



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Communication Server 1000E 7.5 and Avaya Session Border Controller for Enterprise 4.0.5 with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Avaya Session Border Controller for Enterprise 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 in the Avaya Solutions and Interoperability Test Lab, utilizing CenturyLink SIP Trunk services.

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
2.3.1.	Avaya	6
2.3.2.	CenturyLink	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	8
5.	Configure Avaya Communication Server 1000E	8
5.1.	Administer an IP Telephony Node.....	10
5.1.1.	Obtain Node IP Address	10
5.1.2.	Terminal Proxy Server (TPS)	11
5.1.3.	Quality of Service (QoS)	12
5.1.4.	Voice Gateway and Codecs	13
5.1.5.	SIP Gateway.....	14
5.1.6.	Synchronize Node Configuration	17
5.2.	Virtual Superloops.....	19
5.3.	Media Gateway	20
5.4.	Virtual D-Channel, Routes and Trunks.....	23
5.4.1.	Virtual D-Channel Configuration	23
5.4.2.	Routes and Trunks Configuration.....	25
5.5.	Dialing and Numbering Plans	27
5.5.1.	Digit Manipulation Block	27
5.5.2.	Route List Block	29
5.5.3.	NARS Access Code	33
5.5.4.	Numbering Plan Area Codes	34
5.5.5.	Special Number to Route to NRS	36
5.5.6.	Incoming Digit Translation.....	37
5.6.	Zones and Bandwidth.....	38
5.7.	Customer Information and Calling Line Identification.....	40
5.8.	Example CS1000E Telephone Users	42
5.8.1.	Example SIP Phone DN 7108, Codec Considerations.....	42
5.8.2.	Example Digital Phone DN 7107 with Call Waiting.....	43
5.8.3.	Example Analog Port with DN 5711, Fax	44
5.9.	Save Configuration.....	45
5.10.	Network Routing Service Configuration.....	45
5.10.1.	Domains	47
5.10.2.	Endpoint for the SIP Signaling Gateway	48
5.10.3.	Endpoint for Avaya Session Border Controller for Enterprise	50

5.10.4.	Routing Entry for CS1000E SIP Signaling Gateway	52
5.10.5.	Routing Entry for Avaya Session Border Controller for Enterprise	53
5.10.6.	Activate Configuration	55
6.	Configure Avaya Session Border Controller for Enterprise	56
6.1.	Global Profiles.....	59
6.1.1.	Routing Profile.....	59
6.1.2.	Topology Hiding Profile	61
6.1.3.	Server Interworking Profile	64
6.1.4.	Signaling Manipulation.....	71
6.1.5.	Server Configuration.....	73
6.2.	Domain Policies	Error! Bookmark not defined.
6.2.1.	Media Rule.....	83
6.2.2.	Signaling Rule.....	85
6.2.3.	Application Rule	88
6.2.4.	Endpoint Policy Group	90
6.3.	Device Specific Settings.....	91
6.3.1.	Network Management.....	91
6.3.2.	Media Interface	93
6.3.3.	Signaling Interface	94
6.3.4.	End Point Flows - Server Flow	94
7.	CenturyLink SIP Trunk Configuration	98
8.	Verification Steps.....	99
8.1.	Avaya Communication Server 1000E Verifications.....	99
8.1.1.	IP Network Maintenance and Reports Commands.....	99
8.1.2.	System Maintenance Commands.....	101
8.1.3.	Network Routing Service Routing Verification	103
8.2.	Avaya Session Boarder Controller for Enterprise Verification	105
8.2.1.	Incidents	105
8.2.2.	Diagnostics.....	106
8.2.3.	Trace Settings.....	107
9.	Conclusion	109
10.	Additional References.....	109
Appendix A	110

1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E release 7.5 and Avaya Session Border Controller for Enterprise release 4.0.5 integration with CenturyLink SIP Trunk (Legacy Qwest) 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 Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Avaya SBCE 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) and Avaya SBCE 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**.

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

2.1. Interoperability Compliance Testing

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 UNISim, 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 UNISim, 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.

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.
- **History-Info and Diversion Headers:** CenturyLink SIP Trunk does not support SIP History-Info Headers. Instead, CenturyLink SIP Trunk requires that SIP Diversion Header be sent for redirected calls. The CS1000E includes History-Info header in messaging sent to Avaya SBCE. Avaya SBCE can add a Diversion Header required by CenturyLink. This is performed by creating a Sigma script in the Avaya SBCE configuration. See **Section 6.1.4** and **Appendix A**.

CenturyLink SIP Trunk (Legacy Qwest) passed compliance testing.

2.3. Support

2.3.1. Avaya

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

2.3.2. CenturyLink

For technical support on the CenturyLink SIP Trunk service, contact CenturyLink using the Customer Care links at www.centurylink.com

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to CenturyLink SIP Trunk. This is the configuration used for compliance testing.

The Avaya components used to create the simulated customer site included:

- Communication Server 1000E on CP+DC server as co-resident configuration
- Communication Server 1000E Media Gateway
- Network Routing Server
- Call Pilot Voicemail
- Avaya Session Border Controller for Enterprise
- Avaya 1165E IP telephones (UNISTim)
- Avaya 1140E IP telephone (SIP)
- Avaya 2050 IP Softphone (UNISTim)
- Avaya one-X® Communicator (SIP)
- Avaya digital and analog telephones

The configuration is comprised of the Avaya CPE location connected via an Internet connection to the CenturyLink SIP Trunks East and West servers. The Avaya CPE location simulates a customer site.

Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers.

For security reasons, any actual public IP addresses used in the configuration have been either blocked out or 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.

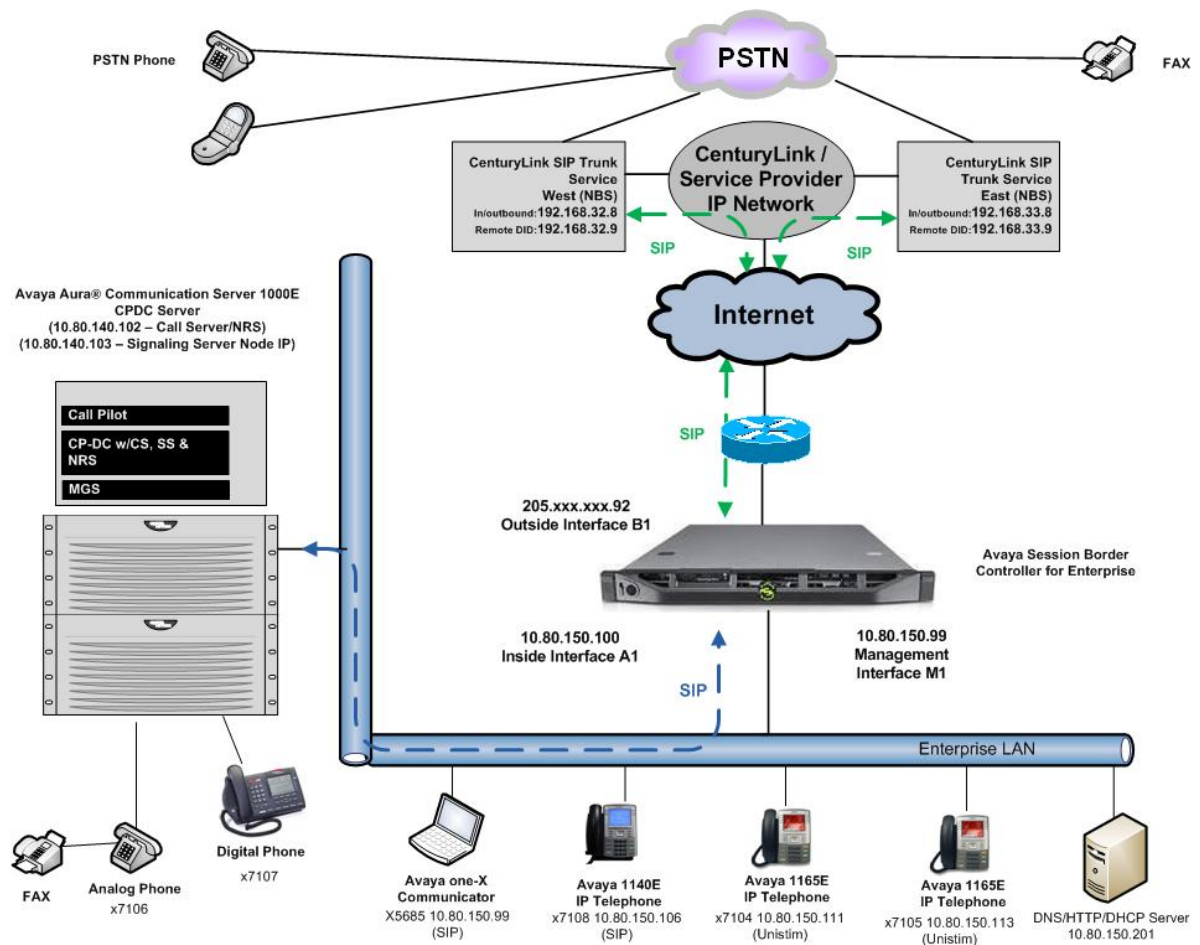


Figure 1: Avaya Interoperability Test Lab Configuration

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">● Call Server: 7.50 .17 GA (CoRes) Service Pack: 7.50.17_20120110● SSG Server: 7.50.17 GA● SLG Server: 7.50.17 GA● NRS/SPS Server: 7.50.17 GA
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
Avaya Session Border Controller for Enterprise	4.0.5Q9
Avaya 1165E (UNISim)	0626C8A
Avaya 1140E (SIP)	04.03.09.00
Avaya 2050 IP Softphone (UNISim)	4.2.0062
Avaya one-X Communicator (SIP)	CS6.1.0.25
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.

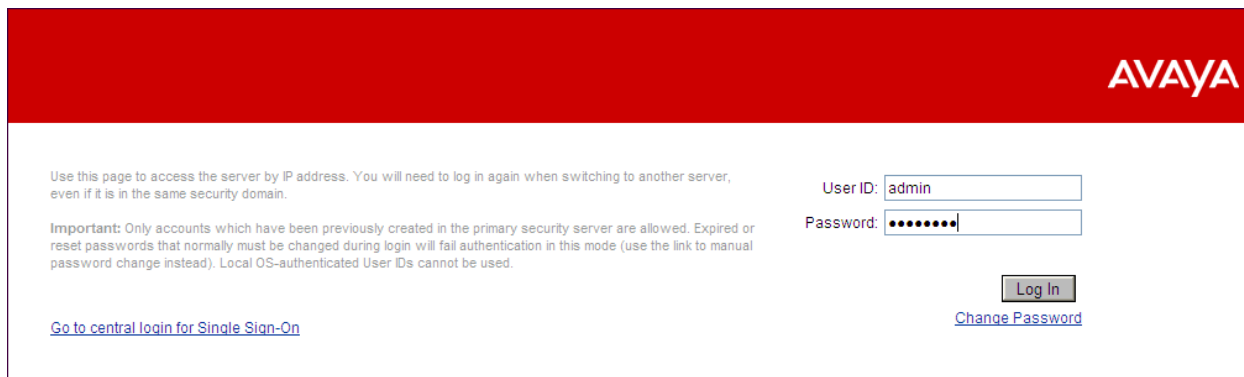
5. Configure Avaya Communication Server 1000E

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 Network Routing Service (NRS), 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 NRS, 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 10**.

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 message: "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." To the right of this message are input fields for "User ID:" (containing "admin") and "Password:" (containing "*****"). Below the password field is a "Log In" button. To the left of the "Log In" button is a link: "Go to central login for Single Sign-On". Below the "Log In" button is a link: "Change Password".

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

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

User ID: admin

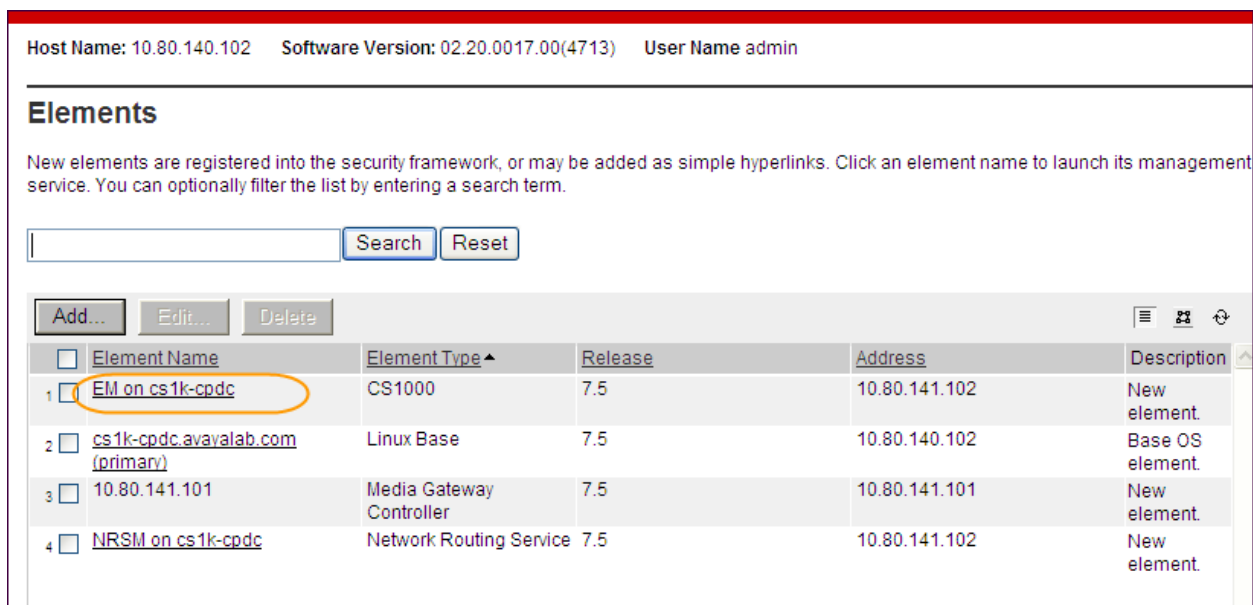
Password: *****

Log In

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

[Change Password](#)

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 header with "Host Name: 10.80.140.102", "Software Version: 02.20.0017.00(4713)", and "User Name admin". Below the header is a section titled "Elements" with a description: "New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term." There is a search input field with "Search" and "Reset" buttons. Below the search field are three buttons: "Add...", "Edit...", and "Delete". To the right of these buttons are three icons: a list icon, a refresh icon, and a search icon. Below the buttons is a table with the following data:

<input type="checkbox"/>	Element Name	Element Type ^	Release	Address	Description
<input type="checkbox"/>	EM on cs1k-cpdc	CS1000	7.5	10.80.141.102	New element.
<input type="checkbox"/>	cs1k-cpdc.avaya.com (primary)	Linux Base	7.5	10.80.140.102	Base OS element.
<input type="checkbox"/>	10.80.141.101	Media Gateway Controller	7.5	10.80.141.101	New element.
<input type="checkbox"/>	NRSIM 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 'CS1000 Element Manager' interface. The left sidebar contains a tree view with 'System' expanded and 'Nodes: Servers, Media Cards' selected. The main area is titled 'IP Telephony Nodes' and shows a table of nodes. The table has columns: Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. One node is listed with ID 1005, Component 1, and Status 'Synchronized'. Below the table are 'Show' 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 register with the Network Routing Service to establish the SIP Gateway as described later in **Section 5.1.5**. This is also the IP address UNiStim phones and SIP phones will use to register to the CS1000E.

The screenshot shows the 'Node Details' screen for Node ID 1005. The form contains fields for 'Node ID' (1005), 'Call server IP address' (10.80.141.102), 'Embedded LAN (ELAN)' with 'Gateway IP address' (10.80.141.1) and 'Subnet mask' (255.255.255.0), and 'Telephony LAN (TLAN)' with 'Node IPv4 address' (10.80.140.103) and 'Subnet mask' (255.255.255.0). There is also a field for 'Node IPv6 address'. The 'TLAN address type' is set to 'IPv4 only'. A 'Save' button and a 'Cancel' button are at the bottom right.

* Required Value.

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 * 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
- SNTIP
- 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 Codes | Fax

General

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

Voice activity detection threshold: -17 (-20 - +10 DBM)
Idle noise level: -65 (-327 - +327 DBM)

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

Voice Codes

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.

The screenshot shows the 'Voice Codecs' configuration window. At the top, 'Codec G.711' is checked and labeled 'Enabled (required)'. Below this, 'Voice payload size' is set to 20 milliseconds per frame. 'Voice playback (jitter buffer) delay' is set to 40 milliseconds for the nominal value and 80 milliseconds for the maximum value. A note states: 'Maximum delay may be automatically adjusted based on nominal settings.' At the bottom, the 'Voice Activity Detection (VAD)' checkbox is unchecked.

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

The screenshot shows the 'Voice Codecs' configuration window for Codec G.729. 'Codec G.729' is checked and labeled 'Enabled'. The 'Voice payload size' is 20 milliseconds per frame. The 'Voice playback (jitter buffer) delay' is 40 milliseconds nominal and 80 milliseconds maximum. A note states: 'Maximum delay may be automatically adjusted based on nominal settings.' The 'Voice Activity Detection (VAD)' checkbox is unchecked.

5.1.5. SIP Gateway

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

The screenshot shows the 'CS1000 Element Manager' interface. The left sidebar contains a tree view with 'Nodes: Servers, Media Cards' selected. The main area is titled 'Node Details (ID: 1005 - SIP Line, LTPS, Gateway (SIPGw))'. It shows 'Subnet mask: 255.255.255.0' and 'Node IPv6 address:'. Below this, there are two lists: 'IP Telephony Node Properties' and 'Applications (click to edit configuration)'. In the 'Applications' list, 'Gateway (SIPGw)' is highlighted with a red circle. Other applications include SIP Line, Terminal Proxy Server (TPS), Personal Directories (PD), Presence Publisher, and IP Media Services. At the bottom right are 'Save' and 'Cancel' buttons.

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. This name will be used to register with the Network Routing Server (**Section 5.10.2**)
- **Application node ID:** Enter **<Node id>**. In the sample configuration, Node **1005** was used matching the node show in **Section 5.1**.

