



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

---

# **Application Notes for Configuring Cincinnati Bell eVantage IP Service with Avaya Communication Server 1000E 7.5, Avaya Aura® Session Manager 6.2, Avaya Session Border Controller for Enterprise 4.0.5 – Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cincinnati Bell eVantage IP Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E, Avaya Aura® Session Manager, Avaya Session Border Controller for Enterprise and various Avaya endpoints.

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

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results .....	5
2.3.	Support .....	6
3.	Reference Configuration .....	6
4.	Equipment and Software Validated .....	7
5.	Configure Avaya Communication Server 1000E .....	8
5.1.	Administer an IP Telephony Node.....	9
5.1.1.	Obtain Node IP Address .....	9
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 .....	19
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.	Route List Block .....	27
5.5.2.	NARS Access Code .....	29
5.5.3.	Numbering Plan Area Codes .....	30
5.5.4.	Special Numbers to Route to Session Manager.....	32
5.5.5.	Incoming Digit Translation.....	33
5.6.	Zones and Bandwidth.....	34
5.7.	Example CS1000E Telephone Users .....	36
5.7.1.	Example SIP Phone DN 7108, Codec Considerations.....	36
5.7.2.	Example Digital Phone DN 7107 with Call Waiting.....	37
5.7.3.	Example Analog Port with DN 7106, Fax .....	38
5.8.	Save Configuration.....	39
6.	Configure Avaya Aura® Session Manager .....	40
6.1.	Avaya Aura® System Manager Login and Navigation .....	40
6.2.	Specify SIP Domain .....	41
6.3.	Add Location.....	42
6.4.	Adaptations.....	45
6.5.	Add SIP Entities .....	48
6.6.	Add Entity Links .....	52
6.7.	Add Routing Policies .....	53
6.8.	Add Dial Patterns .....	54

6.9.	Add/Verify Avaya Aura® Session Manager Instance .....	57
7.	Configure Avaya Session Border Controller for Enterprise .....	59
7.1.	Network Management .....	62
7.2.	Routing Profile .....	63
7.3.	Topology Hiding Profile .....	65
7.4.	Server Interworking Profile.....	67
7.4.1.	Server Interworking Profile – Enterprise .....	67
7.4.2.	Server Interworking Profile – Cincinnati Bell .....	71
7.5.	Server Configuration .....	74
7.5.1.	Server Configuration – Session Manager .....	74
7.5.2.	Server Configuration - Cincinnati Bell .....	77
7.6.	Media Rule .....	81
7.7.	Signaling Rule .....	83
7.8.	Application Rule .....	85
7.9.	Endpoint Policy Group.....	86
7.10.	Media Interface .....	88
7.11.	Signaling Interface.....	89
7.12.	End Point Flows - Server Flow.....	89
8.	Cincinnati Bell eVantage IP Service Configuration .....	93
9.	Verification .....	93
9.1.	Avaya Communication Server 1000E Verification .....	93
9.1.1.	IP Network Maintenance and Reports Commands .....	93
9.1.2.	System Maintenance Commands.....	95
9.2.	Avaya Aura® Session Manager Verification.....	97
9.3.	Avaya Session Border Controller for Enterprise Verification .....	97
9.3.1.	Incidents .....	98
9.3.2.	Diagnostics.....	99
9.3.3.	Trace Settings.....	100
10.	Conclusion .....	102
11.	Additional References.....	102

# 1. Introduction

These Application Notes describe a sample configuration of Avaya Communication Server 1000E release 7.5 Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5 (Avaya SBCE) integration with Cincinnati Bell eVantage IP Service.

In the sample configuration, the Avaya Session Border Controller for Enterprise is used as an edge device between Avaya Customer Premise Equipment (CPE) and Cincinnati Bell eVantage IP Service. 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 Cincinnati Bell eVantage IP Service access method.

The Cincinnati Bell eVantage IP Service solution is a turn-key business trunking solution for customers. Cincinnati Bell eVantage IP Service provides customers with a single IP connection that converges voice and data services to drive optimization, reduce costs, and offer enhanced features not typically available in the traditional PSTN network. Voice services, such as local, long distance and toll free calling, as well as a high speed data and Internet services, are the primary applications of the Cincinnati Bell eVantage solution.

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

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya Communication Server 1000E (CS1000E), Session Manager, and Avaya SBCE to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to Cincinnati Bell eVantage IP 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 UNISTim, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider
- Outgoing PSTN calls from various phone types. Phone types included UNISTim, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client)
- Various call types including: local, long distance, and outbound toll-free
- Codecs G.729A, G.729B and G.711MU
- DTMF transmission using RFC 2833
- G711 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

Items not supported or not tested included the following:

- Inbound toll-free, operator, operator services (0 + 10 digits) and emergency calls (911) are supported but were not tested as part of the compliance test
- Calls forwarded off-net were not supported on the test circuit used for the compliance test, but Cincinnati Bell eVantage IP Service production environment does support these types of calls.
- SIP REFER method is not supported by Avaya CS1000E
- CS1000E Mobile-X features were not tested

## 2.2. Test Results

Interoperability testing of Cincinnati Bell eVantage IP Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

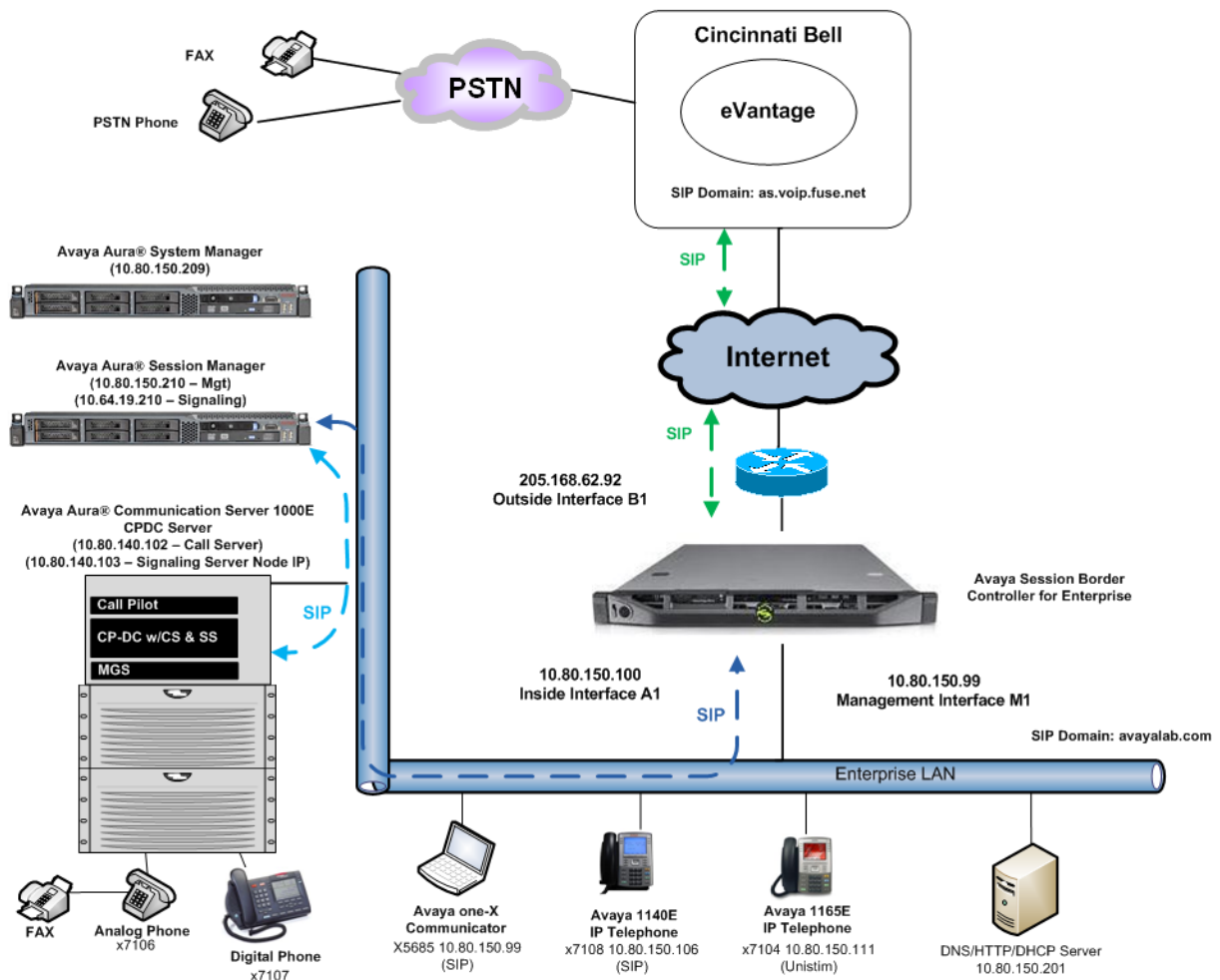
- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and 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/Cincinnati Bell eVantage IP Service solution. It is listed here simply as an observation.
- **T.38 Fax:** At the time of original publication of these Application Notes, Cincinnati Bell eVantage IP Service supported fax over T.38 within their local calling area only. Any fax calls placed outside of the Cincinnati Bell local calling area will be transferred using G.711 codec. The recommended workaround is to configure the CS1000E fax endpoints to use the G.711 codec for outbound calling. See **Section 5.7.3**

Cincinnati Bell eVantage IP Service passed compliance testing.

For technical support on the Cincinnati Bell eVantage IP Service, contact Cincinnati Bell using the Customer Care links at [www.CincinnatiBell.com](http://www.CincinnatiBell.com).

### 3. Reference Configuration

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



### Figure 1: Avaya Interoperability Test Lab Configuration

## 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Communication Server 1000E running on CP+DC server as co-resident configuration	<ul style="list-style-type: none"><li>• Call Server: 7.50 .17 GA (CoRes) Service Pack: 7.50.17_20120919</li><li>• SSG Server: 7.50.17 GA</li><li>• SLG Server: 7.50.17 GA</li></ul>
Communication Server 1000E Media Gateway	CSP Version: MGCC CD03 MSP Version: MGCM AB02 APP Version: MGCA BA15 FPGA Version: MGCF AA19 BOOT Version: MGCB BA15 DSP1 Version: DSP4 AB06 BCSP Version: MGCC CD01
Avaya Session Border Controller for Enterprise	4.0.5Q18
Avaya 1165E (UNISTim)	0626C8A
Avaya 1140E (SIP)	04.03.12.00
Avaya one-X Communicator (SIP)	CS6.1.1.02 SP1 36207
Avaya M3904 (Digital)	n/a
Avaya 6210 Analog Telephone	n/a
Cincinnati Bell eVantage IP Service Components	
Component	Release
BroadSoft	Version 17

**Table 1: Equipment and Software Tested**

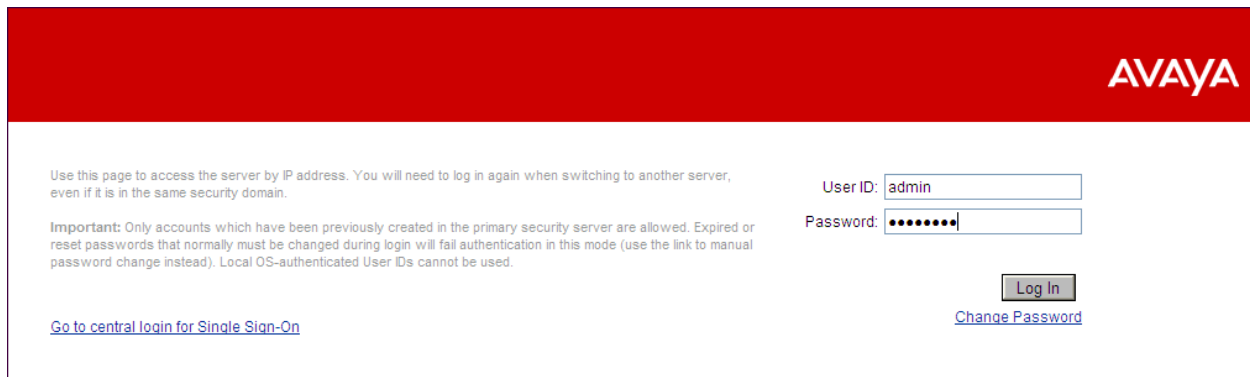
The specific configuration above was used for the compatibility testing.

