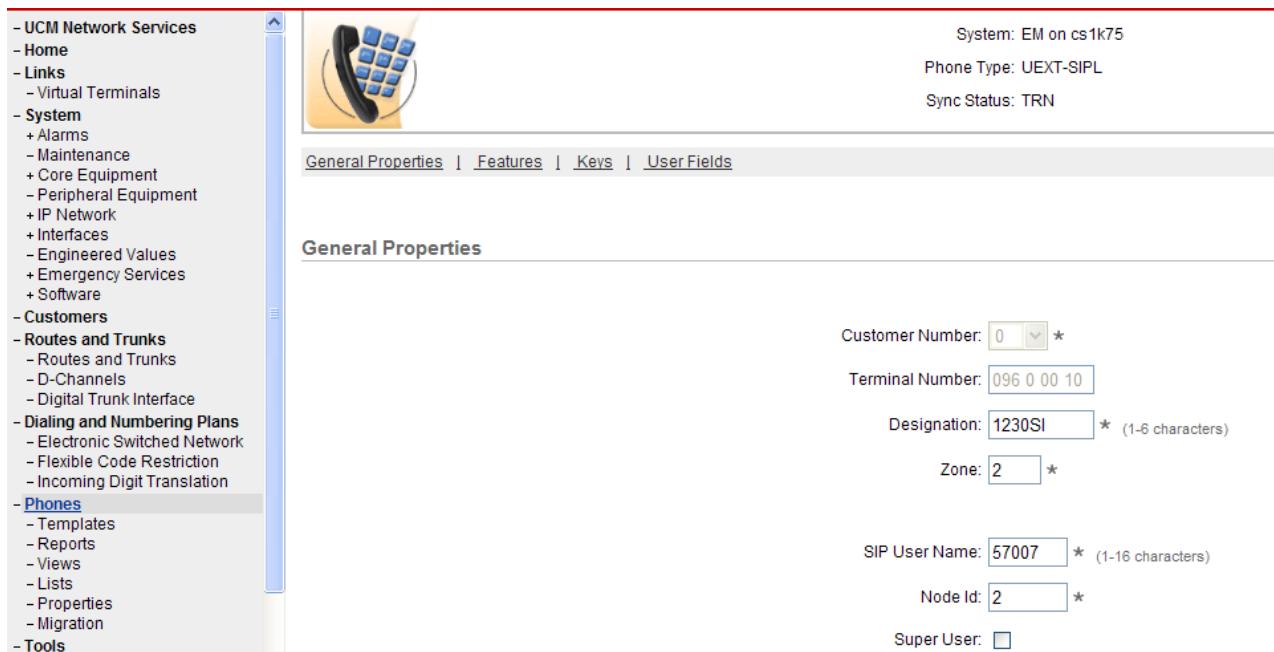
Terminal Number:

Designation: * (1-6 characters)

Zone: *

5.9.2 Example SIP Phone DN 57007, Codec Considerations

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



The screenshot displays the configuration page for a SIP phone in the UCM Network Services interface. On the left is a navigation menu with categories like Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Phones' section is currently selected. The main content area shows the 'General Properties' tab for a phone with the icon of a telephone handset. At the top right, system information is displayed: 'System: EM on cs1k75', 'Phone Type: UEXT-SIPL', and 'Sync Status: TRN'. Below this is a tabbed interface with 'General Properties', 'Features', 'Keys', and 'User Fields'. The 'General Properties' tab is active, showing fields for 'Customer Number' (0), 'Terminal Number' (096 0 00 10), 'Designation' (1230SI), 'Zone' (2), 'SIP User Name' (57007), 'Node Id' (2), and a 'Super User' checkbox. Each field has a required field asterisk and some have character count hints.

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

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

General Properties

Customer Number: 0 *

Terminal Number: 096 0 00 10

Designation: 1230SI * (1-6 characters)

Zone: 2 *

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

Node Id: 2 *

Super User: ☐


5.9.3 Example Digital Phone DN 57005 with Call Waiting

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

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

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

Phone Details

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

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

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

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

The screenshot displays the 'Keys' configuration page. It features a table with columns for Key No., Key Type, and Key Value. Key 0 is configured as 'SCR - Single Call Ringing' with a Directory Number of 57005. Key 1 is configured as 'CWT - Call Waiting'. To the right of the table, there are additional configuration options for Key 0, including a checkbox for 'Multiple Appearance Redirection Prime(MARP)', fields for First Name (CS1KR7), Last Name (Digital), Display Format (First, Last), and Language (Roman). There are also fields for CLID Entry (Numeric or D) and ANIE Entry.

Keys

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

5.9.4 Example Analog Port with DN 57021, Fax

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

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, Tools, and Security. The 'Phones' category is selected. The main area is titled 'Phone Details' and shows a phone icon. To the right of the icon, it says 'System: EM on cs1k75', 'Phone Type: 2500', and 'Sync Status: TRN'. Below this is a tabbed interface with 'General Properties' selected. The 'General Properties' section contains fields for 'Customer Number' (0), 'Terminal Number' (004 0 03 00), 'Designation' (ANLG1), and 'Directory Number' (57021). A search icon is next to the Directory Number field.

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

Phone Details

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

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

General Properties

Customer Number: *

Terminal Number:

Designation: * (1-6 characters)

Directory Number: 🔍

When an analog port is used for a fax machine, Modem Pass Through Allowed (MPTA) can be set to cause G.711 to be used, even if the zone configuration would otherwise have resulted in G.729. For example, if MPTA is configured, and an inbound call arrives from Verizon IP Trunk Service, the CS1000E will respond with a 200 OK, selecting G.711 for the call in the SDP answer, even if the SDP offer from Verizon listed G.729 before G.711. Similarly, for an outbound call with MPTA configured, the CS1000E will send the INVITE with an SDP offer for G.711. Recall that T.38 was not available from Verizon using the production Verizon circuit used for the testing associated with these Application Notes.

To configure MPTA, scroll down to the **Features** area and locate the feature with description “Modem Pass Through”. From the drop-down menu, select “MPTA” as shown below.

Features

Feature	Description	
MINA	Message Intercept Treatment	Denied ▾
MLWU_LANG	Language for Automatic Wake Up	Language 0 (RAN1/RAN2) ▾
MPT	Modem Pass Through	MPTA ▾

5.10. Save Configuration

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

The screenshot displays the Avaya Communication Server 1000E web interface. On the left is a navigation tree with categories: System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Tools' category is expanded, showing 'Backup and Restore' and 'Call Server'. The 'Call Server' option is selected. The main content area shows the 'Call Server Backup' page. At the top, it indicates 'Managing: 10.7.8.61' and 'Username: admin'. Below this is a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The page title is 'Call Server Backup'. There is an 'Action' label followed by a dropdown menu currently set to 'Backup'. To the right of the dropdown are 'Submit' and 'Cancel' buttons.

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

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

The configuration of Avaya Communication Server 1000E is complete.

6. Configure Avaya Aura® Session Manager Release 6.1

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

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two. For more information, consult the references in Section 11.

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 Acme Packet Net-Net SBC(s).

The following administration activities will be described:

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

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

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



Avaya Aura® System Manager 6.1

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

Log On

Recommended access to System Manager is via FQDN.

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

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

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

User ID:

Password:

[Change Password](#)

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

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

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

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

6.1. SIP Domain

Select **Domains** from the left navigation menu. Two domains can be added, one for the enterprise SIP domain, and one for the Verizon network SIP domain. In the shared environment of the Avaya Solution and Interoperability Test lab, a domain “avaya.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. Click **Commit** when finished.

- **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 ? Commit Cancel

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. Click **Commit** when finished.

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

Home / Elements / Routing / Domains- Domain Management

Domain Management Help ? Commit Cancel

1 Item | Refresh Filter: Enable

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

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

Home / Elements / Routing / Domains- Domain Management

Domain Management Help ? Commit Cancel

1 Item | Refresh Filter: Enable

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

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

Domain Management

Edit
New
Duplicate
Delete
More Actions ▾

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

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

Location Pattern

<input type="button" value="Add"/> <input type="button" value="Remove"/>		
1 Item Refresh		
<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.7.7.60	CS1000 7.5 TLAN

6.2.2 Location for Session Border Controller

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

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

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

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

Click **Commit** to save.

The screen below shows the top portion of the screen for the Location defined for the Acme Packet SBC named “Acme1”.

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

Location Details

General

* **Name:**

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Scrolling down, the following screen shows the lower portion of the Location for “Acme1”. The **IP Address Pattern** is the “inside” or private IP Address (67.206.67.1) of the SBC “Acme1”.

Location Pattern

1 Item | [Refresh](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 65.206.67.1	

Select : All, None

If two enterprise SBCs are being used in a Verizon “2-CPE” configuration, the procedure may be repeated to associate a named location with the second SBC. The following screen shows the top portion of the Location Details for the SBC named “Acme2”.

Location Details

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

The following screen shows the bottom portion of the Location Details for the SBC named “Acme2”. The **IP Address Pattern** is the “inside” or private IP Address (67.206.67.21) of the SBC “Acme2”.

Location Pattern

1 Item | [Refresh](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 65.206.67.21	Inside IP of Acme2

Select : All, None

6.3. Configure Adaptations

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

6.3.1 Adaptation for Avaya Communication Server 1000E Entity

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

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

Home / Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

* Adaptation name:	<input type="text" value="CS1000"/>
Module name:	<input type="text" value="CS1000Adapter"/>
Module parameter:	<input type="text" value="osrcd=avaya.com odstd=avaya.com"/>
Egress URI Parameters:	<input type="text"/>
Notes:	<input type="text" value="CS1000 7.5"/>

Scrolling down, in the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from CS1000E users to Verizon. The text below and the screen example that follows explain how to use Session Manager to convert between CS1000E directory numbers and the corresponding Verizon DID numbers.

- **Matching Pattern** Enter Avaya CS1000E extensions (or extension 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., 5)
- **Max** Enter maximum number of digits (e.g., 5)
- **Phone Context** Enter value of **Private CDP domain name** defined in the CS1000E for any patterns matching SIP endpoints registered to Session Manager.
- **Delete Digits** Enter “0”, unless digits should be removed from dialed number before routing by Session Manager. For CS1000E extension conversion to the corresponding Verizon DID, enter the number of digits in the extension to remove all digits.
- **Insert Digits** Enter the Verizon DID corresponding to the matched extension.
- **Address to modify** Select “both”

Notes:

Digit Conversion for Incoming Calls to SM

Add

Remove

5 Items

Refresh

Filter: Ena

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

Scroll down and make corresponding changes in the **Digit Conversion for Outgoing Calls from SM** section for calls from Verizon to CS1000E users.