The values defined for the sample configuration are shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, Interfaces, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main content area is titled 'Node ID: 1005 - Virtual Trunk Gateway Configuration Details'. It includes a breadcrumb trail: 'System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration'. Below the title, there are tabs for 'General', 'SIP Gateway Settings', and 'SIP Gateway Services'. The 'General' tab is active, showing a 'Vtrk gateway application' dropdown set to 'SIP Gateway (SIPGw)' and a checkbox for 'Enable gateway service on this node' which is checked. The 'General' section contains several required fields: 'SIP domain name' (avayalab.com), 'Local SIP port' (5060), 'Gateway endpoint name' (node1005), 'Gateway password', and 'Application node ID' (1005). There is also an 'Enable failsafe NRS' checkbox and a radio button for 'SIP ANAT' set to 'IPv4'. On the right, the 'Virtual Trunk Network Health Monitor' section has a checkbox for 'Monitor IP addresses (listed below)' which is unchecked, and a 'Monitor IP' field with an 'Add' button. Below this is a 'Monitor addresses' list with a 'Remove' button. At the bottom, there is a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' and 'Save' and 'Cancel' buttons.

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 Network Routing Server (NRS).
In the sample configuration, the NRS is co-resident with the Call Server so **10.80.104.102** was used.
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**
- **Options:** Check both **Support registration** and **Primary CDS proxy**.

The values defined for the sample configuration are shown below.

The screenshot shows the 'SIP Gateway Settings' window with the 'Proxy Or Redirect Server:' tab selected. Under 'Proxy Server Route 1:', the following settings are configured: Primary TLAN IP address is 10.80.140.102, Port is 5060, Transport protocol is TCP, and both 'Support registration' and 'Primary CDS proxy' options are checked. A secondary TLAN IP address of 0.0.0.0 is also shown with its respective port and protocol settings.

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

The screenshot shows the 'SIP Gateway Settings' window for 'Proxy Server Route 2:'. The settings are: Primary TLAN IP address is 10.80.140.102, Port is 5060, Transport protocol is TCP, 'Registration not supported' is checked, and 'Primary CDS proxy' is checked.

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. For compliance testing, +1 was added for **National** calling.

SIP URI Map:	
Public E.164 domain names	Private domain names
National: <input type="text" value="+1"/>	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" value="PrivateSpecial"/>
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))

Embedded LAN (ELAN)
Gateway IP address:
Subnet mask:

Telephony LAN (TLAN)
Node IPv4 address:
Subnet mask:
Node IPv6 address:

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 top header includes the Avaya logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". The left sidebar contains a navigation menu with categories like "UCM Network Services", "Links", "System", "Alarms", "Maintenance", "Core Equipment", "Loops", "Superloops" (highlighted), "MSDL/MISP Cards", "Conference/TDS/Multifrequency", "Tone Senders and Detectors", "Peripheral Equipment", "IP Network", and "Interfaces". The main content area displays the "Superloops" configuration page. It includes a status bar showing "Managing: 10.80.141.102" and "Username: admin", along with the breadcrumb "System » Core Equipment » Superloops". Below this, there are "Add..." and "Delete" buttons, and a "Refresh" link. A table lists the configured superloops:

	Superloop Number ▲	Superloop Type
1	4	IPMG
2	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.

Media Gateways				
<div>Add... Digital Trunking... Reboot Delete Virtual Terminal More Actions</div> <div>Refresh</div>				
	IPMG	IP Address	Zone	Type
	004.00	10.80.141.101	1	MGS
	004.01	10.80.141.201	1	MGS

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

- 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

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.

The screenshot displays the Avaya CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, Links, System, IP Network, Interfaces, Customers, and Routes and Trunks. The 'Media Gateways' link is selected. The main panel is titled '- VGW and IP phone codec profile'. It contains various configuration options with checkboxes, dropdown menus, and text input fields. At the bottom, there is a section for '+ Codec G711' with a 'Select' button.

Setting	Value	Unit/Range
Enable echo canceller	<input checked="" type="checkbox"/>	
Echo canceller tail delay	128	(milliseconds)
Enable dynamic attenuation	<input checked="" type="checkbox"/>	
Voice activity detection threshold	1	(0 - 4 DBM)
Idle noise level	0	(0 - 1 DBM)
R factor calculation	<input type="checkbox"/>	
DTMF tone detection	<input checked="" type="checkbox"/>	
Enable low latency mode	<input checked="" type="checkbox"/>	
Remove DTMF delay (squelch DTMF from TDM to IP)	<input checked="" type="checkbox"/>	
Enable modem/fax pass through mode	<input checked="" type="checkbox"/>	
Enable V.21 FAX tone detection	<input checked="" type="checkbox"/>	
Fax TCF method	2	
FAX maximum rate	14400	(bps)
FAX playout nominal delay	100	(0 - 300 milliseconds)
FAX no activity timeout	20	(10 - 32000 milliseconds)
FAX packet size	20	
+ Codec	G711	
Select	<input checked="" type="checkbox"/>	

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.

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

IPMG	IP Address	Zone	Type
004 00	10.80.141.101	1	MGS
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 (with sub-items: - 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 (with sub-items: - Engineered Values, + Emergency Services, + Software), - Customers, - Routes and Trunks (with sub-items: - Routes and Trunks, - D-Channels (highlighted), - Digital Trunk Interface), and - Dialing and Numbering Plans. The main content area is titled 'D-Channels' and includes a 'Maintenance' section with links for 'D-Channel Diagnostics (LD 96)', 'Network and Peripheral Equipment (LD 32, Virtual D-Channels)', 'MSDL Diagnostics (LD 96)', 'TMDI Diagnostics (LD 96)', and 'D-Channel Expansion Diagnostics (LD 48)'. Below this is a 'Configuration' section with a form 'Choose a D-Channel Number: 0 and type: DCH' and a 'to Add' button. At the bottom, a table lists the configuration for Channel 15: Channel: 15, Type: DCH, Card Type: DCIP, and Description: VtrkNode1005, with 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: and type:

- 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"/> more PRI
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 Help

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

Routes and Trunks

Customer	Total routes	Total trunks	Action
- Customer: 0	2	64	Add route
- Route: 15	Type: TIE	Description: VTRKN1005SIP	Edit Add trunk
+ Trunk: 1 - 32	Total trunks: 32		
+ Route: 17	Type: TIE	Description: VTRKN1005SIPLINE	Edit Add trunk

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):	<input type="text" value="RDB"/>
Customer number (CUST):	<input type="text" value="00"/>
Route number (ROUT):	<input type="text" value="15"/>
Designator field for trunk (DES):	<input type="text" value="VTRKN1005SIP"/>
Trunk type (TKTP):	<input type="text" value="TIE"/>
Incoming and outgoing trunk (ICOG):	<input type="text" value="Incoming and Outgoing (IAO)"/>
Access code for the trunk route (ACOD):	<input type="text" value="7900015"/>
Trunk type M911P (M911P):	<input type="checkbox"/>

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 5.5.6**.

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 Network Routing Server 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. Digit Manipulation Block

A Digit Manipulation Block was created to properly identify International calls over the SIP Trunk between Avaya Communication Server 1000E and Network Routing Server.

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **Digit Manipulation Block (DGT)** on the **Electronic Switched Network (ESN)** page as shown below.

AVAYA **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)

The **Digit Manipulation Block List** screen is displayed. In the sample configuration, a Digit Manipulation Block is needed to set the proper call type for International calls. Select an available Digit Manipulation Block Index number (other than 1) in the **Please Choose the** field and click **to Add**, or edit an existing entry by clicking the corresponding **Edit** button. In the sample configuration, **Digit Manipulation Block Index 2** is used. Select **INTL** for **Call Type to be used by the manipulated digits**.

Digit Manipulation Block List

Please choose the

- Digit Manipulation Block Index -- 2	<input type="button" value="Edit"/>
---------------------------------------	-------------------------------------

Number of leading digits to be deleted: 0
Call Type to be used by the manipulated digits : INTL

5.5.2. 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 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, the left sidebar contains a navigation menu with categories like 'UCM Network Services', 'Home', 'Links', 'System', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', and 'Electronic Switched Network'. The 'Electronic Switched Network' option is selected. The main content area shows the 'Electronic Switched Network (ESN)' configuration page. It includes a status bar with 'Managing: 10.80.141.102' and 'Username: admin'. The page title is 'Electronic Switched Network (ESN)'. The main content area lists various services under 'Customer 00', including 'Network Control & Services' and 'Coordinated Dialing Plan (CDP)'. The 'Route List Block (RLB)' option is highlighted with a yellow circle.

AVAYA **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)

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.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like Interfaces, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'Dialing and Numbering Plans' section is expanded, showing 'Electronic Switched Network' as the selected option. The main content area is titled 'Route List Blocks'. At the top, it displays 'Managing: 10.80.141.102 Username: admin' and a breadcrumb trail: 'Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network'. Below the title, there is a form with the label 'Please enter a route list index' followed by a text input field and a '(0 - 1999)' range indicator, and a 'to Add' button. Below this, there is a list of existing route list blocks. The first entry is '+ Route List Block Index -- 11' with an 'Edit' button. The second entry is '- Route List Block Index -- 15' with an 'Edit' button. Below the list, there are configuration options: 'Initial Set: 0', 'Number of Alternate Routing Attempts: 5', and 'Set Minimum Facility Restriction Level : 0'. At the bottom, there is a '+ Data Entry Index -- 0' with an 'Edit' button.

AVAYA **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

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 as shown below.

Data Entry of a Route List Block

Route List Block Index: 15

General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 0

ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: ☐

Incoming CLID Table: 0 (0 - 200)

Options

Local Termination entry: ☐

Route Number: 15

Skip Conventional Signaling: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

Strategy on Congestion: No Reroute (NRR)

Repeat these steps to create a separate **Route List Block** used for International calls. In addition select the **Digit Manipulation Index** created in **Section 5.5.1**. In the sample configuration Route List Block 11 was created for International calls.

Route List Blocks

Please enter a route list index (0 - 1999)

- Route List Block Index -- 11

Edit

Initial Set: 0

Number of Alternate Routing Attempts: 5

Set Minimum Facility Restriction Level : 0

- Data Entry Index -- 0

Edit

Route Number: 15

Expensive Route: N

Facility Restriction Level: 0

Digit Manipulation Index: 2

ISL D-Channel Down Digit Manipulation Index: 0

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: NO

5.5.3. 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 5.5.2**. 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.

AVAYA CS1000 Element Manager

Managing: 10.80.141.102 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Service and Basic Parameters

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1:

NARS Access Code 2:

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

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

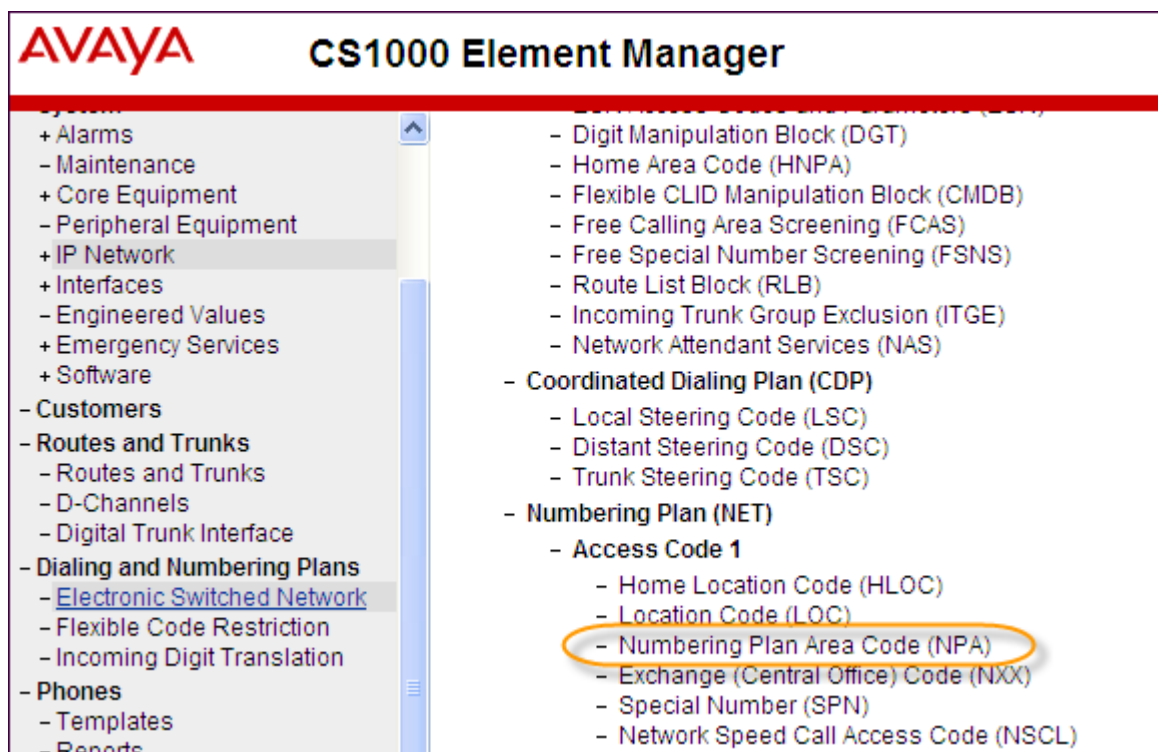
- Number of digits in CDP DN (DSC + DN or LSC + DN): (3 - 10)

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

5.5.4. 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.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The top header includes the AVAYA logo, 'CS1000 Element Manager', and links for 'Help' and 'Logout'. A navigation menu on the left lists various system components like Alarms, Maintenance, Core Equipment, etc. The main content area shows the breadcrumb path: 'Managing: 10.80.141.102 Username: admin' followed by 'Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List'. The title 'Numbering Plan Area Code List' is displayed. Below the title, there is a form 'Please enter an area code' with an input field and a 'to Add' button. A list of configured area codes is shown, each with an 'Edit' button: 1303, 1502, 1615, 1720, 1732, and 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 the NRS 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 the NRS.

The screenshot shows the 'Numbering Plan Area Code' configuration screen. The title 'Numbering Plan Area Code' is at the top. Below it, the section 'General Properties' contains three fields: 'Numbering Plan Area code translation:' with a value of '1303', 'Route List Index:' with a dropdown menu showing '15', and 'Incoming Trunk group Exclusion Index:' with a dropdown menu showing a downward arrow.

5.5.5. Special Number to Route to NRS

In the testing associated with these Application Notes, special service numbers such as x11, international calls, and operator assisted calls were also routed to the NRS 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 5.5.4**).

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. With the exception of 011, Route list index **15** has been selected in the same manner as shown for the NPAs in the prior section. For International calls, Route list index **11** was selected.

Special Number List

Please enter a Special Number

- Special Number -- 0

Edit

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

Edit

Flexible length: 0
International dialing plan: NO
Type of call that is defined by the special number: NONE
Route list index: 11

- Special Number -- 411

Edit

Flexible length: 0
International dialing plan: NO
Type of call that is defined by the special number: NONE
Route list index: 15

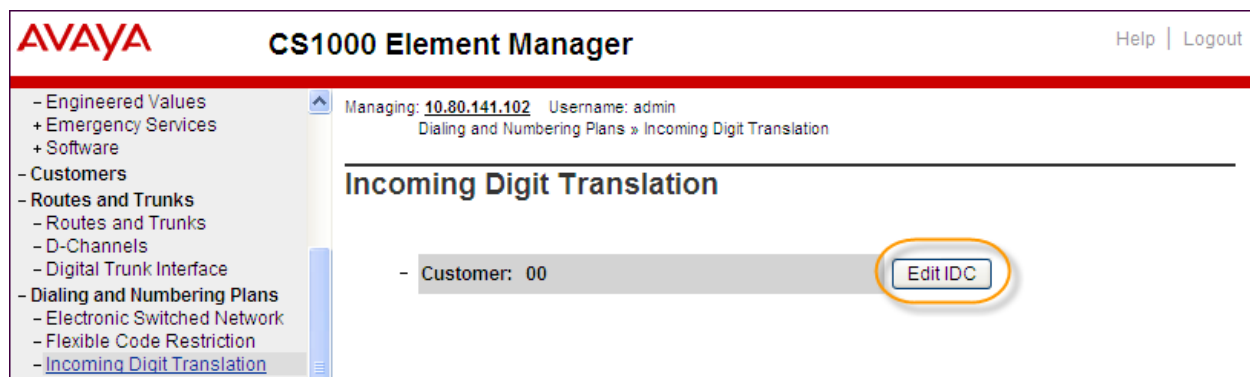
- Special Number -- 911

Edit

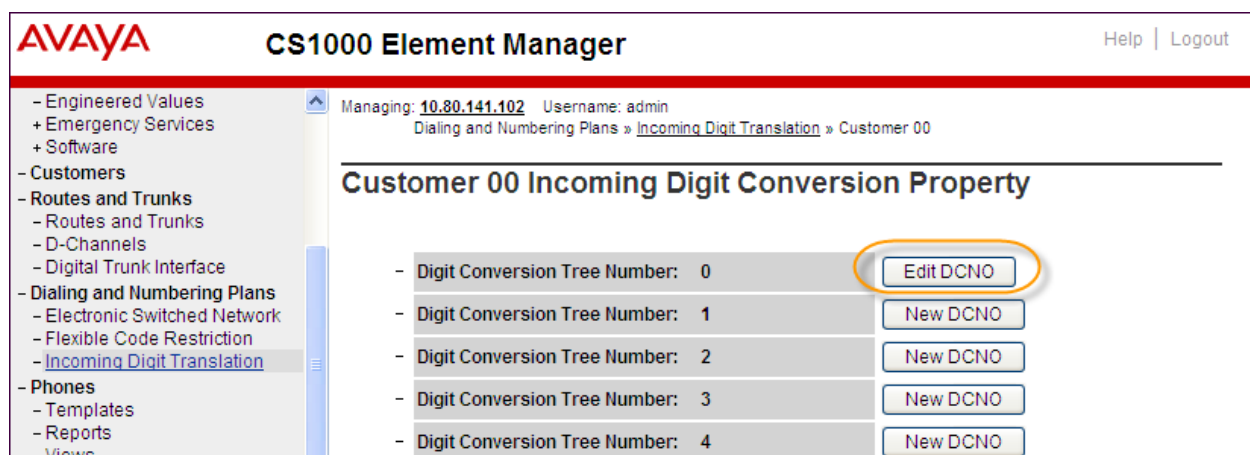
Route list index: 15
Flexible length: 0
International dialing plan: NO
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE

5.5.6. Incoming Digit Translation

In general, the incoming digit translation can be used to manipulate the digits received for an incoming call. Expand **Dialing and Numbering Plans** on the left panel and select **Incoming Digit Translation**. Click on the **Edit IDC** button as shown on the following screen.