## 5. Configure Avaya Communication Server 1000E

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

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

Configuration will be shown using the web based Avaya Unified Communications Management GUI. The Avaya Unified Communications Management GUI may be launched directly via <https://<ipaddress>> where the relevant <ipaddress> in the sample configuration is 10.80.140.102. The following screen shows an abridged log in screen. Log in with appropriate credentials.



The image shows a web-based login interface for the Avaya Unified Communications Management GUI. At the top right, the AVAYA logo is displayed in white on a red background. Below the logo, there is a login form with the following elements:

- 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."
- An "Important" note: "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."
- A link: "Go to central login for Single Sign-On"
- Input fields for "User ID:" (containing "admin") and "Password:" (masked with dots).
- A "Log In" button.
- A link: "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**.

Host Name: 10.80.140.102    Software Version: 02.20.0017.00(4713)    User Name admin

## Elements

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

<input type="checkbox"/>	Element Name	Element Type ^	Release	Address	Description
<input type="checkbox"/>	<b>EM on cs1k-cpdc</b>	CS1000	7.5	10.80.141.102	New element.
<input type="checkbox"/>	<a href="#">cs1k-cpdc.avaya.com (primary)</a>	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"/>	<a href="#">NRS on cs1k-cpdc</a>	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.

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

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

### IP Telephony Nodes

Click the Node ID to view or edit its properties.

<input type="checkbox"/>	Node ID ^	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/>	<a href="#">1005</a>	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.80.140.103		Synchronized

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

The **Node Details** screen is displayed with additional details as shown below. Under the **Node Details** heading at the top of the screen, make a note of the **TLAN Node IPV4 address**. In the sample screen below, the **Node IPV4 address** is **10.80.140.103**. This IP address will be needed when configuring Session Manager with a SIP Entity for the CS1000E in **Section 6.5**.

CS1000 Element Manager

Help | Logout

Managing: 10.80.141.102 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

Node ID: 1005 \* (0-9999)

Call server IP address: 10.80.141.102 \*

Embedded LAN (ELAN)  
Gateway IP address: 10.80.141.1 \*  
Subnet mask: 255.255.255.0 \*

TLAN address type: ☒ IPv4 only  
☐ IPv4 and IPv6

Telephony LAN (TLAN)  
Node IPv4 address: 10.80.140.103 \*  
Subnet mask: 255.255.255.0 \*

Node IPv6 address:

\* Required Value.

Save Cancel

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

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader

Print | Refresh

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

Show: ☐ IPv6 address

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

### 5.1.2. Terminal Proxy Server (TPS)

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

AVAYA CS1000 Element Manager

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value.      Save      Cancel

Check the **UNISim 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 » UNISim Line Terminal Proxy Server (LTPS) Configuration

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

Firmware | DTLS | Network Connect Server

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

Firmware

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

DTLS

DTLS policy: Off

### 5.1.3. Quality of Service (QoS)

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

AVAYA CS1000 Element Manager

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value. Save Cancel

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

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

Node ID: 1005 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☐

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

VLAN tagging: ☐ 802.1Q support

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

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

### 5.1.4. Voice Gateway and Codecs

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

AVAYA CS1000 Element Manager

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value.

Save Cancel

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

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

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

General | Voice 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.

**Voice Codecs**

Codec G.711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

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

**General | Voice Codecs | Fax**

Codec G.729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

### 5.1.5. SIP Gateway

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

**AVAYA CS1000 Element Manager**

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

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

Subnet mask: 255.255.255.0 \* Subnet mask: 255.255.255.0 \*

Node IPv6 address:

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

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

\* Required Value.

Save Cancel

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

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

The values defined for the sample configuration are shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header shows the AVAYA logo and the title "CS1000 Element Manager". Below the header, a navigation tree on the left lists various system components like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes, Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Software, Customers, Routes and Trunks, Routes and Trunks, D-Channels, Digital Trunk Interface, 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". The configuration is divided into two tabs: "General" and "SIP Gateway Settings". The "General" tab is active, showing fields for "Vtrk gateway application" (set to "SIP Gateway (SIPGw)"), "SIP domain name" (set to "avayalab.com"), "Local SIP port" (set to "5060"), "Gateway endpoint name" (set to "node1005"), "Gateway password" (empty), and "Application node ID" (set to "1005"). There is also a checkbox for "Enable failsafe NRS" and a radio button for "SIP ANAT" (set to "IPv4"). The "Virtual Trunk Network Health Monitor" section on the right has a checkbox for "Monitor IP addresses (listed below)" and a list of "Monitor addresses" with an "Add" button and a "Remove" button. At the bottom, there are "Save" and "Cancel" buttons, and a note: "Note: Changes made on this page will NOT be transmitted until the Node is also saved."

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

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

- **Primary TLAN IP address:** Enter the IP address of the Session Manager SIP signaling interface. In the sample configuration **10.64.19.210** was used.
- **Port:** Enter **5060**
- **Transport protocol:** Select **TCP**

The values defined for the sample configuration are shown below.

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

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

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

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

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



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

The screenshot shows the 'SIP Gateway Services' configuration page. Under the 'SIP URI Map' section, there are two columns: 'Public E.164 domain names' and 'Private domain names'. The 'Public' column has fields for National, Subscriber, Special number, and Unknown. The 'Private' column has fields for UDP (set to 'udp'), CDP (set to 'cdp.udp'), Special number, Vacant number, and Unknown.

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.

The screenshot shows the 'Node Details' screen for ID 1005. The left sidebar contains a navigation tree with 'Nodes: Servers, Media Cards' selected. The main area shows configuration for 'Embedded LAN (ELAN)' and 'Telephony LAN (TLAN)'. The 'ELAN' section has fields for Gateway IP address (10.80.141.1) and Subnet mask (255.255.255.0). The 'TLAN' section has fields for Node IPv4 address (10.80.140.103) and Subnet mask (255.255.255.0). Below these are 'IP Telephony Node Properties' and 'Applications (click to edit configuration)' which include 'SIP Line' and 'Terminal Proxy Server (TPS)'. At the bottom right, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a yellow circle.

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

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

### Node Saved

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

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

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

You may initiate a transfer manually at a later time.

Once the transfer is complete, the **Synchronize Configuration Files (Node ID <id>)** page is displayed. Place a check mark next to the appropriate Hostname and click **Start Sync**. The screen will automatically refresh until the synchronization is finished.

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

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

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

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

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k-cpdc	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

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

The **Synchronization Status** field will update from **Sync required** (as shown above) to **Synchronized** (as shown below). After synchronization completes, place a check mark next to the appropriate Hostname and click **Restart Applications**.

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

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

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

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

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k-cpdc	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Synchronized

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

## 5.2. Virtual Superloops

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

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

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

## 5.3. Media Gateway

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

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

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

The **IPMG 4 0 Media Gateway Survivable (MGS) Configuration** window appears. The **Telephony LAN (TLAN) IP Address** under the **DSP Daughterboard 1** heading will be the IP Address in the SDP portion of SIP messages, for calls requiring a gateway resource. For example, for a call from a digital telephone to the PSTN via Cincinnati Bell eVantage IP Service, 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:

**Navigation Tree:**

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

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

**AVAYA CS1000 Element Manager**

**- VGW and IP phone codec profile**

Enable echo canceller ☒

Echo canceller tail delay  ( milliseconds )

Enable dynamic attenuation ☒

Voice activity detection threshold  ( 0 - 4 DBM )

Idle noise level  ( 0 - 1 DBM )

R factor calculation ☐

DTMF tone detection ☒

Enable low latency mode ☒

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

Enable modem/fax pass through mode ☒

Enable V.21 FAX tone detection ☒

Fax TCF method

FAX maximum rate  ( bps )

FAX playout nominal delay  ( 0 - 300 milliseconds )

FAX no activity timeout  ( 10 - 32000 milliseconds )

FAX packet size

+ Codec **G711** Select ☒

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

**AVAYA CS1000 Element Manager**

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

**- Codec G711** **Select** ☒

Codec name **G711**

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

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

Modifications may cause changes to dependent settings

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

Modifications may cause changes to dependent settings

VAD ☐

**- Codec G729A** **Select** ☒

Codec name **G729A**

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

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

Modifications may cause changes to dependent settings

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

Modifications may cause changes to dependent settings

VAD ☐

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

**AVAYA CS1000 Element Manager** Help | Logout

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

**Media Gateways**

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

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

## 5.4. Virtual D-Channel, Routes and Trunks

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

### 5.4.1. Virtual D-Channel Configuration

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

The screenshot displays the Avaya Communication Server 1000E web interface. On the left is a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System (with sub-items: + Alarms, - Maintenance, + Core Equipment, - Peripheral Equipment, - IP Network (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 (with sub-items: - Routes and Trunks (selected), - Routes and Trunks, - D-Channels, - Digital Trunk Interface, - 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 to 'Choose a D-Channel Number' (set to 0) and 'type' (set to DCH), with a 'to Add' button. At the bottom, a table lists the configuration for Channel 15: Channel: 15, Type: DCH, Card Type: DCIP, 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"/> <a href="#">more PRI</a>
Secondary PRI2 loops:	<input type="text"/>
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 <small>Range: 1 - 4000</small>
Signalling server resource capacity:	3700 <small>Range: 0 - 3700</small>

**- Basic options (BSCOPT)**

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

- PINX customer number:

- Progress signal:

- Calling Line Identification :

- Output request Buffers: 128

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

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

- Remote Capabilities: [Edit](#)



## 5.4.2. Routes and Trunks Configuration

In addition to configuring a virtual D-channel, a **Route** and associated **Trunks** must be configured. Expand **Routes and Trunks** on the left panel and expand the customer number. In the example screen that follows, it can be observed that Route 15 has 32 trunks in the sample configuration.