Digit Conversion for Outgoing Calls from SM

Add

Remove

10 Items

Refresh

Filter: Ena

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7329450231	* 10	* 10		* 10	57005	both ▼	Verizon DID to CS1K Digital
<input type="checkbox"/>	* 7329450235	* 10	* 10		* 10	57003	both ▼	Verizon DID to CS1K IP-Uni
<input type="checkbox"/>	* 7329450236	* 10	* 10		* 10	57007	both ▼	Verizon DID to CS1K SIP ph
<input type="checkbox"/>	* 7329450288	* 10	* 10		* 10	57021	both ▼	Verizon DID to CS1K analog

As an example, using these screens, CS1000E extension user 57003 corresponds to Verizon IP Trunk Service DID 732-945-0235. **Table 1** in Section 3 lists other example mappings.

Click **Commit**.

6.3.2 Adaptation for SBC Entity

The adaptation shown in this section will be assigned to the SIP entity for each SBC, as shown in Section 6.4.2.

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

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select “**VerizonAdapter**” from drop-down menu (or add an adapter with name “VerizonAdapter” if not previously defined)
- **Module Parameter:** Enter “osrcd=<CPE-domain-known-to-Verizon>.com” and “odstd=<Verizon-domain>.com”. The <CPE-domain-known-to-Verizon> is the SIP domain for the CPE configured in the Verizon network (i.e., the SIP domain Verizon would expect in the P-Asserted-Identity for a call from the CPE to the PSTN), and <Verizon-domain> is the Verizon network SIP domain (i.e., the SIP domain Verizon would expect in the Request-URI for an INVITE sent from the CPE to the PSTN). Enter “fromto=true” to allow the From and To headers to be modified by Session Manager (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers). Although not used in the sample configuration, note that Session Manager Release 6.1 introduces a new module parameter that may be used as an alternative to using the SBC to remove multipart MIME message bodies. The rationale and SBC configuration for sending only SDP in the message body to Verizon is shown in Section 7.8.2. To have Session Manager strip MIME message bodies on egress to the SBC, such that only SDP is present in the message body sent to the SBC, “MIME=no” can be entered as a module parameter.

Home / Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

* Adaptation name:	<input type="text" value="History_Diversion_IPT"/>
Module name:	<input type="text" value="VerizonAdapter"/>
Module parameter:	<input type="text" value="osrcd=adevc.avaya.globalipcom.c"/>
Egress URI Parameters:	<input type="text"/>
Notes:	<input type="text"/>

Click **Commit**.

6.3.3 List of Adaptations

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

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

6.4. SIP Entities

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

6.4.1 SIP Entity for Avaya Communication Server 1000E

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

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

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

In the **SIP Link Monitoring** section:

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

Click **Commit** to save the definition of the new SIP Entity.

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

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

SIP Entity Details

General

* **Name:** CS1000-R75

* **FQDN or IP Address:** 10.7.7.60

Type: SIP Trunk

Notes: CS1000 7.5

Adaptation: CS1000

Location: CS1K75-Location

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.2 SIP Entity for SBC

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

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

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

In the **SIP Link Monitoring** section:

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

The following screen shows the SIP Entity defined for the Acme Packet Net-Net SBC named “Acme1” in the sample configuration.

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

SIP Entity Details

Commit

General

* Name:

Acme1

* FQDN or IP Address:

65.206.67.1

Type:

Other

Notes:

Inside IP Acme1

Adaptation:

History_Diversion_IPT

Location:

Acme1

Time Zone:

America/New_York

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

If two enterprise SBCs are being used in a Verizon “2-CPE” configuration, the procedure may be repeated to create a SIP entity for the second SBC. The following screen shows the SIP Entity defined for the SBC named “Acme2”.

SIP Entity Details

Commit

General

* Name:

Acme2

* FQDN or IP Address:

65.206.67.21

Type:

Other

Notes:

Acme2 Inside

Adaptation:

History_Diversion_IPT

Location:

Acme2

Time Zone:

America/New_York

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

6.5. Entity Links

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

6.5.1 Entity Link to Avaya Communication Server 1000E Entity

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

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

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

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

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

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	Trusted	Notes
* CS100075-Link	* SM1	TCP	* 5060	* CS1000-R75	* 5060	<input checked="" type="checkbox"/>	CS1000 R7.5

6.5.2 Entity Link to SBC

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

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

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

The following screen shows the entity link defined for the SIP trunk between Session Manager and the Acme Packet Net-Net SBC named “Acme1”.

Home / Elements / Routing / Entity Links- Entity Links

Entity Links Commit

1 Item Refresh Filter:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* Acme1	* SM1	TCP	* 5060	* Acme1	* 5060	<input checked="" type="checkbox"/>	

If two enterprise SBCs are being used in a Verizon “2-CPE” configuration, the procedure may be repeated to create an entity link between Session Manager and a second SBC. The following screen shows the entity link defined for the SIP trunk between Session Manager and the Acme Packet Net-Net SBC named “Acme2”.

Entity Links Commit

1 Item Refresh Filter:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* Acme2	* SM1	TCP	* 5060	* Acme2	* 5060	<input checked="" type="checkbox"/>	

6.6. Routing Policies

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

6.6.1 Routing Policy to Avaya Communication Server 1000E

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

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

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

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

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

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

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

Routing Policy Details Commit Cancel routing Help ?

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

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

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

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

6.6.2 Routing Policy to SBC

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

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

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

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

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

The following screen shows the Routing Policy for the Acme Packet Net-Net SBC named “Acme1”.

Routing Policy Details

Commit C

General

* Name: Acme1-to-VZ

Disabled: ☐

Notes: Outbound to Verizon via Acme1

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Acme1	65.206.67.1	Other	Inside IP Acme1

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh

Filter: En

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

If two enterprise SBCs are being used in a Verizon “2-CPE” configuration, the procedure may be repeated to create a routing policy for the second SBC. The following screen shows the Routing Policy for the Acme Packet Net-Net SBC named “Acme2”. To allow “Acme2” to receive outbound calls from Session Manager even when “Acme1” is operational, the default **Ranking** of 0 (also assigned to “Acme1”) can be retained. If it is intended that Acme1 should always be tried by Session Manager before Acme2, the **Ranking** of Acme2 can be changed to a larger number such as “1”. Both the “load sharing” approach where Acme1 and Acme2 use the same ranking and the strict rank order priority approach were successfully tested in the sample configuration.

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

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Acme2	65.206.67.21	Other	Acme2 Inside

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enabled

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

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 IP Trunk Service. Other dial patterns will be configured to route inbound calls from Verizon IP Trunk 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 DID number)
- **Min:** Enter the minimum number of digits.
- **Max:** Enter the maximum number of digits.
- **SIP Domain:** Select a SIP Domain from drop-down menu or select “All” if Session Manager should route incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

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

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

- In the **Originating Location** list, select “**Apply the Selected Routing Policies to All Originating Locations**” or alternatively, select a specific location. In the example below, the specific SBC locations were selected as the originating locations.
- In the **Routing Policies** table, select the Routing Policy defined for Avaya Communication Server 1000E.

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

Click **Commit** to save. The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional Verizon DID 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

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain: -ALL- ▼

Notes:

Originating Locations and Routing Policies

2 Items | [Refresh](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	Acme1	Acme Net-Net Inside	CS1K-R75-RP	0	<input type="checkbox"/>	CS1000-R75
<input type="checkbox"/>	Acme2	Acme2 Net-Net Inside	CS1K-R75-RP	0	<input type="checkbox"/>	CS1000-R75

6.7.2 Outbound Calls to Verizon

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

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

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

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

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

Click **Commit** to save. The following screen shows an example Dial Pattern defined for the sample configuration. Repeat this procedure as needed to allow additional PSTN numbers to be routed to the Verizon network via an Acme Packet Net-Net SBC. In the screen below, the Rank shown for the policy for “Acme1” and “Acme2” are the same, and either “Acme1” or “Acme2” may be chosen for an outbound call (see also Section 6.6). If “Acme1” should be used preferentially over “Acme2”, the routing policy for Acme2 in Section 6.6 can be assigned a higher valued ranking. Both approaches were tested successfully.

Wildcards may be used in the **Pattern** field so that blocks of matching numbers are routed based on a single dial pattern.

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

2 Items | [Refresh](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	-ALL-	Any Locations	Acme1-to-VZ	0	<input type="checkbox"/>	Acme1
<input type="checkbox"/>	-ALL-	Any Locations	Acme2-to-VZ	0	<input type="checkbox"/>	Acme2

7. Configure Acme Packet Net-Net SBC

This section illustrates relevant aspects of the Acme Packet Net-Net SBC configuration. In the sample configuration, the Acme Packet Net-Net SBC 4250 platform was used, and the approach may be used for other Net-Net platforms such as the 3800 and 4500.

Avaya Aura® Communication Manager has been certified previously by both Avaya and Verizon with the Acme Packet SBC. The Acme Packet SBCs used in the testing associated with these CS1000E Application Notes have also been used in a configuration to test Communication Manager behind Session Manager. Compared to the Acme Packet Net-Net SBC configuration documented in reference [VZ-IP-Trunk-CM] with Communication Manager (see references in Section 11), modest additions to the SBC configuration are recommended to support the CS1000E. To summarize the additions, the sip-manipulations performed by the SBC on egress to Verizon are expanded so that SIP headers and SIP message body information uniquely generated by the CS1000E are removed. This is recommended to avoid sending Verizon unnecessary message content, as shown in Section 7.8.2. Also, the SBC may be used to re-mark the Differentiated Services Code Point (DSCP) for both SIP signaling and RTP media, as shown in Section 7.9.

Unless otherwise noted, this section will show the relevant configuration for “Acme1” only, as the configuration of “Acme2” is conceptually the same.

7.1. Acme Packet Command Line Interface Summary

The Acme Packet Session Border Controller is configured using the Acme Packet Command Line Interface (CLI). The following are the generic CLI steps for configuring various elements.