Click on the **New DCNO** to create the digit translation mechanism. 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 details:

	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 contains a navigation menu with categories: UCM Network Services, Home, Links, System, and IP Network. The 'System' category is expanded, showing 'Zones' as the selected option. 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 as shown below. In production environments, it is likely that more zones will be required. Select the zone associated with the virtual trunk to the NRS and click **Edit** as shown below. In the sample configuration, this is Zone number **99**.

Bandwidth Zones							
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Import..."/> <input type="button" value="Export"/> <input type="button" value="Maintenance..."/> <input type="button" value="Delete"/> <input type="button" value="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. Customer Information and Calling Line Identification

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

AVAYA CS1000 Element Manager Help | Logd

Managing: 10.80.141.102 Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option: Connections restricted

Flexible orbiting prevention timer: 6

Country code: 1 (0 - 9999)
Code for processing the called number

National access code: 1

International access code: 011

Options: ☒ Transfer on ringing of supervised external trunks
☒ Connection of supervised external trunks

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan: Private dialing plan

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

Calling Line Identification

Information for incoming/outgoing calls: No manipulation is done

Size: 4000 (0 - 4000)

Country code: 1 (0 - 9999)
Code displayed as part of calling number

Calling Line Identification Entries

Click the **Calling Line Identification Entries** link as show above, and search for **the Calling Line Identification Entries** by **Entry ID**. As shown below, the **Use DN as DID** parameter was set to **YES** for the **Entry ID 0** and **1** used in the sample configuration.

Calling Line Identification Entries

Search for CLID

Start range :

End range :

'End range' should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add...Delete

Refresh

<input type="checkbox"/>	Entry Id ▲	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1 <input type="checkbox"/>	0	303	555			YES	
2 <input type="checkbox"/>	1	614	555			YES	

5.8. 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.


5.8.1. 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: ☐

5.8.2. 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 tree with categories like UCM Network Services, System, Customers, Routes and Trunks, and Phones. The 'Phones' section is selected. The main area shows 'Phone Details' for a phone managed by 'EM on cs1k-cpdc(10.80.141.102)'. It includes a photo of a digital phone and fields for System (EM on cs1k-cpdc), Phone Type (M3904), and Sync Status (TRN). Below this are tabs for General Properties, Features, Keys, and User Fields. The 'General Properties' tab is active, showing fields for Customer Number (0), Terminal Number (004 0 03 00), and Designation (DIG).

The following screen shows basic key information for the telephone. It can be observed that the telephone can support call waiting with tone, and uses **CLID Entry 0** (see **Section 5.7**).

Although not shown in detail below, to use call waiting with tone, assign a key **CWT – Call Waiting**, set the feature **SWA – Call waiting from a Station** to **Allowed**, and set the feature **WTA – Warning Tone** to **Allowed**.

The screenshot displays the 'Keys' configuration page in the AVAYA CS1000 Element Manager. It features a table with columns for Key No., Key Type, and Key Value. Key 0 is configured with Key Type 'SCR - Single Call Ringing' and Key Value '7107'. Below the table, there are checkboxes for 'Multiple Appearance Redirection Prime(MARP)' and 'CLID Entry (Numeric or D)' (set to 0). There are also input fields for 'ANIE Entry' and 'First Name' (John), 'Last Name' (Digital), 'Display Format' (First, Last), and 'Language' (Roman).

5.8.3. Example Analog Port with DN 5711, Fax


The following screen shows basic information for an analog port in the configuration that may be used with a telephone or fax machine and uses CLID Entry 1 (see **Section 5.7**). The port is configured as Directory Number 5711.

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: 0 *

Terminal Number: 004 0 04 00

Designation: ANA0 * (1-6 characters)

Directory Number: 5711 🔍

CLID entry: 1

ANIE entry:

Marp ☒

First Name	Last Name	Display Format	Language
John	Single	First, Last ▼	Roman ▼

5.9. 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 shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories: Phones, Tools, and Security. Under Tools, 'Backup and Restore' is expanded, and 'Call Server' is selected. The main area displays 'Managing: 10.80.141.102 Username: admin' and a breadcrumb trail: 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The title is 'Call Server Backup'. Below it, there is an 'Action' dropdown menu set to 'Backup', and 'Submit' and 'Cancel' buttons.

5.10. Network Routing Service Configuration

In this section, it shows how to configure a Network Routing Service (NRS) on Communication Server 1000E. Follow the steps below to setup the NRS server. It is assumed that the NRS has been deployed on the Communication Server 1000 Unified Communications Management (UCM) environment with all latest Service Pack applied.

The Avaya Unified Communications Management Elements page will be used for configuration. Click on the Element Name corresponding to **Network Routing Service** in the Element Type column. In the abridged screen below, the user would click on the Element Name **NRSM on cs1k-cpdc**.

The screenshot shows the AVAYA Avaya Unified Communications Management interface. The left navigation tree has 'Tools' expanded, and 'Network Routing Service' is selected. The main area shows 'Host Name: 10.80.140.102 Software Version: 02.20.0017.00(4713) User Name admin'. Below this is the 'Elements' section with a description: 'New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.' There is a search bar with 'Search' and 'Reset' buttons. Below the search bar are 'Add...', 'Edit...', and 'Delete' buttons. A table lists the elements:

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	EM on cs1k-cpdc	CS1000	7.5	10.80.141.102	New element.
<input type="checkbox"/>	cs1k-cpdc.avaya.com (primary)	Linux Base	7.5	10.80.140.102	Base OS element.
<input type="checkbox"/>	10.80.141.101	Media Gateway Controller	7.5	10.80.141.101	New element.
<input type="checkbox"/>	NRSM on cs1k-cpdc	Network Routing Service	7.5	10.80.141.102	New element.

The **NRS Server** screen is displayed with additional details as shown below. Under the **Server Configuration** heading, make a note of the **Primary TLAN IPV4 address**. In the sample screen below, the **IPV4 address** is **10.80.140.102**. This IP address will be needed when configuring the Avaya SBCE with a Route Profile to the CS1000E NRS in **Section 6.1.1** and the Server Configuration for the CS1000E NRS in **Section 6.1.5.1**.

AVAYA Network Routing Service Manager Help | Logout

«UCM Network Services

- System
 - NRS Server
 - Database
 - System Wide Settings
- Numbering Plans
 - Domains
 - Endpoints
 - Routes
 - Network Post-Translation
 - Collaborative Servers
- Tools
 - SIP Phone Context
 - Routing Tests
 - H.323
 - SIP
 - Backup
 - Restore
 - GK/NRS Data upgrade

Managing: 10.80.141.102
System » NRS Server

NRS Server

Service Status

	Service Name	Service Status
1 <input type="checkbox"/>	SIP Proxy Server (SPS)	In service
2 <input type="checkbox"/>	Gatekeeper (GK)	In service
3 <input type="checkbox"/>	Network Connection Server (NCS)	In service

Server Configuration

NRS Setting

Host name HostName
 Address type IPv4 only
 Primary TLAN IPv4 address 10.80.140.102
 Secondary TLAN IPv4 address 0.0.0.0
 Secondary server host name SecondaryHostName
 Control priority 40
 Server mate communication port 5005
 Realm name realmName
 Server role Primary

H.323 Gatekeeper Settings
 Location request (LRQ) response timeout 3

Scroll down and verify the **SIP Server Settings**. The **Primary server UDP port** and **Primary server TCP port** settings should match the ports entered in the SIP Gateway in **Section 5.1.5**.

Server Configuration

SIP Server Settings

Public name for non-trusted networks unknown
 Public number for non-trusted networks 000-000
 UDP Transport enabled ☒
 Primary server UDP IPv4 10.80.140.102
 Primary server UDP port 5060
 Secondary server UDP IPv4 0.0.0.0
 Secondary server UDP port 5060
 TCP Transport enabled ☒
 Primary server TCP IPv4 10.80.140.102
 Primary server TCP port 5060
 Secondary server TCP IPv4 0.0.0.0

5.10.1. Domains

Create a SIP domain for each domain for which the NRS will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Expand **Numbering Plans** on the left panel and select **Domains**. Click on the radio button of the **Standby database**. Then with the **Service Domains (1)** tab selected, click on the **Add** button. In the sample screen below, the domain name is **avayalab.com**.

AVAYA Network Routing Service Manager

Managing: ☐ Active database 10.80.141.102
☒ Standby database [Numbering Plans » Domains](#)

Domains
Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Service Domains (1) **L1 Domains (UDP) (1)** **L0 Domains (CDP) (1)**

Add... **Delete** [Refresh](#)

<input type="checkbox"/>	Domain Name ^	Description	# of L1 Domains	# of L0 Domains	# of Gateway Endpoints
1 <input type="checkbox"/>	avayalab.com		1	1	2

1 - 1 of 1 Service Domain(s) Page 1 of 1 [First](#) [Previous](#) [Next](#) [Last](#)

Select the **L1 Domains (UDP) (1)** tab, and in the **Filter by Domain** select the newly created domain. Click on the **Add** button and enter **udp** as the L1 Domain name as shown below.

Domains
Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Service Domains (1) **L1 Domains (UDP) (1)** **L0 Domains (CDP) (1)**

Filter by Domain: avayalab.com

Add... **Delete** [Refresh](#)

<input type="checkbox"/>	ID ^	Description	# of L0 Domains	# of Gateway Endpoints	# of Routing Entries	Context
1 <input type="checkbox"/>	udp		1	2	9	avayalab.com

1 - 1 of 1 L1 Domain(s) Page 1 of 1 [First](#) [Previous](#) [Next](#) [Last](#)

Select the **L0 Domains (CDP) (1)** tab and in the **Filter by Domain**, select the newly created domain and the newly created L1 domain. Click on the **Add** button and enter **cdp** as the L0 Domain name as shown below.

Domains
Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Service Domains (1) | L1 Domains (UDP) (1) | L0 Domains (CDP) (1)

Filter by Domain : /

Add... Delete Refresh

ID	Description	# of Gateway Endpoints	# of Routing Entries	Context
1	cdp	2	9	avayalab.com / udp

1 - 1 of 1 L0 Domain(s) Page 1 of 1 First Previous Next Last

5.10.2. Endpoint for the SIP Signaling Gateway

An Endpoint must be added for the CS1000E SIP Signaling Gateway and for the Avaya SBCE. Create a dynamic gateway endpoint for the CS1000E SIP Signaling Gateway. Expand **Numbering Plans** on the left panel and select **Endpoints**. Verify the **Standby database** radio button is still selected. Select the newly created domains in the **Limit results to Domain** section and click the **Add** button as shown below.

AVAYA Network Routing Service Manager Help | Logout

Managing: ☐ Active database 10.80.141.102
☒ Standby database Numbering Plans » Endpoints

Search for Endpoints Hide

Enter an endpoint ID (use * for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID:

Limit results to Domain: / /

Results per page: 50 Search

Gateway Endpoints (2) | User Endpoints (0)

Add... Delete SIP phone context... Refresh

ID	Supported Protocols	SIP mode	Call Signaling IP	Description	# of Routing Entries	Context	
1	ASBCE	Static SIP endpoint	Proxy Mode	10.80.150.100	Avaya Session Border Controller for Enterprise	6	avayalab.com / udp / cdp
2	node1005	Dynamic SIP endpoint	Proxy Mode	Not available		3	avayalab.com / udp / cdp

In the detail gateway endpoint configuration page that appears, enter the following values. Use default values for all remaining fields:

- **End point name:** Enter a descriptive name. This must match the name defined for the **Gateway endpoint name** in **Section 5.1.5**.
- **Trust Node:** Checked
- **E.164 country code:** Enter the proper country code.
- **Static endpoint address type:** Select **IP version 4**.
- **H.323 support:** Select **H.323 not supported**.
- **SIP Support:** Select **Dynamic SIP endpoint**.
- **SIP TCP transport enabled:** Checked.
- **SIP TCP port:** **5060**
- **Persistent TCP support enabled:** Checked.

Click **Save** to continue (not shown).

Edit Gateway Endpoint avayalab.com / udp / cdp)

End point name: node1005 *

Description:

Trust Node: ☒

Tandem gateway endpoint name: Not Applicable

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code: 1

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length: (0-99)

E.164 national dialing access code:

E.164 national dialing code length: (0-99)

E.164 local (subscriber) dialing access code:

Edit Gateway Endpoint avayalab.com / udp / cdp)

Static endpoint address type: IP version 4

Static endpoint address:

H.323 support: H.323 not supported

SIP support: Dynamic SIP endpoint

SIP mode: ☒ Proxy Mode ☐ Redirect Mode

SIP TCP transport enabled: ☒

SIP TCP port: 5060

SIP UDP transport enabled: ☐

SIP UDP port: 5060

SIP TLS transport enabled: ☐

SIP TLS port: 5061

Persistent TCP support enabled: ☒

End to end security support: ☐

Network Connection Server enabled: ☐

5.10.3. Endpoint for Avaya Session Border Controller for Enterprise

Create a static gateway endpoint for the Avaya Session Border Controller for Enterprise. Expand **Numbering Plan** on the left panel and select **Endpoints**. Verify the **Standby database** radio button is still selected. Select the newly created domains in the **Limit results to Domain** section and click the **Add** button as shown below.

AVAYA Network Routing Service Manager Help | Logout

Managing: ☐ Active database 10.80.141.102 ☒ Standby database [Numbering Plans » Endpoints](#)

Search for Endpoints Hide

Enter an endpoint ID (use * for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID: *

Limit results to Domain: avayalab.com / udp / cdp

Results per page: 50 Search

Gateway Endpoints (2) | User Endpoints (0)

Add... Delete SIP phone context... Refresh

	ID	Supported Protocols	SIP mode:	Call Signaling IP	Description	# of Routing Entries	Context
1	ASBCE	Static SIP endpoint	Proxy Mode	10.80.150.100	Avaya Session Border Controller for Enterprise	6	avayalab.com / udp / cdp
2	node1005	Dynamic SIP endpoint	Proxy Mode	Not available		3	avayalab.com / udp / cdp

In the detail gateway endpoint configuration page that appears, enter the following values. Use default values for all remaining fields:

- **End point name:** Enter a descriptive name.
- **Trust Node:** Checked.
- **E.164 country code:** Enter the proper country code.
- **Static endpoint address type:** Select **IP version 4**.
- **Static endpoint address:** Enter the IP address of the Avaya SBCE inside interface (see **Section 6.3.1**).
- **H.323 support:** Select **H.323 not supported**.
- **SIP Support:** Select **Static SIP endpoint**.
- **SIP TCP transport enabled:** Checked.
- **SIP TCP port:** **5060**.
- **Persistent TCP support enabled:** Checked.

Click **Save** to continue (not shown).

Edit Gateway Endpoint avayalab.com / udp / cdp)

End point name: ASBCE *

Description: Avaya Session Border Controller for

Trust Node: ☒

Tandem gateway endpoint name: Not Applicable

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code: 1

E.164 area code:

E.164 international dialing access code:

E.164 international dialing code length: (0-99)

E.164 national dialing access code:

E.164 national dialing code length: (0-99)

E.164 local (subscriber) dialing access code:

Edit Gateway Endpoint avayalab.com / udp / cdp)

Static endpoint address type: IP version 4

Static endpoint address: 10.80.150.100

H.323 support: H.323 not supported

SIP support: Static SIP endpoint

SIP mode: ☒ Proxy Mode ☐ Redirect Mode

SIP TCP transport enabled: ☒

SIP TCP port: 5060

SIP UDP transport enabled: ☐

SIP UDP port: 5060

SIP TLS transport enabled: ☐

SIP TLS port: 5061

Persistent TCP support enabled: ☒

End to end security support: ☐

Network Connection Server enabled: ☐

5.10.4. Routing Entry for CS1000E SIP Signaling Gateway

The NRS determines how to route SIP messages based on the information given in the Routing Entries. For compliance testing CenturyLink provided two sets of DID ranges, 303-555-7xxx and 614-555-0xxx. Route Entries **3035557** and **6145550** were created for the CS1000E SIP Signaling Gateway with the **Endpoint Name** of **node1005**. To add a Routing Entry, expand **Numbering Plans** on the left panel and select **Routes**. Select the domain names in the **Limit results to Domain** fields and select the **Endpoint Name** created for the CS100E SIP Signaling Gateway as shown below.

The screenshot shows the Avaya Network Routing Service Manager interface. On the left is a navigation tree with 'Numbering Plans' expanded and 'Routes' selected. The main area is titled 'Search for Routing Entries'. It contains search filters: 'DN Prefix' (set to '*'), 'DN Type' (set to 'All DN Types'), 'Limit results to Domain' (set to 'avayalab.com / udp / cdp'), and 'Endpoint Name' (set to 'node1005'). Below the filters is a table of routing entries. The table has columns for 'DN Prefix', 'DN Type', 'Route Cost', 'SIP URI Phone Context', and 'Context'. Two entries are listed: 1. DN Prefix: 3035557, DN Type: Private level 0 regional (CDP steering code), Route Cost: 1, SIP URI Phone Context: cdp.udp, Context: avayalab.com / udp / cdp / node1005. 2. DN Prefix: 6145550, DN Type: Private level 0 regional (CDP steering code), Route Cost: 1, SIP URI Phone Context: cdp.udp, Context: avayalab.com / udp / cdp / node1005. The 'Add...' button is highlighted with an orange circle.

DN Prefix	DN Type	Route Cost	SIP URI Phone Context	Context
1 3035557	Private level 0 regional (CDP steering code)	1	cdp.udp	avayalab.com / udp / cdp / node1005
2 6145550	Private level 0 regional (CDP steering code)	1	cdp.udp	avayalab.com / udp / cdp / node1005

In the Routing Entry configuration page that appears, enter the following values:

- **DN type:** Private level 0 regional (CDP steering code).
- **DN prefix:** Enter a prefix to match (e.g., 3035557).
- **Route cost:** 1

The screenshot shows the 'Edit Routing Entry (avayalab.com / udp / cdp / node1005)' configuration page. It contains three fields: 'DN type' (set to 'Private level 0 regional (CDP steering code)'), 'DN prefix' (set to '3035557'), and 'Route cost' (set to '1'). A legend at the bottom left indicates that '*' denotes a required value. 'Save' and 'Cancel' buttons are at the bottom right.

