



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Avaya Communication Server 1000E 7.5, Avaya Aura® Session Manager 6.2, Acme Packet 3820 Net-Net® Session Director 6.3.0 with CenturyLink SIP Trunk Service (Legacy Qwest) – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Avaya Aura® Session Manager, and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	5
2.3.	Support .....	6
3.	Reference Configuration .....	6
4.	Equipment and Software Validated .....	7
5.	Configure Avaya Communication Server 1000E .....	7
5.1.	Administer an IP Telephony Node.....	9
5.1.1.	Obtain Node IP Address .....	9
5.1.2.	Terminal Proxy Server (TPS) .....	10
5.1.3.	Quality of Service (QoS) .....	11
5.1.4.	Voice Gateway and Codecs .....	12
5.1.5.	SIP Gateway.....	13
5.1.6.	Synchronize Node Configuration .....	16
5.2.	Virtual Superloops.....	18
5.3.	Media Gateway .....	18
5.4.	Virtual D-Channel, Routes and Trunks.....	22
5.4.1.	Virtual D-Channel Configuration .....	22
5.4.2.	Routes and Trunks Configuration .....	24
5.5.	Dialing and Numbering Plans .....	26
5.5.1.	Route List Block .....	26
5.5.2.	NARS Access Code .....	28
5.5.3.	Numbering Plan Area Codes .....	29
5.5.4.	Special Numbers to Route to Session Manager.....	31
5.5.5.	Incoming Digit Translation.....	32
5.6.	Zones and Bandwidth.....	33
5.7.	Example CS1000E Telephone Users .....	35
5.7.1.	Example SIP Phone DN 7108, Codec Considerations.....	35
5.7.2.	Example Digital Phone DN 7107 with Call Waiting.....	36
5.7.3.	Example Analog Port with DN 7106, Fax .....	37
5.8.	Save Configuration.....	38
6.	Configure Avaya Aura® Session Manager .....	39
6.1.	Avaya Aura® System Manager Login and Navigation .....	39
6.2.	Add/View Avaya Aura® Session Manager Instance .....	41
6.3.	Specify SIP Domain .....	43
6.4.	Add Location.....	43
6.5.	Adaptations.....	47
6.6.	Add SIP Entities .....	50
6.7.	Add Entity Links .....	54
6.8.	Add Routing Policies .....	54

6.9.	Add Dial Patterns .....	56
7.	Configure Acme Packet 3820 Net-Net® Session Director.....	59
7.1.	Acme Packet Command Line Interface Summary .....	61
7.2.	System Configuration.....	62
7.3.	Physical and Network Interfaces.....	63
7.4.	Realm .....	65
7.5.	SIP Configuration.....	67
7.6.	SIP Interface.....	68
7.7.	Session Agent.....	69
7.8.	Session Agent Group.....	72
7.9.	SIP Manipulation.....	73
7.10.	Steering Pools .....	77
7.11.	Local Policy .....	77
8.	CenturyLink SIP Trunk Service Configuration .....	79
9.	Verification .....	79
9.1.	Avaya Communication Server 1000E Verifications.....	79
9.1.1.	IP Network Maintenance and Reports Commands.....	79
9.1.2.	System Maintenance Commands.....	81
9.2.	Avaya Aura® Session Manager Verifications .....	82
10.	Conclusion .....	83
11.	Additional References.....	84
	Appendix A: Acme Packet 3820 Configuration .....	85

# 1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E release 7.5 Avaya Aura® Session Manager 6.2, and Acme Packet 3820 Net-Net Session Director 6.3.0 (Acme Packet 3820) integration with CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6. CenturyLink can offer SIP trunk service using several different platform technologies in the CenturyLink network. These Application Notes correspond to the SIP trunk service offered using a Sonus platform in the network.

In the sample configuration, the Acme Packet 3820 is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Acme Packet 3820 performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

CenturyLink SIP Trunk is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

CenturyLink SIP Trunk will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). CenturyLink SIP Trunk will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

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

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Communication Server 1000E (CS1000E), Session Manager, and Acme Packet 3820 to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunk service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

## 2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included UNISTim, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included UNISTim, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, emergency calls (911) and local directory assistance (411).
- Inbound toll-free calls.
- Codecs G.729A, G.729B and G.711MU.
- DTMF transmission using RFC 2833.
- T.38 Fax.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and Mobile-X (extension to cellular).

Items not supported or not tested included the following:

- SIP REFER method is not supported by Avaya CS1000E.
- Mid-Call features using Mobile-X were not tested.

## 2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk solution. It is listed here simply as an observation.
- **Mobile-X:** Mobile-X extended calls does not contain the original called party number in the FROM or PAI headers. CenturyLink requires a valid phone number in the FROM, PAI or Diversion headers to allow the call to go through. A header manipulation rule was created in the Acme Packet 3820 to add a valid Diversion header for Mobile-X calls. See **Section 7.9** and **Appendix A**.

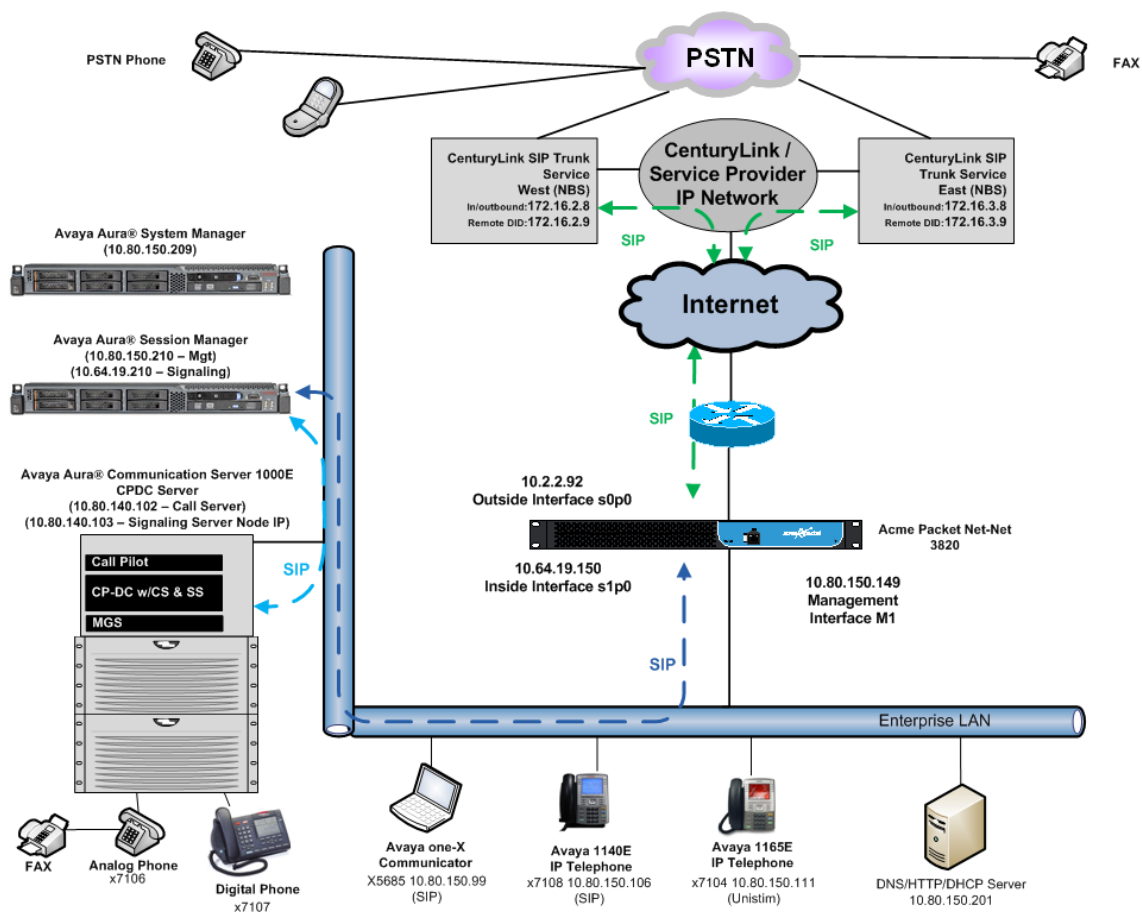
CenturyLink SIP Trunk (Legacy Qwest) passed compliance testing.

## 2.3. Support

For technical support on the CenturyLink SIP Trunk service, contact CenturyLink using the Customer Care links at [www.centurylink.com](http://www.centurylink.com).

## 3. Reference Configuration

**Figure 1** illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the CenturyLink SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Acme Packet 3820 provides NAT functionality and SIP header manipulation. The Acme Packet 3820 receives traffic from CenturyLink SIP Trunk on port 5060 and sends traffic to the CenturyLink SIP Trunk using destination port 5060, using the UDP protocol. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.



**Figure 1: Avaya Interoperability Test Lab Configuration**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya IP Telephony Solution Components	
Component	Release
Avaya Communication Server 1000E running on CP+DC server as co-resident configuration	<ul style="list-style-type: none"><li>• Call Server: 7.50 .17 GA (CoRes) Service Pack: 7.50.17_20120110</li><li>• SSG Server: 7.50.17 GA</li><li>• SLG Server: 7.50.17 GA</li></ul>
Communication Server 1000E Media Gateway	CSP Version: MGCC CD02 MSP Version: MGCM AB01 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP4 AB01 BCSP Version: MGCC CD01
Acme Packet Net-Net Session Director 3820	6.3.0 MR-1
Avaya 1165E (UNISim)	0626C8A
Avaya 1140E (SIP)	04.03.09.00
Avaya one-X Communicator (SIP)	CS6.1.1.02
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
Sonus Network Border Switch (NBS)	07.03.05 R006

Table 1: Equipment and Software Tested

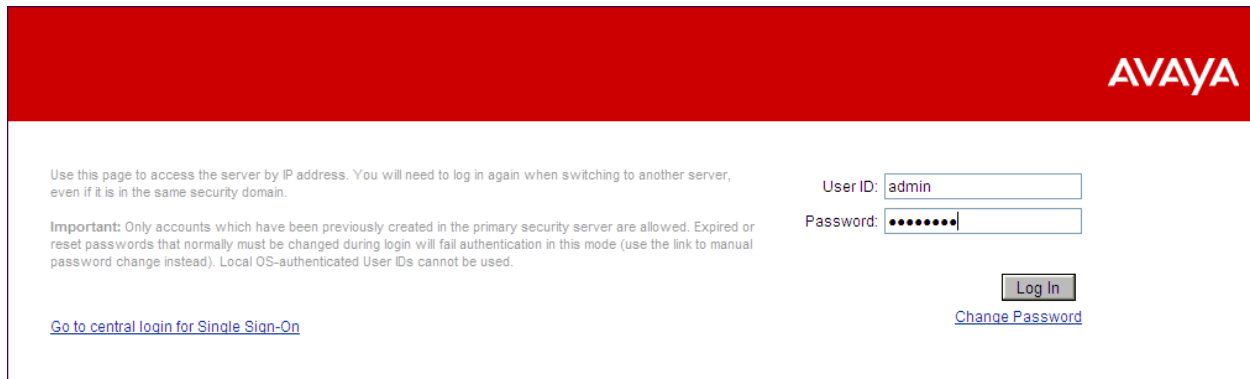
The specific configuration above was used for the compatibility testing.

## 5. Configure Avaya Communication Server 1000E

This section describes the Avaya Communication Server 1000E configuration, focusing on the routing of calls to CenturyLink over a SIP trunk. In the sample configuration, Avaya Communication Server 1000E Release 7.5 was deployed as a co-resident system with the SIP Signaling Server, and Call Server applications all running on the same CP+DC server platform.

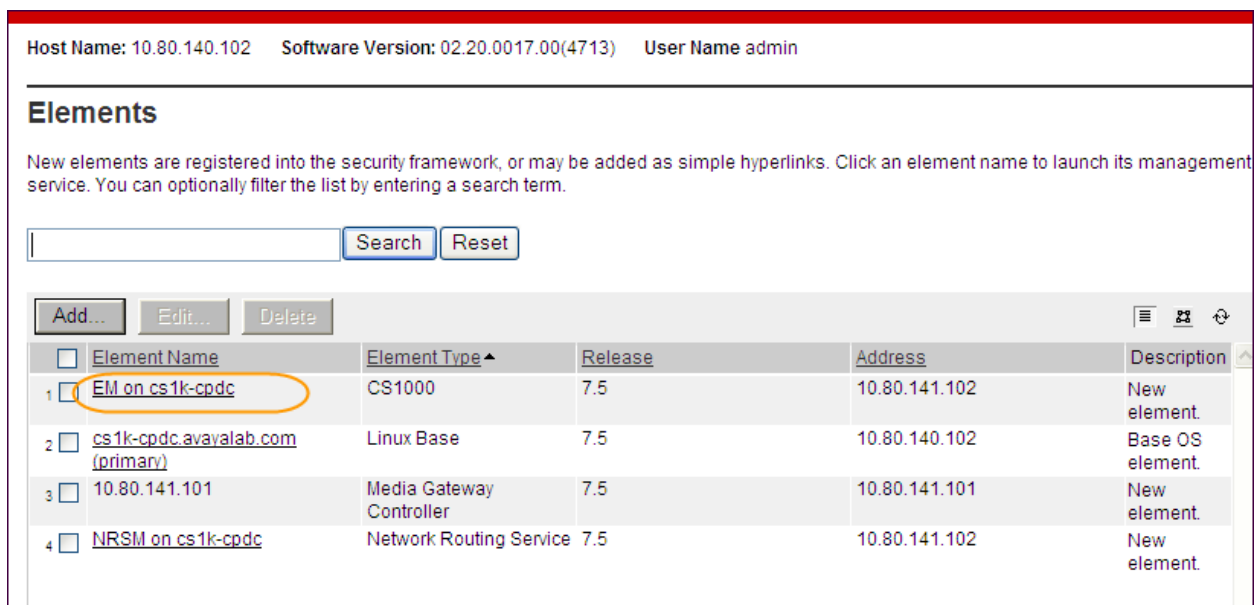
This section focuses on the SIP Trunking configuration. Although sample screens are illustrated to document the overall configuration, it is assumed that the basic configuration of the Call Server and SIP Signaling Server applications has been completed, and that the Avaya Communication Server 1000E is configured to support analog, digital, UNISim, and SIP telephones. 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://<ipaddress>> where the relevant <ipaddress> in the sample configuration is 10.80.140.102. The following screen shows an abridged log in screen. Log in with appropriate credentials.



The login screen features a red header with the AVAYA logo. Below the header, there is a white area with instructions and login fields. The instructions state: "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." and "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." The login fields include "User ID:" with the value "admin" and "Password:" with a masked password "\*\*\*\*\*". There are "Log In" and "Change Password" buttons. A link "Go to central login for Single Sign-On" is also present.

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 cs1k-cpdc**.



The Elements page shows a table of registered elements. The table has columns: Element Name, Element Type, Release, Address, and Description. The first element, "EM on cs1k-cpdc", is highlighted with an orange circle. The table also includes a search bar and buttons for "Add...", "Edit...", and "Delete".