1. Access the console port of the Acme Packet Session Border Controller using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the Session Border Controller for cable connection). Use the following settings for the serial port on the PC.
 - Bits per second: 115200
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
2. Log in to the Acme Packet Session Border Controller with the proper user password.
3. Enable the Super-user mode by entering the **enable** command and then the super user password. The command prompt will change to include a “#” instead of a “>” while in Super user mode. This level of system access (i.e. at the “acmesystem#” prompt) will be referred to as the *main* level of the CLI. Specific sub-levels of the CLI will then be accessed to configure specific *elements* and specific *parameters* of those elements.
4. In Super-user mode, enter the “**configure terminal**” command. The “**configure terminal**” command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the *configuration* level.
5. Enter the name of an element to be configured.
6. Enter the name of a sub-element.
7. Enter the name of an element parameter followed by its value.

8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat as needed to configure other elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

7.2. System Configuration, Physical, and Network Interfaces

The system configuration defines system-wide parameters for the SBC. For example, a default-gateway can be defined for a management network. A parameter named source-routing may be enabled. By default, the SBC's FTP, ICMP, telnet, and SNMP services cannot be accessed via the media interfaces. These services can be administratively enabled, if desired, in the context of HIP or host-in-path functions. The parameter source-routing was enabled in the sample configuration to allow source routing of HIP packets based on source IP addresses (i.e., the SBC will send replies out the same interface from which it received the request).

```
system-config
  hostname                               acmesbc
  <text removed for brevity>
  source-routing                       enabled
```

In the sample configuration, for each SBC, the Ethernet interface slot 0 / port 0 was connected to the external network (facing Verizon), and Ethernet slot 1 / port 0 was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address. Key physical interface (*phy-interface*) fields include:

- **name**: A descriptive string used to reference the interface.
- **operation-type**: *Media* indicates both signaling and media packets can be sent.
- **slot / port**: The identifier of the specific Ethernet interface used.

```
phy-interface
  name                                M00
  operation-type                      Media
  port                                0
  slot                                0
  virtual-mac                          00:08:25:01:be:e8
  admin-state                          enabled
  auto-negotiation                     enabled
  <text removed for brevity>
phy-interface
  name                                M10
  operation-type                      Media
  port                                0
  slot                                1
  virtual-mac                          00:08:25:01:be:ee
  admin-state                          enabled
  auto-negotiation                     enabled
  <text removed for brevity>
```

Key network interface (**network-interface**) fields include:

- **name:** The name of the physical interface (defined previously) that is associated with this network interface.
- **ip-address:** IP Address of the network interface. The IP Address for the “outside” network interface facing Verizon is “1.1.1.2” for “Acme1” and “2.2.2.2” for “Acme2”. The IP Address for the “inside” network interface is “65.206.67.1” for “Acme1” and “65.206.67.21” for “Acme2”.
- **dns-ip-primary:** If DNS-SRV to a Verizon DNS server will be used to determine the Verizon SIP signaling IP Address and port, then the Verizon DNS server IP address may be entered on the “outside” network interface. In the sample configuration, the Verizon DNS Server IP Address is 172.30.209.4 as shown in **Figure 1**.
- **dns-domain:** If DNS-SRV to a Verizon DNS server will be used to determine the Verizon SIP signaling IP Address and port, then a DNS domain may be entered on the “outside” network interface. In the sample configuration, “globalipcom.com” was entered.
- **netmask:** Subnet mask for the IP subnet.
- **gateway:** The subnet gateway address.

The settings for the “outside” network interface of “Acme1” are shown below. (The settings for “Acme2” used ip-address 2.2.2.2.)

```
network-interface
  name                M00
  sub-port-id         0
  description
  hostname
  ip-address           1.1.1.2
  pri-utility-addr
  sec-utility-addr
  netmask              255.255.255.0
  gateway              1.1.1.1
  < text removed for brevity >
  dns-ip-primary       172.30.209.4
  dns-ip-backup1
  dns-ip-backup2
  dns-domain           globalipcom.com
  dns-timeout          11
  hip-ip-list          1.1.1.2
  < text removed for brevity >
```

The settings for the private or “inside” network interface of the “Acme1” SBC is shown below. (The settings for “Acme2” used ip-address 65.206.67.21.)

```
network-interface
  name                M10
  sub-port-id         0
  description
  hostname
  ip-address          65.206.67.1
  < text removed for brevity >
  netmask             255.255.255.0
  gateway             65.206.67.254
  < text removed for brevity >
  hip-ip-list          65.206.67.1
  ftp-address          65.206.67.1
  icmp-address         65.206.67.1
  < text removed for brevity >
```

7.3. Realms

A realm represents a group of related components. Defining realms allows flows to pass through a connection point between two networks. Two realms were defined for the compliance test. The **OUTSIDE** realm was defined for the external network towards Verizon and the **INSIDE** realm was defined for the internal network facing Session Manager and the CS1000E.

Key realm (*realm-config*) parameters include:

- **identifier:** A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces:** The network interfaces located in this realm.
- **mm-in-realm:** Although not required in a peering configuration, this parameter was enabled in the sample configuration. This parameter allows calls within the same realm to have media flow through the SBC.
- **out-manipulationid:** *NAT_IP* This name refers to a set of sip-manipulations (defined in Section 7.8) that are performed on outbound traffic from the SBC.
- **class-profile:** If it is desired to have the SBC re-mark traffic, a class-profile can be assigned to the realm. In the sample configuration, the class-profile “marksip-profile” (see Section 7.9) was used to re-mark the DSCP in SIP signaling and RTP media packets flowing towards Verizon on the “OUTSIDE” realm.

The realm-config settings for “Acme1” are shown below. (The settings for “Acme2” are identical.)

```

realm-config
  identifier                OUTSIDE
  description
  addr-prefix               0.0.0.0
  network-interfaces

  mm-in-realm               M00:0
  mm-in-network             enabled
  mm-same-ip                 enabled
  mm-in-system              enabled
  <text removed for brevity>
  in-translationid
  out-translationid
  in-manipulationid
  out-manipulationid       NAT_IP
  manipulation-string
  manipulation-pattern
  class-profile             marksip-profile
  <text removed for brevity>
realm-config
  identifier                INSIDE
  description
  addr-prefix               0.0.0.0
  network-interfaces

  mm-in-realm               M10:0
  mm-in-network             enabled
  mm-same-ip                 enabled
  mm-in-system              enabled
  media-policy
  in-translationid
  out-translationid
  in-manipulationid
  out-manipulationid
  < text removed for brevity >

```


7.4. SIP Configuration

The SIP configuration (*sip-config*) defines global system-wide SIP parameters. Key SIP configuration (*sip-config*) parameters include:

- **home-realm-id**: The name of the realm on the private side of the SBC was used.
- **nat-mode**: None. No SIP-NAT function is necessary.
- **options max-udp-length=0** Enables UDP fragmented packets
- **options set-inv-exp-at-100-resp** Sets SIP Timer C when a 100 Trying is received in response to INVITE.

The sip-config settings for “Acme1” are shown below. (The settings for “Acme2” are identical.)

```
sip-config
state                                enabled
operation-mode                      dialog
dialog-transparency                 enabled
home-realm-id                       INSIDE
egress-realm-id                     INSIDE
nat-mode                            None
< text removed for brevity >
options                             max-udp-length=0
                                   set-inv-exp-at-100-resp
< text removed for brevity >
```

7.5. SIP Interface

The SIP interface (*sip-interface*) defines the receiving characteristics of the SIP interfaces on the SBC. Two SIP interfaces were defined, one for each realm. Key SIP interface (*sip-interface*) fields include:

- **realm-id**: The name of the realm assigned to this interface.
- **sip port**
 - **address**: The IP address assigned to this sip-interface.
 - **port**: The port assigned to this sip-interface. Port 5060 is used for UDP and TCP.
 - **transport-protocol**: UDP transport is used on the “outside” for communication with Verizon, and TCP transport is used on the “inside” to Session Manager.
 - **allow-anonymous**: Defines from whom SIP requests will be allowed. The value of *agents-only* is used. Thus, SIP requests will only be accepted from configured session agents (as defined in Section 7.6).
- **trans-expire**: Sets the expiration timer in seconds for SIP transactions. In the sample configuration, trans-expire was changed from the default of 32 seconds in the global “sip-config” to 6 seconds in the “sip-interface”. As an example implication, assume an incoming call arrives from the PSTN that “Acme1” sends on to Session Manager that appears to be an in-service session agent. However, assume there is no response. After 6 seconds (rather than 32), the transaction times out, and as a result, the call can automatically be diverted by Verizon to “Acme2” more quickly.

The sip-interface settings for “Acme1” are shown below. (The settings for “Acme2” are identical, save for the IP Address differences. The address parameter for the sip-interface on the OUTSIDE realm of “Acme2” is “2.2.2.2”, and the address parameter for the sip-interface on the INSIDE realm of “Acme2” is 65.206.67.21, as shown in **Figure 1**.)

```

sip-interface
  state                enabled
  realm-id             OUTSIDE
  description
  sip-port
    address            1.1.1.2
    port               5060
    transport-protocol UDP
    tls-profile
    allow-anonymous    agents-only
    ims-aka-profile
  <text removed for brevity>
  sip-ims-feature      disabled
  rfc2833-payload      101
  rfc2833-mode         transparent
  <text removed for brevity>
sip-interface
  state                enabled
  realm-id             INSIDE
  description
  sip-port
    address            65.206.67.1
    port               5060
    transport-protocol TCP
    tls-profile
    allow-anonymous    agents-only
    ims-aka-profile
  <text removed for brevity>
  trans-expire         6
  <text removed for brevity>
  sip-ims-feature      disabled
  rfc2833-payload      101
  rfc2833-mode         transparent
  <text removed for brevity>

```

7.6. Session Agent

A session agent defines the characteristics of a signaling peer to the SBC. On the inside interface, the SBC will have a session agent to Avaya Aura® Session Manager. On the outside interface, the SBC will have a session agent to Verizon IP Trunk service. Key session agent (*session-agent*) parameters include:

- **hostname:** Fully qualified domain name or IP address of this SIP peer. If DNS-SRV will be used toward Verizon to determine the SIP signaling address and port, the hostname for the session agent towards Verizon will be “pcelban0001.avayalincroft.globalipcom.com”.
- **ip-address:** The IP address of this SIP peer, if statically assigned. If DNS-SRV will be used toward Verizon to determine the SIP signaling address and port, the ip-address is not entered for the session agent towards Verizon.
- **port:** The port used by the peer for SIP traffic. If DNS-SRV will be used toward Verizon to determine the SIP signaling address and port, the port is not entered for the session agent towards Verizon.
- **app-protocol:** *SIP*
- **transport-method:** *StaticTCP*. With static TCP, a TCP connection can be re-used for multiple sessions.
- **realm-id:** The realm id where this peer resides.
- **description:** A descriptive name for the peer.
- **max-sessions:** Although not used in the sample configuration, this parameter can allow call admission control to be applied for the session agent.
- **ping-method:** *OPTIONS;hops=0* The SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the SBC to set the Max-Forwards field to 0 in outbound OPTIONS pings generated by to this session-agent.
- **ping-interval:** Specifies the interval between SIP OPTIONS “pings” in seconds. Since the intent is to monitor the health of the connection, “pings” may be suppressed if there is traffic to/from the session-agent that shows the connection is up.
- **ping-in-service-response-codes:** Although not defined in the sample configuration, this parameter can be used to specify the list of response codes that keep a session agent in-service. By default, any valid SIP response from the session agent is enough to keep the session agent in service.
- **out-service-response-codes:** Although not defined in the sample configuration, this parameter can be used to specify the list of “OPTIONS ping” response codes that take a session agent out-of-service.
- **options trans-timeouts=1** This parameter defines the number of consecutive non-ping transaction timeouts that will cause the session agent to be marked out-of-service. For example, with this option set to 1, if an INVITE is sent to Session Manager that is currently marked in-service, but no response is received resulting in a transaction timeout, the session agent will be immediately marked out-of-service. This can allow future calls to divert to an alternate path without experiencing a delay due to a transaction timeout. Note that an explicit error response, such as a 503, is not considered a transaction timeout.
- **reuse-connections TCP** Enables TCP connection re-use.
- **tcp-keepalive enabled** Enables standard TCP Keep-Alives

- **tcp-reconn-interval 10** Specifies the idle time, in seconds, before TCP keep-alive messages are sent.

The following shows key parameters for the session-agent to Session Manager.

```

session-agent
  hostname                10.1.2.210
  ip-address              10.1.2.210
  port                    5060
  state                   enabled
  app-protocol            SIP
  app-type
  transport-method        StaticTCP
  realm-id                INSIDE
  egress-realm-id
  description              SM61
  <text removed for brevity>
  max-sessions             0
  max-inbound-sessions     0
  max-outbound-sessions    0
  <text removed for brevity>
  loose-routing           enabled
  send-media-session       enabled
  ping-method              OPTIONS ; hops=0
  ping-interval            60
  ping-send-mode           keep-alive
  ping-all-addresses      disabled
  ping-in-service-response-codes
  out-service-response-codes
  options                  trans-timeouts=1
  <text removed for brevity>
  reuse-connections        TCP
  tcp-keepalive            enabled
  tcp-reconn-interval      10
  < text removed for brevity >

```

The following shows key parameters for the session-agent to Verizon IP Trunk Service. As shown, DNS-SRV was used to determine the SIP Signaling IP Address and port to Verizon. Alternatively, a static IP Address (e.g., 172.30.209.21) may be entered for the hostname and ip-address, and a static port number (e.g., 5071) may be entered for the port parameter.

```
session-agent
  hostname      pcelban0001.avayalincroft.globalipcom.com
  ip-address
  port          0
  state         enabled
  app-protocol  SIP
  app-type
  transport-method  UDP
  realm-id      OUTSIDE
  egress-realm-id
  description   pcelban0001.avayalincroft.globalipcom.com
  allow-next-hop-lp      enabled
  loose-routing      enabled
  send-media-session  enabled
  response-map
  ping-method      OPTIONS ; hops=0
  ping-interval    60
  ping-send-mode   keep-alive
  < text removed for brevity >
```

7.7. Session Agent Groups (SAG)

A session agent group is a logical collection of one or more session agents that behave as a single aggregate entity. In the sample configuration, the use of a SAG was optional, since each SBC connected to a single Session Manager and a single Verizon IP Trunk Service node. The SAG “SERV_PROVIDER” is associated with the Verizon IP Trunk service, and the SAG “ENTERPRISE” is associated with Avaya Aura® Session Manager.

Key session group (*session-group*) parameters include:

- **group-name**: a unique name for the session agent group.
- **app-protocol**: *SIP*
- **strategy**: selects the algorithm to use for distribution of traffic among the session agents in the group. In the sample configuration, this parameter is irrelevant since there is only one session agent in each group.
- **dest**: Identifies the session agents that are members of the session agent group. If DNS SRV is used with the Verizon IP Trunk service, the dest parameter can be the domain entered in the corresponding session-agent configuration. If DNS SRV is not used, the dest parameter can be the static IP Address of the session-agent.
- **sag-recursion** If enabled, allows re-trying another session agent in the session agent group after a failure for the previously selected session agent. Since there is only one session agent in the SAGs in the sample configuration, sag-recursion is moot and is shown in the disabled state.

The following shows the configuration of session agent groups on “Acme1”. The configuration for “Acme2” can be identical.

```

session-group
    group-name          SERV_PROVIDER
    description
    state               enabled
    app-protocol        SIP
    strategy            Hunt
    dest                pcelban0001.avayalincroft.globalipcom.com

    trunk-group
    sag-recursion       disabled
    stop-sag-recurse    401,407

session-group
    group-name          ENTERPRISE
    description
    state               enabled
    app-protocol        SIP
    strategy            RoundRobin
    dest                10.1.2.210

    trunk-group
    sag-recursion       disabled
    stop-sag-recurse    401,407

```

7.8. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages. For example, SIP manipulations can be performed to ensure private network topology hiding and confidentiality. In Section 7.3, the sip-manipulation named NAT_IP was configured as the “out-manipulation” on the OUTSIDE realm.

7.8.1 Header Modification for Topology Hiding or Domain Adaptation

In the sample configuration, where Session Manager is already performing adaptations that insert the proper domains in SIP headers, the header-rules illustrated in this section are not strictly required, but were in place for the testing from shared use of this Acme Packet Net-Net Session Director.

Key SIP manipulation (*sip-manipulation*) parameters include:

- **name:** The name of this set of SIP header rules.
- **header-rule:**
 - **name:** The name of this individual header rule.
 - **header-name:** The SIP header to be modified.
 - **action:** The action to be performed on the header.
 - **comparison-type:** The type of comparison performed when determining a match.
 - **msg-type:** The type of message to which this rule applies.
 - **element-rule:**

- **name:** The name of this individual element rule.
- **type:** Defines the particular element in the header to be modified.
- **action:** The action to be performed on the element.
- **match-val-type:** Element matching criteria on the data type (if any) in order to perform the defined action.
- **comparison-type:** The type of comparison performed when determining a match.
- **match-value:** Element matching criteria on the data value (if any) in order to perform the defined action.
- **new-value:** New value for the element (if any).

The example below shows the ***manipFrom*** header-rule within the NAT_IP sip-manipulation. It specifies that the “From” header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies that if the host part of the URI in this header is an IP address, then replace the IP address with the value of \$LOCAL_IP. The value of \$LOCAL_IP is the IP address of the sip-interface of the SBC. Note that if the host does not contain an IP Address, but rather contains a domain, such as “adevc.avaya.globalipcom.com” (as sent by Session Manager), then the match and replacement will not occur, allowing the enterprise domain “adevc.avaya.globalipcom.com” to be sent to Verizon.

```

sip-manipulation
  name          NAT_IP
  description    Topology hiding for SIP headers
  split-headers
  join-headers
  header-rule
    name          manipFrom
    header-name    From
    action          manipulate
    comparison-type case-sensitive
    msg-type        request
    methods
    match-value
    new-value
    element-rule
      name          FROM
      parameter-name
      type          uri-host
      action          replace
      match-val-type ip
      comparison-type case-sensitive
      match-value
      new-value      $LOCAL_IP
    < text removed for brevity >

```

The example below shows the *manipTo* header-rule within the same NAT_IP sip-manipulation. It specifies that the “To” header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies that if the host part of the URI in this header is an IP address, then replace the IP address with the value of \$REMOTE_IP. The value of \$REMOTE_IP is the IP address of the SIP peer. Note that if the host does not contain an IP Address, but rather contains a domain, such as “pcelban0001.avaya.globalipcom.com” (as sent by Session Manager), then the match and replacement will not occur, allowing the domain to be sent to Verizon.

header-rule		
name	manipTo	
header-name	To	
action	manipulate	
comparison-type	case-sensitive	
msg-type	request	
methods		
match-value		
new-value		
element-rule		
name	TO	
parameter-name		
type	uri-host	
action	replace	
match-val-type	ip	
comparison-type	case-sensitive	
match-value		
new-value	\$REMOTE_IP	

The example below shows the *manipPAI* header-rule within the same NAT_IP sip-manipulation. This header-rule is similar to the manipFrom header rule illustrated previously. It specifies that the “P-Asserted-Identity” header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies that if the host part of the URI in this header is an IP address, then replace the IP address with the value of \$LOCAL_IP.

header-rule	
name	manipPAI
header-name	P-Asserted-Identity
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	PAI
parameter-name	
type	uri-host
action	replace
match-val-type	ip
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP

The example below shows the *manipDiversion* header-rule within the same NAT_IP sip-manipulation. It specifies that the “Diversion” header in SIP request messages will be manipulated based on the element rule defined. The element rule specifies that if the host part of the URI will be replaced with the enterprise domain known to Verizon “adevc.avaya.globalipcom.com”. This header-rule was not required for the integration of the CS1000E through Session Manager 6.1 as documented in these Application Notes, but was part of the NAT_IP sip-manipulation during the testing associated with these Application Notes.

header-rule	
name	manipDiversion
header-name	Diversion
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	DIVERSION
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	adevc.avaya.globalipcom.com

7.8.2 Stripping Unnecessary SIP Headers and Message Body Information

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

The example below shows the optional ***delPLocation*** header-rule within the same NAT_IP sip-manipulation. This header-rule deletes the P-Location header inserted by Session Manager to prevent the P-Location header from being sent unnecessarily to Verizon.

```
header-rule
    name                delPLocation
    header-name          P-Location
    action               delete
    comparison-type      pattern-rule
    msg-type             any
    methods
    match-value
```

The example below shows the ***delAlertInfo*** header-rule within the same NAT_IP sip-manipulation. This header-rule deletes the Alert-Info header to prevent the header from being sent unnecessarily to Verizon.

```
header-rule
    name                delAlertInfo
    header-name          Alert-Info
    action               delete
    comparison-type      case-sensitive
    msg-type             request
    methods
    match-value
    new-value
```

The SBC can also be used to strip information from the message body that is not required or expected by Verizon. For example, for an outbound call, the message body of an INVITE message sent from the Avaya CS1000E will contain a MIME Multipart message body containing the SDP information expected by Verizon, but also containing “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex” application parts that are not processed by Verizon. On the production circuit used for testing, Verizon was able to properly parse the Multipart MIME message body, and outgoing calls from the CS1000E to Verizon could be completed successfully without the configuration shown below. Nevertheless, the procedure can substantially reduce the message size, so the following procedures are recommended to strip out CS1000 application information and send only SDP in the message body to Verizon. As noted in Section 6.3.2, as an alternative to the SBC configuration

shown below, Session Manager Release 6.1 may be used to perform the multipart MIME stripping function by setting the module parameter “MIME=no” in the adapter assigned to the SBC entity.