5.10.5. Routing Entry for Avaya Session Border Controller for Enterprise

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. To add a Routing Entry for Avaya SBCE, expand **Numbering Plans** on the left panel and select **Routes**. Select the domain names in the **Limit results to Domain** fields and select the **Endpoint Name** created for the Avaya SBCE as shown below.

The screenshot shows the Avaya Network Routing Service Manager interface. On the left is a navigation tree with 'Numbering Plans' expanded and 'Routes' selected. The main area is titled 'Search for Routing Entries'. It contains search filters: 'DN Prefix' (set to '*'), 'DN Type' (set to 'All DN Types'), 'Limit results to Domain' (set to 'avayalab.com / udp / cdp'), and 'Endpoint Name' (set to 'ASBCE'). Below the search filters is a table of routing entries. The table has columns for 'DN Prefix', 'DN Type', 'Route Cost', 'SIP URI Phone Context', and 'Context'. There are 6 routing entries listed. The 'Add...' button is highlighted with an orange circle.

Search for Routing Entries

Enter a DnPrefix and Dn Type (use * for all) and click Search. You may narrow the search by specifying a particular domain.

DN Prefix: * DN Type: All DN Types

Limit results to Domain: avayalab.com / udp / cdp

Endpoint Name: ASBCE

Results per page: 50 Search

Routing Entries (6) Default Routes (0) Emergency Fallback Routes (0)

Add... Copy... Move... Import... Export... Routing test... Delete Refresh

	DN Prefix	DN Type	Route Cost	SIP URI Phone Context	Context
1	0	Private level 0 regional (CDP steering code)	1	cdp.udp	avayalab.com / udp / cdp / ASBCE
2	011	E.164 international	1	+	avayalab.com / udp / cdp / ASBCE
3	1	E.164 national	1	+1	avayalab.com / udp / cdp / ASBCE
4	303	E.164 national	1	+1	avayalab.com / udp / cdp / ASBCE
5	411	Private level 0 regional (CDP steering code)	1	cdp.udp	avayalab.com / udp / cdp / ASBCE

In the Routing Entry configuration page that appears (not shown), enter the following values:

- **DN type:** Select the appropriate entry based on the type of call (see examples below).
- **DN prefix:** Enter a prefix to match (see examples below). The full list of DN prefixes used during the compliance testing is shown in the previous screen.
- **Route cost:** 1

Click **Save** to continue.

The screen below shows the route entry added for any number that begins with a 1. This represents long distance calls based on the North American Numbering Plan. The **DN type** is set to **E.164 national**.

The screenshot shows a web form titled "Edit Routing Entry (avayalab.com / udp / cdp / ASBCE)". It contains three input fields: "DN type:" with a dropdown menu set to "E.164 national", "DN prefix:" with a text box containing "1" and an asterisk indicating it is required, and "Route cost:" with a text box containing "1" and a range "(1-255)". At the bottom left, there is a note "* Required value." and at the bottom right, there are "Save" and "Cancel" buttons.

The screen below shows the route entry added for any number that begins with a 011. This represents international calls based on the North American Numbering Plan. The **DN type** is set to **E.164 international**.

The screenshot shows a web form titled "Edit Routing Entry (avayalab.com / udp / cdp / ASBCE)". It contains three input fields: "DN type:" with a dropdown menu set to "E.164 international", "DN prefix:" with a text box containing "011" and an asterisk indicating it is required, and "Route cost:" with a text box containing "1" and a range "(1-255)". At the bottom left, there is a note "* Required value." and at the bottom right, there are "Save" and "Cancel" buttons.

The screen below shows the route entry added for directory assistance. The **DN type** is set to **Private level 0 regional (CDP steering code)**.

Edit Routing Entry (avayalab.com / udp / cdp / ASBCE)

DN type: Private level 0 regional (CDP steering code) ▼

DN prefix: 411 *

Route cost: 1 * (1-255)

* Required value.

Save Cancel

5.10.6. Activate Configuration

All configuration changes thus far have been done on the Standby database. Before the changes will take affect the standby database must be cut over and committed to the active database. Expand **System** on the left panel and select **Database**. Select the **Cut over** button as shown below.

AVAYA Network Routing Service Manager Help Logout

«UCM Network Services

- System
 - NRS Server
 - Database
 - System Wide Settings
- Numbering Plans
 - Domains
 - Endpoints
 - Routes

Managing: 10.80.141.102

System » Database

Database

NRS uses a redundant database with Active and Standby copies. Normally changes are made to the standby database, tested, then cut over into active status.

Database status: Changed

Cut over Revert Commit Roll back

The **Database status** field will update from **Changed** (as shown above) to **Switched over** (as shown below). Click on the **Commit** button to activate the database.

AVAYA Network Routing Service Manager Help Logout

«UCM Network Services

- System
 - NRS Server
 - Database
 - System Wide Settings
- Numbering Plans
 - Domains
 - Endpoints
 - Routes

Managing: 10.80.141.102

System » Database

Database

NRS uses a redundant database with Active and Standby copies. Normally changes are made to the standby database, tested, then cut over into active status.

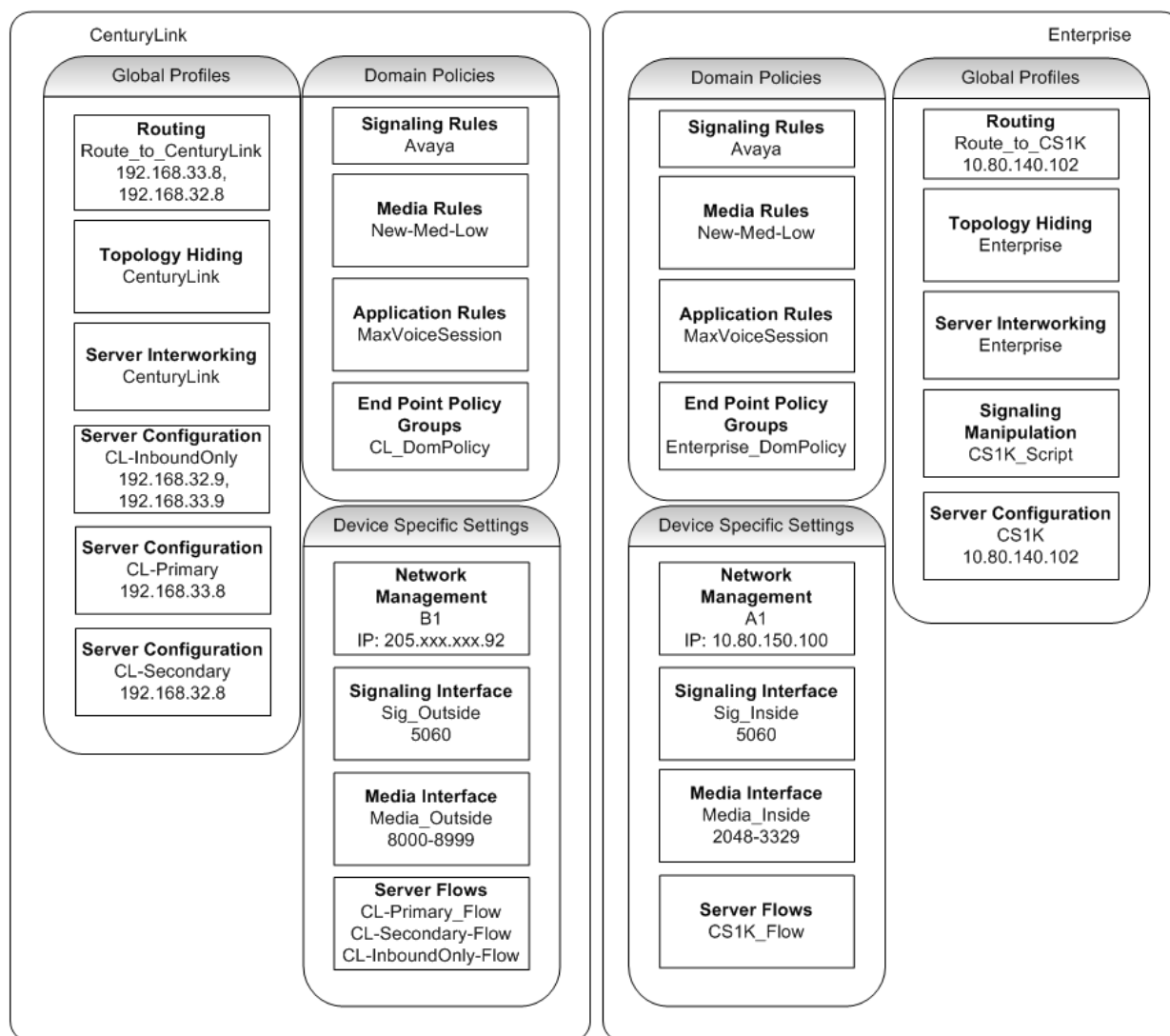
Database status: Switched over

Cut over Revert Commit Roll back

6. Configure Avaya Session Border Controller for Enterprise

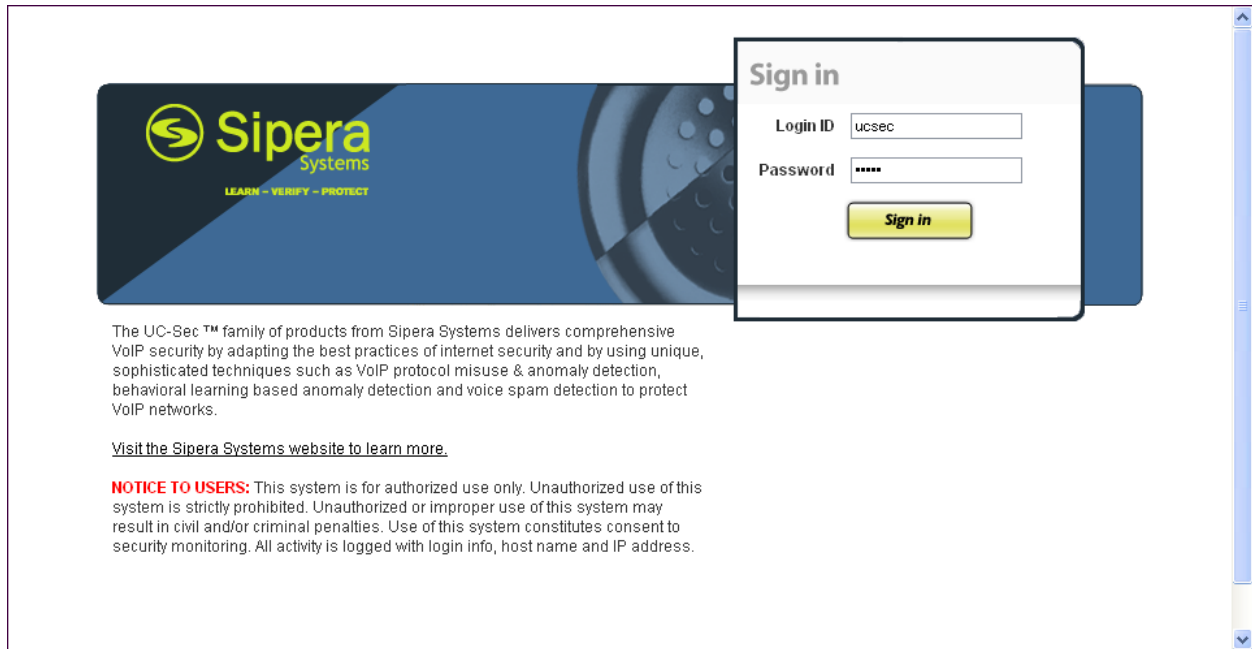
This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed. For additional information on these configuration tasks, see **Reference** [8] and [9].

A pictorial view of this configuration is shown below. It shows the components needed for the compliance test. Each of these components is defined in the Avaya SBCE web configuration as described in the following sections.



Use a WEB browser to access the Element Management Server (EMS) web interface, and enter <https://<ip-addr>/ucsec> in the address field of the web browser, where <ip-addr> is the management LAN IP address of the Avaya SBCE.

Log in with the appropriate credentials. Click **Sign In**.

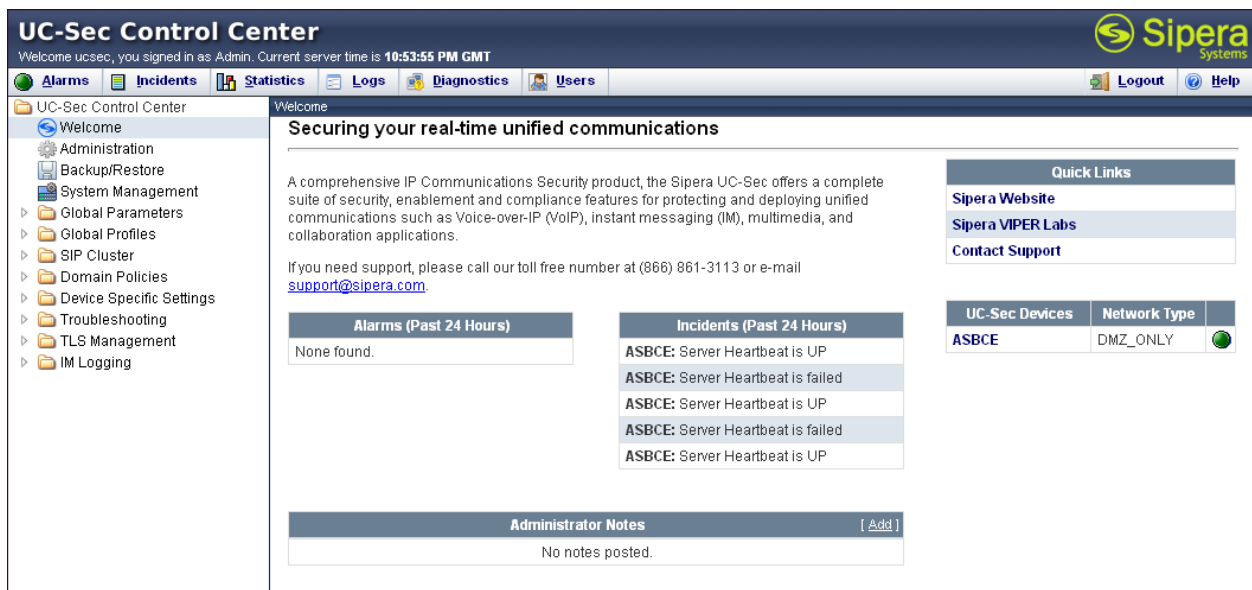


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Sipera Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

The main page of the UC-Sec Control Center will appear.



UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 10:53:55 PM GMT

Alarms **Incidents** **Statistics** **Logs** **Diagnostics** **Users** **Logout** **Help**

UC-Sec Control Center

- Welcome
- Administration
 - Backup/Restore
 - System Management
 - Global Parameters
 - Global Profiles
 - SIP Cluster
 - Domain Policies
 - Device Specific Settings
 - Troubleshooting
 - TLS Management
 - IM Logging

Welcome

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

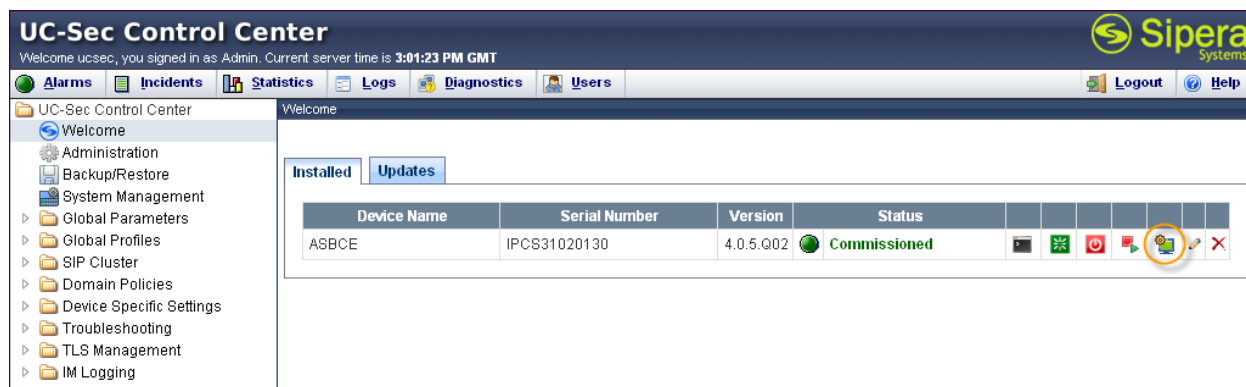
Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	ASBCE: Server Heartbeat is UP
	ASBCE: Server Heartbeat is failed
	ASBCE: Server Heartbeat is UP
	ASBCE: Server Heartbeat is failed
	ASBCE: Server Heartbeat is UP

UC-Sec Devices	Network Type
ASBCE	DMZ_ONLY

Administrator Notes
No notes posted.