	Element Name	Element Type	Release	Address	Description
1	EM on cs1k-cpdc	CS1000	7.5	10.80.141.102	New element.
2	cs1k-cpdc.avayalab.com (primary)	Linux Base	7.5	10.80.140.102	Base OS element.
3	10.80.141.101	Media Gateway Controller	7.5	10.80.141.101	New element.
4	NRSM on cs1k-cpdc	Network Routing Service	7.5	10.80.141.102	New element.



## 5.1. Administer an IP Telephony Node

This section describes how to configure an IP Telephony Node on the Communication Server 1000E.

### 5.1.1. Obtain Node IP Address

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 1005** was used.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'System' expanded and 'Nodes: Servers, Media Cards' selected. The main content area is titled 'IP Telephony Nodes' and shows a table of nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. Node 1005 is highlighted, showing it is a SIP Line, LTPS, Gateway (SIPGw) with ELAN IP 10.80.140.103 and status Synchronized. Below the table are checkboxes for 'Nodes', 'Component servers and cards', and 'IPv6 address'.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1005	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.103		Synchronized

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 **10.80.140.103**. This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E in **Section 6.6**.

The screenshot shows the 'Node Details' screen for Node ID 1005. The page title is 'Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))'. The form contains several fields: Node ID (1005), Call server IP address (10.80.141.102), Embedded LAN (ELAN) Gateway IP address (10.80.141.1) and Subnet mask (255.255.255.0), Telephony LAN (TLAN) Node IPv4 address (10.80.140.103) and Subnet mask (255.255.255.0), and a Node IPv6 address field. The 'TLAN address type' is set to 'IPv4 only'. A legend indicates that asterisks (\*) denote required values. 'Save' and 'Cancel' buttons are at the bottom right.

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

<input type="checkbox"/> Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k-cpdc	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	10.80.141.102	10.80.140.102	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.

### 5.1.2. Terminal Proxy Server (TPS)

On the **Node Details** screen, scroll down in the top window and select the **Terminal Proxy Server (TPS)** link as show below.

**AVAYA CS1000 Element Manager**

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

**Node Details (ID: 1005 - SIP Line, LTPS, Gateway ( SIPGw ))**

Subnet mask: 255.255.255.0 \* Subnet mask: 255.255.255.0 \*  
Node IPv6 address:

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

- SIP Line
- Terminal Proxy Server (TPS)**
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

\* Required Value.

Check the **UNISTim Line Terminal Proxy Server** check box and then click the **Save** button (not shown).

**AVAYA CS1000 Element Manager**

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » UNISTim Line Terminal Proxy Server (LTPS) Configuration

**Node ID: 1005 - UNISTim Line Terminal Proxy Server (LTPS) Configuration Details**

**Firmware | DTLS | Network Connect Server**

UNISTim Line Terminal Proxy Server: ☒ Enable proxy service on this node

**Firmware**

IP address: 0.0.0.0  
Full file path: download/firmwa  
Server Account/User ID:   
Password:

**DTLS**

DTLS policy: Off

### 5.1.3. Quality of Service (QoS)

On the **Node Details** screen, scroll down in the top window and select the **Quality of Service (QoS)** link as shown below.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1005 - SIP Line, LTPS, Gateway ( SIPGw ))

Subnet mask: 255.255.255.0 \*      Subnet mask: 255.255.255.0 \*  
Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value.      Save      Cancel

Set the **Control packets** and **Voice packets** values to the desired Diffserv settings required on the internal network. The default Diffserv values are shown below. Click on the **Save** button.

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Quality of Service (QoS)

Node ID: 1005 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☐

Control packets: 41 (0-63)  
Voice packets: 47 (0-63)

VLAN tagging: ☐ 802.1Q support

802.1Q bits value (802.1P): 6 (0-7)

\* Required Value.      Note: Changes made on this page will NOT be transmitted until the Node is also saved.      Save      Cancel

### 5.1.4. Voice Gateway and Codecs

On the **Node Details** screen, scroll down in the top window and select the **Voice Gateway (VGW) and Codecs** link as shown below.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1005 - SIP Line, LTPS, Gateway ( SIPGw ))

Subnet mask: 255.255.255.0 \* Subnet mask: 255.255.255.0 \*  
Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value.

Save Cancel

The following screen shows the General parameters used in the sample configuration.

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1005 - Voice Gateway (VGW) and Codecs

General | Voice Codescs | 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 (squellch DTMF from TDM to IP)  
☒ Modem/Fax pass-through  
☒ V.21 Fax tone detection  
☐ R factor calculation

Voice Codescs

Codec G711: ☒ Enabled (required)  
Voice payload size: 20 (milliseconds per frame)  
Voice playout (litter buffer) delay: 40 80 (milliseconds)

\* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Save Cancel

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 G.711: ☒ 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. In the sample configuration, the CS1000E was configured to include G.729A and G.711 in SDP Offers, in that order. During compliance testing, the G.729B codec was also tested by checking the **Voice Activity Detection (VAD)** box.

**General | Voice Codecs | Fax**

Codec G.729: ☒ 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)

### 5.1.5. SIP Gateway

The SIP Gateway is the SIP trunk between the CS1000E and Session Manager. On the **Node Details** screen, scroll down in the top window and select the **Gateway (SIPGw)** link as show below.

**AVAYA CS1000 Element Manager**

Managing: 10.80.141.102 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

**Node Details (ID: 1005 - SIP Line, LTPS, Gateway ( SIPGw ))**

Subnet mask: 255.255.255.0 \*

Subnet mask: 255.255.255.0 \*

Node IPv6 address:

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)**
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

\* Required Value.

Save Cancel

On the **Node ID: <id> – Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields.

- **Sip domain name:** Enter the appropriate SIP domain for the customer network. In the sample configuration, **avayalab.com** was used in the Avaya Solutions and Interoperability Test lab environment.
- **Local SIP port:** Enter **5060**.
- **Gateway endpoint name:** Enter a descriptive name.
- **Application node ID:** Enter **<Node id>**. In the sample configuration, Node **1005** was used matching the node shown in **Section 5.1.1**.

The values defined for the sample configuration are shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header shows the AVAYA logo and the title "CS1000 Element Manager". Below the header, a navigation tree on the left lists various system components like "UCM Network Services", "Home", "Links", "System", "Alarms", "Maintenance", "Core Equipment", "Peripheral Equipment", "IP Network", "Nodes: Servers, Media Cards", "Maintenance and Reports", "Media Gateways", "Zones", "Host and Route Tables", "Network Address Translation (NAT)", "QoS Thresholds", "Personal Directories", "Unicode Name Directory", "Interfaces", "Engineered Values", "Emergency Services", "Software", "Customers", "Routes and Trunks", "Routes and Trunks", "D-Channels", "Digital Trunk Interface", "Dialing and Numbering Plans", "Electronic Switched Network", and "Flexible Code Restriction". The main content area is titled "Node ID: 1005 - Virtual Trunk Gateway Configuration Details". It features a breadcrumb trail: "System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration". Below the breadcrumb, there are tabs for "General", "SIP Gateway Settings", and "SIP Gateway Services". The "General" tab is active, showing a "Vtrk gateway application" section with a checkbox "Enable gateway service on this node" which is checked. The "General" section contains several input fields: "Vtrk gateway application" (a dropdown menu set to "SIP Gateway (SIPGw)"), "SIP domain name" (text box with "avayalab.com"), "Local SIP port" (text box with "5060" and a note "(1 - 65535)"), "Gateway endpoint name" (text box with "node1005"), "Gateway password" (text box), and "Application node ID" (text box with "1005" and a note "(0-9999)"). There is also a checkbox for "Enable failsafe NRS" which is unchecked. Below these fields, it says "SIP ANAT: IPv4" with a radio button selected. To the right of the "General" section is the "Virtual Trunk Network Health Monitor" section, which includes a checkbox "Monitor IP addresses (listed below)" which is unchecked. Below this checkbox, it says "Information will be captured for the IP addresses listed below." There is a "Monitor IP:" text box followed by an "Add" button. Below that is a "Monitor addresses:" section with a large empty text box and a "Remove" button. At the bottom of the page, there is a note: "Note: Changes made on this page will NOT be transmitted until the Node is also saved." and two buttons: "Save" and "Cancel".

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 **10.64.19.210** was used.
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**

The values defined for the sample configuration are shown below.

The screenshot shows the 'SIP Gateway Settings' tab in a web interface. Under the 'Proxy Or Redirect Server:' section, 'Proxy Server Route 1:' is selected. The configuration fields are as follows:

- Primary TLAN IP address:** 10.64.19.210 (with a tooltip: 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"')
- Port:** 5060 (range 1 - 65535)
- Transport protocol:** TCP (dropdown menu)
- Options:** ☐ Support registration, ☐ Primary CDS proxy
- Secondary TLAN IP address:** 0.0.0.0 (with a tooltip: 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"')
- Port:** 5060 (range 1 - 65535)
- Transport protocol:** TCP (dropdown menu)

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

The screenshot shows the 'SIP Gateway Settings' tab in a web interface. Under the 'Proxy Or Redirect Server:' section, 'Proxy Server Route 2:' is selected. The configuration fields are as follows:

- Primary TLAN IP address:** 10.64.19.210 (with a tooltip: 'The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"')
- Port:** 5060 (range 1 - 65535)
- Transport protocol:** TCP (dropdown menu)
- Options:** ☐ Registration not supported, ☐ Primary CDS proxy

Scroll down to the **SIP URI Map** section. The values defined for the sample configuration are shown below. 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 To and From headers. If the value is configured to blank, the CS1000E will omit the “phone-context=” in the SIP header altogether.

SIP URI Map:	
Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text" value="udp"/>
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.

### 5.1.6. Synchronize Node Configuration

On the **Node Details** screen click **Save** as shown below.

**AVAYA CS1000 Element Manager**

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

**Node Details (ID: 1005 - SIP Line, LTPS, Gateway ( SIPGw ))**

☐ IPv4 and IPv6

Embedded LAN (ELAN)	Telephony LAN (TLAN)
Gateway IP address: <input type="text" value="10.80.141.1"/>	Node IPv4 address: <input type="text" value="10.80.140.103"/>
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**

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)

**Applications (click to edit configuration)**

- SIP Line
- Terminal Proxy Server (TPS)

\* Required Value.

**Save** **Cancel**



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

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Node Saved

### Node Saved

Node ID: 1005 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

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

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. Place a check mark next to the appropriate Hostname and click **Start Sync**. The screen will automatically refresh until the synchronization is finished.

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

### Synchronize Configuration Files (Node ID <1005>)

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"/>	cs1k-cpdc	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, place a check mark next to the appropriate Hostname and click **Restart Applications**.

Managing: 10.80.141.102 Username: admin  
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

### Synchronize Configuration Files (Node ID <1005>)

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

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

## 5.2. Virtual Superloops

Expand **System** → **Core Equipments** on the left panel and select **Superloops**. In the sample configuration, Superloop 4 is for the Media Gateway and Superloop 252 is the virtual Superloop used by the IP phones and SIP trunks.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Loops, Superloops (selected), MSDL/MISP Cards, Conference/TDS/Multifrequency, Tone Senders and Detectors, Peripheral Equipment, IP Network, and Interfaces. The main content area is titled 'Superloops' and shows a table with two entries: Superloop 4 (IPMG) and Superloop 252 (Virtual). Above the table are buttons for 'Add...', 'Delete', and 'Refresh'. The top of the page displays the managing IP (10.80.141.102) and username (admin).

Superloop Number	Superloop Type
1 <input type="radio"/> 4	IPMG
2 <input type="radio"/> 252	Virtual

## 5.3. Media Gateway

Expand **System** → **IP Network** on the left panel and select **Media Gateways**. Click the link in the **Type** column for the appropriate Media Gateway to be modified as shown below.

The screenshot shows the 'Media Gateways' configuration page. It features a table with columns for IPMG, IP Address, Zone, and Type. There are two entries: one with IPMG 004.00 and IP Address 10.80.141.101, and another with IPMG 004.01 and IP Address 10.80.141.201. Both have Zone 1 and Type MGS. The 'MGS' link in the Type column of the first row is circled in orange. Above the table are buttons for 'Add...', 'Digital Trunking...', 'Reboot', 'Delete', 'Virtual Terminal', and 'More Actions', along with a 'Refresh' link.

IPMG	IP Address	Zone	Type
004.00	10.80.141.101	1	<a href="#">MGS</a>
004.01	10.80.141.201	1	<a href="#">MGS</a>

The **IPMG 4 0 Media Gateway Survivable(MGS) Configuration** window appears. 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 CenturyLink SIP Trunk, the IP Address in the SDP in the INVITE message will be **10.80.140.104** in the sample configuration.

**AVAYA CS1000 Element Manager**

Managing: **10.80.141.102** Username: admin  
System » IP Network » **Media Gateways** » IPMG 4 0 Media Gateway Survivable(MGS) Configuration

**IPMG 4 0 Media Gateway Survivable(MGS) Configuration**

- UCM Network Services
  - Home
  - Links
    - Virtual Terminals
  - System
    - + Alarms
    - Maintenance
    - + Core Equipment
    - Peripheral Equipment
    - IP Network
      - Nodes: Servers, Media Cards
      - Maintenance and Reports
      - **Media Gateways**
      - Zones
      - Host and Route Tables
      - Network Address Translation
      - QoS Thresholds
      - Personal Directories
      - Unicode Name Directory
    - + Interfaces
    - Engineered Values
    - + Emergency Services
    - + Software
  - Customers
    - Routes and Trunks
      - Routes and Trunks
      - D-Channels
      - Digital Trunk Interface
  - Dialing and Numbering Plans
    - Electronic Switched Network
    - Flexible Code Restriction
    - Incoming Digit Translation
  - Phones
    - Templates
    - Reports

**- Media Gateway (MGS)**

Hostname:  \*

Embedded LAN (ELAN) IP address:

Embedded LAN (ELAN) gateway IP address:

Embedded LAN (ELAN) subnet mask:

Telephony LAN (TLAN) IP address:

Telephony LAN (TLAN) gateway IP address:

Telephony LAN (TLAN) subnet mask:

**- DSP Daughterboard**

Type of the DSP daughterboard:  ▼

Telephony LAN (TLAN) IP address:

Telephony LAN (TLAN) gateway IP address:

Telephony LAN (TLAN) IPv6 address:

Telephony LAN (TLAN) subnet mask:

Hostname:  \*

+ /GW and IP phone codec profile

Scroll down to the area of the screen containing **VGW and IP phone codec profile** and expand it. The fax T.38 settings used for compliance testing is shown below.