The example below shows the *delXNT* header-rule within the same NAT_IP sip-manipulation. This header-rule deletes the “x-nt-e164-clid” header inserted by the CS1000E to prevent this header from being sent unnecessarily to Verizon.

```
header-rule
    name                delXNT
    header-name          x-nt-e164-clid
    action               delete
    comparison-type      case-sensitive
    msg-type             any
    methods
    match-value
    new-value
```

The example below shows optional, but highly recommended mime-rules within the same NAT_IP sip-manipulation. These mime-rules remove specific application message body parts that are present in outbound INVITE messages from the CS1000E. The *delXNTMCDN* mime-rule removes the “x-nt-mcdn-frag-hex” and the *delXNTEPID* mime-rule removes the “x-nt-epid-frag-hex”. These mime-rules will result in only SDP sent in the INVITE to Verizon. Implicitly, these rules cause the SBC to change corresponding headers such as the Content-Type and Content-Length headers to reflect the new Content-Type (i.e., only SDP), and message body length after the CS1000-specific application content is removed from the body of the message.

```
mime-rule
    name                delXNTMCDN
    content-type         application/x-nt-mcdn-frag-hex
    action               delete
    comparison-type      case-sensitive
    msg-type             request
    methods              INVITE
    format               ascii-string
    match-value
    new-value

mime-rule
    name                delXNTEPID
    content-type         application/x-nt-epid-frag-hex
    action               delete
    comparison-type      case-sensitive
    msg-type             request
    methods              INVITE
    format               ascii-string
    match-value
    new-value
```

7.9. Quality Of Service (QoS) Markings for SIP Signaling and RTP Media

The procedure in this section is optional. The procedure can be used to achieve SIP signaling and RTP media re-marking using the Acme Packet Net-Net SBC.

Recall that the class-profile “marksip-profile” was assigned as the class-policy for the OUTSIDE realm facing Verizon. A portion of the realm-config for the OUTSIDE realm is repeated below, with the class-profile shown in bold.

```
realm-config
  identifier                OUTSIDE
  network-interfaces
                             M00:0

  out-manipulationid        NAT_IP
  class-profile             marksip-profile
```

If it is desired to have the SBC re-mark SIP signaling to a specific Differentiated Services Code Point before the SIP message is sent to Verizon, a media-policy tos-setting can be defined with media-type “message”, media-sub-type “sip”, and a specific tos-value. In the example below, tos-value 0x68 is shown to have the SBC re-mark SIP signaling to a value associated with “Assured Forwarding”. If it is desired to have the SBC re-mark RTP media to a specific Differentiated Services Code Point before the RTP media is sent to Verizon, the same media-policy can also include another tos-setting with media-type “audio” and a specific desired tos-value for media. In the example below, tos-value 0xb8 is shown to have the SBC re-mark RTP media to a value associated with “Expedited Forwarding”.

```
media-policy
  name                        marksip
  tos-settings
    media-type                message
    media-sub-type            sip
    tos-value                 0x68
    media-attributes
  tos-settings
    media-type                audio
    media-sub-type
    tos-value                 0xb8
    media-attributes
```

As shown below, a class-policy is defined with a name “marksip-profile”. This class-policy contains the media-policy “marksip” shown in the screen above.

```
class-policy
  profile-name                marksip-profile
  to-address                  *
  media-policy                marksip
  <text removed for brevity>
```

With this configuration, the SBC will mark all SIP signaling sent to Verizon for “assured forwarding” and all RTP media sent to Verizon for “expedited forwarding”.

7.10. Steering Pools

Steering pools define sets of ports that are used for steering media flows (e.g., RTP) through the SBC. Two steering pools were defined, one for each realm.

Key steering pool (*steering-pool*) parameters include:

- **ip-address:** The address of the interface on the SBC.
- **start-port:** An even number of the port that begins the range.
- **end-port:** An odd number of the port that ends the range.
- **realm-id:** The realm to which this steering pool is assigned.

The following shows the steering-pool configuration on “Acme1”. For “Acme2”, the configuration is similar, except that the IP Address on the INSIDE realm is 65.206.6.21 and the IP Address on the OUTSIDE realm is 2.2.2.2.

```
steering-pool
  ip-address          65.206.67.1
  start-port          49152
  end-port            65535
  realm-id            INSIDE
  <text removed for brevity>

steering-pool
  ip-address          1.1.1.2
  start-port          49152
  end-port            65515
  realm-id            OUTSIDE
  <text removed for brevity>
```

7.11. Local Policies

Local policies control the routing of SIP calls from one realm to another. Key local policy (*local-policy*) parameters include:

- **from-address:** A policy filter indicating a match for the from-address. An asterisk (“*”) is a wildcard matching anything.
- **to-address:** A policy filter indicating a match for the to-address. An asterisk (“*”) is a wildcard matching anything.
- **source-realm:** A policy filter indicating the matching source realm in order for the policy rules to be applied.
- **policy-attribute:**
 - **next-hop:** Where the message should be sent when the policy rules match.
 - **realm:** The realm associated with the next-hop.

The first policy below provides a simple routing rule indicating that messages originating from the ***OUTSIDE*** realm are to be sent to the ***INSIDE*** realm via the session agent group (SAG) named “ENTERPRISE”. These local-policy settings are the same for “Acme1” and “Acme2”.

```
local-policy
  from-address
  to-address
  source-realm
  <text removed for brevity>
  state
  policy-priority
  policy-attribute
  next-hop
  realm
  action
  <text removed for brevity>
  app-protocol
  state
  <text removed for brevity>
  *
  *
  OUTSIDE
  enabled
  none
  SAG:ENTERPRISE
  INSIDE
  replace-uri
  SIP
  enabled
```

The simple policy shown below indicates that messages originating from the ***INSIDE*** realm are to be sent to the ***OUTSIDE*** realm via session agent group “SERV_PROVIDER”.

```
local-policy
  from-address
  to-address
  source-realm
  <text deleted for brevity>
  state
  policy-attribute
  next-hop
  realm
  action
  app-protocol
  state
  <text deleted for brevity>
  *
  *
  INSIDE
  enabled
  SAG:SERV_PROVIDER
  OUTSIDE
  none
  SIP
  enabled
```

7.12. Access Control

The following access-control was defined to “permit” SIP UDP traffic from Verizon IP Trunk Service (i.e., source-address 172.30.209.21:5071)

```
access-control
  realm-id                OUTSIDE
  description             VZ-WM
  source-address          172.30.209.21:5071
  destination-address     0.0.0.0
  application-protocol    SIP
  transport-protocol      UDP
  access                  permit
  <text deleted for brevity>
```

7.13. Host Routes

The following host-route was defined for the Verizon IP Trunk Service DNS server (i.e., 172.30.209.4). The gateway is the routing interface for the public or outside of the SBC facing Verizon.

```
host-routes
  dest-network            172.30.209.4
  netmask                 255.255.255.255
  gateway                 1.1.1.1
  <text deleted for brevity>
```

The following host-route was defined for the network used by Session Manager. The gateway is the routing interface for the private side or inside network facing the enterprise equipment.

```
host-routes
  dest-network            10.1.2.0
  netmask                 255.255.255.0
  gateway                 65.206.67.254
  <text deleted for brevity>
```

8. Verizon Business IP Trunk Service Offer Configuration

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

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

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

9. Verification Steps

This section provides example verifications of the Avaya configuration with Verizon Business IP Trunk 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.

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

Node Maintenance and Reports

- Node ID: 2 Node IP: 10.7.7.60

Hostname	ELAN IP	Type	TN
cs1k75	10.7.8.61	Signaling Server-Avaya CPPMv1	NO TN

GEN CMD SYS LOG ON

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

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

Group [v] Command -- Select A Group -- [v] RUN

IP address 10.7.8.61 Number of pings 3 PING

Click on a button to invoke a command.

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

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

General Commands

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

Group	Sip	Command	SIPGwShow	Sip	RUN
IP address	10.7.8.61	Number of pings	3		PING

SIPNPM Status	: Active
Primary Proxy IP address	: 10.1.2.210
Primary Proxy port	: 5060
Primary Proxy Transport	: TCP
Secondary Proxy IP address	: 0.0.0.0
Secondary Proxy port	: 5060
Secondary Proxy Transport	: TCP
Primary Proxy2 IP address	: 10.1.2.210
Primary Proxy2 port	: 5060
Primary Proxy2 Transport	: TCP

As another example, the following screen shows the results of the “vtrkShow” **Command** from the “Vtrk” **Group**. The command was run with an incoming call up from the Verizon IP Trunk Service to an IP-UNISTim telephone. Therefore, one channel is busy, and 19 idle.

General Commands

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

Group	Vtrk	Command	vtrkShow	Protocol		Start	
IP address	10.7.8.61	Number of pings	3				

```

-----
VTRK Summary
-----
VTRK status      : Active
Master status    : On
VTRK REG Node    : 2
Protocol         : H323 SIP SIPL
D-Channel        : 1
Customer         : 0
Channels Idle    : 19
Channels Busy    : 1
Channels Mbsy    : 0
Channels Pend    : 0
Channels Dsbl    : 0
  
```

The next screen capture shows the output of the **Command** “SIPGWSHowch” in **Group** “Sip” for channel 1, while an incoming call was up (using channel 1) from the Verizon IP Trunk Service to an IP-UNISTim phone. In the output below, the scroll bar (not shown) was used to scroll down to the area showing that the codec in use was “G_729A_20MS”. Note that the Remote IP (65.206.67.1) is the IP Address of the inside private interface of the SBC “Acme1”.