[Add]

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



The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: ASBCE

Network Configuration

General Settings

Appliance Name	ASBCE
Box Type	SIP
Deployment Mode	Proxy

Device Settings

HA Mode	NO
Secure Channel Mode	NONE
Two Bypass Mode	NO

Network Settings

IP	Public IP	Netmask	Gateway	Interface
10.80.150.100	10.80.150.100	255.255.255.0	10.80.150.1	A1
205.192.192.92	205.192.192.92	255.255.255.128	205.192.192.1	B1

DNS Configuration

Primary DNS	10.80.150.201
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.80.150.100

Management IP(s)

IP	10.80.150.99
----	--------------

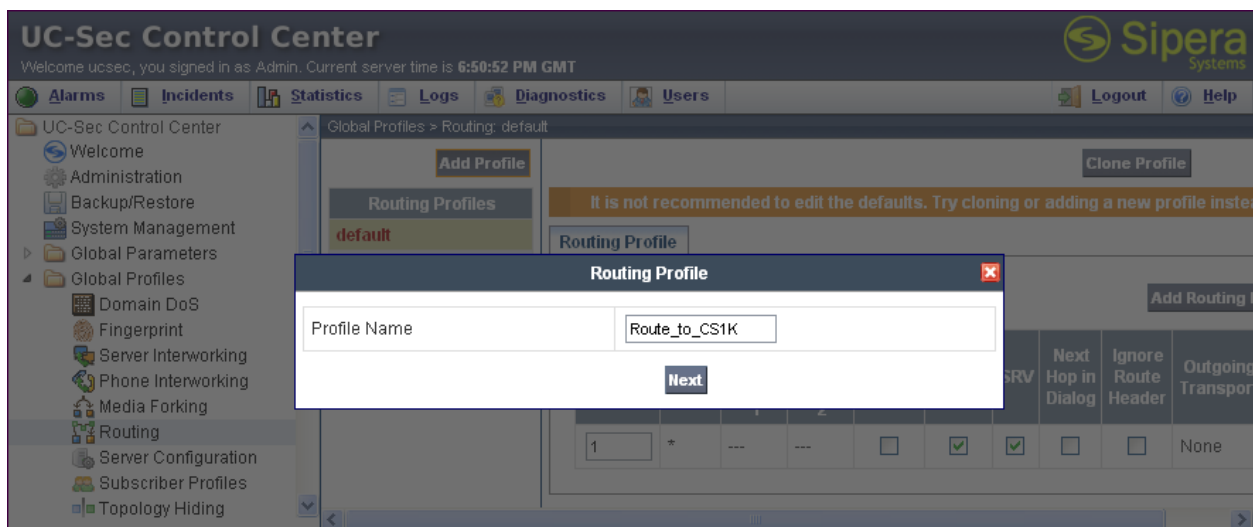
6.1. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

6.1.1. Routing Profile

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

Create a Routing Profile for the CS1000E and CenturyLink SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.



In the new window that appears, enter the following values (not shown). Use default values for all remaining fields:

- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server:** Checked.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish**.

In the shared test environment the following screen shows the Routing Profile to CS1000E. The **Next Hop Server 1** IP address must match the IP address of the NRS in **Section 5.10**. The Outgoing Transport must match the Avaya SBCE Endpoint created on the NRS in **Section 5.10.3**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Global Parameters, Global Profiles, and Routing. The main area displays the 'Routing Profiles' configuration for 'Route_to_CS1K'. A table lists routing rules with columns for Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. The first rule has a priority of 1, URI Group of *, Next Hop Server 1 of 10.80.140.102, and Outgoing Transport of TCP.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.80.140.102	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to CenturyLink. For compliance testing CenturyLink had four SIP servers 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 SIP servers allocated for outbound traffic were added to the Routing Profile.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Routing' selected. The main panel displays the 'Routing Profiles' section, showing a list of profiles including 'default', 'SP1', 'Route_to_CS1K', 'Route_to_SessionMgr', 'Route_to_CM-Lab1', 'SP2', 'remote-test', and 'Route_to_CenturyLink'. The 'Route_to_CenturyLink' profile is selected. The right pane shows the configuration for this profile, including a table for routing rules.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	+	192.168.33.8:5060	192.168.32.8:5060	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

6.1.2. Topology Hiding Profile

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

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

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Topology Hiding' selected. The main panel displays the 'Topology Hiding Profiles' section, showing a list of profiles including 'default'. The 'default' profile is selected. The right pane shows the configuration for this profile, including a table for topology hiding rules. A 'Clone Profile' button is highlighted in the top right corner.

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

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

Clone Profile

Profile Name

default

Clone Name

Enterprise

Finish

Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in the NRS (**Section 5.10.1**). Click **Finish** to save the changes.

Edit Topology Hiding Profile

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

Finish

It is not necessary to modify the **CenturyLink** profile from the default values. The following screen shows the Topology Hiding Policy created for CenturyLink.

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

CenturyLink

Topology Hiding

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

[Edit](#)

When creating or editing Topology Hiding Profiles, there are six types of headers available for selection in the Header drop-down list to choose from. In addition to the six headers, there are additional headers not listed that are affected when either of two types of listed headers (e.g., **To Header** and **From Header**) are selected in the **Header** drop-down list. **Table 2** lists the six headers along with all of the other affected headers in three header categories (e.g., **Source Headers**, **Destination Headers**, and **SDP Headers**).

Topology Hiding Headers	
Main Header Names	Header(s) Affected by Main Header
Source Headers	
Record-Route	
From	(1) Referred-By (2) P-Asserted Identity
Via	
Destination Headers	
To	(1) ReferTo
Request-Line	
SDP Headers	
Origin Header	

Table 2: Topology Hiding Headers

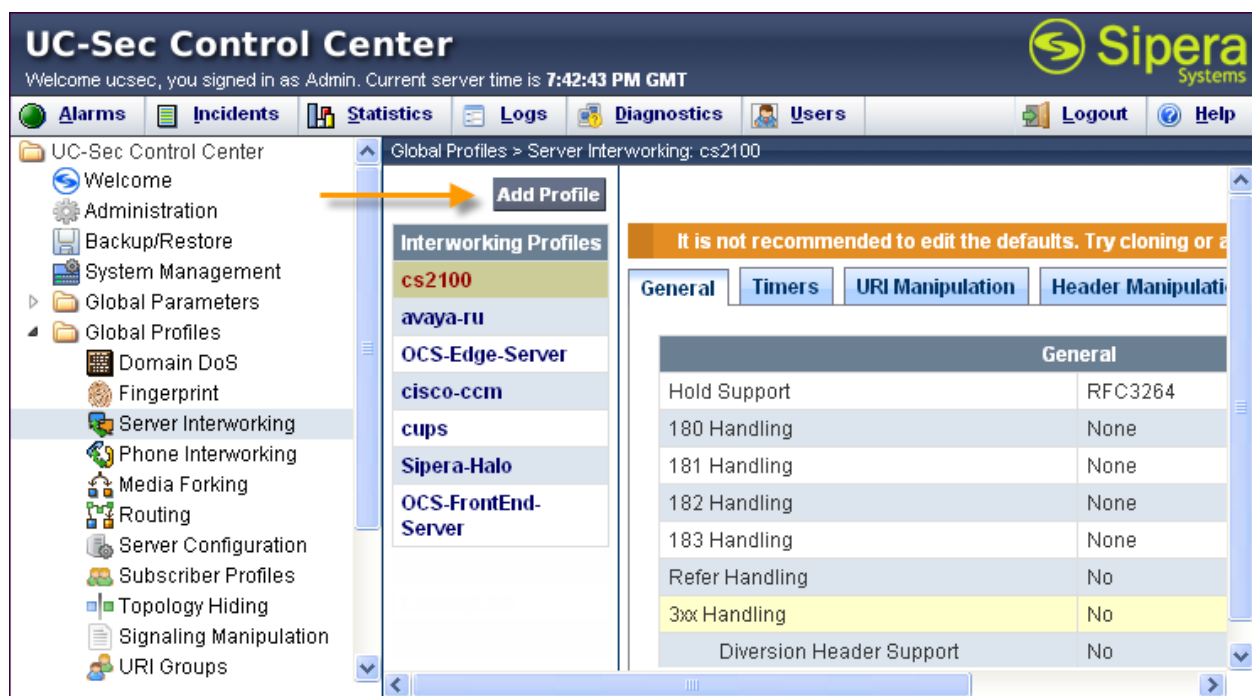
6.1.3. Server Interworking Profile

The Server Interworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or modified, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for **Enterprise** and **CenturyLink**.

6.1.3.1 Server Interworking Profile – Enterprise

To create a new Server Interworking Profile for the enterprise, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown below.



Enter a descriptive name for the new profile and click **Next** to continue.

Interworking Profile

Profile Name

CS1K

Next

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

- **Hold Support:** Select **RFC2543 - c=0.0.0.0**.
- **T.38 Support:** Checked.

Click **Next** to continue.

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

Back **Next**

Default values can be used for the next window that appears. Click **Next** to continue.

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
<input type="button" value="Back"/> <input type="button" value="Next"/>	



Default values can be used for the next window that appears. Click **Next** to continue.

Interworking Profile	
Configuration is not required. All fields are optional.	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
Transport Timers	
TCP Connection Inactive Timer	<input type="text"/> seconds, [600 - 3600]
<input type="button" value="Back"/> <input type="button" value="Next"/>	

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

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

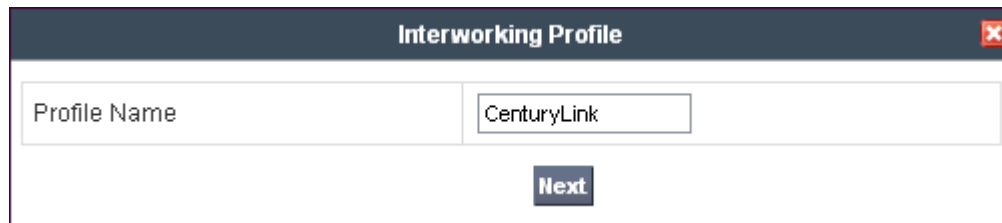
Click **Finish** to save changes.

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

Back **Finish**

6.1.3.2 Server Interworking Profile – CenturyLink

To create a new Server Interworking Profile for CenturyLink, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown in the previous section. Enter a descriptive name for the new profile and click **Next** to continue.

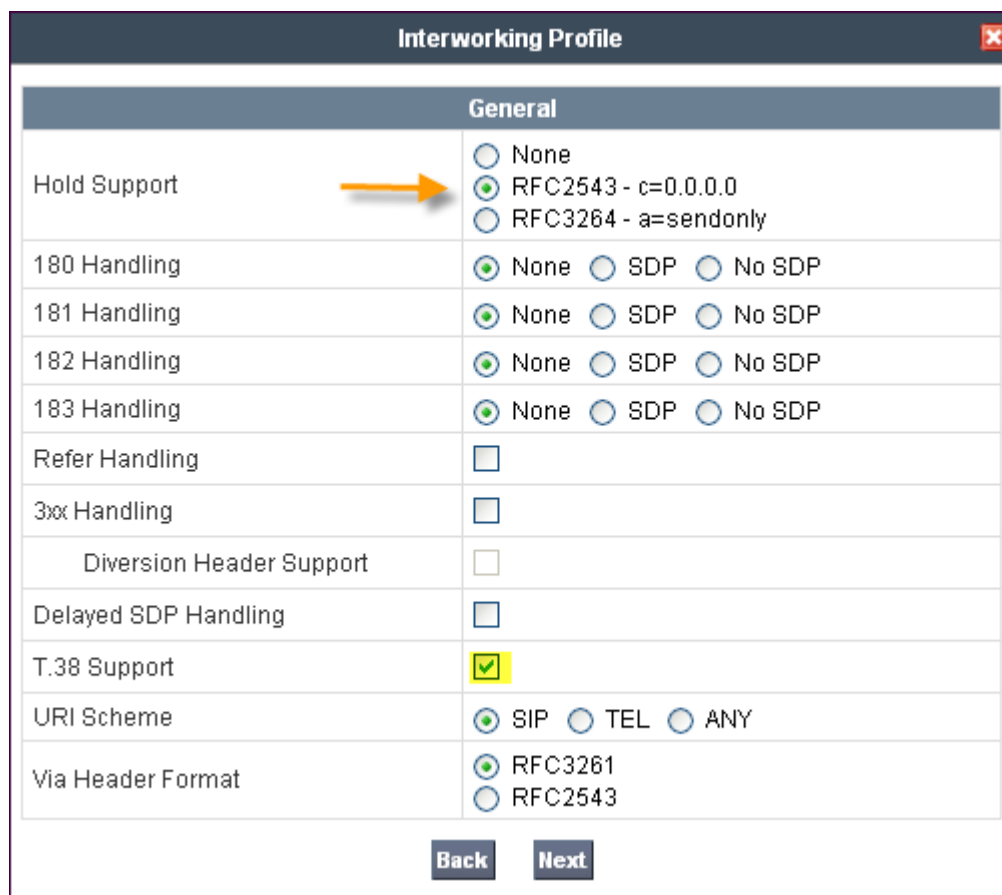


The screenshot shows a dialog box titled "Interworking Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "CenturyLink". Below the input field is a button labeled "Next".

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

- **Hold Support:** Select **RFC2543 - c=0.0.0.0**.
- **T.38 Support:** Checked.

Click **Next** to continue.



The screenshot shows a configuration window titled "Interworking Profile" with a close button (X) in the top right corner. The window contains a table with the following settings:

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

At the bottom of the window are two buttons: "Back" and "Next".

Default values can be used for the next window that appears. Click **Next** to continue.

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Default values can be used for the next window that appears. Click **Next** to continue.

Interworking Profile	
Configuration is not required. All fields are optional.	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
Transport Timers	
TCP Connection Inactive Timer	<input type="text"/> seconds, [600 - 3600]
<input type="button" value="Back"/> <input type="button" value="Next"/>	

On the **Advanced Settings** the default values can be used. Click **Finish** to save changes.

Interworking Profile

Advanced Settings

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

Back

Finish

6.1.4. Signaling Manipulation

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

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

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding, add a Diversion header, remove unwanted headers and convert the multipart Content-Type to a standard Session Description Protocol (SDP) in the message body.

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script**. A new blank SigMa Editor window will open.

The following sample script is written in two sections. The first section will act on the response of an inbound call from CenturyLink (e.g., 180 Ringing and 200 OK) while the second acts on the request of an outbound call to CenturyLink. The script is further broken down as follows:

- **within session “ALL”** Transformations applied to all SIP sessions.
- **act on response** Actions to be taken to the response of an INVITE (e.g., 180 Ringing and 200 OK).
- **%DIRECTION=“INBOUND”** Applied to a messages arriving to Avaya SBCE.
- **%ENTRY_POINT=“PRE_ROUTING”** The “hook point” to apply the script before the SIP message has routed through Avaya SBCE.
- **%HEADERS[“p-asserted-identity”][1]** Used to retrieve an entire header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message.
- **.regex_replace (“avayalab\.com”, “255.xxx.xxx.92:5060”)** An action to replace a given match with the provide string (e.g., find “avayalab.com” and replace it with the external interface).

The P-Asserted-Identity header will be modified by replacing the domain “avayalab.com” with the external IP address of Avaya SBCE and the SIP port of 5060 in both the response and request sessions. The request sessions are also modified by removing unwanted headers, unwanted

MIMEs in the body of the message and adding a Diversion header. During a call forward off-net over a SIP trunk, CS1000E sends the original calling party number in the FROM header and the called party number in the History-Info header. If the number in the FROM header is not one that is assigned to the SIP trunk, they require a Diversion header to have a number that is assigned and ignores the History-Info header.



The screenshot shows the Sigma Editor window with a title bar 'Sigma Editor'. Below the title bar is a section labeled 'Options' containing a 'Title' field with the text 'CS1K_Script' and a 'Save' button. The main area of the editor contains a script with line numbers 1 through 30. The script is a configuration for a SIP trunk, specifically for topology hiding and header manipulation. It includes comments and actions for inbound requests and responses, such as replacing the 'p-asserted-identity' header and creating a 'Diversion' header.

```
1 // Topology Hiding of PAI header within 180 Ringing response
2
3 within session "ALL"
4 {
5   act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6   {
7     %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com", "205.168.62.92:5060");
8   }
9 }
10 /* Topology Hiding of PAI header for subsequent re-INVITES; Create a Diversion header to allow call-fwd; Remove unwanted
11    headers and convert the SIP content from multipart/mixed to SDP */
12 within session "ALL"
13 {
14   act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
15   {
16     // Topology Hiding
17
18     %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com", "205.168.62.92:5060");
19
20     //Create a Diversion Header
21
22     %HEADERS["Diversion"][1] = "<sip:3036157104@205.168.62.92:5060>";
23
24     // Remove unwanted Headers
25
26     remove(%HEADERS["Alert-Info"][1]);
27     remove(%HEADERS["X-nt-e164-clid"][1]);
28
29     // Remove unwanted mimes from the body.
30
```


The following screen shows the finished Signaling Manipulation Script **CS1K_Script**. The script will later be added to the Server Configuration for the CS1000E in **Section 6.1.5.1**. The details of these script elements can be found in **Appendix A**.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with categories like Administration, System Management, Global Profiles, and Signaling Manipulation. The main content area is titled 'Global Profiles > Signaling Manipulation: CS1K_Script'. It features a 'Signaling Manipulation Scripts' list on the left with 'CM_Script' and 'CS1K_Script' (highlighted). The right pane shows the script content for 'CS1K_Script', which includes comments and SIP manipulation commands. At the top right of the script editor are buttons for 'Download Script', 'Clone Script', and 'Delete Script'. At the bottom right is an 'Edit' button.

```
// Topology Hiding of PAI header within 180 Ringing response
within session "ALL"
{
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.xxx.xxx.92:5060");
  }
}
/* Topology Hiding of PAI header for subsequent re-INVITES; Create a Diversion header to allow call-fwd; Remove
unwanted headers and convert the SIP content from multipart/mixed to SDP */
within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    // Topology Hiding

    %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.xxx.xxx.92:5060");

    //Create a Diversion Header

    %HEADERS["Diversion"][1] = "<sip:30355571048205.xxx.xxx.92:5060>";

    // Remove unwanted Headers

    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["X-nt-el64-clid"][1]);

    // Remove unwanted mimes from the body.

    // The SBC will not remove the SDP MIME, so "X-nt-mcdn-frag-hex" = %BODY[1]
    // After "X-nt-mcdn-frag-hex" is removed, "X-nt-esn5-frag-hex" moves up one...
    // So the same command removes "X-nt-epid-frag-hex".

    remove(%BODY[1]);
    remove(%BODY[1]);
    remove(%BODY[1]);
  }
}
```

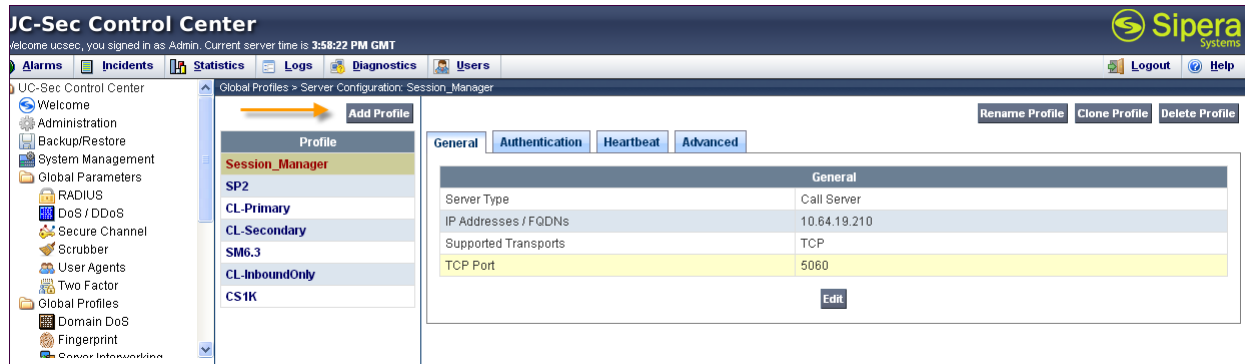
6.1.5. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

In the sample configuration, separate Server Configurations were created for CS1000E and CenturyLink.