**AVAYA CS1000 Element Manager**

- UCM Network Services

- [Home](#)

- Links

- Virtual Terminals

- System

+ Alarms

- Maintenance

+ Core Equipment

- Peripheral Equipment

- IP Network

- Nodes: Servers, Media Cards

- Maintenance and Reports

- [Media Gateways](#)

- Zones

- Host and Route Tables

- Network Address Translation

- QoS Thresholds

- Personal Directories

- Unicode Name Directory

+ Interfaces

- Engineered Values

+ Emergency Services

+ Software

- Customers

- Routes and Trunks

- Routes and Trunks

- D-Channels

- Digital Trunk Interface

- Dialing and Numbering Plans

- Electronic Switched Network

- Flexible Code Restriction

- Incoming Digit Translation

- VGW and IP phone codec profile

Enable echo canceller ☒

Echo canceller tail delay  ( milliseconds )

Enable dynamic attenuation ☒

Voice activity detection threshold  ( 0 - 4 DBM )

Idle noise level  ( 0 - 1 DBM )

R factor calculation ☐

DTMF tone detection ☒

Enable low latency mode ☒

Remove DTMF delay (squench DTMF from TDM to IP) ☒

Enable modem/fax pass through mode ☒

Enable V.21 FAX tone detection ☒

Fax TCF method

FAX maximum rate  ( bps )

FAX playout nominal delay  ( 0 - 300 milliseconds )

FAX no activity timeout  ( 10 - 32000 milliseconds )

FAX packet size

+ Codec **G711** Select ☒

The **Codec G.711** is enabled by default. Ensure that the **Select** box is checked for **Codec G729A** and the **VAD** (Voice Activity Detection) box is un-checked. The **Voice payload size** of **20** can be used with CenturyLink SIP Trunk for both G.729A and G.711. Click **Save** (not shown) at the bottom of the window. Then click **OK** in the dialog box (not shown) to save the IPMG configuration. During compliance testing, the G.729B codec was also tested by checking the **Voice Activity Detection (VAD)** box. Scroll down and click **Save** and then click **OK** on the new dialog box that appears to save the configuration.

**AVAYA CS1000 Element Manager**

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

**- Codec G711** ☒ **Select**

Codec name **G711**

Voice payload size **20** (ms/frame)

Voice playback (jitter buffer) nominal delay **40**

Modifications may cause changes to dependent settings

Voice playback (jitter buffer) maximum delay **80**

Modifications may cause changes to dependent settings

VAD ☐

**- Codec G729A** ☒ **Select**

Codec name **G729A**

Voice payload size **20** (ms/frame)

Voice playback (jitter buffer) nominal delay **40**

Modifications may cause changes to dependent settings

Voice playback (jitter buffer) maximum delay **80**

Modifications may cause changes to dependent settings

VAD ☐

After the configuration is saved, the **Media Gateways** page is displayed. Select the appropriate Media Gateway and click **Reboot** to load the new configuration.

**AVAYA CS1000 Element Manager**

Managing: **10.80.141.102** Username: admin  
System » IP Network » Media Gateways

**Media Gateways**

Buttons: Add... Digital Trunking... **Reboot** Delete Virtual Terminal More Actions Refresh

	IPMG	IP Address	Zone	Type
<input checked="" type="radio"/>	004 00	10.80.141.101	1	MGS
<input type="radio"/>	004 01	10.80.141.201	1	MGS

## 5.4. 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.

### 5.4.1. Virtual D-Channel Configuration

Expand **Routes and Trunks** on the left panel and select **D-Channels**. In the sample configuration, there is a virtual D-Channel 15 associated with the Signaling Server.

The screenshot displays the Avaya Communication Server 1000E web interface. On the left is a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System (with sub-items: + Alarms, - Maintenance, + Core Equipment, - Peripheral Equipment, - IP Network, - Nodes: Servers, Media Cards, - Maintenance and Reports, - Media Gateways, - Zones, - Host and Route Tables, - Network Address Translation, - QoS Thresholds, - Personal Directories, - Unicode Name Directory), + Interfaces, - Engineered Values, + Emergency Services, + Software, - Customers, - Routes and Trunks (with sub-items: - Routes and Trunks, - D-Channels, - Digital Trunk Interface), and - Dialing and Numbering Plans. The 'D-Channels' item is selected. The main content area is titled 'D-Channels' and includes a 'Maintenance' section with links: [D-Channel Diagnostics](#) (LD 96), [Network and Peripheral Equipment](#) (LD 32, Virtual D-Channels), [MSDL Diagnostics](#) (LD 96), [TMDI Diagnostics](#) (LD 96), and [D-Channel Expansion Diagnostics](#) (LD 48). Below this is a 'Configuration' section with the text 'Choose a D-Channel Number: 0 and type: DCH' followed by a 'to Add' button. At the bottom, there is a table with one row: Channel: 15, Type: DCH, Card Type: DCIP, Description: VtrkNode1005, and an 'Edit' button.

Managing: 10.80.141.102 Username: admin  
Routes and Trunks » D-Channels

### D-Channels

#### Maintenance

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

#### Configuration

Choose a D-Channel Number: 0 and type: DCH

- Channel: 15	Type: DCH	Card Type: DCIP	Description: VtrkNode1005	<input type="button" value="Edit"/>
---------------	-----------	-----------------	---------------------------	-------------------------------------

Select **Edit** to verify the configuration, as shown below. Verify **DCIP** has been selected for **D Channel Card Type** field and the **Interface type for D-Channel** is set to **Meridian Meridian 1(SL1)**. Under the Basic Options section, verify **128** is selected for the **Output request Buffers** value.

### D-Channels 15 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	VtrkNode1005
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> <a href="#">more PRI</a>
Secondary PRI2 loops:	<input type="text"/>
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 <small>Range: 1 - 4000</small>
Signalling server resource capacity:	3700 <small>Range: 0 - 3700</small>

**- Basic options (BSCOPT)**

Primary D-channel for a backup DCH:  Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification :

- Output request Buffers: 128

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

- Channel Negotiation option: No alternative acceptable, exclusive. (1)

- Remote Capabilities: [Edit](#)

## 5.4.2. 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 panel and expand the customer number. In the example screen that follows, it can be observed that Route 15 has 32 trunks in the sample configuration.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin  
Routes and Trunks » Routes and Trunks

Help |

**Routes and Trunks**

Customer	Total routes	Total trunks	Action
- Customer: 0	2	64	<a href="#">Add route</a>
- <a href="#">Route: 15</a>	Type: TIE	Description: VTRKN1005SIP	<a href="#">Edit</a> <a href="#">Add trunk</a>
+ <a href="#">Trunk: 1 - 32</a>	Total trunks: 32		
+ <a href="#">Route: 17</a>	Type: TIE	Description: VTRKN1005SIPLINE	<a href="#">Edit</a> <a href="#">Add trunk</a>

Select **Edit** to verify the configuration, as shown below. 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.

**Customer 0, Route 15 Property Configuration**

- Basic Configuration

Route data block (RDB) (TYPE):

Customer number (CUST):

Route number (ROUT):

Designator field for trunk (DES):

Trunk type (TKTP):

Incoming and outgoing trunk (ICOG):

Access code for the trunk route (ACOD):  \*

Trunk type M911P (M911P): ☐



Further down in the **Basic Configuration** section verify the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1**. Also verify **SIP (SIP)** has been selected for **Protocol ID for the route (PCID)** field. 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. The **D channel number (DCH)** field must match the D-Channel number shown in **Section 5.4.1**.

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

- Zone for codec selection and bandwidth management (ZONE): 00099 (0 - 8000)

- Node ID of signaling server of this route (NODE): 1005 (0 - 9999)

- Protocol ID for the route (PCID): SIP (SIP) ▼

- Print correlation ID in CDR for the route (CRID): ☐

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE): Route uses ISDN Signaling Link (ISLD) ▼

- D channel number (DCH): 15 (0 - 254)

- Interface type for route (IFC): Meridian M1 (SL1) ▼

- Private network identifier (PNI): 00001 (0 - 32700)

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- Trunk route optimization (TRO): ☐

- Recognition of DT12 ABCD FALT signal for ISL (FALT): ☐

- Channel type (CHTY): B-channel (BCH) ▼

- Call type for outgoing direct dialed TIE route (CTYP): Unknown Call type (UKWN) ▼

- Insert ESN access code (INAC): ☐

- Integrated service access route (ISAR): ☐

- Display of access prefix on CLID (DAPC): ☐

- Mobile extension route (MBXR): ☒

- Screen indicator (SIND): ☒

- Mobile extension outgoing type (MBXOT): National number (NPA) ▼

- Mobile extension timer (MBXT): 0 (0 - 8000 milliseconds)

Calling number dialing plan (CNDP): Unknown (UKWN) ▼

Scroll down and expand the **Basic Route Options** section. Check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below. The DCNO is created later on in **Section 5.5.5**.

**AVAYA CS1000 Element Manager** Help | Logout

- UCM Network Services
  - Home
  - Links
    - Virtual Terminals
  - System
    - + Alarms
    - Maintenance
    - + Core Equipment
    - Peripheral Equipment
    - + IP Network
    - + Interfaces
    - Engineered Values
    - + Emergency Services
    - + Software
  - Customers
  - Routes and Trunks
    - **Routes and Trunks**
    - D-Channels
    - Digital Trunk Interface
  - Dialing and Numbering Plans
    - Electronic Switched Network
    - Flexible Code Restriction
    - Incoming Digit Translation

**- Basic Route Options**

Attendant announcement (ATAN) : No Attendant Announcement (NO) [v]

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

**North American toll scheme (NATL) : ☒**

Controls or timers (CNTL) : ☐

Conventional (Tie trunk only) (CNVT) : ☐

**Incoming DID digit conversion on this route (IDC) : ☒**

- Day IDC tree number (DCNO) : 0 (0 - 254)

- Night IDC tree number (NDNO) : 0 (0 - 254)

- Display external dialed digits (DEXT) : ☐

Multifrequency compelled or MFC signaling (MFC) : No MFC (NO) [v]

Process notification networked calls (PNNC) : ☐

## 5.5. Dialing and Numbering Plans

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 CenturyLink SIP Trunk. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks.

### 5.5.1. Route List Block

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

# CS1000 Element Manager

Managing: **10.80.141.102** Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN)

## Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - Digit Manipulation Block (DGT)
    - Home Area Code (HNPA)
    - Flexible CLID Manipulation Block (CMDB)
    - 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)

- [UCM Network Services](#)
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - [Electronic Switched Network](#)
  - Flexible Code Restriction
  - Incoming Digit Translation

The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click to **Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, route list block index **15** is used. 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.

# CS1000 Element Manager

Managing: **10.80.141.102** Username: admin  
Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » Network

## Route List Blocks

Please enter a route list index  ( 0 - 1999 )

- + Route List Block Index -- 11
- Route List Block Index -- 15

Initial Set: 0  
Number of Alternate Routing Attempts: 5  
Set Minimum Facility Restriction Level : 0

- + Data Entry Index -- 0

- + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - [Electronic Switched Network](#)
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration

Under the **Options** section, select **<Route id>** in the **Route Number** field. In the sample configuration route number **15** was used. Default values may be retained for remaining fields.

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, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Software, Customers, and Routes and Trunks. The main area is titled 'Options'. It contains several configuration fields: 'Local Termination entry' (checkbox), 'Route Number' (dropdown menu with '15' selected and highlighted by a yellow circle), 'Skip Conventional Signaling' (checkbox), 'Use Tone Detector' (checkbox), 'Conversion to LDN' (checkbox), 'Expensive Route' (checkbox), and 'Strategy on Congestion' (dropdown menu with 'No Reroute (NRR)' selected). A copyright notice at the bottom reads 'Copyright © 2002-2012 Avaya Inc. All rights reserved.'

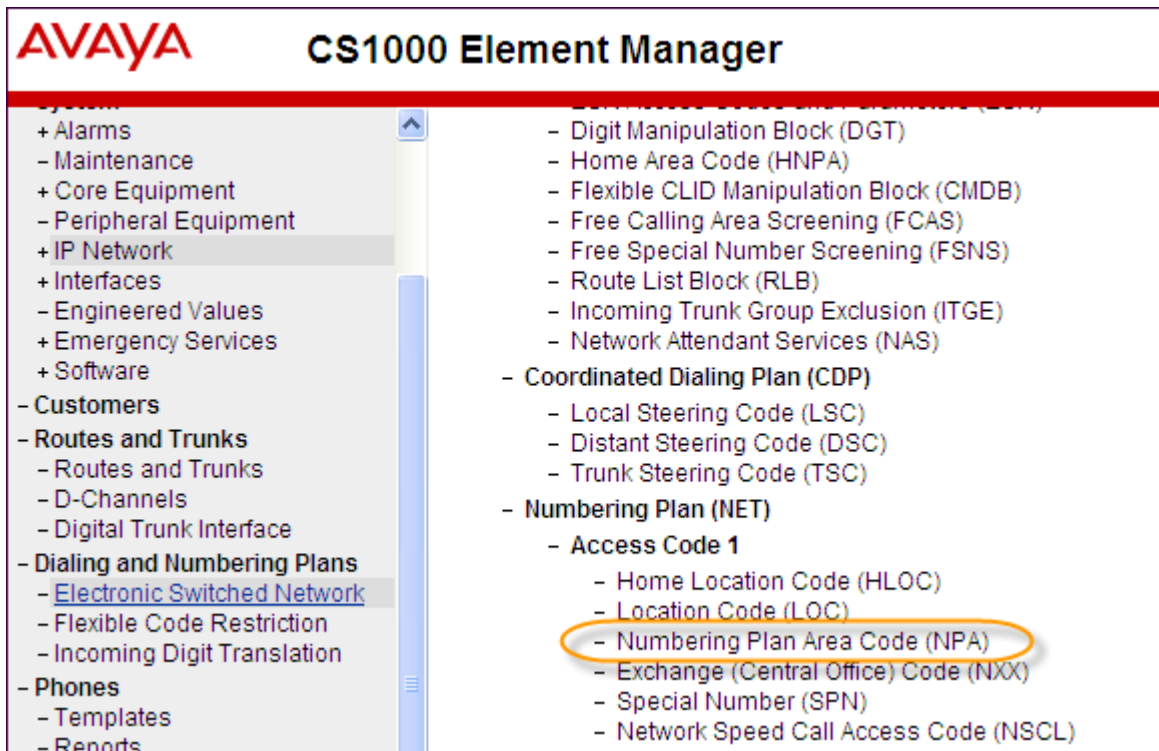
### 5.5.2. NARS Access Code

Expand **Dialing and Numbering Plans** on the left 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 5.5.1**. 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.

The screenshot shows the AVAYA CS1000 Element Manager interface for 'ESN Access Codes and Basic Parameters'. The left navigation tree is expanded to 'Dialing and Numbering Plans', with 'Electronic Switched Network' selected. The main area shows 'General Properties' for 'Managing: 10.80.141.102' with 'Username: admin'. The breadcrumb trail is 'Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Service and Basic Parameters'. The 'NARS/BARS Access Code 1' field is highlighted with a yellow circle and contains the value '9'. Other fields include 'NARS Access Code 2' (empty), 'NARS/BARS Dial Tone after dialing AC1 or AC2 access codes' (checked), 'Expensive Route Warning Tone' (checked), 'Expensive Route Delay Time' (6, range 0-10), 'Coordinated Dialing Plan feature for this customer' (checked), 'Maximum number of Steering Codes' (2000, range 1-64000), 'Number of digits in CDP DN (DSC + DN or LSC + DN)' (4, range 3-10), 'Routing Controls' (checkbox), and 'Check for Trunk Group Access Restrictions' (checkbox).