AVAYA CS1000 Element Manager

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

### Routes and Trunks

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

Select **Edit** to verify the configuration, as shown below. As can be observed in the **Incoming and outgoing trunk (ICOG)** parameter, incoming and outgoing calls are allowed. The **Access code for the trunk route (ACOD)** will in general not be dialed, but the number that appears in this field may be observed on Avaya CS1000E display phones if an incoming call on the trunk is anonymous or marked for privacy.

### Customer 0, Route 15 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE):

Customer number (CUST):

Route number (ROUT):

Designator field for trunk (DES):

Trunk type (TKTP):

Incoming and outgoing trunk (ICOG):

Access code for the trunk route (ACOD):

Trunk type M911P (M911P): ☐

Further down in the **Basic Configuration** section verify the **Node ID of signaling server of this route (NODE)** matches the node shown in **Section 5.1.1**. 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):  (0 - 8000)

- Node ID of signaling server of this route (NODE):  (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):  (0 - 254)

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

- Private network identifier (PNI):  (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 - 8000 milliseconds)

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

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

**AVAYA CS1000 Element Manager** Help | Logout

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

**- Basic Route Options**

Attendant announcement (ATAN) : No Attendant Announcement (NO) ▼

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

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

Controls or timers (CNTL) : ☐

Conventional (Tie trunk only) (CNVT) : ☐

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

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

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

- Display external dialed digits (DEXT) : ☐

Multifrequency compelled or MFC signaling (MFC) : No MFC (NO) ▼

Process notification networked calls (PNNC) : ☐

## 5.5. Dialing and Numbering Plans

This section provides the configuration of the routing used in the sample configuration for routing calls over the SIP Trunk between Avaya Communication Server 1000E and Session Manager for calls destined for the Cincinnati Bell eVantage IP Service. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks.

### 5.5.1. Route List Block

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

# CS1000 Element Manager

Managing: **10.80.141.102** Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN)

---

- [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

## 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.

# CS1000 Element Manager

Managing: **10.80.141.102** Username: admin

Dialing and Numbering Plans » [Electronic Switched Network \(ESN\)](#) » Customer 00 » 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

## 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.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Software, Customers, and Routes and Trunks. The main area is titled 'Options' and contains several configuration fields: 'Local Termination entry' (checkbox), 'Route Number' (dropdown menu with '15' selected and highlighted by a yellow circle), 'Skip Conventional Signaling' (checkbox), 'Use Tone Detector' (checkbox), 'Conversion to LDN' (checkbox), 'Expensive Route' (checkbox), and 'Strategy on Congestion' (dropdown menu with 'No Reroute (NRR)' selected). A copyright notice at the bottom reads 'Copyright © 2002-2012 Avaya Inc. All rights reserved.'

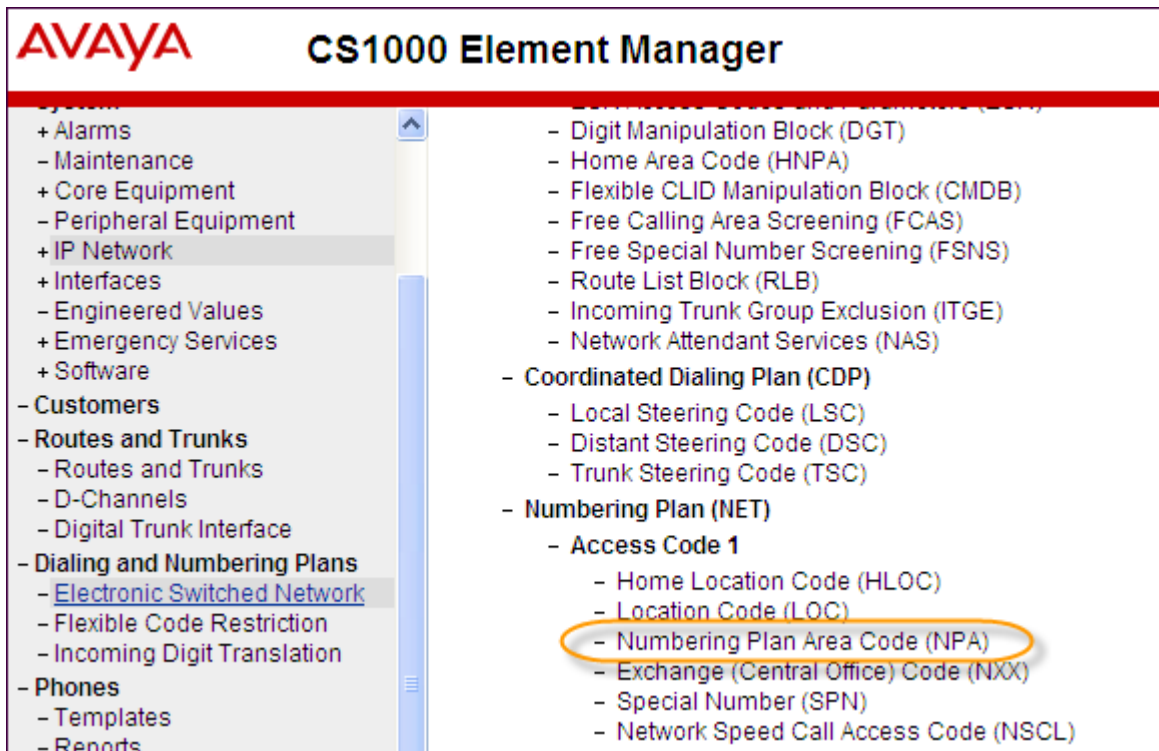
### 5.5.2. NARS Access Code

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Select **ESN Access Codes and Parameters (ESN)**. Although not repeated below, this link can be observed in the first screen in **Section 5.5.1**. In the **NARS/BARS Access Code 1** field, enter the number the user will dial before the target PSTN number. In the sample configuration, the single digit **9** was used.

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

### 5.5.3. Numbering Plan Area Codes

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



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

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 prominently displayed. Below the title, there is a form labeled 'Please enter an area code' with an input field and a 'to Add' button. A list of existing area codes is shown below, 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 Session Manager as shown in **Section 5.4.2**. Default parameters may be retained for other parameters. Repeat this procedure for the dial strings associated with other numbering plan area codes that should route to the SIP Trunk to Session Manager.

The screenshot shows the 'Numbering Plan Area Code' configuration page. The title 'Numbering Plan Area Code' is at the top. Below it, the section 'General Properties' contains the following 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.



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

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

Expand **Dialing and Numbering Plans** on the left panel and select **Electronic Switched Network**. Scroll down and select **Special Number (SPN)** under the appropriate access code heading (as can be observed in the first screen in **Section 5.5.3**).

Add a new number by entering it in the **Please enter a Special Number** box and click **to Add** or click **Edit** to view or change a special number that has been previously configured. In the screen below, it can be observed that various dial strings such as **0**, **011**, **411** and **911** calls are listed. Route list index **15** has been selected in the same manner as shown for the NPAs in the prior section.

**Special Number List**

Please enter a Special Number

---

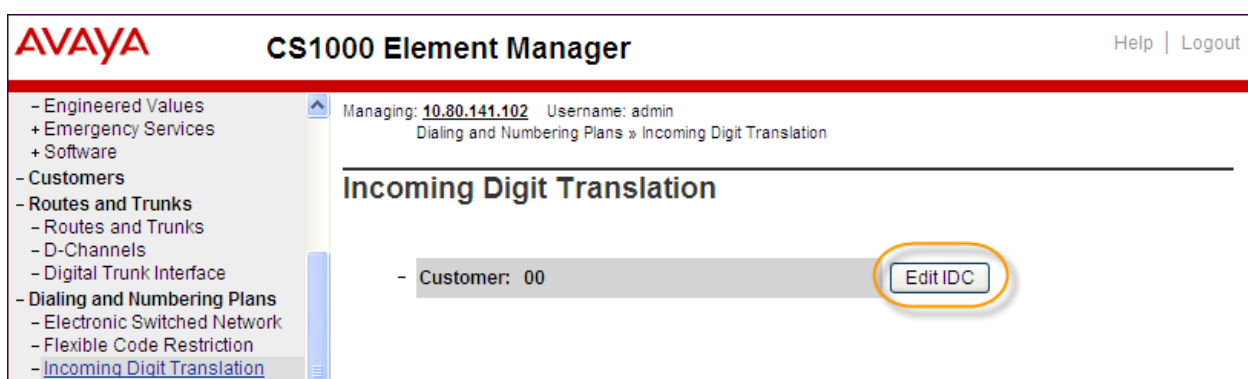
- <b>Special Number -- 0</b>	<input type="button" value="Edit"/>
Flexible length: 0	
International dialing plan: NO	
Type of call that is defined by the special number: NONE	
Route list index: 15	
- <b>Special Number -- 011</b>	<input type="button" value="Edit"/>
Flexible length: 0	
International dialing plan: YES	
Type of call that is defined by the special number: INTL	
Route list index: 15	
- <b>Special Number -- 411</b>	<input type="button" value="Edit"/>
Flexible length: 0	
International dialing plan: NO	
Type of call that is defined by the special number: NONE	
Route list index: 15	
- <b>Special Number -- 911</b>	<input type="button" value="Edit"/>
Flexible length: 0	
International dialing plan: NO	
Type of call that is defined by the special number: NONE	
Route list index: 15	



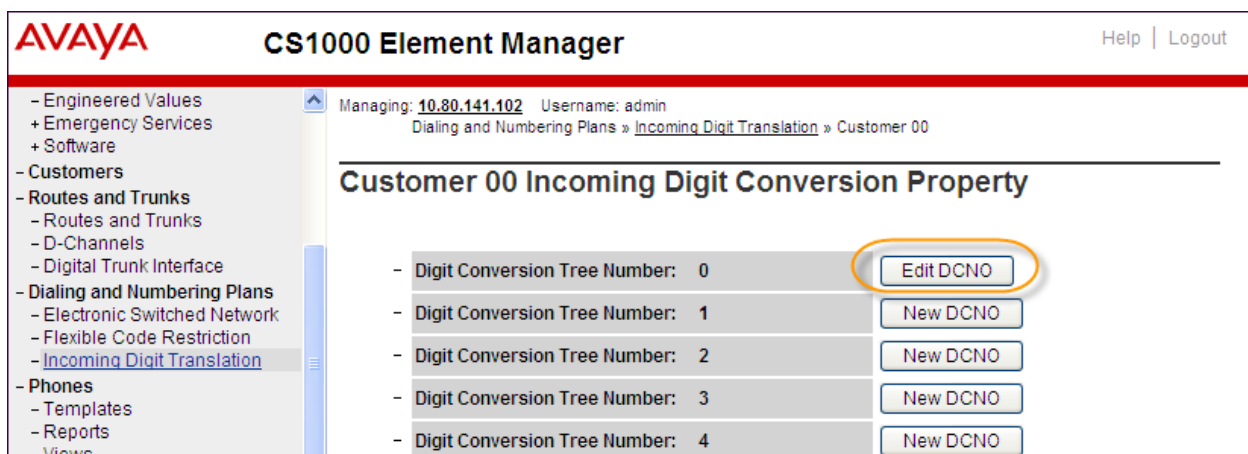
### 5.5.5. Incoming Digit Translation

In general, the incoming digit translation can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation as shown in **Section 6.4**, and digit manipulation via the CS1000E Incoming Digit Translation table may not be necessary. If the DID number sent by Cincinnati Bell is unchanged by Session Manager, then the DID number can be mapped to an extension using the Incoming Digit Translation. Both Session Manager digit conversion and CS1000E incoming digit translation methods were tested successfully.