6.1.5.1 Server Configuration – CS1000E

To add a Server Configuration Profile for CS1000E, navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** as shown below.



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

The screenshot shows a dialog box titled 'Add Server Configuration Profile'. It contains a text input field for 'Profile Name' with the value 'CS1K' entered. Below the input field is a 'Next' button.

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

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the NRS (see **Section 5.10**).
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Endpoint on the NRS in **Section 5.10.3**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Endpoint on the NRS in **Section 5.10.3**.

Click **Next** to continue.

Add Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma separated list	10.80.140.102
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
<div>Back Next</div>	

Verify **Enable Authentication** is unchecked as the CS1000E does not require authentication. Click **Next** to continue.

Add Server Configuration Profile - Authentication

Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Back **Next**

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

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS to the CS1000E. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds

Back Next

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 6.1.3.1**. Select the **Signaling Manipulation Script** created in **Section 6.1.4**. Use default values for all remaining fields. Click **Finish** to save the configuration.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CS1K <input type="button" value="v"/>
Signaling Manipulation Script	CS1K_Script <input type="button" value="v"/>
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

At the bottom of the dialog are two buttons: "Back" and "Finish".

6.1.5.2 Server Configuration - CenturyLink

For compliance testing CenturyLink had four SIP servers 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. Separate Server Configuration Profiles were created for the Primary and Secondary inbound and outbound IP addresses. A third Server Configuration Profile was created for the inbound only IP addresses.

To add Server Configuration Profiles for CenturyLink, navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** (not shown). Enter a descriptive name for the new profile and click **Next**.

The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. The dialog contains the following field and control:

Profile Name	CL-Primary
--------------	------------

At the bottom of the dialog is a button labeled "Next".

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

- **Server Type:** Select **Trunk Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of the SIP proxy of the service provider. In the sample configuration, this is 192.168.33.8 for the Primary server and 192.168.32.8 for the Secondary server. This will associate the inbound SIP messages from CenturyLink's SIP server to this Sever Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and CenturyLink. For compliance testing **UDP** was used.
- **UDP Port:** Enter the port number that CenturyLink uses to send SIP traffic. For compliance testing **5060** was used.

Click **Next** to continue.

The screenshot shows a window titled "Add Server Configuration Profile - General". It contains the following fields and options:

Server Type	Trunk Server (dropdown)
IP Addresses / Supported FQDNs <small>Comma seperated list</small>	192.168.33.8
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	(disabled text box)
UDP Port	5060
TLS Port	(disabled text box)

At the bottom of the window are two buttons: "Back" and "Next".

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

Add Server Configuration Profile - Authentication

Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Back **Next**

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

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

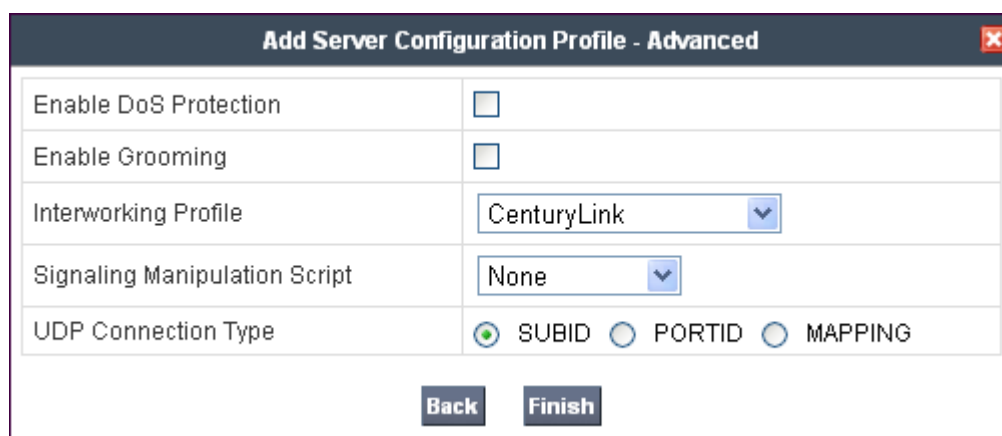
Click **Next** to continue.

The SIP OPTIONS are sent to the SIP servers entered in the **IP Addresses /Supported FQDNs** in the **Server Configuration Profile** as show previously. The URI of PING@centurylink.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. CenturyLink does not look at the From and To headers when replying to SIP OPTIONS so any URI can be used as long as it is in the proper format (USER@DOMAIN).

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	PING@centurylink.com
To URI	PING@centurylink.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds

Back Next

In the new window that appears, select the **Interworking Profile** created for CenturyLink in **Section 6.1.3.2**. Use default values for all remaining fields. Click **Finish** to save the configuration.



Add Server Configuration Profile - Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CenturyLink
Signaling Manipulation Script	None
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Back **Finish**

Once configuration is completed, the **CL-Primary** server configuration profile will appear as follows.



UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 2:50:33 PM GMT

Global Profiles > Server Configuration: CL-Primary

Profile

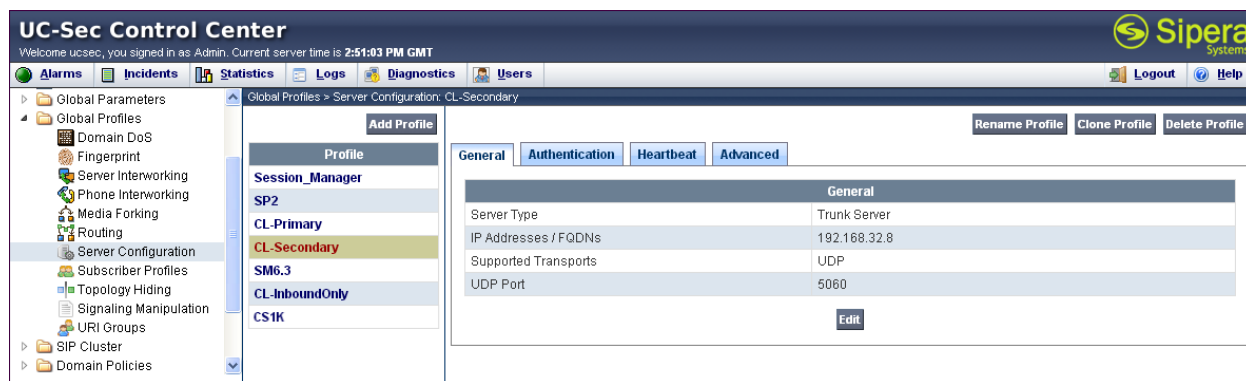
Session_Manager
SP2
CL-Primary
CL-Secondary
SM6.3
CL-InboundOnly
CS1K

General **Authentication** **Heartbeat** **Advanced**

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.33.8
Supported Transports	UDP
UDP Port	5060

Edit

Repeat these procedures to create a separate server configuration for the secondary IP address for CenturyLink. Once configuration is completed, the **CL-Secondary** server configuration profile will appear as follows.



UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 2:51:03 PM GMT

Global Profiles > Server Configuration: CL-Secondary

Profile

Session_Manager
SP2
CL-Primary
CL-Secondary
SM6.3
CL-InboundOnly
CS1K

General **Authentication** **Heartbeat** **Advanced**

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.32.8
Supported Transports	UDP
UDP Port	5060

Edit

The inbound only IP addresses can be placed into one server configuration profile with the Heartbeat disabled as shown below.

The image displays two screenshots of the UC-Sec Control Center web interface, showing the configuration of a server profile.

Top Screenshot: The 'General' tab is selected. The profile is named 'CL-InboundOnly'. The configuration shows:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.33.9, 192.168.32.9
Supported Transports	UDP
UDP Port	5060

Bottom Screenshot: The 'Heartbeat' tab is selected. The configuration shows:

Heartbeat	
Enable Heartbeat	<input type="checkbox"/>
TCP Probe	<input type="checkbox"/>

6.2. Domain Policies

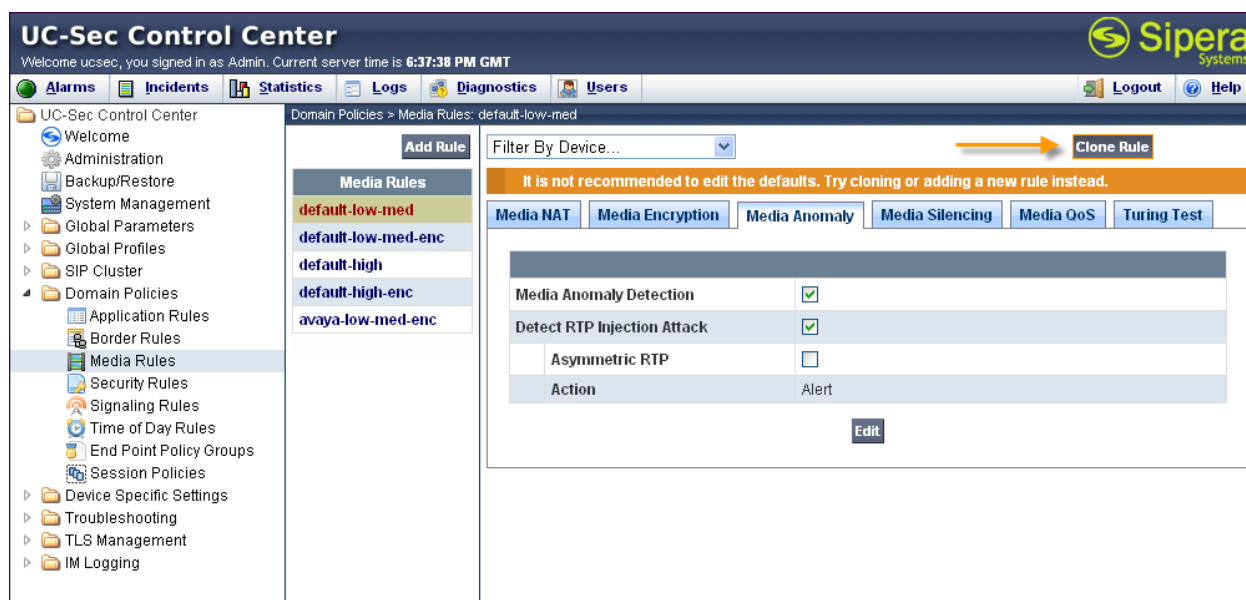
The Domain Policies feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control, and normalize call flows. There are default policies available to use, or a custom domain policy can be created.

6.2.1. Media Rule

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

Create a custom Media Rule to set the Quality of Service and Media Anomaly Detection. The sample configuration shows a custom Media Rule **New-Low-Med** was created for CenturyLink and the enterprise.

To create a custom Media Rule, navigate to **UC-Sec Control Center** → **Domain Policies** → **Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.



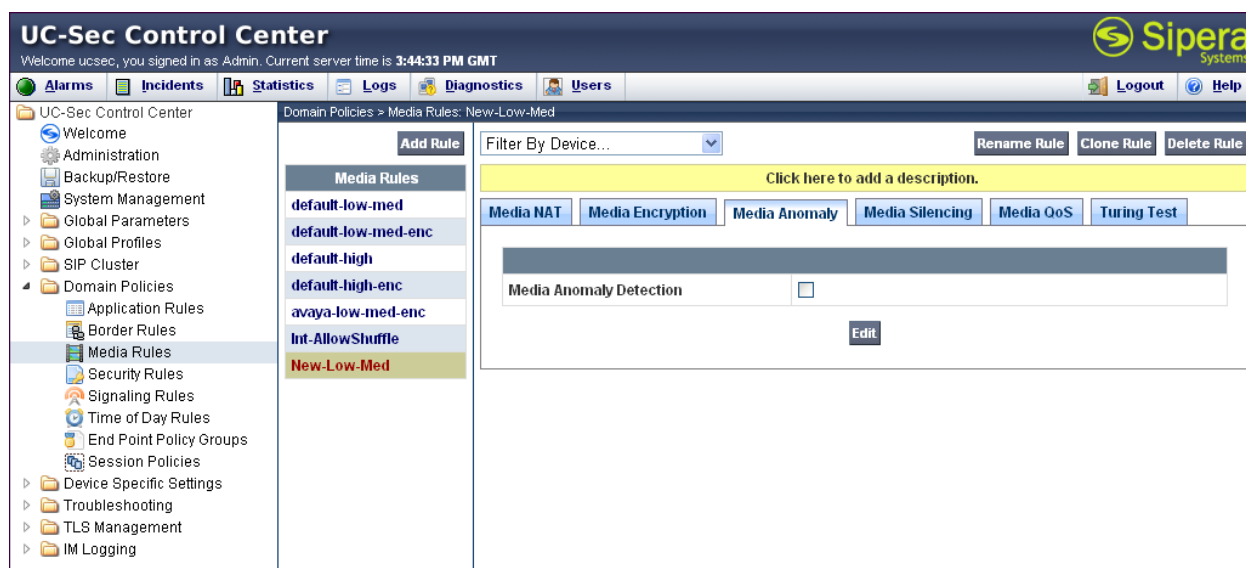
Enter a descriptive name for the new rule and click **Finish**.

Clone Rule

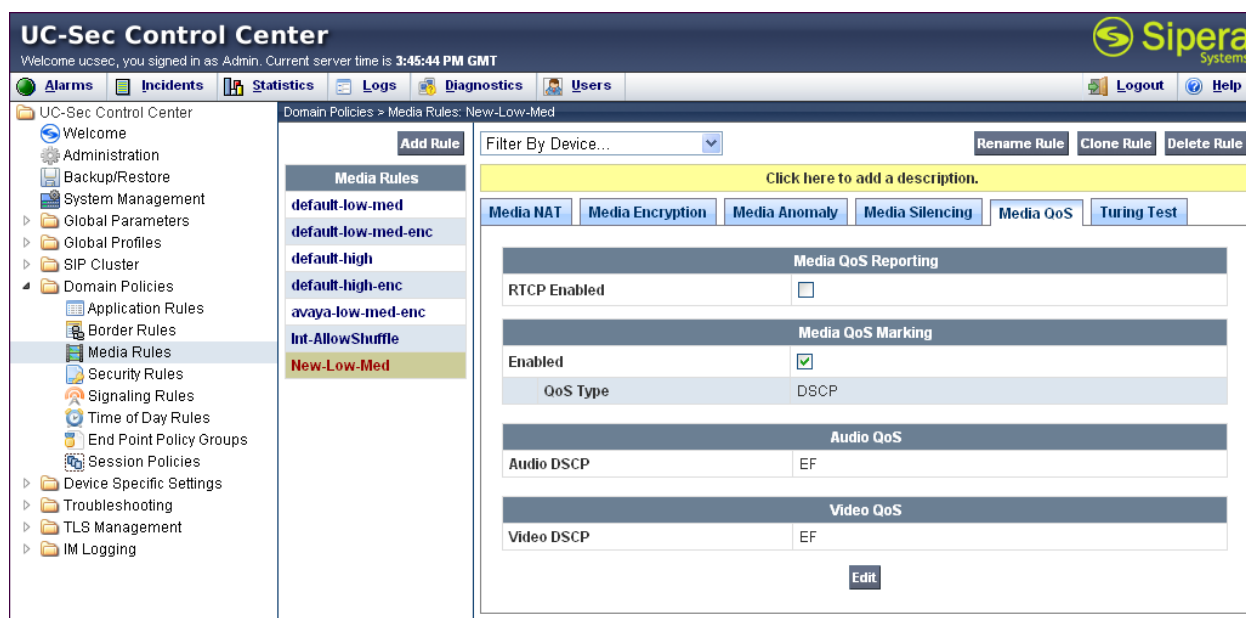
Rule Name	default-low-med
Clone Name	<input style="width: 80%;" type="text" value="New-Low-Med"/>

When the RTP packets of a call are shuffled from one IP endpoint to another within the CS1000E, Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created during an audio shuffle. To modify the rule, select the **Media Anomaly** tab and click **Edit**. Uncheck **Media Anomaly Detection** and click **Finish** (not shown).

The following screen shows the **New-Low-Med** rule with **Media Anomaly Detection** disabled.



On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for the media. The following screen shows the QoS values used for compliance testing.

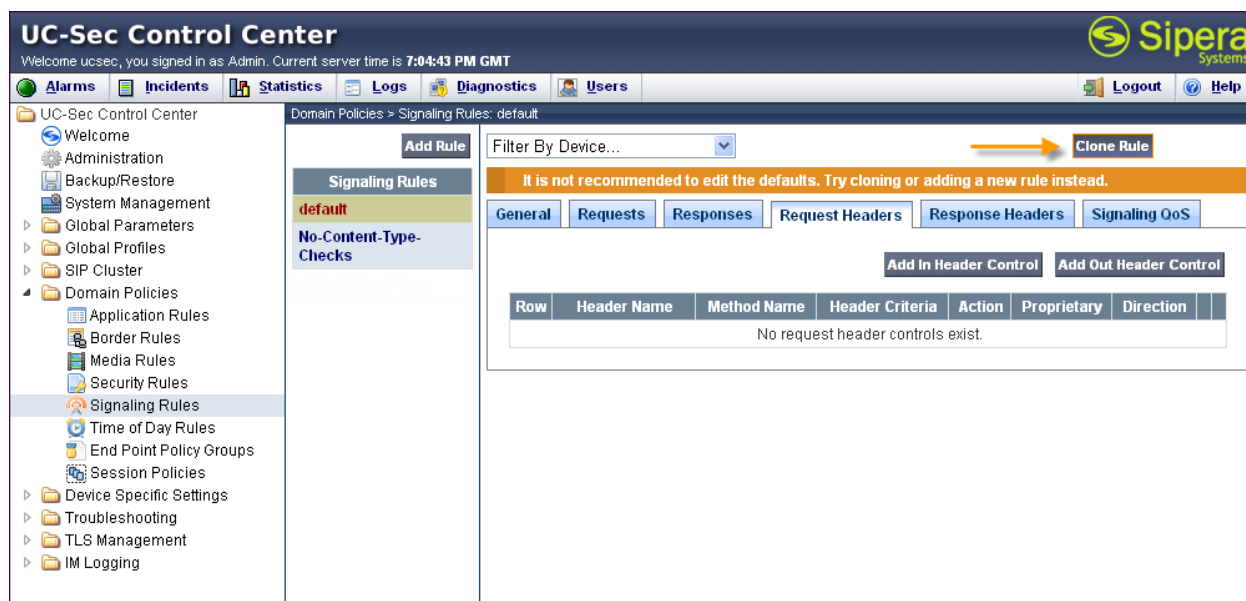


6.2.2. Signaling Rule

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

criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the default signaling rule to add the proper quality of service to the SIP message. To clone a signaling rule, navigate to **UC-Sec Control Center** → **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



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

The 'Clone Rule' dialog box is shown. It has two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'Avaya'. A 'Finish' button is located at the bottom right of the dialog.