### 5.5.3. Numbering Plan Area Codes

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



Add a new NPA by entering it in the **Please enter an area code** box and click **to Add** or click **Edit** to view or change an NPA that has been previously configured. In the screen below, it can be observed that various dial strings such as **1303** and **1800** are configured.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: **10.80.141.102** Username: admin  
 Dialing and Numbering Plans » **Electronic Switched Network (ESN)** » Customer 00 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List

### Numbering Plan Area Code List

Please enter an area code

- + Numbering Plan Area Code -- 1303
- + Numbering Plan Area Code -- 1502
- + Numbering Plan Area Code -- 1615
- + Numbering Plan Area Code -- 1720
- + Numbering Plan Area Code -- 1732
- + Numbering Plan Area Code -- 1800

In the screen below, the entry for **1303** is displayed. In the Route List Index, **15** is selected to use the route list associated with the SIP Trunk to Session Manager as shown in **Section 5.4.2**. Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to Session Manager.

### Numbering Plan Area Code

#### General Properties

Numbering Plan Area code translation:

Route List Index:

Incoming Trunk group Exclusion Index:

#### 5.5.4. Special Numbers to Route to Session Manager

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

Expand **Dialing and Numbering Plans** on the left 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 5.5.3**).

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**, **411** and **911** calls are listed. Route list index **15** has been selected in the same manner as shown for the NPAs in the prior section.

The screenshot shows a web interface titled "Special Number List". At the top, there is a text input field labeled "Please enter a Special Number" followed by a "to Add" button. Below this, there is a list of four special numbers, each with an "Edit" button to its right. The entries are:

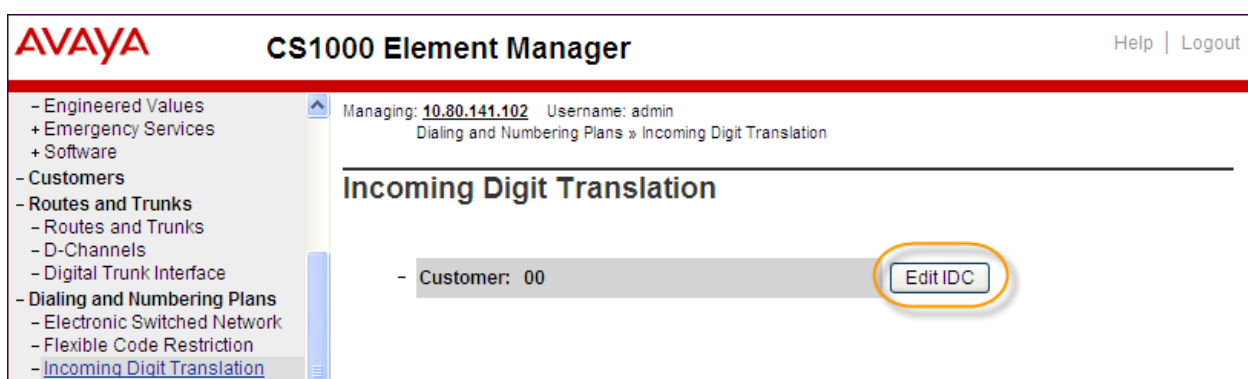
- Special Number -- 0**: Flexible length: 0, International dialing plan: NO, Type of call that is defined by the special number: NONE, Route list index: 15.
- Special Number -- 011**: Flexible length: 0, International dialing plan: YES, Type of call that is defined by the special number: INTL, Route list index: 15.
- Special Number -- 411**: Flexible length: 0, International dialing plan: NO, Type of call that is defined by the special number: NONE, Route list index: 15.
- Special Number -- 911**: Flexible length: 0, International dialing plan: NO, Type of call that is defined by the special number: NONE, Route list index: 15.



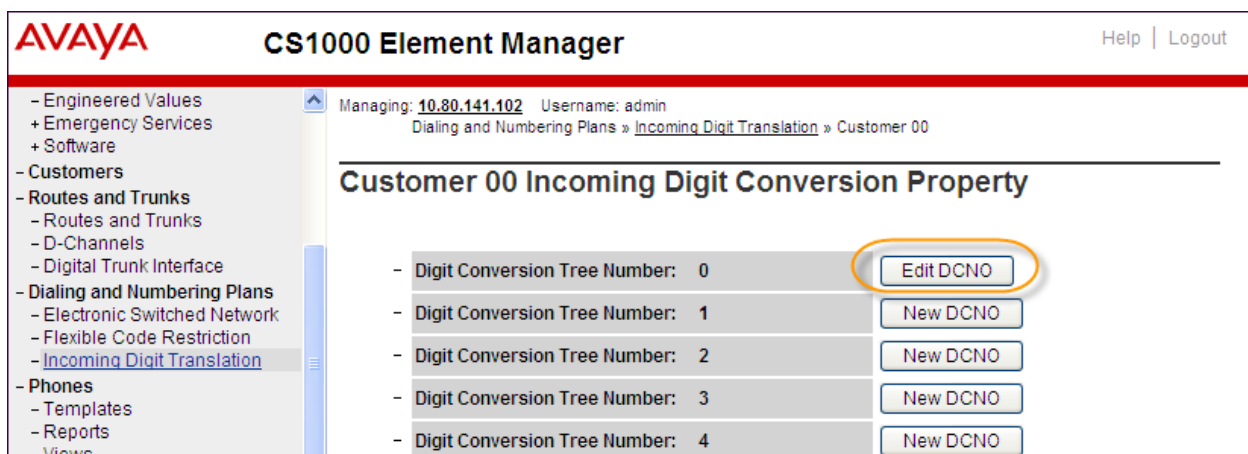
### 5.5.5. Incoming Digit Translation

In general, the incoming digit translation can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the CS1000E Incoming Digit Translation table may not be necessary. If the DID number sent by CenturyLink is unchanged by Session Manager, then the DID number can be mapped to an extension using the Incoming Digit Translation. Both Session Manager digit conversion and CS1000E incoming digit translation methods were tested successfully.

Expand **Dialing and Numbering Plans** on the left panel and select **Incoming Digit Translation**. Click on the **Edit IDC** button as shown below.



Click on the **New DCNO** to create the digit translation mechanism or if editing an existing one, select the **Edit DCNO** button next to the appropriate Digit Conversion Tree Number. In this example, **Digit Conversion Tree Number (DCNO) 0** has been created as shown below.





Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000E system phones DN. This **DCNO** has been assigned to route 15 as shown in **Section 5.4.2**.

In the following configuration, the incoming call from PSTN with the prefix 303-555-71xx will be translated to CS1000E DN 71xx. The PSTN with the prefix 614-555-01xx will be translated to CS1000E DN 51xx. The DID 303-555-7799 is translated to 5000 for Voicemail accessing purpose.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories: Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Dialing and Numbering Plans' category is expanded, showing 'Incoming Digit Translation' as the selected option. The main content area is titled 'Digit Conversion Tree 0 Configuration' and shows a 'Regular IDC tree' with 'Send calling party DID disabled'. Below this, there are buttons for 'Add...', 'Delete IDC', 'Delete IDC tree', and 'Refresh'. A table displays the configuration for three entries:

	Incoming Digits	Converted Digits	CPND Name	CPND language
1	30355571	71	,	Roman characters
2	61455501	51	,	Roman characters
3	3035557799	5000	,	Roman characters

## 5.6. Zones and Bandwidth

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar shows the 'System' category expanded, with 'IP Network' selected. The 'Zones' option is highlighted. The main content area is titled 'Zones' and contains the following text:

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

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

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

Select **Bandwidth Zones**. In the sample lab configuration, two zones are configured. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to Session Manager and click **Edit** as shown below. In the sample configuration, this is Zone number **99**.

Bandwidth Zones

Add...Edit...Import...ExportMaintenance...Delete

Refresh

	Zone +	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	1000000	BQ	1000000	BQ	SHARED	MO	IPSETS
2	99	1000000	BB	1000000	BB	SHARED	VTRK	VTRUNK

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

### Edit Bandwidth Zone

- Zone Basic Property and Bandwidth Management
- Adaptive Network Bandwidth Management and CAC
- Alternate Routing for Calls between IP Stations
- Branch Office Dialing Plan and Access Codes
- Branch Office Time Difference and Daylight Saving Time Property
- Media Services Zone Properties

The following screen shows the Zone 99 configuration. Note that **Best Bandwidth (BB)** is selected for the zone strategy parameters so that codec G.729A is preferred over codec G.711MU for calls with CenturyLink SIP Trunk.

### Zone Basic Property and Bandwidth Management

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

## 5.7. Example CS1000E Telephone Users

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


### 5.7.1. Example SIP Phone DN 7108, Codec Considerations

The following screen shows basic information for a SIP phone in the configuration. The telephone is configured as Directory Number 7108. Note that the telephone is in Zone 1 and is associated with Node 1005 (see **Section 5.1**). A call between this telephone and another telephone in Zone 1 will use a **best quality** strategy (see **Section 5.6**) and therefore can use G.711MU. If this same telephone calls out to the PSTN via the CenturyLink SIP Trunk, the call would use a **best bandwidth** strategy, and the call would use G.729A.

**AVAYA** CS1000 Element Manager Help | Logout

Managing: [EM on cs1k-cpdc\(10.80.141.102\)](#)  
[Phones»Phone Details](#)

### Phone Details

 System: EM on cs1k-cpdc  
Phone Type: UEXT-SIPL  
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) | [User Fields](#) Custom View: All

#### General Properties

Customer Number:  \*

Terminal Number:

Designation:  \* (1-6 characters)

Zone:  \*

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

Node Id:  \*

Super User: ☐

## 5.7.2. Example Digital Phone DN 7107 with Call Waiting


The following screen shows basic information for a digital phone in the configuration. The telephone is configured as Directory Number 7107.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation menu with categories like UCM Network Services, System, Customers, and Phones. The main content area is titled 'Phone Details' and shows information for a phone managed by 'EM on cs1k-cpdc(10.80.141.102)'. It includes a photo of a phone, the system name, phone type (M3904), and sync status (TRN). Below this is a 'General Properties' section with fields for Customer Number (0), Terminal Number (004 0 03 00), and Designation (DIG).

**AVAYA CS1000 Element Manager**

Managing: [EM on cs1k-cpdc\(10.80.141.102\)](#)  
[Phones»Phone Details](#)

### Phone Details

 System: EM on cs1k-cpdc  
Phone Type: M3904  
Sync Status: TRN

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

### General Properties

Customer Number:  \*

Terminal Number:

Designation:  \* (1-6 characters)

The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone. Although not shown in detail below, to use call waiting with tone, assign a key **CWT – Call Waiting**, set the feature **SWA – Call waiting from a Station** to **Allowed**, and set the feature **WTA – Warning Tone** to **Allowed**.

The screenshot shows the 'Keys' configuration page. It features a table with columns for Key No., Key Type, and Key Value. Key 0 is configured as 'SCR - Single Call Ringing' with Directory Number 7107. Key 1 is configured as 'CWT - Call Waiting'. The 'Key Value' section includes a checkbox for 'Multiple Appearance Redirection Prime(MARP)', fields for First Name (John), Last Name (Digital), Display Format (First, Last), and Language (Roman), as well as CLID Entry (0) and ANIE Entry fields.

### Keys

Key No.	Key Type	Key Value
0	SCR - Single Call Ringing	Directory Number: 7107 <input checked="" type="checkbox"/> Multiple Appearance Redirection Prime(MARP) First Name: John, Last Name: Digital, Display Format: First, Last, Language: Roman CLID Entry (Numeric or D): 0 ANIE Entry:
1	CWT - Call Waiting	

### 5.7.3. Example Analog Port with DN 7106, 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 7106.

**AVAYA****CS1000 Element Manager**

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - + Engineered Values
  - + Emergency Services
  - + Software
- Customers
- Routes and Trunks
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- **Phones**
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore
  - Date and Time
  - + Logs and reports
- Security
  - + Passwords
  - + Policies
  - + Login Options

Managing: [EM on cs1k-cpdc\(10.80.141.102\)](#)  
[Phones»Phone Details](#)

### Phone Details



System: EM on cs1k-cpdc  
Phone Type: 500  
Sync Status: TRN


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

### General Properties

Customer Number:  \*

Terminal Number:

Designation:  \* (1-6 characters)

Directory Number:  

CLID entry:

ANIE entry:

Marp ☒

First Name	Last Name	Display Format	Language
<input type="text" value="John"/>	<input type="text" value="Single"/>	<input type="text" value="First, Last"/> ▼	<input type="text" value="Roman"/> ▼

## 5.8. Save Configuration

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

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories: Phones, Tools, and Security. Under Tools, 'Backup and Restore' is expanded, showing 'Call Server' as the selected option. The main content area is titled 'Call Server Backup'. At the top of this area, it shows 'Managing: 10.80.141.102' and 'Username: admin', followed by a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. Below the title, there is an 'Action' label followed by a dropdown menu currently set to 'Backup'. To the right of the dropdown are two buttons: 'Submit' and 'Cancel'.

## 6. Configure Avaya Aura® Session Manager

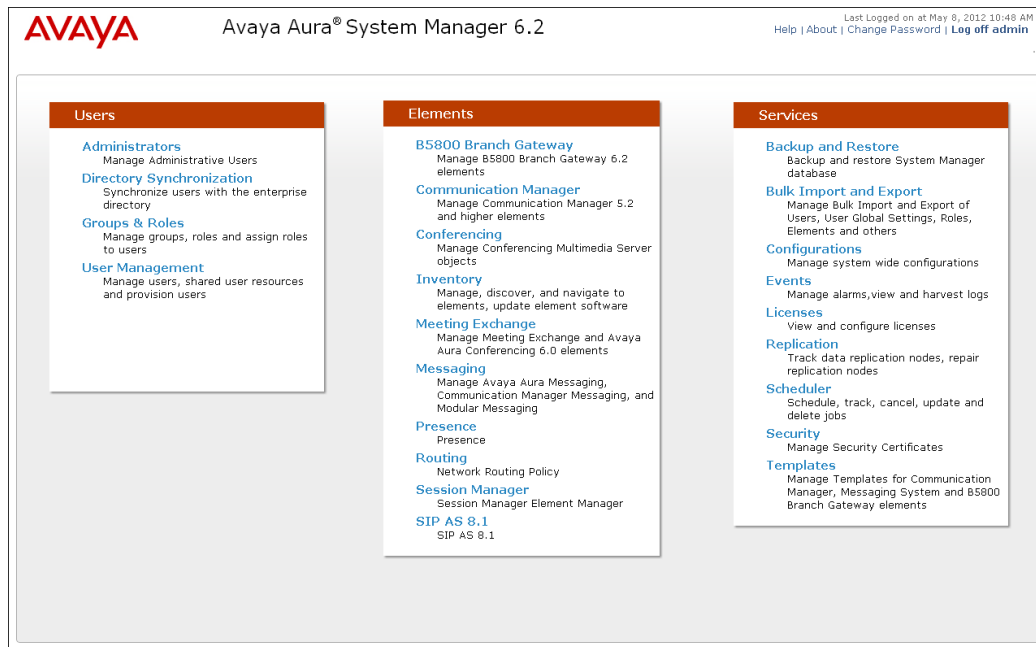
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to CS1000E, Acme Packet 3820 and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager Instance, corresponding to the Session Manager server to be administered in System Manager.