General Commands

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

Group	Sip	Command	SIPGWSHowch	Sip	1
IP address	10.7.8.61	Number of pings	3		

```

Channels Busy / Idle / Total : 1 / 9 / 10
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
-----
0xb1700468  1 VTRK      Terminate BUSY      Ringing Sent    Connected Connected
Codec
AirTime FS  MS  Fax DestNum RemoteIP
-----
G_729A_20MS      96 yes m  no  57003  65.206.67.1  ::      SIP
  
```

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 57003 was specified. An incoming call was up from the Verizon IP Trunk Service to the IP-UNISTim phone with DN 57003. 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 (65.206.67.1) is the IP Address of the inside private interface of the Acme Packet SBC “Acme1”.

General Commands

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

Group	Sip	Command	SIPGWShownum	Sip	57003
IP address	10.7.8.61	Number of pings	3		

```

Output Type Used      : RPT
Channel tracing       : -1
Calling/Called Party Number: 57003
Numbering Plan Indicator: Undefined
Type Of Number: Undefined

```

Handle	Chan Type	Direction	CallState	SIPState	RxState	TxState
0xb1700468	1 VTRK	Terminate	BUSY	Ringing Sent	Connected	Connected
Codec	AirTime	FS	MS	Fax	DestNum	RemoteIP
G_729A_20MS	272	yes	m	no	57003	65.206.67.1
					URI	Scheme
					::	SIP

The following screen shows the output of the **Command** “SIPGWShowch” in **Group** “Sip” for channel 10, when an outgoing call was up (using channel 10) from an IP UNISTim telephone to PSTN telephone number 19088485704 via the Verizon IP Trunk Service. Again, the use of G.729A to the inside IP Address (65.206.67.1) of the SBC can be observed.

General Commands

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

Group	Sip	Command	SIPGWShowch	Sip	10
IP address	10.7.8.61	Number of pings	3		

```

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
0xb1700468	10 VTRK	Originate	BUSY	Invite Sent	Connected	Connected
Codec	AirTime	FS	MS	Fax	DestNum	RemoteIP
G_729A_20MS	4	yes	m	no	19088485704	65.206.67.1
					URI	Scheme
					::	SIP

The following screen, similar to the previous, shows the output of the **Command** “SIPGWShowch” in **Group** “Sip” for channel 10, when an outgoing call was up (using channel

10) from an IP UNISTim telephone to PSTN telephone number 19088485704 via the Verizon IP Trunk Service. For this call, note that “Acme2” was used for the outbound call. Again, the use of G.729A to the inside IP Address (65.206.67.21) of the SBC can be observed.

General Commands

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

Group	Sip	Command	SIPGwShowch	Sip	10
IP address	10.7.8.61	Number of pings	3		