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



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



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

In the following configuration, the incoming DID 5135555180 will be translated to CS1000E DN 2900.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The main content area is titled 'Digit Conversion Tree 0 Configuration'. It shows a breadcrumb path: 'Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration'. Below the title, it indicates 'Regular IDC tree' and 'Send calling party DID disabled'. There are buttons for 'Add...', 'Delete IDC', 'Delete IDC tree', and 'Refresh'. A table displays the configuration with columns: Incoming Digits, Converted Digits, CPND Name, and CPND language. The table contains one entry: Incoming Digits '5135555180', Converted Digits '2900', CPND Name '.', and CPND language 'Roman characters'.

Incoming Digits	Converted Digits	CPND Name	CPND language
5135555180	2900	.	Roman characters

## 5.6. Zones and Bandwidth

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar shows the navigation tree with 'System' expanded and 'IP Network' selected. The main content area is titled 'Zones'. It contains a description: 'Zones are used to group related information for either bandwidth or dial plan numbering purposes.' Below this, there are two sections: 'Bandwidth Zones' and 'Numbering Zones'. 'Bandwidth Zones' states: 'Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.' 'Numbering Zones' states: 'Numbering zones are used to route calls through a centralized call server.'

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

Bandwidth Zones

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

Refresh

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

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

### Edit Bandwidth Zone

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

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

### Zone Basic Property and Bandwidth Management

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

## 5.7. Example CS1000E Telephone Users

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

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

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

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header shows the AVAYA logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". The left-hand navigation menu lists various system components, with "Phones" currently selected. The main content area is titled "Phone Details" and shows the configuration for a specific phone. The "General Properties" tab is active, displaying fields for Customer Number (0), Terminal Number (252 0 09 01), Designation (SIPL2), Zone (1), SIP User Name (7108), Node Id (1005), and Super User (unchecked). The "Phone Details" tab shows a phone icon and system information: System: EM on cs1k-cpdc, Phone Type: UEXT-SIPL, and Sync Status: TRN.

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: 0 \*  
Terminal Number: 252 0 09 01  
Designation: SIPL2 \* (1-6 characters)  
Zone: 1 \*  
SIP User Name: 7108 \* (1-16 characters)  
Node Id: 1005 \*  
Super User: ☐

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


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

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

**AVAYA CS1000 Element Manager**

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

### Phone Details

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

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

### General Properties

Customer Number:  \*

Terminal Number:

Designation:  \* (1-6 characters)

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

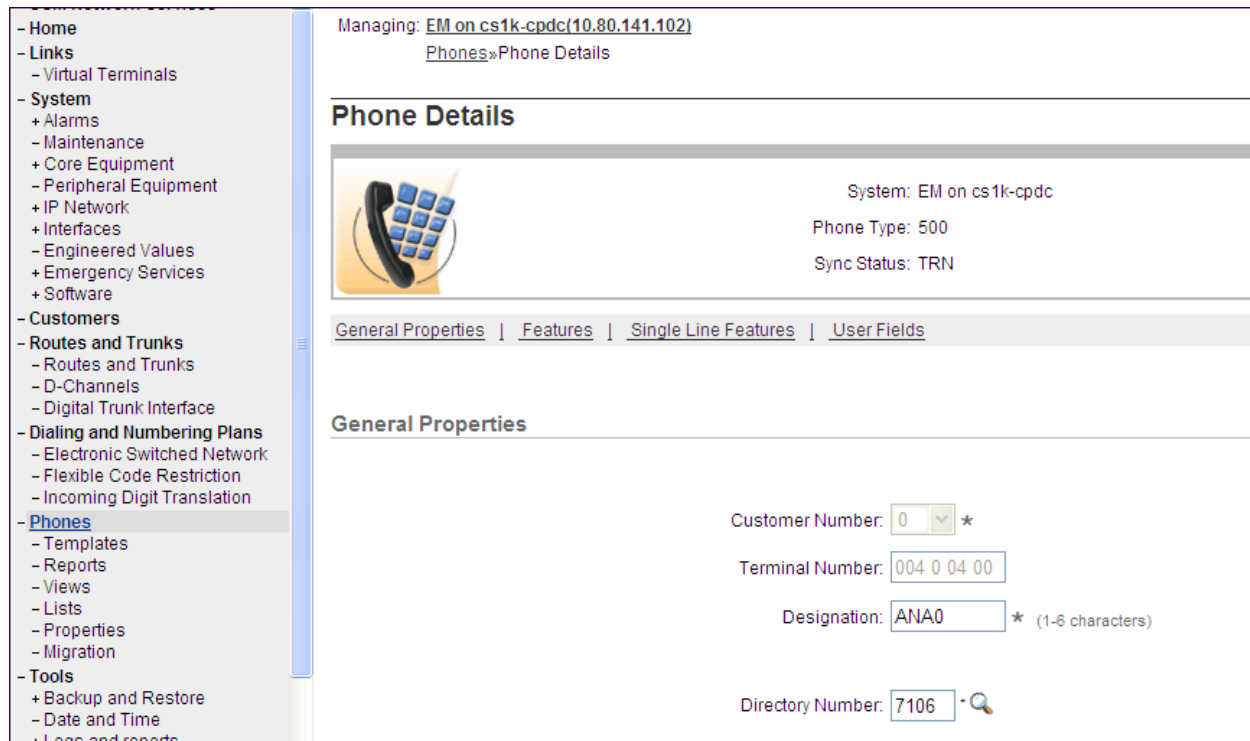
The screenshot shows the 'Keys' configuration page. It features a table with columns for Key No., Key Type, and Key Value. Key 0 is configured as 'SCR - Single Call Ringing' with Directory Number 7107. Key 1 is configured as 'CWT - Call Waiting'. The 'Key Value' section includes a search icon, a checkbox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

### Keys

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


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

The following screen shows basic information for an analog port in the configuration that may be used with a telephone or fax machine. The port is configured as Directory Number 7106.



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

### Phone Details

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

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

#### General Properties

Customer Number:  \*

Terminal Number:

Designation:  \* (1-6 characters)

Directory Number:  🔍

When an analog port is used for a fax machine, Modem Pass Through Allowed (MPTA) can be set to cause G.711 to be used instead of T.38 for fax calls, even if the zone configuration would otherwise have resulted in G.729. For example, if MPTA is configured, and an inbound call arrives from Cincinnati Bell eVantage IP Service, the CS1000E will respond with a 200 OK, selecting G.711 for the call in the SDP answer, even if the SDP offer from Cincinnati Bell listed G.729 before G.711. Similarly, for an outbound call with MPTA configured, the CS1000E will send the INVITE with an SDP offer for G.711. See **Section 2.2** for T.38 limitations with the Cincinnati Bell eVantage IP Service.

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

Features		
Feature	Description	Value:
MINA	Message Intercept Treatment	<input type="text" value="Denied"/>
MLWU_LANG	Language for Automatic Wake Up	<input type="text" value="Language 0 (RAN1/RAN2)"/>
MPT	Modem Pass Through	<input type="text" value="MPTA"/>

## 5.8. Save Configuration

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

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories: Phones, Tools, and Security. The 'Tools' category is expanded, showing sub-items like 'Backup and Restore' and 'Call Server'. The 'Call Server' item is selected. The main content area is titled 'Call Server Backup'. At the top of this area, it shows 'Managing: 10.80.141.102' and 'Username: admin'. Below this, a breadcrumb trail reads 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. The 'Action' section features a dropdown menu currently set to 'Backup', with 'Submit' and 'Cancel' buttons to its right.

## 6. Configure Avaya Aura® Session Manager

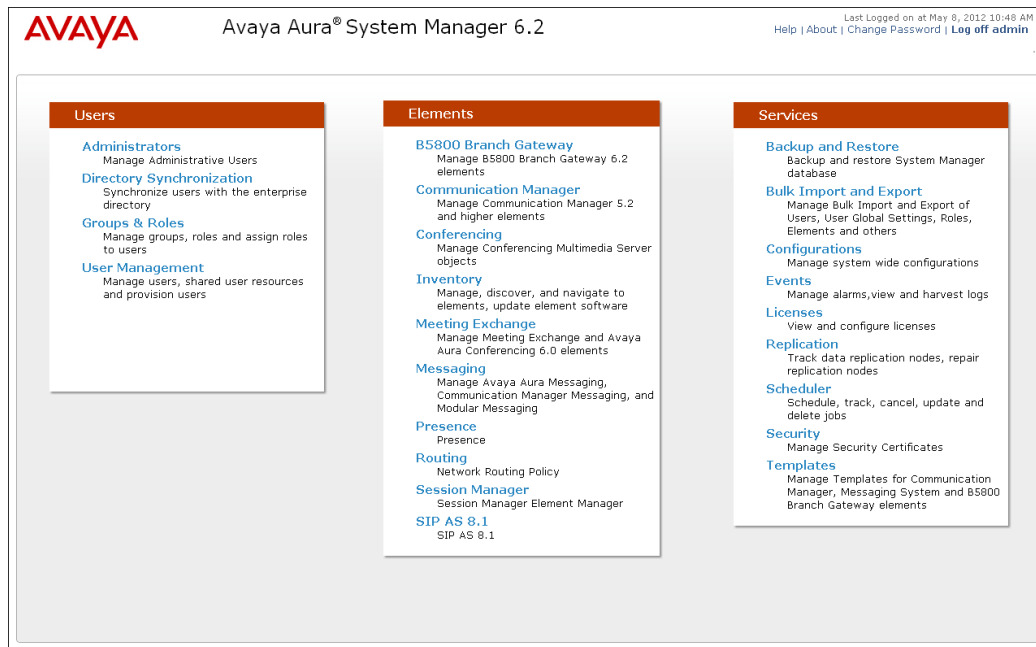
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

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

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

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





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

**AVAYA** Avaya Aura® System Manager 6.2 Last Logged on at May 8, 2012 10:48 AM  
Help | About | Change Password | Log off admin

**Routing** \* Home

Home / Elements / Routing

### Introduction to Network Routing Policy Help ?

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

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

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
  - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
  - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
  - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
  - Between Session Managers
  - Between Session Managers and "other SIP Entities"

## 6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

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

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

Home / Elements / Routing / Domains

**Domain Management** Help ?

Commit Cancel

Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.

1 Item | Refresh Filter: Enable

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

### 6.3. Add Location

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

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

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

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.5**), so it was not necessary to add a pattern.