It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

### 6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL <https://<ip-address>/SMGR>, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed.



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.

Avaya Aura® System Manager 6.2

Last Logged on at May 8, 2012 10:48 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing \* Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing

Help ?

### Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"

- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers

- Between Session Managers and "other SIP Entities"



## 6.2. Add/View Avaya Aura® Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager instance already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the screen below:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

The screen below shows the Session Manager values used for the compliance test.

Home / Elements / Session Manager

[Help ?](#)

### Edit Session Manager

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

[General](#) | [Security Module](#) | [NIC Bonding](#) | [Monitoring](#) | [CDR](#) | [Personal Profile Manager \(PPM\)](#) - [Connection Settings](#) | [Event Server](#) | [Expand All](#) | [Collapse All](#)

**General**

**SIP Entity Name** DenverSM

**Description** Session Manager

**\*Management Access Point Host Name/IP** 10.80.150.210

**\*Direct Routing to Endpoints** Enable

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.

Security Module ▾

SIP Entity IP Address

10.64.19.210

\*Network Mask

255.255.255.0

\*Default Gateway

10.64.19.1

\*Call Control PHB

46

\*QOS Priority

6

\*Speed & Duplex

Auto ▾

VLAN ID

### 6.3. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**).

Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the **avayalab.com** domain.

The screenshot shows a web interface for 'Domain Management'. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / Domains'. Below this, the title 'Domain Management' is displayed. To the right of the title are buttons for 'Commit', 'Cancel', and 'Help ?'. A warning message states: 'Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.' Below the warning, there is a table with one item. The table has columns: 'Name', 'Type', 'Default', and 'Notes'. The 'Name' column contains '\* avayalab.com'. The 'Type' column contains 'sip' with a dropdown arrow. The 'Default' column contains an unchecked checkbox. The 'Notes' column is empty. Above the table, there is a 'Filter: Enable' button. Below the table, there is a 'Refresh' button.

Name	Type	Default	Notes
* avayalab.com	sip	<input type="checkbox"/>	

### 6.4. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.6**), so it was not necessary to add a pattern.

The following screen shows the addition of **SessionManager**, this location will be used for Session Manager. Click **Commit** to save.

Home / Elements / Routing / Locations

Help ?

CommitCancel

Location Details

General

\* Name:

SessionManager

Notes:

Session Manager

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

\* Minimum Multimedia Bandwidth:

64

Kbit/Sec

\* Default Audio Bandwidth:

80

Kbit/sec

**Note:** Call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for CS1000E and Acme Packet 3820. Displayed below is the screen for **CS1K-Location** used for CS1000E.

[Home](#) / [Elements](#) / [Routing](#) / [Locations](#)

[Help ?](#)

**Location Details**

Commit

Cancel

**General**

**\* Name:**

CS1K-Location

**Notes:**

CS1000 lab 140

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**

Kbit/sec

**Total Bandwidth:**

**Multimedia Bandwidth:**

**Audio Calls Can Take Multimedia Bandwidth:**

☒

**Per-Call Bandwidth Parameters**

**Maximum Multimedia Bandwidth (Intra-Location):**

1000

Kbit/Sec

**Maximum Multimedia Bandwidth (Inter-Location):**

1000

Kbit/Sec

**\* Minimum Multimedia Bandwidth:**

64

Kbit/Sec

**\* Default Audio Bandwidth:**

80

Kbit/sec

Below is the screen for **Loc19-ACME** used for Acme Packet 3820.

[Home](#) / [Elements](#) / [Routing](#) / [Locations](#)

[Help ?](#)

**Location Details**

Commit

Cancel

**General**

**\* Name:**

Loc19-ACME

**Notes:**

Acme SBC to ITSP

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**

Kbit/sec

**Total Bandwidth:**

**Multimedia Bandwidth:**

**Audio Calls Can Take Multimedia Bandwidth:**

☒

**Per-Call Bandwidth Parameters**

**Maximum Multimedia Bandwidth (Intra-Location):**

1000

Kbit/Sec

**Maximum Multimedia Bandwidth (Inter-Location):**

1000

Kbit/Sec

**\* Minimum Multimedia Bandwidth:**

64

Kbit/Sec

**\* Default Audio Bandwidth:**

80

Kbit/sec

## 6.5. Adaptations

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

The following screen shows the adaptations that were available in the sample configuration.

The screenshot shows the 'Adaptations' page in a web application. The breadcrumb navigation is 'Home / Elements / Routing / Adaptations'. There is a 'Help ?' link in the top right. Below the title 'Adaptations', there are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and a 'More Actions' dropdown. A table lists 6 items, with a 'Refresh' link and a 'Filter: Enable' option. The table has columns for a checkbox, Name, Module name, Egress URI Parameters, and Notes. The items listed are: CS1K-Adaptation (CS1000Adapter fromto=true, CS1K Adaptor), Diversion-Adapter (DiversionTypeAdapter MIME=no, Convert History-Info to Diversion), Loc19-CM-Lab Adaptation (DigitConversionAdapter, Convert 10 digit DID to Ext.), and Remove+ (DigitConversionAdapter fromto=true, Remove +). At the bottom, there is a 'Select : All, None' option.

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	<a href="#">CS1K-Adaptation</a>	CS1000Adapter fromto=true		CS1K Adaptor
<input type="checkbox"/>	<a href="#">Diversion-Adapter</a>	DiversionTypeAdapter MIME=no		Convert History-Info to Diversion
<input type="checkbox"/>	<a href="#">Loc19-CM-Lab Adaptation</a>	DigitConversionAdapter		Convert 10 digit DID to Ext.
<input type="checkbox"/>	<a href="#">Remove+</a>	DigitConversionAdapter fromto=true		Remove +

The adapter named **CS1K-Adaptation** will later be assigned to the SIP Entity linking Session Manager to CS1000E for calls involving CenturyLink SIP Trunking. This adaptation uses the **CS1000Adapter** to convert digits between CS1000E and CenturyLink. The **Module parameter fromto=true** will include the FROM and TO headers in the digit conversion.

The screenshot shows the 'Adaptation Details' page for 'CS1K-Adaptation'. The breadcrumb navigation is 'Home / Elements / Routing / Adaptations'. There is a 'Help ?' link and 'Commit' and 'Cancel' buttons in the top right. The section is titled 'General'. The form fields are: '\* Adaptation name:' (CS1K-Adaptation), 'Module name:' (CS1000Adapter dropdown), 'Module parameter:' (fromto=true), 'Egress URI Parameters:' (empty), and 'Notes:' (CS1K Adaptor).

\* Adaptation name: CS1K-Adaptation

Module name: CS1000Adapter

Module parameter: fromto=true

Egress URI Parameters:

Notes: CS1K Adaptor

Scrolling down, in the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from CS1000E users to CenturyLink. The text below and the screen example that follows explain how to use Session Manager to convert between CS1000E directory numbers and the corresponding CenturyLink 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., 4).
- **Max:** Enter maximum number of digits (e.g., 4).
- **Delete Digits:** Enter **0**, unless digits should be removed from dialed number before routing by Session Manager. For CS1000E extensions that do not match the last digits of the CenturyLink DID, enter the number of digits in the extension to remove all digits.
- **Insert Digits:** Enter the CenturyLink DID corresponding to the matched extension or DID prefix for a range of extensions.
- **Address to modify:** Select **both**.

Digit Conversion for Incoming Calls to SM
Add Remove

4 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 5555	* 4	* 4		* 4	8555555224	both ▼		ACD 5555
<input type="checkbox"/>	* 56	* 4	* 4		* 0	614555	both ▼		ext range 56xx
<input type="checkbox"/>	* 710	* 4	* 4		* 0	303555	both ▼		ext range 710x
<input type="checkbox"/>	* 7109	* 4	* 4		* 4	3035557104	both ▼		ext 7109

Select : All, None



Scrolling down, the following screen shows a portion of the **CS1K-Adaptation** adapter that can be used to convert digits between the CS1000E extension numbers and the DID numbers assigned by CenturyLink.

An example portion of the settings for **Digit Conversion for Outgoing Calls from SM** (i.e., inbound to CS1000E) is shown below. It can be observed that the first two entries are used to match a range of numbers while the last entry is used to match on a specific number.

Digit Conversion for Outgoing Calls from SM

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

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

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 30355571	* 10	* 10		* 6		both		Convert 10 digit DID to
<input type="checkbox"/>	* 614555	* 10	* 10		* 6		both		
<input type="checkbox"/>	* 855	* 10	* 10		* 10	5555	both		Inbound Toll Free

Select : All, None

The adapter named **Diversion-Adapter** will later be assigned to the SIP Entity linking Session Manager to the Acme Packet 3820. This adaptation uses the **DiversionTypeAdapter** to convert History-Info headers to Diversion headers. This is necessary to support call forwarding of inbound calls back to the PSTN. Also, **MIME=no** was entered as a **Module Parameter** to have Session Manager strip MIME message bodies on egress to the Acme Packet 3820, such that only SDP is present in the message body.

Home / Elements / Routing / Adaptations

[Help ?](#)

**Adaptation Details** [Commit](#) [Cancel](#)

**General**

\* **Adaptation name:**

**Module name:**

**Module parameter:**

**Egress URI Parameters:**

**Notes:**

## 6.6. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes CS1000E and Acme Packet 3820. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for CS1000E and **SIP Trunk** for Acme Packet 3820.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows a web interface for configuring SIP Entities. The breadcrumb trail at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". In the top right corner, there are "Commit" and "Cancel" buttons, and a "Help ?" link. The "General" section is active and contains the following fields:

- Name:** DenverSM
- \* FQDN or IP Address:** 10.64.19.210
- Type:** Session Manager (selected from a dropdown menu)
- Notes:** Session Manager
- Location:** SessionManager (selected from a dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/Denver (selected from a dropdown menu)
- Credential name:** (empty text field)

The "SIP Link Monitoring" section is also visible and contains one field:

- SIP Link Monitoring:** Use Session Manager Configuration (selected from a dropdown menu)

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.7**.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save.

For the compliance test, four **Port** entries were added.

### Port

TCP Failover port:

TLS Failover port:

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

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5081"/>	TLS <input type="button" value="v"/>	avayalab.com <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5071"/>	TLS <input type="button" value="v"/>	avayalab.com <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP <input type="button" value="v"/>	avayalab.com <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS <input type="button" value="v"/>	avayalab.com <input type="button" value="v"/>	<input type="text"/>

Select : All, None

The following screen shows the addition of CS1000E. The **FQDN or IP Address** field is set to the IP address of the Node IP on CS1000E defined in **Section 5.1.1**. The **Adaptation** field is set to the **CS1K-Adaptation** created in **Section 6.5** and the Location is set to the one defined for CS1000E in **Section 6.4**.

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

[Help ?](#)

**SIP Entity Details**

Commit

Cancel

**General**

\* Name:

CS1K

\* FQDN or IP Address:

10.80.140.103

Type:

Other

Notes:

CS1K Lab 140

Adaptation:

CS1K-Adaptation

Location:

CS1K-Location

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

none

CommProfile Type Preference:

**SIP Link Monitoring**

SIP Link Monitoring:

Use Session Manager Configuration

The following screen shows the addition of Acme Packet 3820 SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Adaptation** field is set to the **Diversion-Adapter** created in **Section 6.5** and the Location is set to the one defined for Acme Packet 3820 in **Section 6.4**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.

The screenshot displays the 'SIP Entity Details' configuration page for 'Loc19-ACME'. The breadcrumb navigation at the top reads 'Home / Elements / Routing / SIP Entities'. In the top right corner, there is a 'Help ?' link and 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (Loc19-ACME), '\* FQDN or IP Address' (10.64.19.150), 'Type' (Other), 'Notes' (ACME PACKET), 'Adaptation' (Diversion-Adapter), 'Location' (Loc19-ACME), and 'Time Zone' (America/Denver). Below this is an 'Override Port & Transport with DNS SRV' checkbox, which is unchecked. Further down are fields for '\* SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), 'Call Detail Recording' (none), and 'CommProfile Type Preference' (empty). The 'SIP Link Monitoring' section includes 'SIP Link Monitoring' (Link Monitoring Enabled), '\* Proactive Monitoring Interval (in seconds)' (900), '\* Reactive Monitoring Interval (in seconds)' (120), and '\* Number of Retries' (1).

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

**General**

\* Name: Loc19-ACME

\* FQDN or IP Address: 10.64.19.150

Type: Other

Notes: ACME PACKET

Adaptation: Diversion-Adapter

Location: Loc19-ACME

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

**SIP Link Monitoring**

SIP Link Monitoring: Link Monitoring Enabled

\* Proactive Monitoring Interval (in seconds): 900

\* Reactive Monitoring Interval (in seconds): 120

\* Number of Retries: 1

## 6.7. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to CS1000E for use only by service provider traffic and one to Acme Packet 3820. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system. For CS1000E, select the CS1000E SIP Entity defined in **Section 6.6**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 6.6** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to CS1000E and Acme Packet 3820.

Entity Link to CS1000E:

The screenshot shows the 'Entity Links' configuration page. At the top right are 'Commit' and 'Cancel' buttons. Below is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row contains: Name: '\* SM to CS1K', SIP Entity 1: '\* DenverSM' (dropdown), Protocol: 'TCP' (dropdown), Port: '\* 5060', SIP Entity 2: '\* CS1K' (dropdown), Port: '\* 5060', Connection Policy: 'Trusted' (dropdown), and Notes: 'To CS1K'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to CS1K	* DenverSM	TCP	* 5060	* CS1K	* 5060	Trusted	To CS1K

Entity Link to Acme Packet 3820:

The screenshot shows the 'Entity Links' configuration page. At the top right are 'Commit' and 'Cancel' buttons. Below is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row contains: Name: '\* SM to Loc19-ACME', SIP Entity 1: '\* DenverSM' (dropdown), Protocol: 'TCP' (dropdown), Port: '\* 5060', SIP Entity 2: '\* Loc19-ACME' (dropdown), Port: '\* 5060', Connection Policy: 'Trusted' (dropdown), and Notes: 'To ACME SBC'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to Loc19-ACME	* DenverSM	TCP	* 5060	* Loc19-ACME	* 5060	Trusted	To ACME SBC

## 6.8. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.6**. Two routing policies must be added; one for CS1000E and one for

Acme Packet 3820. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown). The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for CS1000E and Acme Packet 3820.

Routing Policy for CS1000E:

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

\* Name: To-CS1K

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K	10.80.140.103	Other	CS1K Lab 140

## Routing Policy for Acme Packet 3820:

Home / Elements / Routing / Routing Policies

Help ?

Routing Policy Details

Commit Cancel

General

\* Name: To-Loc19-ACME

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Loc19-ACME	10.64.19.150	Other	ACME PACKET

### 6.9. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from CS1000E to CenturyLink and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.