```

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
-----
0xb1700468  10 VTRK      Originate BUSY      Invite Sent    Connected Connected
Codec                AirTime FS  MS  Fax DestNum RemoteIP  URI Scheme
-----
G_729A_20MS          13 yes m  no  19088485704 65.206.67.21  ::      SIP
  
```

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

General Commands

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

Group	SipLine	Command	sigSetShowAll	<input type="button" value="RUN"/>
IP address	10.7.8.61	Number of pings	3	<input type="button" value="PING"/>

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

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

General Commands

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

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

IP Address	NAT	Model Name	Type	RegType	State	Up

10.7.7.121		1120E IP Deskphone	1120	Regular	online	
10.7.7.122		1140E IP Deskphone	1140	Regular	online	
10.7.7.123		2007 Phase 2 IP Deskphone	2007	Regular	busy	

9.1.2 System Maintenance Commands

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

Managing: 10.7.8.61 Username: admin
System » Maintenance

Maintenance

☒ Select by Overlay

☐ Select by Functionality

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

Maintenance

☒ Select by Overlay

☐ Select by Functionality

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

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

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

D-Channel Diagnostics

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

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
<input type="radio"/> 001	VirDchToSS	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 Outbound Call

This section illustrates an example outbound call from the Avaya CS1000E IP UNISim user with Directory Number 57003 to PSTN telephone number 1-908-848-5704.

The following screen capture shows a Wireshark trace filtered on SIP messages sent from and to the IP Address of the Avaya CS1000E. The INVITE message is selected and the message header area is expanded to show the content of the SIP headers in the INVITE sent by the CS1000E. As can be observed, in the sample configuration, the CS1000E sends the directory number of the user placing the call in SIP headers such as the From and P-Asserted-Identity headers. Session Manager will adapt the directory number to a Verizon DID in the From and PAI headers. The domain in the headers in source and destination headers is “avaya.com” which Session Manager will adapt to the source and destination domains expected by Verizon. Proprietary headers such as “x-nt-el64-clid” can be observed, and such headers will be removed by the SBC. The History-Info header can be observed and will be removed by the Session Manager “VerizonAdapter”.

Filter: sip && ip.addr == 10.7.7.60

No.	Time	Source	Destination	Protocol	Info
315	9.808979	10.7.7.60	10.1.2.210	SIP/SDP	Request: INVITE sip:19088485704@avaya.com;user=phone, with session description
317	9.810857	10.1.2.210	10.7.7.60	SIP	Status: 100 Trying
367	11.407425	10.1.2.210	10.7.7.60	SIP/SDP	Status: 183 Session Progress, with session description
369	11.429285	10.7.7.60	10.1.2.210	SIP	Request: OPTIONS sip:19088485704@65.206.67.1:5060;transport=tcp
379	11.562142	10.1.2.210	10.7.7.60	SIP	Status: 200 OK
525	16.147003	10.1.2.210	10.7.7.60	SIP/SDP	Status: 200 OK, with session description
527	16.177740	10.7.7.60	10.1.2.210	SIP	Request: ACK sip:19088485704@65.206.67.1:5060;transport=tcp

Session Initiation Protocol

- Request-Line: INVITE sip:19088485704@avaya.com;user=phone SIP/2.0
- Message Header
 - From: <sip:57003@avaya.com;user=phone>;tag=561a150-3c07070a-13c4-55013-82446-6b80c63e-82446
 - To: <sip:19088485704@avaya.com;user=phone>
 - Call-ID: 6ad5690-3c07070a-13c4-55013-82446-48feaea0-82446
 - CSeq: 1 INVITE
 - Via: SIP/2.0/TCP 10.7.7.60:5060;branch=z9hg4bk-82446-1fcd31c-35128bb8
 - Max-Forwards: 70
 - Supported: 100rel,x-nortel-sipvc,replaces
 - User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
 - P-Asserted-Identity: <sip:57003@avaya.com;user=phone>
 - Privacy: none
 - x-nt-el64-clid: +57003@avaya.com;user=phone
 - History-Info: <sip:19088485704@avaya.com;user=phone>;index=1
 - Alert-Info: <cid:external@avaya.com>
 - Contact: <sip:57003@avaya.com:5060;maddr=10.7.7.60;transport=tcp;user=phone>
 - Allow: INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
 - Content-Type: multipart/mixed;boundary=unique-boundary-1
 - Content-Length: 881
- Message Body

The following screen capture shows the same Wireshark trace, filtered so that messages sent to and from Session Manager (10.1.2.210) are also visible. The INVITE message sent by Session Manager is selected and the message header area is expanded to show the content of some of the SIP headers in the INVITE. As can be observed from the selected frame 320, the Request-URI has been adapted such that the Verizon domain appears. The To header has been similarly adapted by Session Manager (i.e., “pcelban0001.avayalincroft.globalipcom.com”). The directory number of the CS1000E user placing the call has also been adapted by Session Manager to the Verizon DID 7329450235 in the From and P-Asserted-Identity headers, and the domain has been set to the CPE domain known to Verizon (i.e., “adevc.avaya.globalipcom.com). The “P-Location” header inserted by Session Manager will later be removed by the SBC.

No.	Time	Source	Destination	Protocol	Info
315	9.808979	10.7.7.60	10.1.2.210	SIP/SDP	Request: INVITE sip:19088485704@avaya.com;user=phone, with session description (appl
317	9.810857	10.1.2.210	10.7.7.60	SIP	Status: 100 Trying
320	9.814865	10.1.2.210	65.206.67.1	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com;user=phone
321	9.821620	65.206.67.1	10.1.2.210	SIP	Status: 100 Trying
365	11.404871	65.206.67.1	10.1.2.210	SIP/SDP	Status: 183 Session Progress, with session description
367	11.407425	10.1.2.210	10.7.7.60	SIP/SDP	Status: 183 Session Progress, with session description
369	11.429285	10.7.7.60	10.1.2.210	SIP	Request: OPTIONS sip:19088485704@65.206.67.1:5060;transport=tcp

Content-Type: multipart/mixed;boundary=unique-boundary-1	
Content-Length: 881	
To: <sip:19088485704@pcelban0001.avayalincroft.globalipcom.com;user=phone>	
P-Asserted-Identity: <sip:7329450235@adevc.avaya.globalipcom.com;user=phone>	
From: <sip:7329450235@adevc.avaya.globalipcom.com;user=phone>;tag=561a150-3c07070a-13c4-55013-82446-6b80c63e-82446	
Route: <sip:65.206.67.1;transport=tcp;lr;phase=terminating>	
P-Location: SM;origlocname="CS1K75-Location";termlocname="Acme1"	
Max-Forwards: 66	
Message Body	

The following screen shows the same Wireshark trace, but focuses on the message body of the INVITE. The message body contains MIME encapsulated application data for the SDP, “x-nt-mcdn-frag-hex” and “x-nt-epid-frag-hex”. The SDP has been expanded below so that it can be observed that the CS1000E SDP offer prefers G.729 and includes “annexb=no”. The SBC will strip the “x-nt...” information from the message body and send only the SDP to Verizon, after appropriate IP address mappings to the outside IP Address of the SBC.

No.	Time	Source	Destination	Protocol	Info
315	9.808979	10.7.7.60	10.1.2.210	SIP/SDP	Request: INVITE sip:19088485704@avaya.com;user=phone, with session description
317	9.810857	10.1.2.210	10.7.7.60	SIP	Status: 100 Trying
320	9.814865	10.1.2.210	65.206.67.1	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.avayalincroft.globalipcom.com;user=
321	9.821620	65.206.67.1	10.1.2.210	SIP	Status: 100 Trying
365	11.404871	65.206.67.1	10.1.2.210	SIP/SDP	Status: 183 Session Progress, with session description
367	11.407425	10.1.2.210	10.7.7.60	SIP/SDP	Status: 183 Session Progress, with session description

Message Body	
MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "unique-boundary-1"	
[Type: multipart/mixed]	
First boundary: --unique-boundary-1\r\n	
Encapsulated multipart part: (application/sdp)	
Content-Type: application/sdp\r\n\r\n	
Session Description Protocol	
Session Description Protocol Version (v): 0	
Owner/Creator, Session Id (o): - 26556 1 IN IP4 10.7.7.60	
Session Name (s): -	
Connection Information (c): IN IP4 10.7.7.123	
Time Description, active time (t): 0 0	
Media Description, name and address (m): audio 5200 RTP/AVP 18 0 8 101 111	
Connection Information (c): IN IP4 10.7.7.123	
Media Attribute (a): fmtp:18 annexb=no	
Media Attribute (a): rtptime:101 telephone-event/8000	
Media Attribute (a): fmtp:101 0-15	
Media Attribute (a): rtptime:111 x-nt-inforeq/8000	
Media Attribute (a):ptime:20	
Media Attribute (a): sendrecv	
Boundary: \r\n--unique-boundary-1\r\n	
Encapsulated multipart part: (application/x-nt-mcdn-frag-hex)	
Boundary: \r\n--unique-boundary-1\r\n	
Encapsulated multipart part: (application/x-nt-epid-frag-hex)	
Last boundary: \r\n--unique-boundary-1--\r\n	

The following screen from a Wireshark trace taken on the outside “public” side of the SBC shows a portion of the INVITE sent to Verizon. The message is sent from the outside IP address of the “Acme1” SBC (1.1.1.2). The use of UDP and destination port 5071 can be observed.

Filter: sip && ip.addr == 172.30.209.21

Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
7	6.521515	1.1.1.2	172.30.209.21	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.avaya!ncroft.globalipcom.com;
8	6.643423	172.30.209.21	1.1.1.2	SIP	Status: 100 Trying
9	8.092252	172.30.209.21	1.1.1.2	SIP/SDP	Status: 183 Session Progress, with session description
13	8.129410	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:19088485704@172.30.209.21:5071;transport=udp
20	8.251830	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
476	12.832479	172.30.209.21	1.1.1.2	SIP/SDP	Status: 200 OK, with session description
483	12.877418	1.1.1.2	172.30.209.21	SIP	Request: ACK sip:19088485704@172.30.209.21:5071;transport=udp

User Datagram Protocol, Src Port: sip (5060), Dst Port: powerschool (5071)

Session Initiation Protocol

Request-Line: INVITE sip:19088485704@pcelban0001.avaya!ncroft.globalipcom.com;user=phone SIP/2.0

The following screen from the same Wireshark trace shows a portion of the SIP headers in the same INVITE message. Observe that the Request-URI and To headers contain the Verizon domain “pcelban.avaya!ncroft.globalipcom.com” while the From and PAI headers contain the enterprise domain known to Verizon “adevc.avaya!ncroft.globalip.com.com”. Note that the Content-Type and Content-Length headers have been re-written to “application/sdp” and the new significantly reduced size (i.e., 248 compared to 881 in screen illustrated previously). Only the SDP portion of the original CS1000E message body is sent to Verizon as a result of the sip-manipulations implemented on the Acme Packet Net-Net SBC.

No.	Time	Source	Destination	Protocol	Info
7	6.521515	1.1.1.2	172.30.209.21	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.avaya!ncroft.globalipcom.com;
8	6.643423	172.30.209.21	1.1.1.2	SIP	Status: 100 Trying
9	8.092252	172.30.209.21	1.1.1.2	SIP/SDP	Status: 183 Session Progress, with session description
13	8.129410	1.1.1.2	172.30.209.21	SIP	Request: OPTIONS sip:19088485704@172.30.209.21:5071;transport=udp
20	8.251830	172.30.209.21	1.1.1.2	SIP	Status: 200 OK
476	12.832479	172.30.209.21	1.1.1.2	SIP/SDP	Status: 200 OK, with session description
483	12.877418	1.1.1.2	172.30.209.21	SIP	Request: ACK sip:19088485704@172.30.209.21:5071;transport=udp
Content-Type: application/sdp					
Content-Length: 248					
To: <sip:19088485704@pcelban0001.avaya!ncroft.globalipcom.com;user=phone>					
P-Asserted-Identity: <sip:7329450235@adevc.avaya.globalipcom.com;user=phone>					
From: <sip:7329450235@adevc.avaya.globalipcom.com;user=phone>;tag=561a150-3c07070a-13c4-55013-82446-6b80c63e-82446					
Max-Forwards: 65					

The following screen shows a portion of the same INVITE sent to Verizon with the message body expanded. The SBC has removed the CS1000E specific application types in the MIME Multipart message body that was seen on the inside of the SBC, so that Verizon sees only the SDP, with the connection information being the IP Address (1.1.1.2) of the outside of the SBC.

No.	Time	Source	Destination	Protocol	Info
7	6.521515	1.1.1.2	172.30.209.21	SIP/SDP	Request: INVITE sip:19088485704@pcelban0001.avaya!ncroft.globalipcom.com;
8	6.643423	172.30.209.21	1.1.1.2	SIP	Status: 100 Trying
9	8.092252	172.30.209.21	1.1.1.2	SIP/SDP	Status: 183 Session Progress, with session description
Message Body					
Session Description Protocol					
Session Description Protocol Version (v): 0					
Owner/Creator, Session Id (o): - 26556 1 IN IP4 1.1.1.2					
Session Name (s): -					
Connection Information (c): IN IP4 1.1.1.2					
Time Description, active time (t): 0 0					
Media Description, name and address (m): audio 50052 RTP/AVP 18 0 8 101 111					
Connection Information (c): IN IP4 1.1.1.2					
Media Attribute (a): fmp:18 annexb=no					
Media Attribute (a): rtpmap:101 telephone-event/8000					
Media Attribute (a): fmp:101 0-15					
Media Attribute (a): rtpmap:111 X-nt-inforeq/8000					
Media Attribute (a): pt:time:20					
Media Attribute (a): sendrecv					

9.2.2 Example Inbound Call

This section illustrates an inbound call from PSTN telephone 908-848-5704 to Verizon IP Trunk DID 732-945-0235.

The following screen shows a Wireshark trace taken from the outside of the SBC. The INVITE from Verizon in frame 8 is selected and expanded to illustrate the contents of the message header and message body. Note that Verizon sends the calling party number 9088485704 in the From header, and does not include a PAI header. The Request-URI and To header both contain the dialed Verizon DID 7329450235. In the message body, note that the Verizon SDP offer lists G.729 with “annexb=no”, and G.711. In frame 11, a 180 Ringing (without SDP) response is sent to Verizon. In frame 20, the 200 OK with SDP answering the inbound call is sent to Verizon.

No.	Time	Source	Destination	Protocol	Info
8	8.688782	172.30.209.21	1.1.1.2	SIP/SDP	Request: INVITE sip:7329450235@1.1.1.2:5060, with session description
9	8.691401	1.1.1.2	172.30.209.21	SIP	Status: 100 Trying
11	8.844798	1.1.1.2	172.30.209.21	SIP	Status: 180 Ringing
20	18.386976	1.1.1.2	172.30.209.21	SIP/SDP	Status: 200 OK, with session description

Session Initiation Protocol

Request-Line: INVITE sip:7329450235@1.1.1.2:5060 SIP/2.0

Message Header

Via: SIP/2.0/UDP 172.30.209.21:5071;branch=z9hG4bKactjk110agb1m2l5u1r0.1

From: "AVAYA ALPHA"<sip:9088485704@65.211.120.226;user=phone>;tag=414966156-1307474322662-

To: "Lincroft Lab LINCROFT LAB"<sip:7329450235@adevc.avaya.globalipcom.com>

Call-ID: Bw1518426620706111936093204@65.211.120.226

CSeq: 902132340 INVITE

Contact: <sip:9088485704@172.30.209.21:5071;transport=udp>

Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY

Accept: multipart/mixed,application/media_control+xml,application/sdp

Supported:

Max-Forwards: 69

Content-Type: application/sdp

Content-Length: 208

Message Body

Session Description Protocol

Session Description Protocol version (v): 0

Owner/Creator, Session Id (o): Broadworks 94124611 1 IN IP4 172.30.209.132

Session Name (s): -

Connection Information (c): IN IP4 172.30.209.132

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 11212 RTP/AVP 18 0 8 101

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 20 expanded to show the contents of the SDP answer containing G.729 with “annexb=no” returned to Verizon. The use of the value 101 for any transmission of “DTMF” telephone events via RFC 2833 can also be observed.

No. .	Time	Source	Destination	Protocol	Info
8	8.688782	172.30.209.21	1.1.1.2	SIP/SDP	Request: INVITE sip:7329450235@1.1.1.2:5060, with session description
9	8.691401	1.1.1.2	172.30.209.21	SIP	Status: 100 Trying
11	8.844798	1.1.1.2	172.30.209.21	SIP	Status: 180 Ringing
20	18.386976	1.1.1.2	172.30.209.21	SIP/SDP	Status: 200 OK, with session description

Session Initiation Protocol

Status-Line: SIP/2.0 200 OK

Message Header

Message Body

Session Description Protocol

Session Description Protocol version (v): 0

Owner/Creator, Session Id (o): - 26585 1 IN IP4 1.1.1.2

Session Name (s): -

Connection Information (c): IN IP4 1.1.1.2

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 50054 RTP/AVP 18 101 111

Connection Information (c): IN IP4 1.1.1.2

Media Attribute (a): pt=20

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

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

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

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

Media Attribute (a): sendrecv

Proceeding to the Wireshark from the inside of the SBC for this same call, Session Manager will adapt 732-945-0235 such that the call rings the IP UNISTim telephone with Directory Number 57003, an IP UNISTim telephone.

The INVITE message from Session Manager to the CS1000E is selected and a portion of the message header area is illustrated. In frame 510, it can be observed that Session Manager has adapted 7329450235 in the Request-URI to CS1000E DN 57003, while also adapting the domain to “avaya.com”. Session Manager also inserts a P-Asserted-Identity header containing user 9088485704 in the INVITE sent to the CS1000E. From this screen, it can also be observed that CS1000E uses 180 Ringing without SDP (frame 517) for incoming calls.

Filter: (sip && ip.addr == 10.7.7.60) (sip && ip.addr == 65.206.67.1) Expression... Clear Apply					
No. .	Time	Source	Destination	Protocol	Info
506	16.523433	65.206.67.1	10.1.2.210	SIP/SDP	Request: INVITE sip:7329450235@10.1.2.210:5060;transport=tcp, with session descr
507	16.525452	10.1.2.210	65.206.67.1	SIP	Status: 100 Trying
510	16.569093	10.1.2.210	10.7.7.60	SIP/SDP	Request: INVITE sip:57003@avaya.com:5060;transport=tcp, with session description
515	16.663451	10.7.7.60	10.1.2.210	SIP	Status: 100 Trying
517	16.663465	10.7.7.60	10.1.2.210	SIP	Status: 180 Ringing
519	16.666019	10.1.2.210	65.206.67.1	SIP	Status: 180 Ringing
921	26.202065	10.7.7.60	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
924	26.204747	10.1.2.210	65.206.67.1	SIP/SDP	Status: 200 OK, with session description

Content-Length: 202

P-Asserted-Identity: "AVAYA ALPHA" <sip:9088485704@avaya.com>

To: "Lincroft Lab LINCROFT LAB" <sip:57003@avaya.com>

From: "AVAYA ALPHA" <sip:9088485704@avaya.com;user=phone>;tag=414966156-1307474322662-

Route: <sip:10.7.7.60;transport=tcp;lr;phase=terminating>

P-Location: SM;origlocname="Acme1";termlocname="CS1K75-Location"

Max-Forwards: 64

User-Agent: AVAYA-SM-6.1.1.0.611023

Message Body

The following screen capture shows the same Wireshark trace but expands the 200 OK sent by the CS1000E when the user answers the call. The message body area is expanded to show that the CS1000E SDP answer contains the chosen codec G.729 with “annexb=no”. Note that the CS1000E message body does not contain the MIME multipart message body for an incoming call. Although not illustrated, CS1000E includes the user’s Directory Number in the PAI in 180 Ringing and 200 OK, and Session Manager adapts the DN to the Verizon DID 732-945-0235.

No. .	Time	Source	Destination	Protocol	Info
506	16.523433	65.206.67.1	10.1.2.210	SIP/SDP	Request: INVITE sip:7329450235@10.1.2.210:5060;transport=tcp, with session description
507	16.525452	10.1.2.210	65.206.67.1	SIP	Status: 100 Trying
510	16.569093	10.1.2.210	10.7.7.60	SIP/SDP	Request: INVITE sip:57003@avaya.com:5060;transport=tcp, with session description
515	16.663451	10.7.7.60	10.1.2.210	SIP	Status: 100 Trying
517	16.663465	10.7.7.60	10.1.2.210	SIP	Status: 180 Ringing
519	16.666019	10.1.2.210	65.206.67.1	SIP	Status: 180 Ringing
921	26.202065	10.7.7.60	10.1.2.210	SIP/SDP	Status: 200 OK, with session description
924	26.204747	10.1.2.210	65.206.67.1	SIP/SDP	Status: 200 OK, with session description

Content-Type: application/sdp
Content-Length: 251
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): - 26585 1 IN IP4 10.7.7.60
Session Name (s): -
Connection Information (c): IN IP4 10.7.7.123
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 5200 RTP/AVP 18 101 111
Connection Information (c): IN IP4 10.7.7.123
Media Attribute (a): ptim:20
Media Attribute (a): ftmp:18 annexb=no
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute (a): ftmp:101 0-15
Media Attribute (a): rtpmap:111 X-nt-inforeq/8000
Media Attribute (a): sendrecv

9.3. System Manager and Session Manager Verification

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

9.3.1 Verify SIP Entity Link Status

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

From the list of monitored entities, select an entity of interest, such as “Acme1”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. The **Reason Code** column indicates that the SBC has responded to SIP OPTIONS from Session Manager with a SIP 200 OK message. When Session Manager sends SIP OPTIONS to the Acme Packet SBC, the SBC proxies the SIP OPTIONS to Verizon. When Verizon responds with a 200 OK, a 200 OK is sent back to Session Manager.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring- SIP Entity Monitoring

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: Acme1

Summary View

1 Item	Refresh						Filter: E
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Sta
► Show	SM1	65.206.67.1	5060	TCP	Up	200 OK	Up

If **Show** under **Details** is selected, additional time information is presented as shown below.

All Entity Links to SIP Entity: Acme1

Summary View							
1 Item Refresh							
Filter: Enabled							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM1	65.206.67.1	5060	TCP	Up	200 OK	Up
Time Last Down	Time Last Up	Last Message Sent	Last Message Response		Last Response Latency (ms)		
Never	Jun 7, 2011 9:22:06 AM EDT	Jun 7, 2011 9:23:17 AM EDT			130		

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

All Entity Links to SIP Entity: CS1000-R75

Summary View							
1 Item Refresh							
Filter: Enabled							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM1	10.7.7.60	5060	TCP	Up	200 OK	Up
Time Last Down	Time Last Up	Last Message Sent	Last Message Response		Last Response Latency (ms)		
Jun 1, 2011 10:16:31 AM EDT	Jun 1, 2011 10:18:40 AM EDT	Jun 7, 2011 9:23:59 AM EDT			9		

9.3.2 Call Routing Test

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

Call Routing Test

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

SIP INVITE Parameters

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

Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Verizon. In this case, the “Ranking” in the Routing Policy for Acme1 and Acme2 were the same (default 0, see Section 6.6). Under **Routing Decisions**, observe that the call will route via an Acme Packet Net-Net SBC on the path to Verizon. In this example, Acme2 would have been selected before Acme1. If the “Execute Test” button is pressed multiple times without changing the request parameters, some results will list Acme1 before Acme2, and other results will list Acme2 before Acme1. The domain sent to the SBC on the way to Verizon is adapted by Session Manager to “pcelban0001.avayalincroft.globalipcom.com”. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Call Routing Test

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

SIP INVITE Parameters

Called Party URI <input type="text" value="19088485704@avaya.com"/>	Calling Party Address <input type="text" value="10.7.7.60"/>
Calling Party URI <input type="text" value="anyuser@avaya.com"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Tuesday"/>	Time (UTC) <input type="text" value="16:29"/>
Called Session Manager Instance <input type="text" value="SM1"/>	Transport Protocol <input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

Routing Decisions

Route < sip:19088485704@pcelban0001.avayalincroft.globalipcom.com > to SIP Entity Acme1 (65.206.67.1). Terminating Location is Acme1.
Route < sip:19088485704@pcelban0001.avayalincroft.globalipcom.com > to SIP Entity Acme2 (65.206.67.21). Terminating Location is Acme2.

As another example, the following screen shows a call routing test for an inbound call from the PSTN to the enterprise, arriving via Acme Packet SBC “Acme1”. Under **Routing Decisions**, observe that the call will route to the CS1000E (10.7.7.60) using the SIP entity named “CS1000-R75”. The user part of the Request-URI is adapted from the Verizon DID “7329450235” to the CS1000E Directory Number 57003. The host part of the Request-URI is adapted from the enterprise domain know to Verizon “adevc.avaya.globalipcom.com” to the domain “avaya.com” configured in the CS1000E for the shared Avaya Solution and Interoperability Lab test network. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Call Routing Test

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

SIP INVITE Parameters

Called Party URI 7329450235@adevc.avaya.globalipcom.com	Calling Party Address 65.206.67.1
Calling Party URI anyuser@anyhost.com	Session Manager Listen Port 5060
Day Of Week Tuesday	Time (UTC) 12:50
Called Session Manager Instance SM1	Transport Protocol TCP
Execute Test	

Routing Decisions

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

The following screen shows a similar call routing test, using the IP Address of “Acme2” in the Calling Party Address field. The routing decision is identical, since inbound calls from “Acme1” and “Acme2” are configured to behave the same.

Home / Elements / Session Manager / System Tools / Call Routing Test- Call Routing Test

Call Routing Test

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

SIP INVITE Parameters

Called Party URI 7329450235@adevc.avaya.globalipcom.com	Calling Party Address 65.206.67.21
Calling Party URI anyuser@anyhost.com	Session Manager Listen Port 5060
Day Of Week Tuesday	Time (UTC) 12:50
Called Session Manager Instance SM1	Transport Protocol TCP
Execute Test	

Routing Decisions

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

9.4. Acme Packet Net-Net Session Border Controller Verification

This section contains a basic verification that may be performed using the Acme Packet Net-Net Session Border Controller. Consult Acme Packet documentation for additional information.

The command “show sipd agent” may be used to determine the service state and basic call information for defined session agents. As an example, the following command was run on “Acme1” with two inbound calls up from the Verizon IP Trunk Service to Avaya CS1000E users. The output has been edited to remove all session agents that are not related to these Application Notes. Note that the Session Manager session agent 10.1.2.210 is marked with an “I” for in-service and shows a “2” in the Active column under Outbound. Similarly, note that the Verizon IP Trunk Service session agent 172.30.209.21 is marked with an “I” for in-service and shows a “2” in the Active column under Inbound.