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

The screenshot displays the 'Add Location' configuration page in the Session Manager interface. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Locations'. The page is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons in the top right corner. The 'General' section contains fields for 'Name' (set to 'SessionManager') and 'Notes' (set to 'Session Manager'). The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', 'Multimedia Bandwidth', and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes 'Maximum Multimedia Bandwidth (Intra-Location)' (1000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (1000 Kbit/Sec), '\* Minimum Multimedia Bandwidth' (64 Kbit/Sec), and '\* Default Audio Bandwidth' (80 Kbit/sec). The 'Alarm Threshold' section includes 'Overall Alarm Threshold' (80 %), 'Multimedia Alarm Threshold' (80 %), '\* Latency before Overall Alarm Trigger' (5 Minutes), and '\* Latency before Multimedia Alarm Trigger' (5 Minutes). The 'Location Pattern' section at the bottom has 'Add' and 'Remove' buttons, a table with 0 items, a 'Refresh' button, and a 'Filter: Enable' option. The table header shows 'IP Address Pattern' and 'Notes'.

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

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

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

[Help ?](#)

**Location Details**

Commit

Cancel

**General**

**\* Name:**

CS1K-Location

**Notes:**

CS1000 lab 140

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**

Kbit/sec

**Total Bandwidth:**

**Multimedia Bandwidth:**

**Audio Calls Can Take Multimedia Bandwidth:**

☒

**Per-Call Bandwidth Parameters**

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

1000

Kbit/Sec

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

1000

Kbit/Sec

**\* Minimum Multimedia Bandwidth:**

64

Kbit/Sec

**\* Default Audio Bandwidth:**

80

Kbit/sec

Below is the screen for **Loc19-ASBCE** used for Avaya SBCE.

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

[Help ?](#)

**Location Details**

Commit

Cancel

**General**

**\* Name:**

Loc19-ASBCE

**Notes:**

Location 19 Avaya SBC

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**

Kbit/sec

**Total Bandwidth:**

**Multimedia Bandwidth:**

**Audio Calls Can Take Multimedia Bandwidth:**

☒

**Per-Call Bandwidth Parameters**

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

1000

Kbit/Sec

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

1000

Kbit/Sec

**\* Minimum Multimedia Bandwidth:**

64

Kbit/Sec

**\* Default Audio Bandwidth:**

80

Kbit/sec

## 6.4. Adaptations

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

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

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

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

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

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

\* Adaptation name: CS1K-Adaptation

Module name: CS1000Adapter

Module parameter: fromto=true

Egress URI Parameters:

Notes: CS1K Adaptor

Scrolling down, in the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from CS1000E users to Cincinnati Bell. The text below and the screen example that follows explain how to use Session Manager to convert the CS1000E directory numbers that are in the From and P-Asserted-Identity headers to the corresponding Cincinnati Bell DID numbers.

- **Matching Pattern** Enter Avaya CS1000E extensions (or extension ranges via wildcard pattern matching). For other entries, enter the dialed prefix for any SIP endpoints registered to Session Manager (if any).
- **Min** Enter minimum number of digits (e.g., 4).
- **Max** Enter maximum number of digits (e.g., 4).
- **Delete Digits** Enter **0**, unless digits should be removed from dialed number before routing by Session Manager. For CS1000E extensions that do not match the last digits of the Cincinnati Bell DID, enter the number of digits in the extension to remove all digits.
- **Insert Digits** Enter the Cincinnati Bell DID corresponding to the matched extension or DID prefix for a range of extensions.
- **Address to modify** Select **both**.

Digit Conversion for Incoming Calls to SM
Add Remove

5 Items | Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 2900	* 4	* 4		* 4	5135555185	both ▼		Convert Ext to DID
<input type="checkbox"/>	* 51	* 4	* 4		* 0	513555	both ▼		Convert Ext to DID
<input type="checkbox"/>	* 7106	* 4	* 4		* 4	5135555180	both ▼		Convert Ext to DID
<input type="checkbox"/>	* 7107	* 4	* 4		* 4	5135555181	both ▼		Convert Ext to DID
<input type="checkbox"/>	* 7108	* 4	* 4		* 4	5135555182	both ▼		Convert Ext to DID

Select : All, None

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

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

Digit Conversion for Outgoing Calls from SM
Add Remove

5 Items Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 51355551	* 10	* 10		* 10	5180	both ▼		INBOUND DID to Ext
<input type="checkbox"/>	* 5135555180	* 10	* 10		* 10	7106	both ▼		INBOUND DID to Ext
<input type="checkbox"/>	* 5135555181	* 10	* 10		* 10	7107	both ▼		INBOUND DID to Ext
<input type="checkbox"/>	* 5135555182	* 10	* 10		* 10	7108	both ▼		INBOUND DID to Ext
<input type="checkbox"/>	* 5135555185	* 10	* 10		* 10	2900	both ▼		INBOUND DID to Ext

Select : All, None

## 6.5. Add SIP Entities

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

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

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

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

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

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

**General**

\* **Name:**

\* **FQDN or IP Address:**

**Type:**

**Notes:**

**Location:**

**Outbound Proxy:**

**Time Zone:**

**Credential name:**

**SIP Link Monitoring**

**SIP Link Monitoring:**



To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**.

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

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

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

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

### Port

TCP Failover port:

TLS Failover port:

4 Items | [Refresh](#)

Filter: [Enable](#)

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

Select : [All](#), [None](#)

The following screen shows the addition of CS1000E. The **FQDN or IP Address** field is set to the IP address of the Node IP on CS1000E defined in **Section 5.1.1**. The **Adaptation** field is set to the **CS1K-Adaptation** created in **Section 6.4** and the Location is set to the one defined for CS1000E in **Section 6.3**.

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

[Help ?](#)

**SIP Entity Details**

Commit

Cancel

**General**

\* Name:

CS1K

\* FQDN or IP Address:

10.80.140.103

Type:

Other

Notes:

CS1K Lab 140

Adaptation:

CS1K-Adaptation

Location:

CS1K-Location

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

none

CommProfile Type Preference:

**SIP Link Monitoring**

SIP Link Monitoring:

Use Session Manager Configuration

The following screen shows the addition of Avaya SBCE SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for Avaya SBCE in **Section 6.3. Link Monitoring Disabled** was selected for **SIP Link Monitoring**.

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

[Help ?](#)

**SIP Entity Details**

Commit

Cancel

**General**

\* Name:

Loc19-ASBCE

\* FQDN or IP Address:

10.64.19.100

Type:

Other

Notes:

Avaya SBC

Adaptation:

Location:

Loc19-ASBCE

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

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

4

Credential name:

Call Detail Recording:

none

CommProfile Type Preference:

**SIP Link Monitoring**

SIP Link Monitoring:

Link Monitoring Disabled

\* Proactive Monitoring Interval (in seconds):

900

\* Reactive Monitoring Interval (in seconds):

120

\* Number of Retries:

1

## 6.6. Add Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system. For CS1000E, select the CS1000E SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to CS1000E and Avaya SBCE.

Entity Link to CS1000E:

Entity Links

CommitCancel

1 Item | Refresh

Filter: Enable

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

Entity Link to Avaya SBCE:

Entity Links

CommitCancel

1 Item | Refresh

Filter: Enable

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

## 6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added; one for CS1000E and one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

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

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

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

The following screens show the Routing Policies for CS1000E and Avaya SBCE.

Routing Policy for CS1000E:

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

\* Name: To-CS1K

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

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

## Routing Policy for Avaya SBCE:

The screenshot shows the 'Routing Policy Details' page for a policy named 'To-ASBCE'. The page has a breadcrumb trail: Home / Elements / Routing / Routing Policies. In the top right corner, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The 'General' section contains the following fields: 'Name' (To-ASBCE), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (empty). Below this is the 'SIP Entity as Destination' section with a 'Select' button. At the bottom, there is a table with the following data:

Name	FQDN or IP Address	Type	Notes
Loc19-ASBCE	10.64.19.100	Other	Avaya SBC

## 6.8. Add Dial Patterns

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

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

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

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

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

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details
[Help ?](#)

General

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

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

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

Select : All, None

The second example shows that a **10** digit number starting with **51355551** and originating from **Loc19-ASBCE** uses route policy **To-CS1K**. This is a DID range 513-555-5100 through 513-555-5199 assigned to the enterprise from Cincinnati Bell.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

[Help ?](#)

General

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

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

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Loc19-ASBCE	Location 19 Avaya SBC	To-CS1K	0	<input type="checkbox"/>	CS1K	

Select : [All](#), [None](#)



## 6.9. Add/Verify Avaya Aura® Session Manager Instance

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

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

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

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

Home / Elements / Session Manager

[Help ?](#)