On the **Signaling QoS** tab select the proper Quality of Service (QoS). The Sipera E-SBC can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for signaling. The following screen shows the QoS values used for compliance testing.

The screenshot displays the UC-Sec Control Center web interface. The top navigation bar includes tabs for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar shows a tree view of the system configuration, with 'Domain Policies' expanded and 'Signaling Rules' selected. The main content area shows the configuration for the 'Avaya' signaling rule. The 'Signaling QoS' tab is active, displaying a table with the following data:

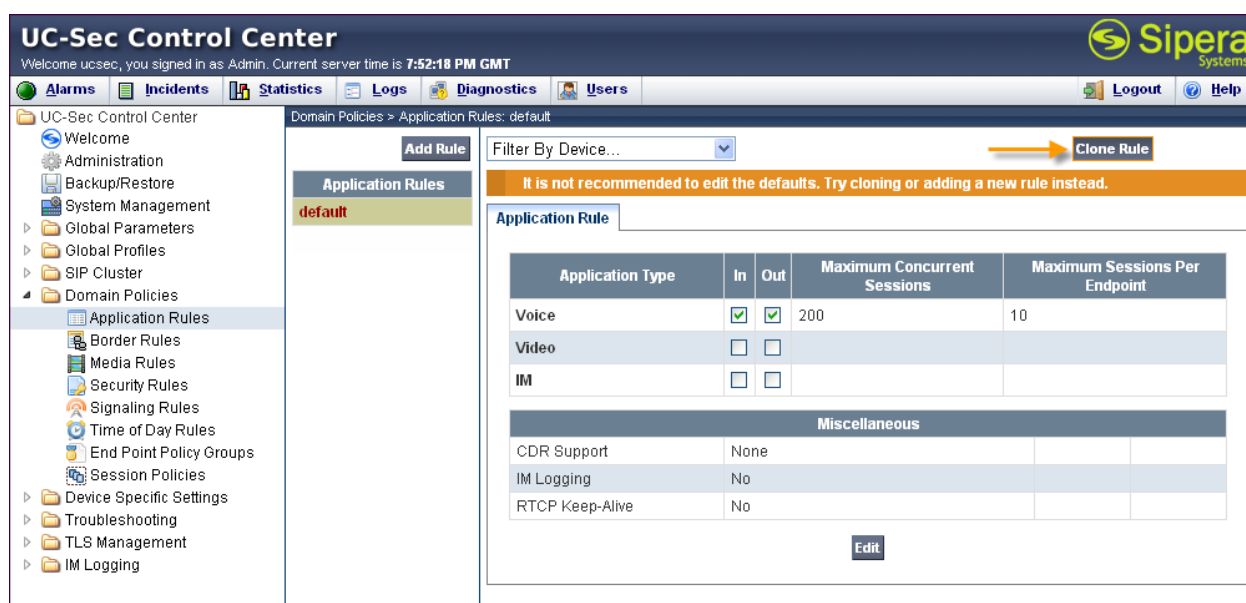
Signaling QoS	QoS Type	DSCP
<input checked="" type="checkbox"/>	DSCP	EF

An 'Edit' button is located below the table. The interface also includes a 'Filter By Device...' dropdown and buttons for 'Add Rule', 'Rename Rule', 'Clone Rule', and 'Delete Rule'.

6.2.3. Application Rule

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

Create an Application Rule to increase the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**. To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	10
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous			
CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

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

Clone Rule

Rule Name	default
Clone Name	<input type="text" value="MaxVoiceSession"/>

Finish

Edit the rule by clicking the **Edit** button as shown above. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. Set the values high enough for the amount of traffic the network is able process. Keep in mind Avaya SBCE takes 30 seconds for sessions to be cleared after disconnect.

The screenshot displays the UC-Sec Control Center web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar shows a tree view of the system configuration, with 'Domain Policies' expanded to show 'Application Rules'. The main content area is titled 'Domain Policies > Application Rules: MaxVoiceSession'. It features a 'Filter By Device...' dropdown, buttons for 'Add Rule', 'Rename Rule', 'Clone Rule', and 'Delete Rule', and a yellow box with the text 'Click here to add a description.' Below this is a table for 'Application Rule' configuration.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous			
CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

An 'Edit' button is located at the bottom right of the configuration area.

6.2.4. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 6.3.4**. Create a separate Endpoint Policy Group for the enterprise and the CenturyLink SIP Trunk.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** as shown below.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Domain Policies' expanded, and 'End Point Policy Groups' selected. The main area shows the 'Add Group' button. Below it, a table lists existing policy groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, and avaya-def-low-enc. A 'Filter By Device...' dropdown is visible at the top right of the main area.

The following screen shows **Enterprise_DomPolicy** created for the enterprise. Set the **Application**, **Media**, and **Signaling** rules to the ones previously created. Set the **Border**, **Security** and **Time of Day** rules to **default** or **default-low**.

The screenshot shows the UC-Sec Control Center interface with 'Enterprise_DomPolicy' selected in the 'End Point Policy Groups' list. The main area displays the configuration for this group. A table lists the rules assigned to the group: Order 1, Application MaxVoiceSession, Border default, Media New-Low-Med, Security default-low, Signaling Avaya, and Time of Day default. The 'Add Policy Set' button is visible at the top right of the main area.

The following screen shows **CL_DomPolicy** created for CenturyLink SIP Trunk. Set the **Application**, **Media**, and **Signaling** rules to the one previously created. Set the **Border**, **Security**, and **Time of Day** rules to **default** or **default-high**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a navigation tree with categories like Administration, System Management, Global Parameters, SIP Cluster, Domain Policies, and End Point Policy Groups. The main area displays the configuration for 'CL_DomPolicy' under 'Domain Policies > End Point Policy Groups'. It includes a 'Filter By Device...' dropdown, buttons for 'Add Group', 'Rename Group', and 'Delete Group', and a table of policy rules.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	MaxVoiceSession	default	default-high	default-high	Avaya	default	

6.3. Device Specific Settings

The Device Specific Settings feature allows aggregate system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

6.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 4:12:09 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
SNMP
End Point Flows
Session Flows
Two Factor
Relay Services
Troubleshooting
TLS Management

Device Specific Settings > Network Management: ASBCE

UC-Sec Devices
ASBCE

Network Configuration **Interface Configuration**

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

A1 Netmask: 255.255.255.0 A2 Netmask: 255.255.255.128 B1 Netmask: 255.255.255.128 B2 Netmask: 255.255.255.128

Add IP Changes will not take effect until the interface is updated. Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface	
10.80.150.100		10.80.150.1	A1	X
205.xxx.xxx.92		205.xxx.xxx.1	B1	X

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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 4:13:26 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
SNMP
End Point Flows
Session Flows
Two Factor
Relay Services
Troubleshooting
TLS Management

Device Specific Settings > Network Management: ASBCE

UC-Sec Devices
ASBCE

Network Configuration **Interface Configuration**

Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

6.3.2. Media Interface

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

To create a new Signaling Interface, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface**.

The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces..

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Media Interface' selected under 'Device Specific Settings'. The main content area is titled 'Media Interface' and contains a table of configured interfaces. A warning message at the top states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add Media Interface' button is located above the table.

Name	Media IP	Port Range		
Media_Inside	10.80.150.100	2048 - 3329		
Media_Outside	205.150.150.92	8000 - 8999		

After the media interfaces are created, an application restart is necessary before the changes will take effect. Navigate to **UC-Sec Control Center → System Management** and click the forth icon from the right to restart the applications as highlighted below.

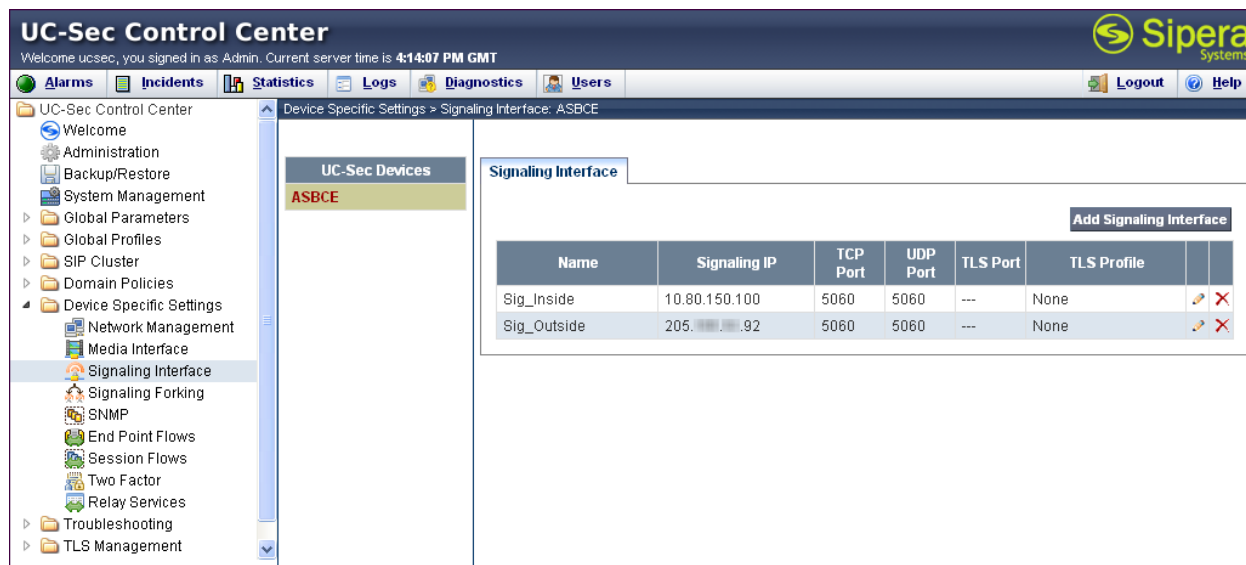
The screenshot shows the UC-Sec Control Center interface with 'System Management' selected in the sidebar. The main content area shows a table of installed applications. A red circle highlights the fourth icon from the right in the table's action column, which represents the restart function.

Device Name	Serial Number	Version	Status						
ASBCE	IPCS31020130	4.0.5.Q09	Commissioned						

6.3.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **UC-Sec Control Center** → **Device Specific Settings** → **Signaling Interface** and click **Add Signaling Interface**.

The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

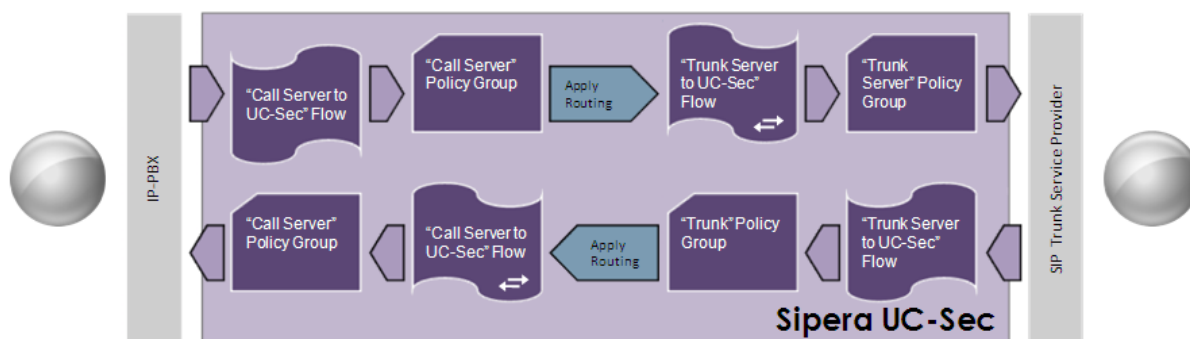


The screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a tree view with the following items: UC-Sec Control Center, Welcome, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, Device Specific Settings (selected), Network Management, Media Interface, Signaling Interface (selected), Signaling Forking, SNMP, End Point Flows, Session Flows, Two Factor, Relay Services, Troubleshooting, and TLS Management. The main content area is titled "Device Specific Settings > Signaling Interface: ASBCE". It features a "Signaling Interface" tab and an "Add Signaling Interface" button. Below the button is a table with the following data:

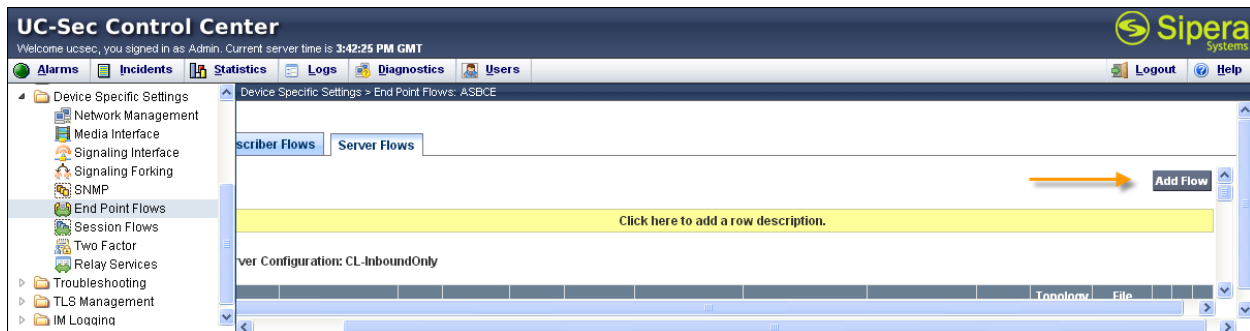
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Sig_Inside	10.80.150.100	5060	5060	---	None		
Sig_Outside	205.192.192.92	5060	5060	---	None		

6.3.4. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Sipera E-SBC to secure a SIP Trunk call.



Create a Server Flow for CS1000E and the CenturyLink SIP Trunk. To create a Server Flow, navigate to **UC-Sec Control Center** → **Device Specific Settings** → **End Point Flows**. Select the **Server Flows** tab and click **Add Flow** as shown in below.



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

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 6.1.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

Click **Finish** to save and exit.

The following screen shows the Server Flow for CL-Primary:

Criteria	
Flow Name	CL-Primary-Flow
Server Configuration	CL-Primary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside
Media Interface	Media_Outside
End Point Policy Group	CL_DomPolicy
Routing Profile	Route_to_CS1K
Topology Hiding Profile	CenturyLink
File Transfer Profile	None
Finish	

The following screen shows the Server Flow for CL-Secondary:

Criteria	
Flow Name	CL-Secondary-Flow
Server Configuration	CL-Secondary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside
Media Interface	Media_Outside
End Point Policy Group	CL_DomPolicy
Routing Profile	Route_to_CS1K
Topology Hiding Profile	CenturyLink
File Transfer Profile	None
Finish	

The following screen shows the Server Flow for CL-InboundOnly-Flow:

Criteria	
Flow Name	CL-InboundOnly-Flow
Server Configuration	CL-InboundOnly
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside
Media Interface	Media_Outside
End Point Policy Group	CL_DomPolicy
Routing Profile	Route_to_CS1K
Topology Hiding Profile	CenturyLink
File Transfer Profile	None
Finish	

The following screen shows the Sever Flow for CS1000E:

Criteria	
Flow Name	CS1K_Flow
Server Configuration	CS1K
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside
Signaling Interface	Sig_Inside
Media Interface	Media_Inside
End Point Policy Group	Enterprise_DomPolicy
Routing Profile	Route_to_CL_Outbound
Topology Hiding Profile	Enterprise
File Transfer Profile	None
Finish	

7. CenturyLink SIP Trunk Configuration

To use CenturyLink SIP Trunk, 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 and requesting information via the online sales links or telephone numbers.