```
acmesbc-pri# show sipd agent
11:58:02-57 (recent)
```

Session Agent	----- Inbound -----			----- Outbound -----			-- Latency --		Max Burst
	Active	Rate	ConEx	Active	Rate	ConEx	Avg	Max	
10.1.2.210	I	0	0.0	0	2	0.0	0	0.003	2
172.30.209.21	I	2	0.0	0	0	0.0	0	0.000	2

10. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager 6.1, and the Acme Packet Net-Net Session Border Controller Release 6.2 can be configured to interoperate successfully with Verizon Business IP Trunk service, inclusive of the “2-CPE” SIP trunk redundancy architecture. This solution allows Avaya Communication Server 1000E users access to the PSTN using the Verizon Business IP Trunk Service.

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

Avaya Communication Server 1000E

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

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

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

Avaya Aura® Communication Manager and Avaya Aura® Session Manager have been certified with Verizon IP Trunk Service by both Avaya and Verizon using the Acme Packet SBC as shown in the Application Notes below.

[VZ-IP-Trunk-CM] Application Notes for Avaya Aura® Communication Manager 6.0, Avaya Aura® Session Manager 6.0, and Acme Packet Net-Net SBC, Issue 1.1

http://devconnect.avaya.com/public/download/dyn/SM6Acme_VzB_IPT.pdf

11.2. Verizon Business

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

- [VZ-Test-Plan] Test Suite for Retail VoIP Interoperability IP Trunking, Version 2.1, 01-18-2011
- [VZ-Spec] Retail VoIP Network Interface Specification (for non-registering devices), Date of Issue 12-10-2010

11.3. Acme Packet

Acme Packet product documentation is available at <http://www.acmepacket.com>. A support account may be required to access the Acme Packet documentation.

©2011 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.