### Edit Session Manager

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

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

**General** ▾

**SIP Entity Name** DenverSM

**Description**

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

**\*Direct Routing to Endpoints**  ▾

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

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

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

Security Module ▾

SIP Entity IP Address

10.64.19.210

\*Network Mask

255.255.255.0

\*Default Gateway

10.64.19.1

\*Call Control PHB

46

\*QOS Priority

6

\*Speed & Duplex

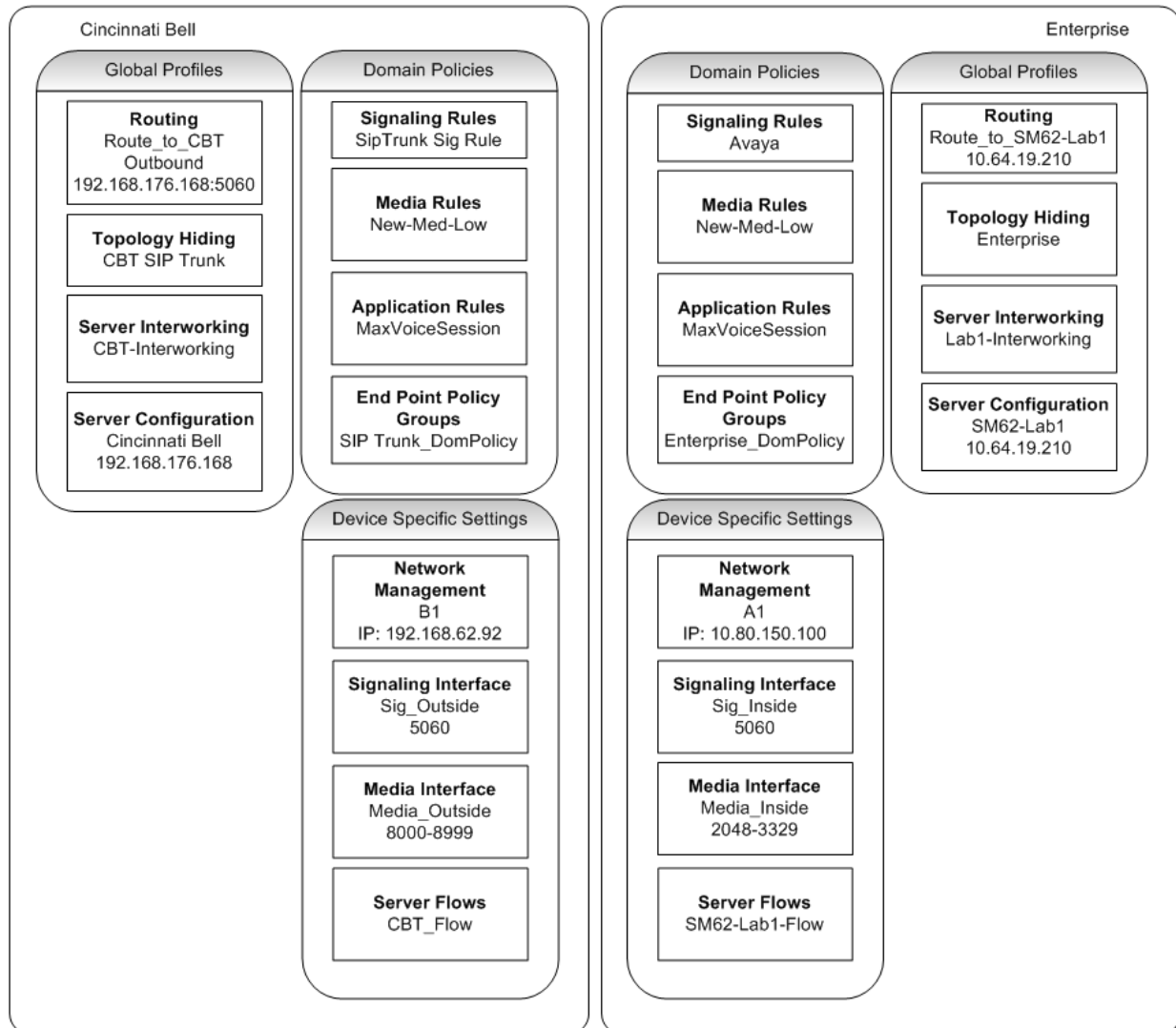
Auto ▾

VLAN ID

## 7. 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.

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](mailto:support@sipera.com).

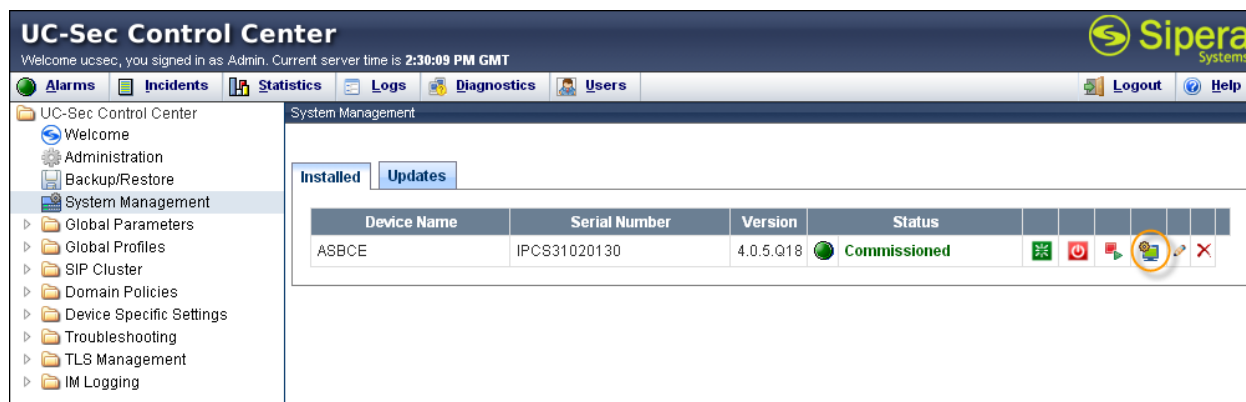
Alarms (Past 24 Hours)	Incidents (Past 24 Hours)
None found.	ASBCE: Server Heartbeat is UP
	ASBCE: Server Heartbeat is failed
	ASBCE: Server Heartbeat is UP
	ASBCE: Server Heartbeat is failed
	ASBCE: Server Heartbeat is UP

UC-Sec Devices	Network Type
ASBCE	DMZ_ONLY

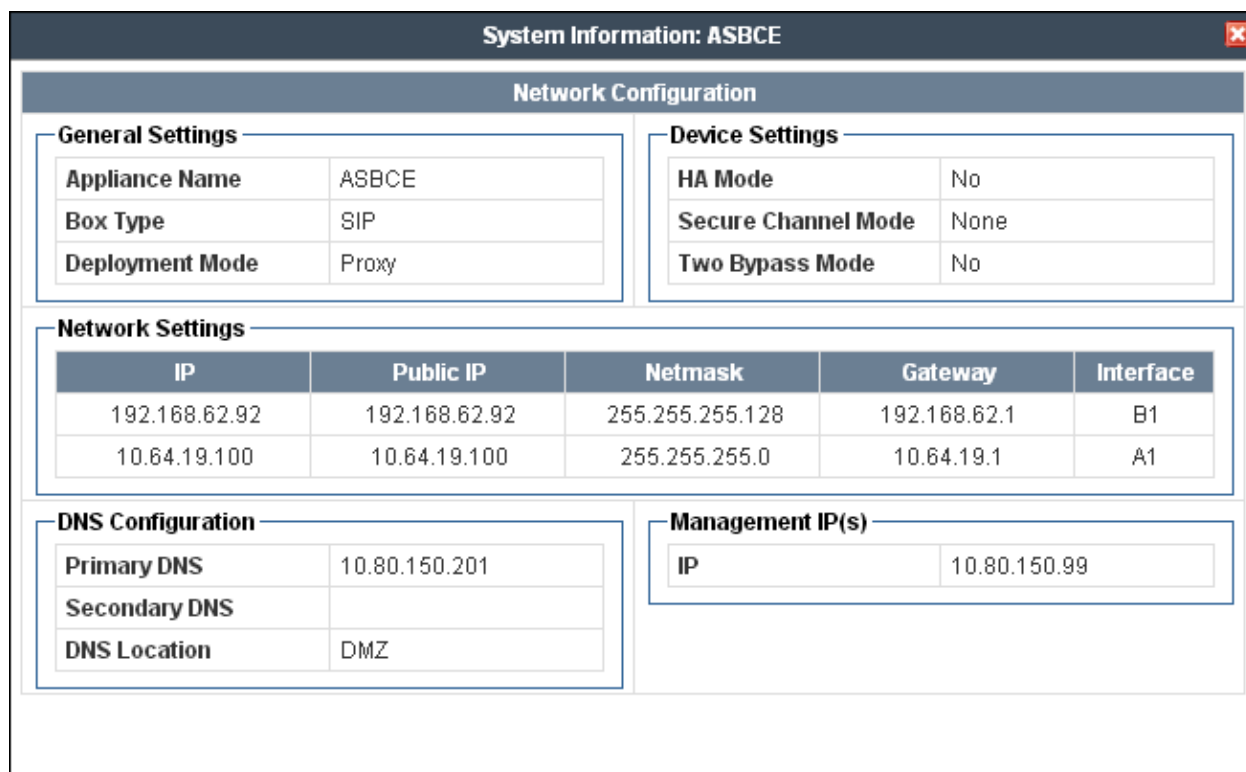
Administrator Notes
No notes posted.

[ 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.



## 7.1. 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**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Device Specific Settings' expanded to show 'Network Management'. The main panel is titled 'Device Specific Settings > Network Management: ASBCE' and has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: '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.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.128), and 'B2 Netmask'. There are also 'Add IP', 'Save Changes', and 'Clear Changes' buttons. A table lists the configured IP addresses:

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.

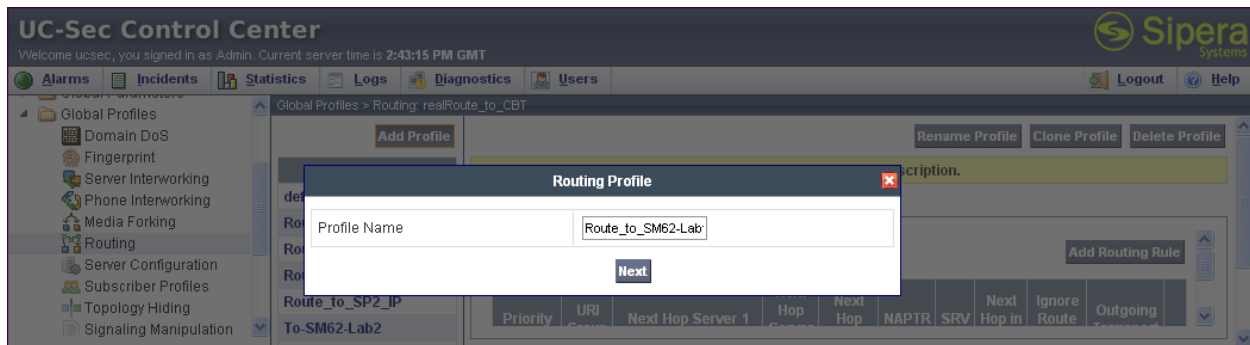
The screenshot shows the UC-Sec Control Center interface with the 'Interface Configuration' tab active. It displays a table of network interfaces and their administrative status:

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

## 7.2. 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 Session Manager and Cincinnati Bell eVantage IP Service. 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 Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity created in **Section 6.5**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.6**.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:46:13 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Route\_to\_SM62-Lab1

Add Profile Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.64.19.210	---	<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 Cincinnati Bell. In the **Next Hop Server 1** field enter the IP address and port that Cincinnati Bell uses to listen for SIP traffic. Enter **UDP** for the **Outgoing Transport** field.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:49:54 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Route\_to\_CBT

Add Profile Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

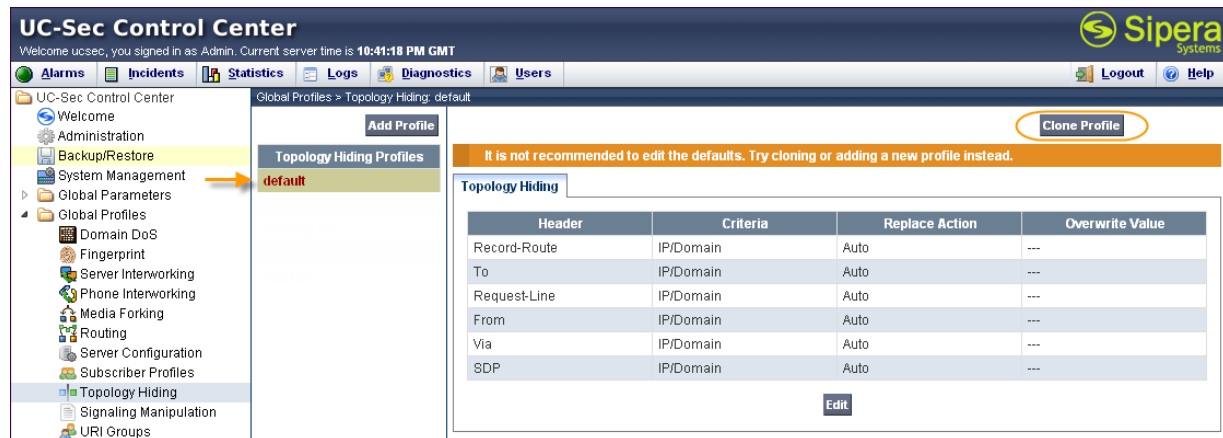
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	192.168.176.168:5060	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP



### 7.3. 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.

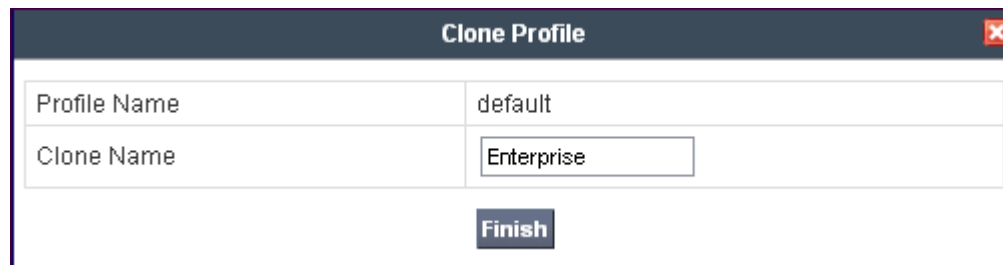
Create a Topology Hiding Profile for the enterprise and Cincinnati Bell eVantage IP Service. In the sample configuration, the **Enterprise** and **CBT SIP Trunk** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center → Global Profiles → Topology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



The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Profiles, and Topology Hiding. The 'Topology Hiding' category is expanded, showing a list of profiles with 'default' selected. The main panel displays the 'Topology Hiding' configuration for the 'default' profile. It includes a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The table lists several SIP headers (Record-Route, To, Request-Line, From, Via, SDP) and their corresponding criteria (IP/Domain) and actions (Auto). A 'Clone Profile' button is highlighted in the top right corner of the main panel.

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**.



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

Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.2**). Click **Finish** to save the changes.

Edit Topology Hiding Profile ✕

Header	Criteria	Replace Action	Overwrite Value	
Record-Route <span style="float: right;">▼</span>	IP/Domain <span style="float: right;">▼</span>	Auto <span style="float: right;">▼</span>		✕
To <span style="float: right;">▼</span>	IP/Domain <span style="float: right;">▼</span>	Overwrite <span style="float: right;">▼</span>	avayalab.com	✕
Request-Line <span style="float: right;">▼</span>	IP/Domain <span style="float: right;">▼</span>	Overwrite <span style="float: right;">▼</span>	avayalab.com	✕
From <span style="float: right;">▼</span>	IP/Domain <span style="float: right;">▼</span>	Overwrite <span style="float: right;">▼</span>	avayalab.com	✕
Via <span style="float: right;">▼</span>	IP/Domain <span style="float: right;">▼</span>	Auto <span style="float: right;">▼</span>		✕
SDP <span style="float: right;">▼</span>	IP/Domain <span style="float: right;">▼</span>	Auto <span style="float: right;">▼</span>		✕

Finish

It is not necessary to modify the **CBT SIP Trunk** profile from the default values. The following screen shows the Topology Hiding Policy created for Cincinnati Bell.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:55:06 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users
Logout Help

Global Parameters

Global Profiles

- Domain DoS
- Fingerprint
- Server Interworking
- Phone Interworking
- Media Forking
- Routing
- Server Configuration
- Subscriber Profiles
- Topology Hiding
- Signaling Manipulation
- URI Groups
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Global Profiles > Topology Hiding: CBT SIP Trunk
Add Profile

Topology Hiding Profiles

- default
- cisco\_th\_profile
- CBT SIP Trunk
- Enterprise

CBT SIP Trunk
Rename Profile Clone Profile Delete Profile

Topology Hiding

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

Edit

DDT; Reviewed:  
SPOC 12/17/2012

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

66 of 103  
CBTCS1K75SM62

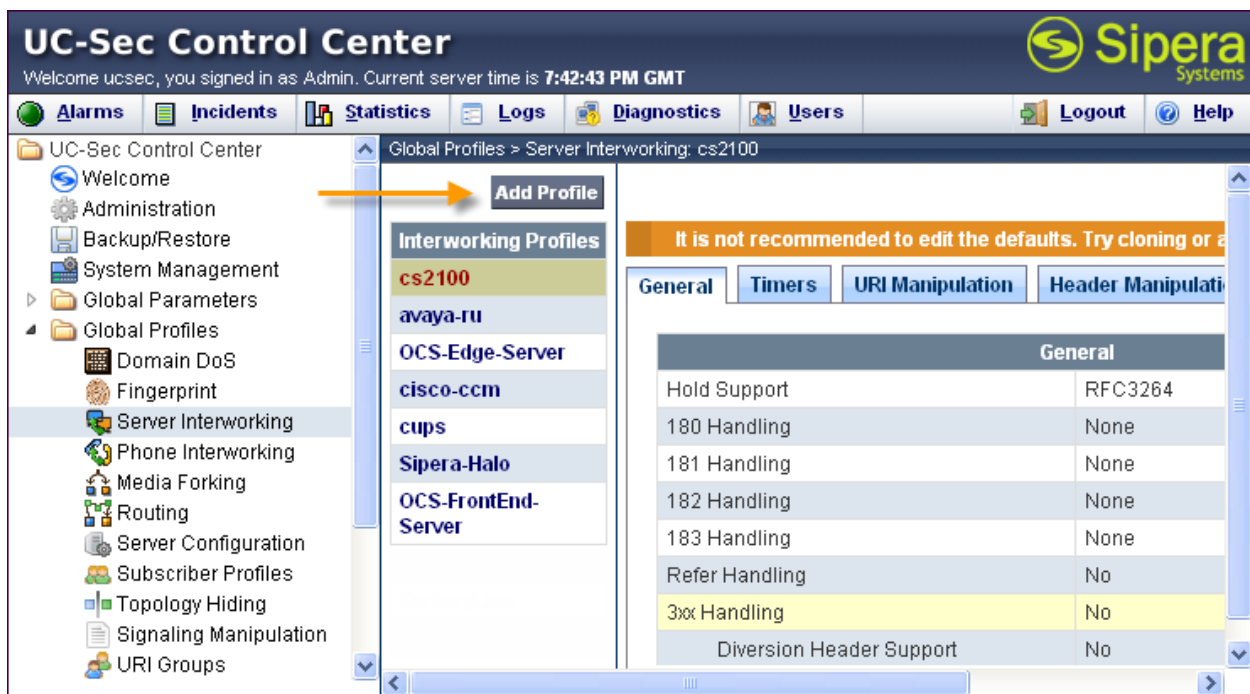
## 7.4. Server Interworking Profile

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 Cincinnati Bell.

### 7.4.1. 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

Enterprise

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 two windows that appear. Click **Next** to continue.

Interworking Profile

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	

DTMF

DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
--------------	---

Back

Next

Interworking Profile

Configuration is not required. All fields are optional.

SIP Timers

Min-SE		seconds, [90 - 86400]
Init Timer		milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire		seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]

Transport Timers

TCP Connection Inactive Timer		seconds, [600 - 3600]
-------------------------------	--	-----------------------

Back

Next

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

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

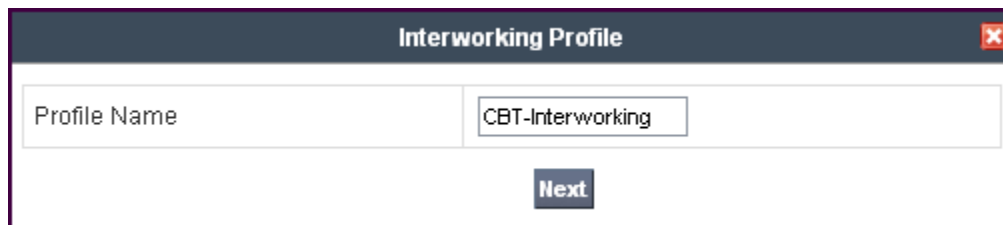
Click **Finish** to save changes.

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<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**

### 7.4.2. Server Interworking Profile – Cincinnati Bell

To create a new Server Interworking Profile for Cincinnati Bell, 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.

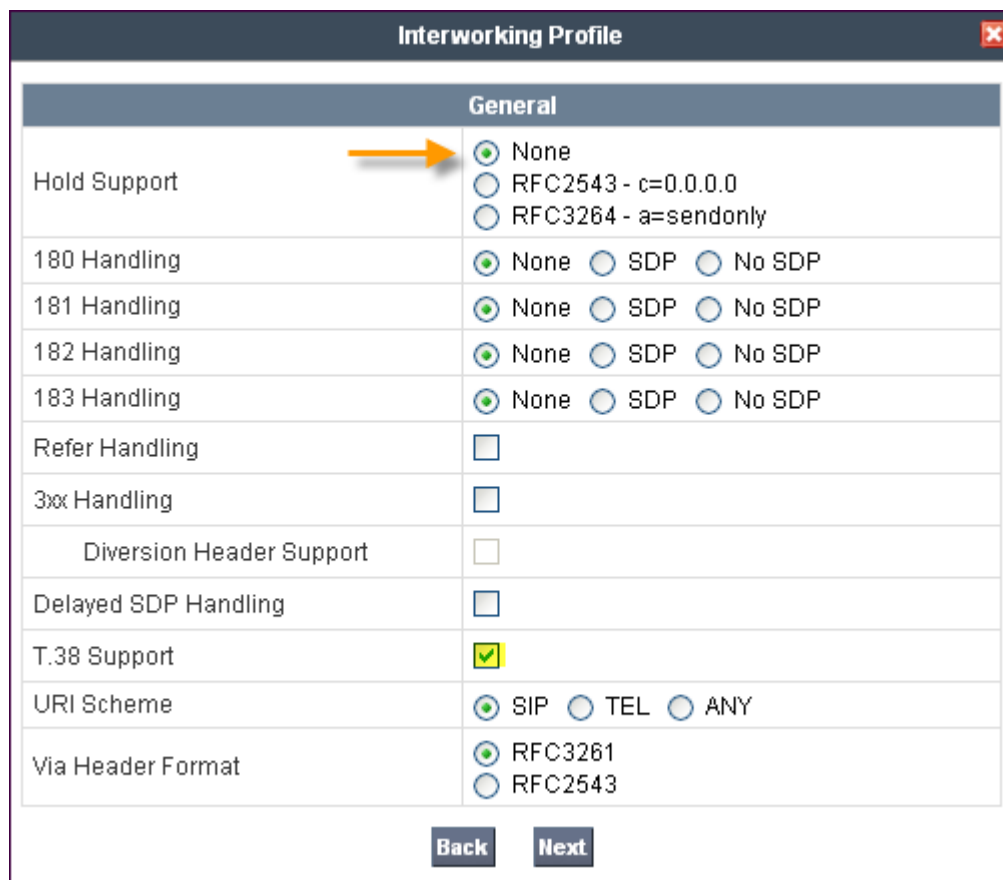


The screenshot shows a dialog box titled "Interworking Profile". It has a "Profile Name" input field containing the text "CBT-Interworking". Below the input field is a "Next" button.