8. Verification Steps

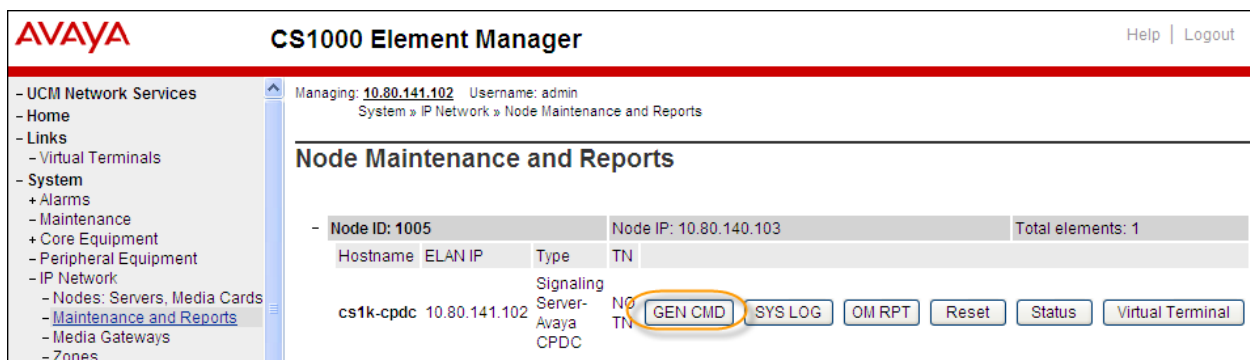
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

8.1. Avaya Communication Server 1000E Verifications

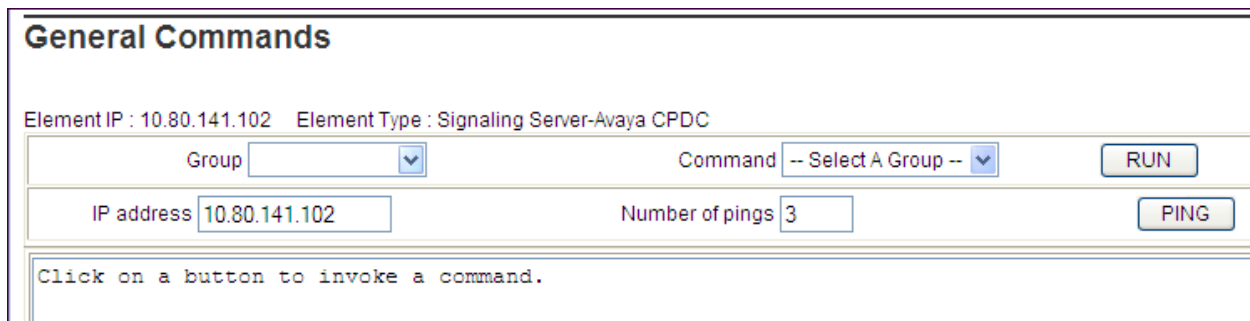
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

8.1.1. 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 the NRS in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click Run. The example output below shows that the NRS (10.80.140.102, 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 : 10.80.140.102
Primary   Proxy port       : 5060
Primary   Proxy Transport  : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port       : 5060
Secondary Proxy Transport  : TCP
Primary Proxy2 IP address  : 10.80.140.102
Primary Proxy2 port       : 5060
Primary Proxy2 Transport  : TCP
Active    Proxy           : Primary :Registered

```

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 UNISlim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**. At the time this screen was captured, the UNISlim 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

8.1.2. 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) ▼		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO) ▼	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO) ▼	<input type="checkbox"/> FDL	<input type="button" value="Submit"/>
Test Interrupt Generation (TEST 100) ▼		<input type="button" value="Submit"/>
Establish D-Channel (EST DCH) ▼		<input type="button" value="Submit"/>

DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
-----	-----	-------------	-------------	-----------	------	------

☐ 015 VtrkNode1005 OPER
 EST ACTV
 AUTO

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

8.1.3. Network Routing Service Routing Verification

Verify the Signaling Server has successfully registered with the Network Routing Server. From the **Network Routing Server Manager**, navigate to **Numbering Plans → Endpoints**. Click on the radio button of the **Active** database. On the **Gateway Endpoints** tab, verify the IP address of the Signaling Server node is in the **Call Signaling IP** column as shown below.

The screenshot displays the Avaya Network Routing Service Manager interface. On the left is a navigation menu with options like «UCM Network Services», System, NRS Server, Database, System Wide Settings, Numbering Plans, Domains, Endpoints, Routes, Network Post-Translation, Collaborative Servers, Tools, SIP Phone Context, Routing Tests, H.323, SIP, Backup, Restore, and GKNRS Data upgrade. The main area shows the 'Managing:' section with 'Active database' selected (indicated by an orange arrow) and 'Standby database' unselected. The IP address 10.80.141.102 is shown. Below this is the 'Search for Endpoints' section with a search bar and filters. The 'Gateway Endpoints (2)' tab is active, showing a table of endpoints. The 'Call Signaling IP' for the endpoint 'node1005' is highlighted with an orange circle.

ID	Supported Protocols	SIP mode	Call Signaling IP	Description	# of Routing Entries	Context
1 ASBCE	Static SIP endpoint	Proxy Mode	10.64.19.100	Avaya Session Border Controller for Enterprise	6	avayalab.com / udp / cdp
2 node1005	Dynamic SIP endpoint	Proxy Mode	10.80.140.103		3	avayalab.com / udp / cdp

Verify the call routing administration on the NRS by executing the Routing Tests. From the Network Routing Service Manager, navigate to **Tools → Routing Tests → SIP**. 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 **Possible Routes Found**, observe the call will route via Avaya SBCE to CenturyLink.

AVAYA

Network Routing Service Manager
[Help](#) | [Logout](#)

«UCM Network Services
 - System
 NRS Server
 Database
 System Wide Settings
 - Numbering Plans
 Domains
 Endpoints
 Routes
 Network Post-Translation
 Collaborative Servers
 - Tools
 SIP Phone Context
 - **Routing Tests**
 H.323
 SIP
 Backup
 Restore
 GK/NRS Data upgrade

Managing: ☒ Active database 10.80.141.102
 ☐ Standby database Tools » Routing Tests » SIP

SIP Routing Test

Service domain name: avayalab.com

L1 domain name: udp

L0 domain name: cdp

Originating endpoint IP address: 10.80.140.103 *

DN to query: 12135551234 *

DN type: E.164 National

Phone context to query (suggest): +1

★ Required value.

Possible Routes Found

#	Terminating endpoint address	Terminating SIP transport	Terminating SIP port	Routing type	Route cost
0	10.80.150.100	0	5060	REGULAR_ROUTE	1

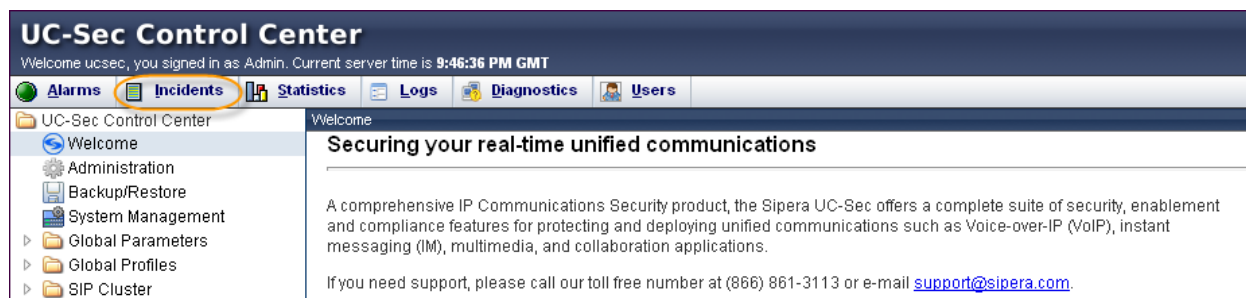
Copyright 2002-2012 Avaya Inc. All rights reserved.

8.2. Avaya Session Boarder Controller for Enterprise Verification

This section contains verification steps that may be performed using the Avaya Session Border Controller for Enterprise.

8.2.1. Incidents

The Incidents Log Viewer display alerts captured by the Avaya SBCE appliance. Select the **Incidents** link along the top of the screen.



The following screen shows an example SIP messages that do not match a Server Flow for an incoming message.

Incident Viewer

Device: Category:

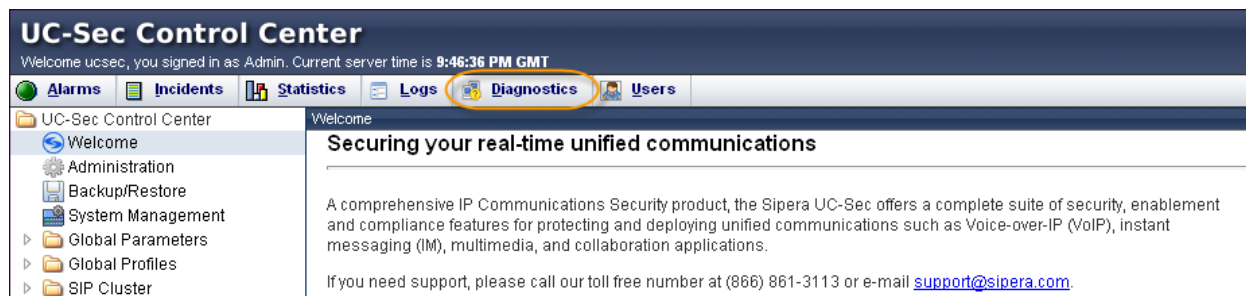
Displaying results 1 to 15 out of 102.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	662168149391824	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168147389246	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168146388212	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145887753	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145636658	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168142392101	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168140391726	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168138390782	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168136390456	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168134389013	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168132388591	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168131388258	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130886109	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130635815	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Server Heartbeat	662165350683634	12/19/11	9:38 PM	Policy	Sipera	Server Heartbeat is UP

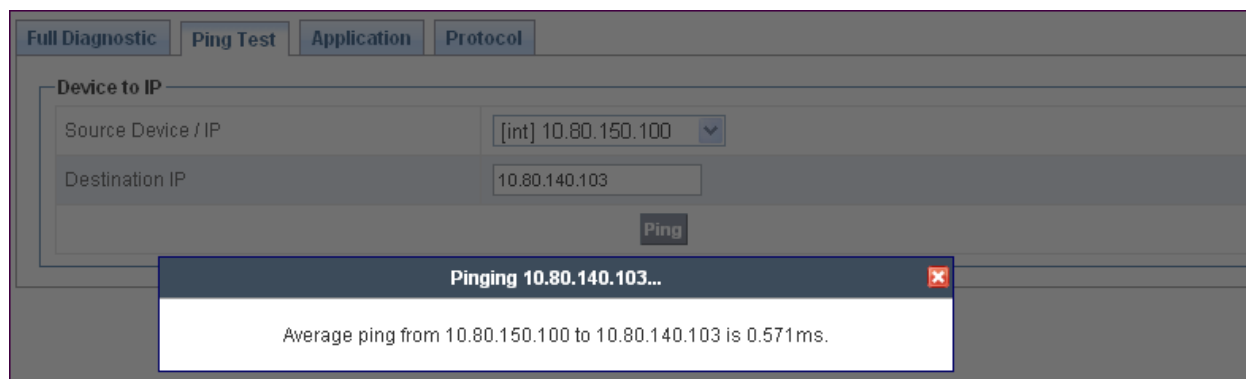
<< < 1 2 3 4 5 > >>

8.2.2. Diagnostics

The Diagnostics tool allows for PING tests and displays application and protocol use. Select the **Diagnostics** link along the top of the screen.



The following screen shows an example PING to the NRS server from the internal signaling interface of the Avaya SBCE.



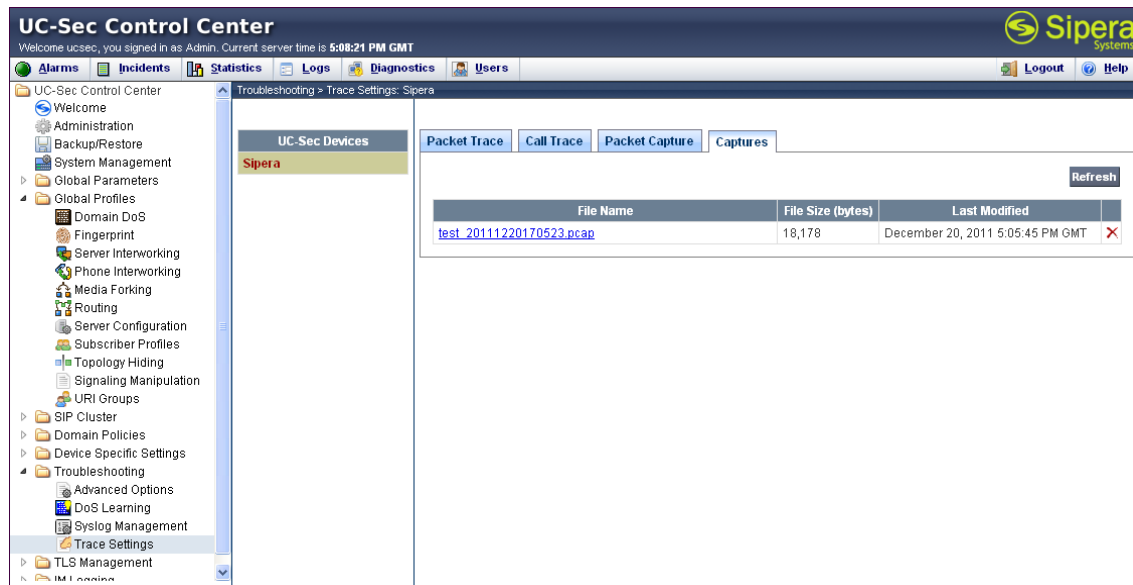
8.2.3. Trace Settings

The Trace Settings tool is for configuring and displaying call traces and packet captures for the Avaya SBCE. Navigate to **Troubleshooting → Trace Settings** as shown below. The following screen shows an example packet capture on interface **A1** with a **Maximum Number of Packets to Capture** set to **1200**. The **Capture Filename** **test.pcap** will be created once the **Start Capture** button is pressed.

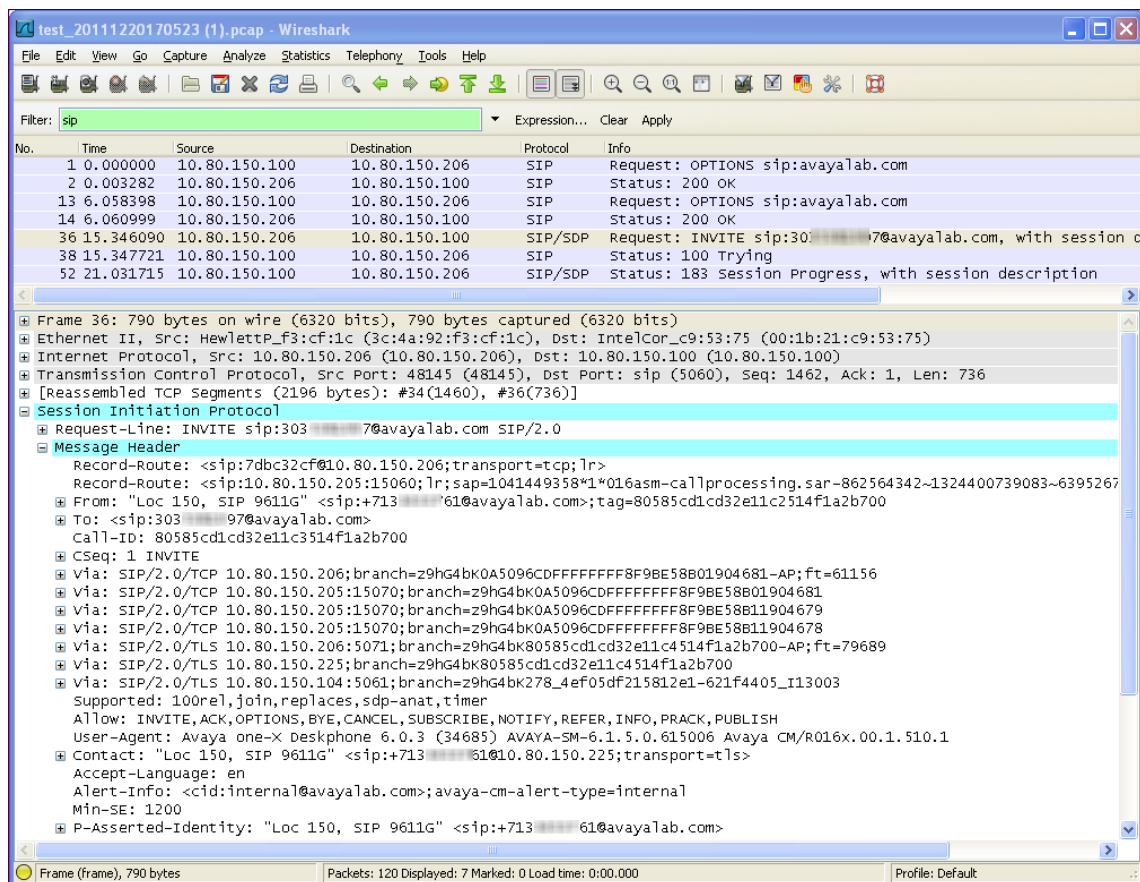
The screenshot displays the UC-Sec Control Center web interface. The top navigation bar includes tabs for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar shows a tree view of system components, with 'Troubleshooting' expanded and 'Trace Settings' selected. The main content area is titled 'Troubleshooting > Trace Settings: Sipera'. It features a 'Packet Capture Configuration' form with the following fields: 'Currently capturing' (No), 'Interface' (A1), 'Local Address (ip:port)' (All), 'Remote Address (*, *:port, ip, ip:port)' (*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (1200), and 'Capture Filename' (test.pcap). Below the form are 'Start Capture' and 'Clear' buttons.

Packet Capture Configuration	
Currently capturing	No
Interface	A1
Local Address (ip:port)	All
Remote Address (*, *:port, ip, ip:port)	*
Protocol	All
Maximum Number of Packets to Capture	1200
Capture Filename	test.pcap

The following screen shows a completed packet capture.



The packet capture file can be downloaded and viewed using a Network Protocol Analyzer like Wireshark:



9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya SBCE and Avaya Communication Server 1000E 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.

10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>. Avaya SBCE documentation is available at <http://www.sipera.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] *Network Routing Service Fundamentals Avaya Communication Server 1000*, Document Number NN43001-130, 03.10 September 2011
- [6] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315, 05.18 January 2012
- [7] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Document Number NN43170-600, Standard 04.02 December 2011
- [8] *UC-Sec Install Guide (102-5224-400v1.01)*
- [9] *UC-Sec Administration Guide (010-5423-400v106)*

Appendix A

Included below is the Sigma Script used during the compliance testing. The contents have been modified to mask the external IP address and the routable phone number of the Diversion header.

```
// Topology Hiding of PAI header within 180 Ringing response

within session "ALL"
{
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com", "205.xxx.xxx.92:5060");
  }
}

/* Topology Hiding of PAI header for subsequent re-INVITES; Create a Diversion header to allow
call-fwd; Remove unwanted headers and convert the SIP content from multipart/mixed to SDP */

within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    // Topology Hiding

    %HEADERS["p-asserted identity"][1].regex_replace("avayalab\.com", "205.xxx.xxx.92:5060");

    //Create a Diversion Header

    %HEADERS["Diversion"][1] = "<sip:3035557104@205.xxx.xxx.92:5060>";

    // Remove unwanted Headers

    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["X-nt-e164-clid"][1]);

    // Remove unwanted mimes from the body.

    // The SBC will not remove the SDP MIME, so "x-nt-mcdn-frag-hex" = %BODY[1]
    // After "x-nt-mcdn-frag-hex" is removed, "x-nt-esn5-frag-hex" moves up one...
    // So the same command removes "x-nt-epid-frag-hex".

    remove(%BODY[1]);
    remove(%BODY[1]);
    remove(%BODY[1]);
  }
}
```

©2013 Avaya Inc. All Rights Reserved.

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

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