Two examples of the dial patterns used for the compliance test are shown below. The first example shows that that in the shared test environment, 11 digit dialed numbers that begin with **1** originating from **CS1K-Location** uses route policy **To-Loc19-ACME**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

\* Pattern: 1

\* Min: 11

\* Max: 11

Emergency Call:

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: 1+ Outbound

Originating Locations and Routing Policies

Add Remove

2 Items | Refresh

Filter: Enable

	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CS1K-Location	CS1000 lab 140	To-Loc19-ACME	0	<input type="checkbox"/>	Loc19-ACME	
<input type="checkbox"/>	Loc19-CMLab	Lab CM 10.64.19.205	To-ASBCE	0	<input type="checkbox"/>	Loc19-ASBCE	

Select : All, None

The second example shows that a **10** digit number starting with **30355571** and originating from **Loc19-ACME** uses route policy **To-CS1K**. This is a DID range 303-555-7100 through 303-555-7199 assigned to the enterprise from CenturyLink.

Home / Elements / Routing / Dial Patterns

[Help ?](#)

Dial Pattern Details

General

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Loc19-ACME	Acme SBC to ITSP	To-CS1K	0	<input type="checkbox"/>	CS1K	

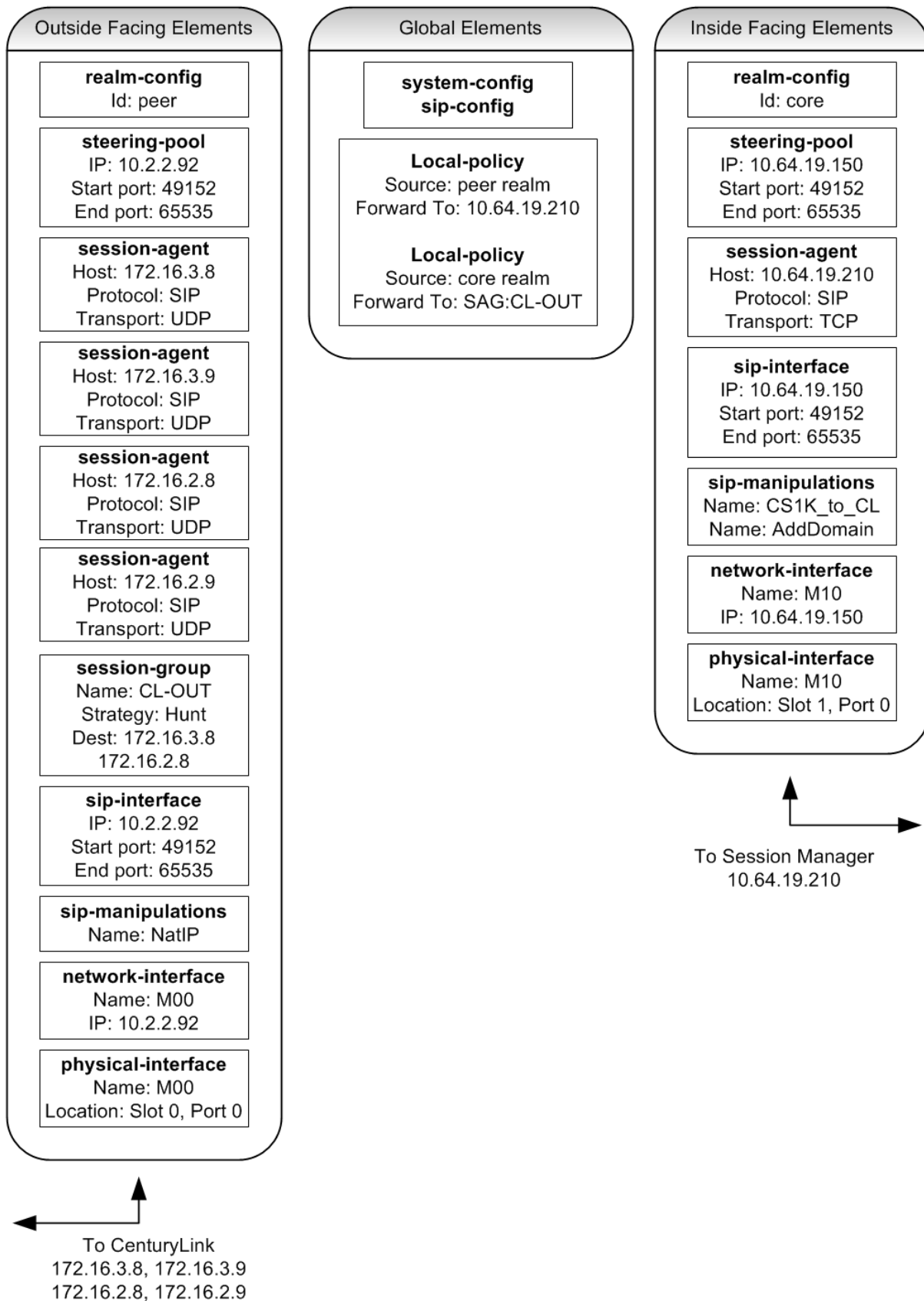
Select : All, None

## 7. Configure Acme Packet 3820 Net-Net® Session Director

This section describes the configuration of the Acme Packet 3820 necessary for interoperability with CenturyLink and Session Manager. The Acme Packet 3820 is configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet 3820.

A pictorial view of this configuration is shown below. It shows the internal components needed for the compliance test. Each of these components is defined in the Acme Packet 3820 configuration file contained in **Appendix A**. However, this section does not cover standard Acme Packet 3820 configurations that are not directly related to the interoperability test. The details of these configuration elements can be found in **Appendix A**.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to CenturyLink and Session Manager. These same fields are highlighted in **Appendix A**. The remaining fields are generally the default/standard value used by the Acme Packet 3820 for that field. For additional details on the administration of the Acme Packet 3820, see **Reference [12]**.



## 7.1. Acme Packet Command Line Interface Summary

The Acme Packet 3820 is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

1. Access the console port of the Acme Packet 3820 using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the 3820 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 3820 with the user password.
3. Enable the Superuser mode by entering the **enable** command and then the superuser password. The command prompt will change to include a “#” instead of a “>” while in Superuser mode. This level of system access (i.e. at the “acmesystem#” prompt) will be referred to as the **main** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific elements and specific parameters of those elements.
4. In Superuser 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 (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., **name M00**).
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 **Steps 5 - 9** to configure all the 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.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

## 7.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet 3820.

The key system configuration (**system-config**) field is:

- **default-gateway**: The IP address of the default gateway for the management network (10.80.150.0/24) from **Figure 1**. In this case, the default gateway is **10.80.150.1**.

```
system-config
  hostname
  description
  location
  mib-system-contact
  mib-system-name

< text removed for brevity >

  call-trace                disabled
  internal-trace            disabled
  log-filter                all
  default-gateway          10.80.150.1
  restart                  enabled
  exceptions
  telnet-timeout            0
  console-timeout           0
  remote-control            enabled
  cli-audit-trail           enabled
  link-redundancy-state     disabled
  source-routing            disabled
  cli-more                  disabled
  terminal-height           24
  debug-timeout             0
```

### 7.3. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet 3820 was connected to the external untrusted network. 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.

The key physical interface (**phy-interface**) fields are:

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

phy-interface	
<b>name</b>	<b>M00</b>
<b>operation-type</b>	<b>Media</b>
<b>port</b>	<b>0</b>
<b>slot</b>	<b>0</b>
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-11-01 09:59:56
phy-interface	
<b>name</b>	<b>M10</b>
<b>operation-type</b>	<b>Media</b>
<b>port</b>	<b>0</b>
<b>slot</b>	<b>1</b>
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2011-11-01 10:00:38

The key network interface (**network-interface**) fields are:

- **name**: The name of the physical interface (defined previously) that is associated with this network interface.
- **description**: A descriptive name to help identify the interface.
- **ip-address**: The IP address on the interface connected to the network on which the CenturyLink SIP trunk service resides. In the compliance test, the IP address **10.2.2.92** was assigned to the public interface and **10.64.19.150** was assigned to the private interface.
- **netmask**: Subnet mask for the IP subnet.
- **gateway**: The subnet gateway address.
- **hip-ip-list**: The list of virtual IP addresses assigned to the Acme Packet 3820 on this interface. If a single virtual IP address is used, this value would be the same as the value entered for the **ip-address** field above.
- **icmp-address**: The list of IP addresses to which the Acme Packet 3820 will answer ICMP requests on this interface.

```
network-interface
  name                M00
  sub-port-id         0
  description         PUBLIC
  hostname
  ip-address          10.2.2.92
  pri-utility-addr
  sec-utility-addr
  netmask             255.255.255.128
  gateway             10.2.2.1
  sec-gateway
  gw-heartbeat
    state              disabled
    heartbeat          0
    retry-count        0
    retry-timeout      1
    health-score       0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout         11
  hip-ip-list         10.2.2.92
  ftp-address
  icmp-address
  snmp-address
  telnet-address
  ssh-address
  last-modified-by    admin@10.80.150.38
  last-modified-date  2011-11-01 12:52:08
```



The settings for the private side network interface are shown below.

network-interface	
name	M10
sub-port-id	0
description	PRIVATE
hostname	
ip-address	10.64.19.150
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	10.64.19.1
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	10.64.19.150
ftp-address	
icmp-address	10.64.19.150
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 12:16:22

## 7.4. Realm

A realm represents a group of related Acme Packet 3820 components. Two realms were defined for the compliance test. The **peer** realm was defined for the external network and the **core** realm was defined for the internal network.

The key realm (**realm-config**) fields are:

- **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.
- **In-manipulationid**: For the **core** realm **CS1K\_To\_CL** was used. This name refers to a set of sip-manipulations that is performed on inbound traffic to the Acme Packet 3820.
- **out-manipulationid**: For the **peer** realm **NatIP** was used and for the **core** realm **AddDomain** was used. These names refer to a set of sip-manipulations (defined in **Section 7.9**) that are performed on outbound traffic from the Acme Packet 3820. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side (**peer**) of the Acme Packet 3820 as well as to outbound traffic from the private side (**core**) of the Acme Packet 3820.

```

realm-config
  identifier
  description
  addr-prefix
  network-interfaces
    mm-in-realm
    mm-in-network
    mm-same-ip
    mm-in-system
  peer
    M00:0
    enabled
    enabled
    enabled
    enabled
  < text removed for brevity >
    out-translationid
    in-manipulationid
    out-manipulationid
    manipulation-string
    manipulation-pattern
    class-profile
    average-rate-limit
    NatIP
    0
  < text removed for brevity >
realm-config
  identifier
  description
  addr-prefix
  network-interfaces
    mm-in-realm
    mm-in-network
    mm-same-ip
    mm-in-system
  core
    M10:0
    enabled
    enabled
    enabled
    enabled
  < text removed for brevity >
    out-translationid
    in-manipulationid
    out-manipulationid
    manipulation-string
    manipulation-pattern
    class-profile
    average-rate-limit
    CS1K_To_CL
    AddDomain
    0
  < text removed for brevity >

```

## 7.5. SIP Configuration

The SIP configuration (**sip-config**) defines the global system-wide SIP parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

The key SIP configuration (**sip-config**) fields are:

- **state: enabled**
- **home-realm-id:** The name of the realm on the private side of the Acme Packet 3820.
- **egress-realm-id:** The name of the realm on the private side of the Acme Packet 3820.
- **options: max-udp=length=0.** This option was used to prevent errors about the packet size being too large.

```
sip-config
  state                enabled
  operation-mode        dialog
  dialog-transparency   enabled
  home-realm-id         core
  egress-realm-id       core
  nat-mode              None
  registrar-domain
  registrar-host
  registrar-port        0
  register-service-route always
  init-timer            500
  max-timer              4000
  trans-expire          32
  invite-expire         180

< text removed for brevity >

  options              max-udp=length=0
  refer-src-routing    disabled
  add-ucid-header      disabled
  proxy-sub-events

< text removed for brevity >
```

## 7.6. SIP Interface

The SIP interface (**sip-interface**) defines the receiving characteristics of the SIP interfaces on the Acme Packet 3820. Two SIP interfaces were defined; one for each realm.

The key SIP interface (**sip-interface**) fields are:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sipport**
  - **address**: The IP address assigned to this sip-interface.
  - **port**: The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
  - **transport-protocol**: The transport method used for this interface.
  - **allow-anonymous**: Defines from whom SIP requests will be allowed. On the peer side, the value of **agents-only** is used. Thus, SIP requests will only be accepted from session agents (as defined in **Section 7.7**) on this interface. On the core side, the value of **all** is used. Thus, SIP requests will be accepted from anyone on this interface.

```
sip-interface
state                enabled
realm-id           peer
description
sip-port
    address          10.2.2.92
    port             5060
    transport-protocol UDP
    tls-profile
    allow-anonymous   agents-only
    ims-aka-profile
carriers
trans-expire         0
invite-expire        0

< text removed for brevity >

sip-interface
state                enabled
realm-id           core
description
sip-port
    address          10.64.19.150
    port             5060
    transport-protocol TCP
    tls-profile
    allow-anonymous   all
    ims-aka-profile
carriers
trans-expire         0
invite-expire        0

< text removed for brevity >
```

## 7.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet 3820 such as Session Manager and CenturyLink SIP Trunk service.

The key session agent (**session-agent**) fields are:

- **hostname**: Fully qualified domain name or IP address of this SIP peer.
- **ip-address**: The IP address of this SIP peer.
- **port**: The port used by the peer for SIP traffic.
- **app-protocol**: **SIP**
- **transport-method**: **UDP**
- **realm-id**: The realm id where this peer resides.
- **description**: A descriptive name for the peer.
- **ping-method**: **OPTIONS;hops=70** This setting defines that the SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Acme Packet 3820 to set the SIP “Max-Forward” field to 70 in outbound SIP OPTIONS pings generated by the Acme Packet 3820 to this session agent.
- **ping-interval**: Specifies the interval (in seconds) between each ping attempt.

The settings for the session agent used for CenturyLink East Inbound/Outbound peer:

```
session-agent
  hostname                172.16.3.8
  ip-address              172.16.3.8
  port                    5060
  state                   enabled
  app-protocol             SIP
  app-type
  transport-method        UDP
  realm-id                peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp       enabled
  constraints              disabled
  max-sessions             0

< text removed for brevity >

  response-map
  ping-method             OPTIONS;hops=70
  ping-interval           60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink East Remote DID peer:

```
session-agent
  hostname          172.16.3.9
  ip-address        172.16.3.9
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints       disabled
  max-sessions      0

< text removed for brevity >

  response-map
  ping-method       OPTIONS;hops=70
  ping-interval     60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink West Inbound/Outbound peer:

```
session-agent
  hostname          172.16.2.8
  ip-address        172.16.2.8
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints       disabled
  max-sessions      0

< text removed for brevity >

  response-map
  ping-method       OPTIONS;hops=70
  ping-interval     60

< text removed for brevity >
```

The settings for the session agent used for CenturyLink West Remote DID peer:

```
session-agent
  hostname          172.16.2.9
  ip-address        172.16.2.9
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          peer
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```

The settings for the session agent used for Session Manager:

```
session-agent
  hostname          10.64.19.210
  ip-address        10.64.19.210
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  TCP
  realm-id          core
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints        disabled
  max-sessions       0

< text removed for brevity >

  response-map
  ping-method        OPTIONS;hops=70
  ping-interval      60

< text removed for brevity >
```

## 7.8. Session Agent Group

Session agents can be configured in a session agent group (SAG), so multiple session agents can be assigned to a route policy for fail-over or load balancing purposes. For compliance testing CenturyLink had four session agents assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two session agents allocated for outbound traffic were added to the SAG.

The key session agent group (**session-group**) fields are:

- **group-name**: A descriptive string used to reference the session agent group.
- **state**: **enabled**
- **app-protocol**: **SIP**
- **strategy**: **Hunt** This strategy will route to the secondary session agent only if the primary fails. An alternative is to use a strategy of **RoundRobin**. This strategy will alternatively select between session agents.
- **dest**: The list of session agents to be added to the group by hostname. For compliance testing **172.16.3.8** and **172.16.2.8** were used.
- **sag-recursion**: **enabled** This allows Acme Packet 3820 to select a different session agent in the SAG if a failure occurs to the first session agent.

session-group	
group-name	CL-OUT
description	
state	enabled
app-protocol	SIP
strategy	Hunt
dest	172.16.3.8 172.16.2.8
trunk-group	
sag-recursion	enabled
stop-sag-recurse	401,407
last-modified-by	admin@10.80.150.38
last-modified-date	2012-06-18 10:27:19



## 7.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 7.4**, it was defined that the set of sip-manipulations named **NatIP** would be performed on outbound traffic in the **peer** realm and **AddDomain** would be performed on outbound traffic in the **core** realm. The sip-manipulation named **CS1K\_To\_CL** would be performed on inbound traffic in the **core** realm. For the complete configuration of these rules refer to **Appendix A**.

The key SIP manipulation (sip-manipulation) fields are:

- **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).

In the configuration file in **Appendix A**, the **NatIP** sip manipulation has many modifications (or header-rules) defined. These header manipulations were added to hide the private IP address and enterprise domain name which appear in the “To”, “From”, “Request-URI”, “Diversion” and “PAI” SIP headers for outbound calls. As well as remove unwanted headers going to the SIP service provider.

Similarly the **AddDomain** sip manipulation was used towards Session Manager to hide the public IP addresses and to add the enterprise domain to the “From” and “PAI” SIP headers.

The **CS1K\_To\_CL** sip manipulation was used to add a “Diversion” header for Mobile X calls from CS1000E. This was added to the inbound traffic to the Acme Packet 3820 so that it could be further modified by the **NatIP** sip manipulation to remove the “History-Info” header and to hide the enterprise domain name.

The example below shows the **natFROM header-rule** in the **NatIP** sip manipulation. It specifies that the “From” header in SIP request messages will be manipulated based on the element rule defined. The element rule **natHost** will match any value in the host part of the URI and replace it with the value of **\$LOCAL\_IP**. The value of **\$LOCAL\_IP** is the outside IP address of the Acme Packet 3820.

```

sip-manipulation
  name                               NatIP
  description
  split-headers
  join-headers
  header-rule
    name                             natFROM
    header-name                       From
    action                            manipulate
    comparison-type                   case-sensitive
    msg-type                          request
    methods
    match-value
    new-value
    element-rule
      name                           natHost
      parameter-name
      type                            uri-host
      action                          replace
      match-val-type                  any
      comparison-type                 case-sensitive
      match-value
      new-value                       $LOCAL_IP

< text removed for brevity >

```

The example below shows the **FromDomain** header-rule in the **AddDomain** sip manipulation. It specifies that the “From” header in SIP request messages will be manipulated based on the element rule defined. The element rule **From** will match any value in the host part of the URI and replace it with the value of **avayalab.com**. The value of **avayalab.com** is the domain name used in the enterprise. This value should match the Domain set in Session Manager (**Section 6.2**) and the CS1000E signaling group Far-end Domain (**Section 5.7**).

```

sip-manipulation
  name                      AddDomain
  description
  split-headers
  join-headers
  header-rule
    name                    FromDomain
    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        any
      comparison-type       case-sensitive
      match-value
      new-value             avayalab.com

< text removed for brevity >

```

The example below shows the **CS1K\_To\_CL** sip manipulation. This manipulation specifies that if the P-Asserted-Identity header does not have a phone number within the range 303-555-7100 to 303-5557199 (the DID range specified by CenturyLink) and does not have a Reason parameter in the “History-Info” header, a static Diversion header will be created.

```

sip-manipulation
  name CS1K_To_CL
  description
  split-headers
  join-headers
  header-rule
    name PAIRegex
    header-name P-Asserted-Identity
    action store
    comparison-type pattern-rule
    msg-type any
    methods INVITE
    match-value
    new-value
    element-rule
      name chkUser
      parameter-name
      type header-value
      action store
      match-val-type any
      comparison-type pattern-rule
      match-value (.*) (30355571) (.*)
      new-value

  header-rule
    name HistRegex
    header-name History-Info
    action store
    comparison-type pattern-rule
    msg-type any
    methods
    match-value
    new-value
    element-rule
      name GetReason
      parameter-name
      type header-value
      action store
      match-val-type any
      comparison-type pattern-rule
      match-value (.*) (reason) (.*)
      new-value

  header-rule
    name AddDiversion
    header-name Diversion
    action add
    comparison-type boolean
    msg-type request
    methods INVITE
    match-value (!$PAIRegex[0] . $chkUser) &!$HistRegex[0] . $GetReason
    new-value "<sip:3035557104@avayalab.com;user=phone>"

```

## 7.10. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.

The key steering pool (**steering-pool**) fields are:

- **ip-address**: The address of the interface on the Acme Packet 3820.
- **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

steering-pool	
ip-address	10.2.2.92
start-port	49152
end-port	65535
realm-id	peer
network-interface	
last-modified-by	admin@console
last-modified-date	2012-06-06 15:07:34
steering-pool	
ip-address	10.64.19.150
start-port	49152
end-port	65535
realm-id	core
network-interface	
last-modified-by	admin@console
last-modified-date	2012-06-06 15:08:02

## 7.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another.

The key local policy (**local-policy**) fields are:

- **from-address**: A policy filter indicating the originating IP address to which this policy applies. An asterisk (\*) indicates any IP address.
- **to-address**: A policy filter indicating the terminating IP address to which this policy applies. An asterisk (\*) indicates any IP address.
- **source-realm**: A policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute**:
  - **next-hop**: The IP address where the message should be sent when the policy rules match.
  - **realm**: The realm associated with the next-hop IP address.

In this case, the first policy provides a simple routing rule indicating that messages originating from the **peer** realm are to be sent to the **core** realm via IP address **10.80.150.206** (Session Manager at the enterprise). The second policy indicates that messages originating from the **core** realm are to be sent to the **peer** realm via the session agent group **CL-OUT** created in **Section 7.8**.

```

local-policy
  from-address          *
  to-address            *
  source-realm          peer
  description
  activate-time         N/A
< text removed for brevity >
  policy-attribute
    next-hop            10.64.19.210
    realm               core
    action              none
< text removed for brevity >
local-policy
  from-address          *
  to-address            *
  source-realm          core
  description
  activate-time         N/A
< text removed for brevity >
  policy-attribute
    next-hop            SAG:CL-OUT
    realm               peer
< text removed for brevity >

```

## 8. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk Service, a customer must request the service from CenturyLink using their sales processes. This process can be initiated by contacting CenturyLink via the corporate web site at [www.centurylink.com](http://www.centurylink.com) and requesting information via the online sales links or telephone numbers

## 9. Verification

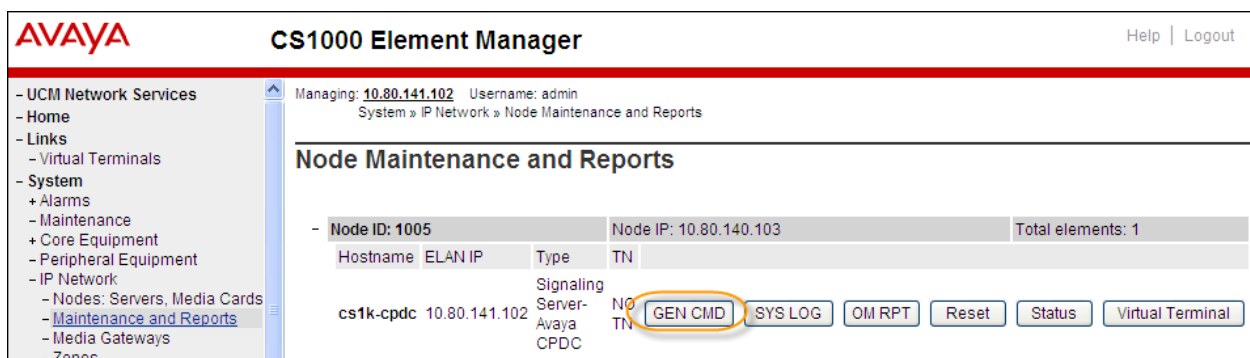
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

### 9.1. Avaya Communication Server 1000E Verifications

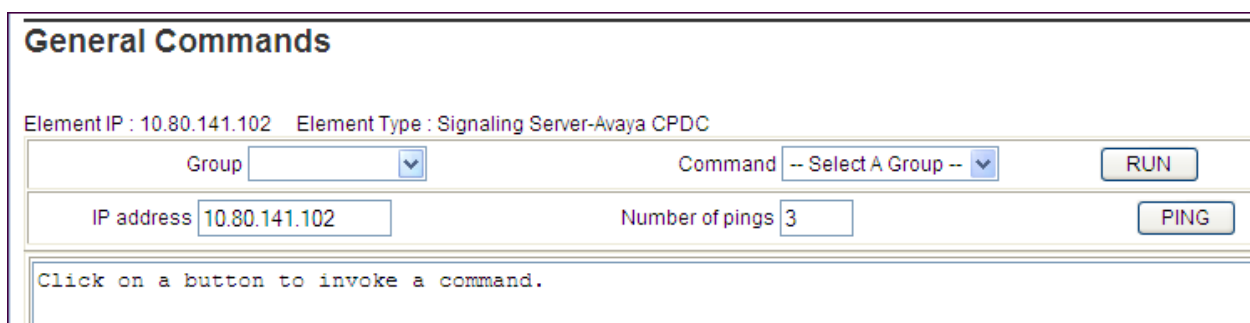
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

#### 9.1.1. IP Network Maintenance and Reports Commands

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



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



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

To check the status of the SIP Gateway to Session Manager in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click Run. The example output below shows that Session Manager (10.64.19.150, port 5060, TCP) has **SIPNPM Status** Active.

### General Commands

Element IP : 10.80.141.102    Element Type : Signaling Server-Avaya CPDC

Group Sip
Command SIPGwShow
Sip
RUN

IP address 10.80.141.102
Number of pings 3
PING

```

SIPNPM Status           : Active
Primary Proxy IP address : 10.64.19.150
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 : 10.64.19.250
Primary Proxy2 port      : 5060
Primary Proxy2 Transport : TCP
Active Proxy             : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 32 / 32
Stack version            : 5.5.0.13
TLS Security Policy      : Security Disabled

```

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 7108 was involved in an active call with the CenturyLink SIP Trunk service.

### General Commands

Element IP : 10.80.141.102    Element Type : Signaling Server-Avaya CPDC

Group SipLine
Command sigSetShowAll
RUN

IP address 10.80.141.102
Number of pings 3
PING

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPV4 Endpoints -----							
7108	7108	252-00-09-01	1	1	0x8d155f8		SIP Lines
5685	5685	252-00-09-02	1	0	0xb7e16e58		SIP Lines
Total User Registered = 2    V4 Registered = 2    V6 Registered = 0							



The following screen shows a means to view IP UNISim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**. At the time this screen was captured, the UNISim telephone with IP address **10.80.150.111** was involved in an active call with the CenturyLink SIP Trunk service.

**General Commands**

Element IP : 10.80.141.102    Element Type : Signaling Server-Avaya CPDC

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

IP address **10.80.141.102**    Number of pings **3**    **PING**

**Set Information**

IP Address	NAT	Model Name	Type	RegType	State	Up
10.80.150.111		1165E IP Deskphone	1165	Regular	busy	1
10.80.150.113		1165E IP Deskphone	1165	Regular	online	1

Total sets = 2

### 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.

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.

**AVAYA**    **CS1000 Element Manager**    Help | Logout

Managing: **10.80.141.102**    Username: admin  
System » Maintenance

**Maintenance**

☒ Select by Overlay    ☐ Select by Functionality

<Select by Overlay>

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

<Select Group>

- D-Channel Diagnostics
- MSDL Diagnostics
- TMDI Diagnostics

On the preceding screen, if **D-Channel Diagnostics** is selected on the right, a screen such as the following is displayed. D-Channel number 15, which is used in the sample configuration, is established **EST** and active **ACTV**.

### D-Channel Diagnostics

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

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
<input checked="" type="radio"/> 015	VtrkNode1005	OPER	EST ACTV	AUTO		

Instruction: Select a command, add value and click on [Submit].

## 9.2. Avaya Aura® Session Manager Verifications

The following steps may be used to verify the Session Manager configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manager and executing the Call Routing Test. Expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows a call routing test for an outbound call to PSTN via CenturyLink. Under **Routing Decisions**, observe the call will rout via Acme Packet 3820 to CenturyLink. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

Home / Elements / Session Manager / System Tools / 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 administration.

### SIP INVITE Parameters

<b>Called Party URI</b> <input type="text" value="7205551997@avayalab.com"/>	<b>Calling Party Address</b> <input type="text" value="10.80.140.103"/>
<b>Calling Party URI</b> <input type="text" value="3035557104@avayalab.com"/>	<b>Session Manager Listen Port</b> <input type="text" value="5060"/>
<b>Day Of Week</b> <input type="text" value="Thursday"/>	<b>Time (UTC)</b> <input type="text" value="20:01"/>
<b>Called Session Manager Instance</b> <input type="text" value="DenverSM"/>	<b>Transport Protocol</b> <input type="text" value="TCP"/>

---

### Routing Decisions

Route < sip:7205551997@avayalab.com > to SIP Entity Loc19-ACME (10.64.19.150). Terminating Location is Loc19-ACME.

2. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
3. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
4. Verify that the user on the PSTN can end an active call by hanging up.
5. Verify that an endpoint at the enterprise site can end an active call by hanging up

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager, and Acme Packet 3820 Net-Net Session Director to the CenturyLink SIP Trunk (Legacy Qwest) Service. The CenturyLink SIP Trunk is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

## 11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Avaya Communication Server 1000E Installation and Commissioning*, November 2010, Document Number NN43041-310.
- [2] *Feature Listing Reference Avaya Communication Server 1000*, November 2010, Document Number NN43001-111, 05.01.
- [3] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [4] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, Document Number NN43001-125, 03.09 October 2011
- [5] *Installing and Configuring Avaya Aura® System Platform, Release 6.2.0*, March 2012.
- [6] *Administering Avaya Aura® System Platform, Release 6.2.0*, February 2012.
- [7] *Implementing Avaya Aura® System Manager, Release 6.2*, March 2012
- [8] *Installing Service Packs for Avaya Aura® Session Manager*, February 2012, Document Number 03-603863
- [9] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473.
- [10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315, 05.18 January 2012
- [11] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Document Number NN43170-600, Standard 04.02 December 2011
- [12] *Acme Packet, "Net-Net 4000 S-CX6.3.0 ACLI Configuration Guide"*, 400-0061-62, Nov 2009
- [13] *Acme Packet, "Net-Net 3800 Series And Net-Net 4500 SSM2 Installation Guide"*, 400-0114-20, Apr 2010
- [14] *Acme Packet, "Net-Net 3820 Hardware Installation Guide"*, 400-0134-10, Mar 2011

## Appendix A: Acme Packet 3820 Configuration

Included below is the Acme Packet 3820 configuration used during the compliance testing. The contents of the configuration can be shown by using the ACLI command **show running-config** at the Acme Packet 3820.

```
ACMESYSTEM# show running-config
local-policy
  from-address
  to-address
  source-realm
  description
  activate-time
  deactivate-time
  state
  policy-priority
  last-modified-by
  last-modified-date
  policy-attribute
    next-hop
    realm
    action
    terminate-recursion
    carrier
    start-time
    end-time
    days-of-week
    cost
    app-protocol
    state
    methods
    media-profiles
    lookup
    next-key
    eloc-str-lkup
    eloc-str-match
local-policy
  from-address
  to-address
  source-realm
  description
  activate-time
  deactivate-time
  state
  policy-priority
  last-modified-by
  last-modified-date
  policy-attribute
    next-hop
    realm
    action
    terminate-recursion
    carrier
    start-time
    end-time
    days-of-week
    cost
    app-protocol
    state
    methods
```

media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	
media-manager	
state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
media-policing	enabled
max-signaling-bandwidth	10000000
max-untrusted-signaling	100
min-untrusted-signaling	30
app-signaling-bandwidth	0
tolerance-window	30
rtcp-rate-limit	0
trap-on-demote-to-deny	disabled
syslog-on-demote-to-deny	disabled
syslog-on-demote-to-untrusted	disabled
anonymous-sdp	disabled
arp-msg-bandwidth	32000
fragment-msg-bandwidth	0
rfc2833-timestamp	disabled
default-2833-duration	100
rfc2833-end-pkts-only-for-non-sig	enabled
translate-non-rfc2833-event	disabled
media-supervision-traps	disabled
dnalg-server-failover	disabled
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 12:25:41
network-interface	
name	M00
sub-port-id	0
description	PUBLIC
hostname	
ip-address	10.2.2.92
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.128
gateway	10.2.2.1
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	10.2.2.92
ftp-address	
icmp-address	10.2.2.92
snmp-address	

```

telnet-address
ssh-address
signaling-mtu                0
last-modified-by             admin@10.80.150.50
last-modified-date           2012-06-06 14:40:39
network-interface
  name                        M10
  sub-port-id                 0
  description                 PRIVATE
  hostname
  ip-address                  10.64.19.150
  pri-utility-addr
  sec-utility-addr
  netmask                    255.255.255.0
  gateway                    10.64.19.1
  sec-gateway
  gw-heartbeat
    state                     disabled
    heartbeat                 0
    retry-count               0
    retry-timeout             1
    health-score              0
  dns-ip-primary              10.80.150.201
  dns-ip-backup1
  dns-ip-backup2
  dns-domain                  avayalab.com
  dns-timeout                 11
  hip-ip-list                 10.64.19.150
  ftp-address
  icmp-address                10.64.19.150
  snmp-address
  telnet-address
  ssh-address
  signaling-mtu                0
  last-modified-by             admin@10.80.150.50
  last-modified-date           2012-06-06 14:42:37
phy-interface
  name                        M00
  operation-type              Media
  port                        0
  slot                        0
  virtual-mac
  admin-state                 enabled
  auto-negotiation            enabled
  duplex-mode                 FULL
  speed                       100
  overload-protection         disabled
  last-modified-by            admin@console
  last-modified-date           2011-11-01 09:59:56
phy-interface
  name                        M10
  operation-type              Media
  port                        0
  slot                        1
  virtual-mac
  admin-state                 enabled
  auto-negotiation            enabled
  duplex-mode                 FULL
  speed                       100
  overload-protection         disabled
  last-modified-by            admin@console
  last-modified-date           2011-11-01 10:00:38
realm-config
  identifier                  peer
  description
  addr-prefix                 0.0.0.0
  network-interfaces
    M00:0
  mm-in-realm                 enabled
  mm-in-network                enabled

```

mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
qos-enable	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
srtp-msm-passthrough	disabled
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	NatIP
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
cac-failure-threshold	0
untrust-cac-failure-threshold	0
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
refer-notify-provisional	none
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	



```

sip-profile
sip-isup-profile
block-rtcp                disabled
hide-egress-media-update  disabled
last-modified-by          admin@10.80.150.38
last-modified-date        2011-11-01 13:03:09
realm-config
  identifier               core
  description
  addr-prefix              0.0.0.0
  network-interfaces
mm-in-realm               enabled
mm-in-network             enabled
mm-same-ip                enabled
mm-in-system              enabled
bw-cac-non-mm             disabled
msm-release               disabled
qos-enable                disabled
generate-UDP-checksum     disabled
max-bandwidth             0
fallback-bandwidth        0
max-priority-bandwidth    0
max-latency               0
max-jitter                0
max-packet-loss           0
observ-window-size        0
parent-realm
dns-realm
media-policy
media-sec-policy
srtp-msm-passthrough      disabled
in-translationid
out-translationid
in-manipulationid         CS1K_To_CL
out-manipulationid        AddDomain
manipulation-string
manipulation-pattern
class-profile
average-rate-limit        0
access-control-trust-level none
invalid-signal-threshold  0
maximum-signal-threshold  0
untrusted-signal-threshold 0
nat-trust-threshold       0
deny-period               30
cac-failure-threshold     0
untrust-cac-failure-threshold 0
ext-policy-svr
diam-e2-address-realm
symmetric-latching        disabled
pai-strip                  disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching       none
restriction-mask           32
accounting-enable          enabled
user-cac-mode              none
user-cac-bandwidth         0
user-cac-sessions          0
icmp-detect-multiplier     0
icmp-advertisement-interval 0
icmp-target-ip             0
monthly-minutes            0
net-management-control     disabled
delay-media-update         disabled
refer-call-transfer        disabled
refer-notify-provisional   none

```

dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-21 12:20:52
session-agent	
hostname	10.64.19.210
ip-address	10.64.19.210
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	core
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	Proxy
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	

ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-06 14:45:58
session-agent	
hostname	172.16.2.8
ip-address	172.16.2.8
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	

load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 12:39:40
session-agent	
hostname	172.16.2.9
ip-address	172.16.2.9
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled

send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.38
last-modified-date	2011-11-01 12:39:46
session-agent	
hostname	172.16.3.8
ip-address	172.16.3.8
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0

ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-18 10:23:25
session-agent	
hostname	172.16.3.9
ip-address	172.16.3.9
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	peer
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0

max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
media-profiles	
in-translationid	
out-translationid	
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-18 10:23:57
session-group	
group-name	CL-OUT
description	
state	enabled
app-protocol	SIP
strategy	Hunt
dest	
	172.16.3.8
	172.16.2.8
trunk-group	

```

sag-recursion          enabled
stop-sag-recurse      401,407
last-modified-by      admin@10.80.150.50
last-modified-date    2012-06-18 10:27:19
sip-config
state                  enabled
operation-mode         dialog
dialog-transparency    enabled
home-realm-id          core
egress-realm-id        core
nat-mode               None
registrar-domain
registrar-host
registrar-port         0
register-service-route always
init-timer             500
max-timer              4000
trans-expire           32
invite-expire          180
inactive-dynamic-conn  32
enforcement-profile
pac-method
pac-interval           10
pac-strategy           PropDist
pac-load-weight        1
pac-session-weight     1
pac-route-weight       1
pac-callid-lifetime    600
pac-user-lifetime      3600
red-sip-port           1988
red-max-trans          10000
red-sync-start-time    5000
red-sync-comp-time     1000
add-reason-header      disabled
sip-message-len        4096
enum-sag-match         disabled
extra-method-stats     disabled
registration-cache-limit 0
register-use-to-for-lp  disabled
options                max-udp-length=0
refer-src-routing       disabled
add-ucid-header        disabled
proxy-sub-events
allow-pani-for-trusted-only disabled
pass-gruu-contact      disabled
sag-lookup-on-redirect disabled
set-disconnect-time-on-by  disabled
last-modified-by      admin@10.80.150.38
last-modified-date    2011-11-21 17:43:22
sip-interface
state                  enabled
realm-id               peer
description
sip-port
address                10.2.2.92
port                   5060
transport-protocol     UDP
tls-profile
multi-home-addr
allow-anonymous        all
ims-aka-profile
carriers
trans-expire           0
invite-expire          0
max-redirect-contacts  0
proxy-mode
redirect-action
contact-mode           none
nat-traversal          none
nat-interval           30

```



tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
subscribe-reg-event	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
tcp-conn-dereg	0
register-keep-alive	none
kpml-interworking	disabled
tunnel-name	
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-06 15:06:55
sip-interface	
state	enabled
realm-id	core
description	
sip-port	
address	10.64.19.150
port	5060
transport-protocol	TCP
tls-profile	
multi-home-addr	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0

invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
subscribe-reg-event	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
tcp-conn-dereg	0
register-keep-alive	none
kpml-interworking	disabled
tunnel-name	
last-modified-by	admin@10.80.150.50
last-modified-date	2012-06-18 10:34:11
sip-manipulation	
name	NatIP
description	
split-headers	
join-headers	
header-rule	
name	natFROM

header-name	From
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	natTO
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	natPAI
header-name	P-Asserted-Identity
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	removePL
header-name	P-Location
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	remoteAlrtInfo
header-name	Alert-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	

header-rule	
name	natRequest
header-name	Request-URI
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	natDiversion
header-name	Diversion
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	natHost
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$LOCAL_IP
header-rule	
name	natREFER
header-name	Refer-To
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	refer
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	\$REMOTE_IP
header-rule	
name	removeHist
header-name	History-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	removeRPI
header-name	Remote-Party-ID
action	delete
comparison-type	case-sensitive
msg-type	any
methods	

```

        match-value
        new-value
    header-rule
        name
        header-name
        action
        comparison-type
        msg-type
        methods
        match-value
        new-value
    last-modified-by
    last-modified-date
sip-manipulation
    name
    description
    split-headers
    join-headers
    header-rule
        name
        header-name
        action
        comparison-type
        msg-type
        methods
        match-value
        new-value
        element-rule
            name
            parameter-name
            type
            action
            match-val-type
            comparison-type
            match-value
            new-value
header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
        name
        parameter-name
        type
        action
        match-val-type
        comparison-type
        match-value
        new-value
header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
        name
        parameter-name
        type
        action
        match-val-type
        comparison-type
        match-value
        new-value

```

```

removeXNTel64
X-nt-e164-clid
delete
case-sensitive
any

```

```

admin@10.80.150.50
2012-06-18 15:26:21

```

```

AddDomain

```

```

FromDomain
From
manipulate
case-sensitive
request

```

```

From
uri-host
replace
any
case-sensitive
avayalab.com

```

```

PaiDomain
P-Asserted-Identity
manipulate
case-sensitive
request

```

```

Pai
uri-host
replace
any
case-sensitive
avayalab.com

```

```

natTO
To
manipulate
case-sensitive
request

```

```

To
uri-host
replace
any
case-sensitive

```

```

        match-value
        new-value $REMOTE_IP
    last-modified-by admin@10.80.150.50
    last-modified-date 2012-06-21 12:09:39
sip-manipulation
    name CS1K_To_CL
    description
    split-headers
    join-headers
    header-rule
        name PAIRegex
        header-name P-Asserted-Identity
        action store
        comparison-type pattern-rule
        msg-type any
        methods INVITE
        match-value
        new-value
        element-rule
            name chkUser
            parameter-name
            type header-value
            action store
            match-val-type any
            comparison-type pattern-rule
            match-value (.*) (30355571) (.*)
            new-value
        header-rule
            name HistRegex
            header-name History-Info
            action store
            comparison-type pattern-rule
            msg-type any
            methods
            match-value
            new-value
            element-rule
                name GetReason
                parameter-name
                type header-value
                action store
                match-val-type any
                comparison-type pattern-rule
                match-value (.*) (reason) (.*)
                new-value
            header-rule
                name AddDiversion
                header-name Diversion
                action add
                comparison-type boolean
                msg-type request
                methods INVITE
                match-value (!$PAIRegex[0].$chkUser) &!$HistRegex[0].$GetReason
                new-value "<sip:3035557104@avayalab.com;user=phone>"
    last-modified-by admin@10.80.150.50
    last-modified-date 2012-06-22 11:06:09
steering-pool
    ip-address 10.2.2.92
    start-port 49152
    end-port 65535
    realm-id peer
    network-interface
    last-modified-by admin@10.80.150.50
    last-modified-date 2012-06-06 15:07:34
steering-pool
    ip-address 10.64.19.150
    start-port 49152
    end-port 65535
    realm-id core
    network-interface

```

```

        last-modified-by          admin@10.80.150.50
        last-modified-date        2012-06-06 15:08:02
system-config
  hostname
  description
  location
  mib-system-contact
  mib-system-name
  mib-system-location
  snmp-enabled                    enabled
  enable-snmp-auth-traps          disabled
  enable-snmp-syslog-notify       disabled
  enable-snmp-monitor-traps       disabled
  enable-env-monitor-traps        disabled
  snmp-syslog-his-table-length    1
  snmp-syslog-level               WARNING
  system-log-level                WARNING
  process-log-level               NOTICE
  process-log-ip-address          0.0.0.0
  process-log-port                0
  collect
    sample-interval               5
    push-interval                 15
    boot-state                    disabled
    start-time                    now
    end-time                      never
    red-collect-state             disabled
    red-max-trans                 1000
    red-sync-start-time           5000
    red-sync-comp-time            1000
    push-success-trap-state       disabled
  call-trace                      disabled
  internal-trace                  disabled
  log-filter                      all
  default-gateway                 10.80.150.1
  restart                        enabled
  exceptions
  telnet-timeout                  0
  console-timeout                 0
  remote-control                  enabled
  cli-audit-trail                 enabled
  link-redundancy-state           disabled
  source-routing                  disabled
  cli-more                       disabled
  terminal-height                 24
  debug-timeout                   0
  trap-event-lifetime             0
  default-v6-gateway              ::
  ipv6-signaling-mtu              1500
  ipv4-signaling-mtu              1500
  cleanup-time-of-day             00:00
  snmp-engine-id-suffix
  snmp-agent-mode                 v1v2
task done
ACMESYSTEM#

```

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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