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

- **Hold Support:** None
- **T.38 Support:** Checked.

Click **Next** to continue.



The screenshot shows the "Interworking Profile" dialog box with the "General" tab selected. The "Hold Support" field is set to "None" (indicated by an orange arrow). The "T.38 Support" field is checked. Other fields are set to their default values.

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

Buttons: Back, Next

Default values can be used for the next two windows that appear. 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
--------------	---

Back

Next

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]
-------------------------------	----------------------	-----------------------

Back

Next



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

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

Click **Finish** to save changes.

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input 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**

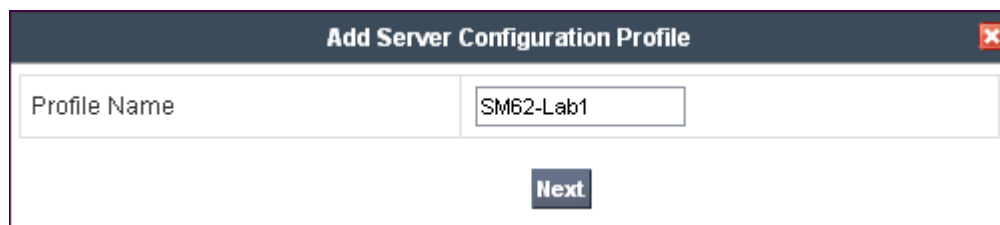
## 7.5. Server Configuration

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 Session Manager and Cincinnati Bell.

### 7.5.1. Server Configuration – Session Manager

To add a Server Configuration Profile for Session Manager, 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 web-based dialog box titled "Add Server Configuration Profile". It features a dark header bar with the title and a red close button. The main area contains a text input field labeled "Profile Name" which has the text "SM62-Lab1" entered. Below the input field is a blue button labeled "Next".

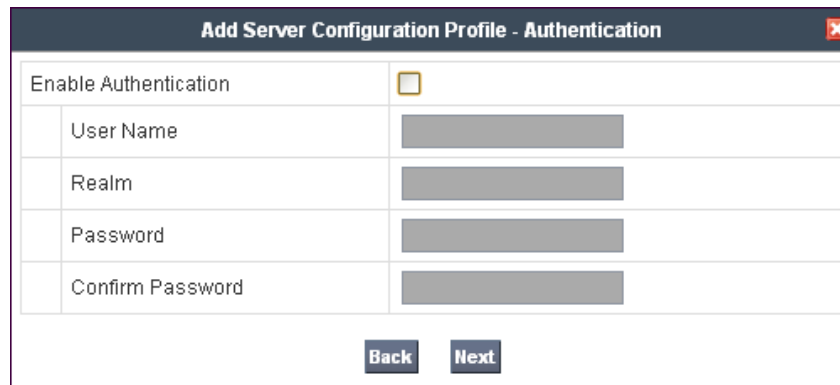
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of Session Manager. This should match the IP address of the SIP Entity for Session Manager in **Section 6.5**.
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link in Session Manager in **Section 6.6**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link in Session Manager in **Section 6.6**.

Click **Next** to continue.

Add Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.64.19.210
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 Session Manager does not require authentication. Click **Next** to continue.

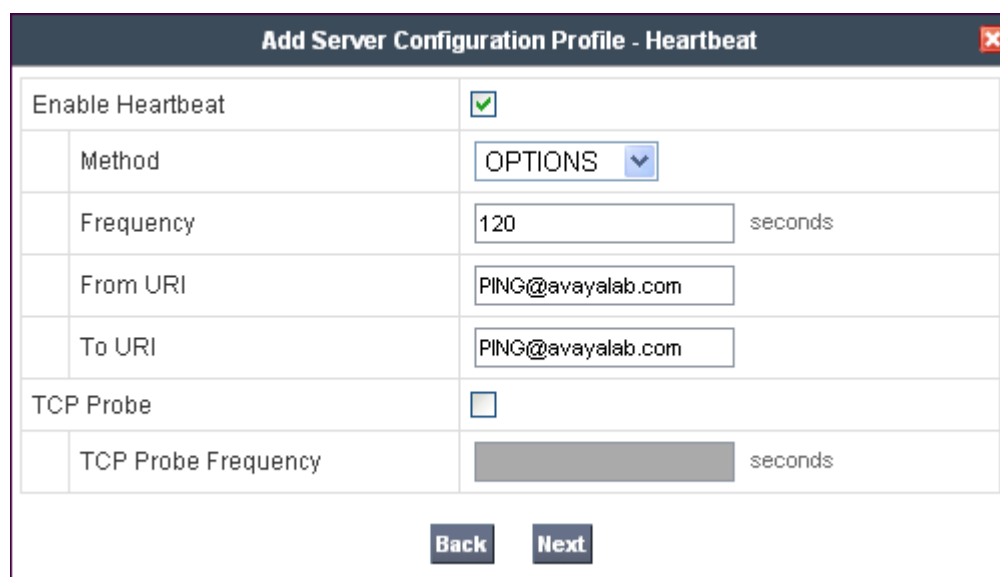


Add Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
<div>Back Next</div>	

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

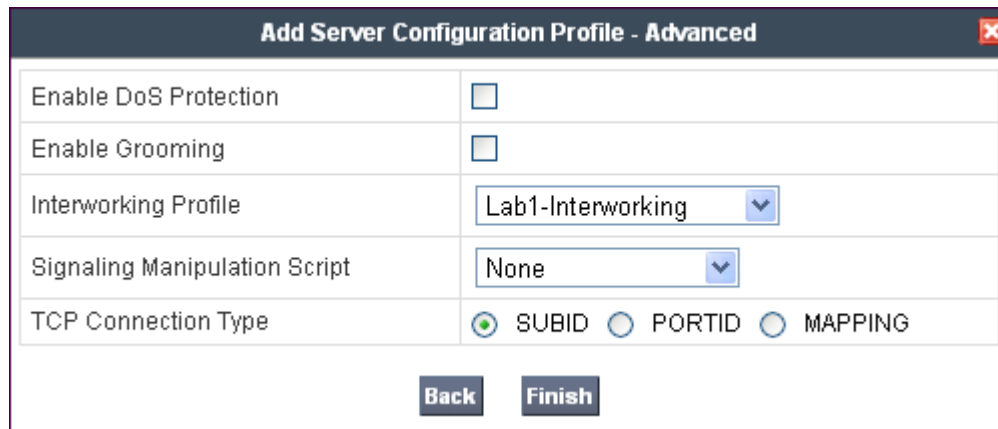
- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS to Session Manager. For compliance testing **120** seconds was chosen.
- **From URI:** Enter an URI to be sent in the 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 <input type="button" value="v"/>
Frequency	120 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	<input type="text"/> seconds
<div>Back Next</div>	

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.4.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.



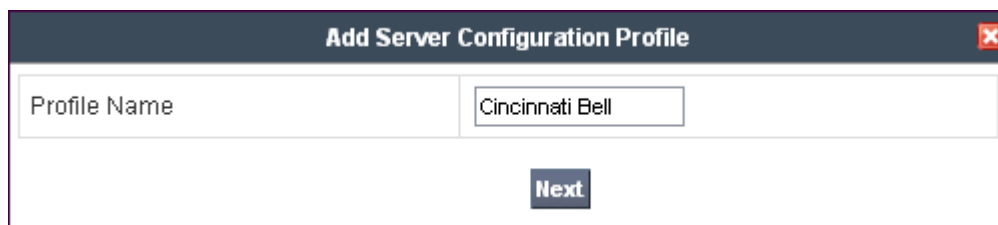
The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains five rows of configuration options:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Lab1-Interworking
Signaling Manipulation Script	None
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".

### 7.5.2. Server Configuration - Cincinnati Bell

To add a Server Configuration Profile for Cincinnati Bell, 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". It contains a single row with a text input field:

Profile Name	Cincinnati Bell
--------------	-----------------

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(es) of the SIP proxy(ies) of the service provider. In the case of the compliance test, this is the IP address of the Cincinnati Bell eVantage IP Service. This will associate the inbound SIP messages from Cincinnati Bell to this Server Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and Cincinnati Bell. For compliance testing **UDP** was used.
- **UDP Port:** Enter the port number that Cincinnati Bell 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 values:

Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Comma separated list</small>	192.168.176.168
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	

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

If using trunk registration, select **Enable Authentication**. Enter the user name provided by Cincinnati Bell in the **User Name** field. Leave the **Realm** blank to have it detected from the server challenge. Enter the password provided by Cincinnati Bell in the **Password** field. Click **Next** to continue.

Add Server Configuration Profile - Authentication

Enable Authentication	<input checked="" type="checkbox"/>
User Name	<input type="text" value="5135555180"/>
Realm (Leave blank to detect from server challenge)	<input type="text"/>
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>

Back

Next

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

- **Enabled Heartbeat:** Checked.
- **Method:** If using trunk registration, select **REGISTER** from the drop-down box. Otherwise, select **OPTIONS**.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send REGISTER/OPTIONS messages to Cincinnati Bell. For compliance testing **120** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP REGISTER/OPTIONS. In the example below **5135555180@192.168.62.92** was used.
- **TO URI:** Enter an URI to be sent in the TO header for SIP REGISTER/OPTIONS. In the example below **5135555180@192.168.176.168** was used.

Click **Next** to continue.

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER ▼
Frequency	120 seconds
From URI	5135555180@192.168.62
To URI	5135555180@192.168.17
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds

Back Next



In the new window that appears, select the **Interworking Profile** created for Cincinnati Bell in **Section 7.4.2**. Use default values for all remaining fields. Click **Finish** to save the configuration.

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

Back Finish

## 7.6. 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 Cincinnati Bell eVantage IP Service 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.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 9:18:08 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
  - Application Rules
  - Border Rules
  - Media Rules
  - Security Rules
  - Signaling Rules
  - Time of Day Rules
  - End Point Policy Groups
  - Session Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Domain Policies > Media Rules: default-low-med

Add Rule

Filter By Device... Clone Rule

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Media NAT Media Encryption Media Anomaly Media Silencing Media QoS Turing Test

Media NAT Learn Media IP dynamically Edit

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

Clone Rule

Rule Name

default-low-med

Clone Name

New-Low-Med

Finish

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.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:45:44 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

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Time of Day Rules

End Point Policy Groups

Session Policies

Device Specific Settings

Troubleshooting

TLS Management

IM Logging

Domain Policies > Media Rules: New-Low-Med

Add Rule

Filter By Device...

Rename Rule

Clone Rule

Delete Rule

Media Rules

default-low-med

default-low-med-enc

default-high

default-high-enc

avaya-low-med-enc

Int-AllowShuffle

New-Low-Med

Click here to add a description.

Media NAT

Media Encryption

Media Anomaly

Media Silencing

Media QoS

Turing Test

Media QoS Reporting

RTCP Enabled

Media QoS Marking

Enabled

QoS Type

DSCP

Audio QoS

Audio DSCP

EF

Video QoS

Video DSCP

EF

Edit

DDT; Reviewed:  
SPOC 12/17/2012

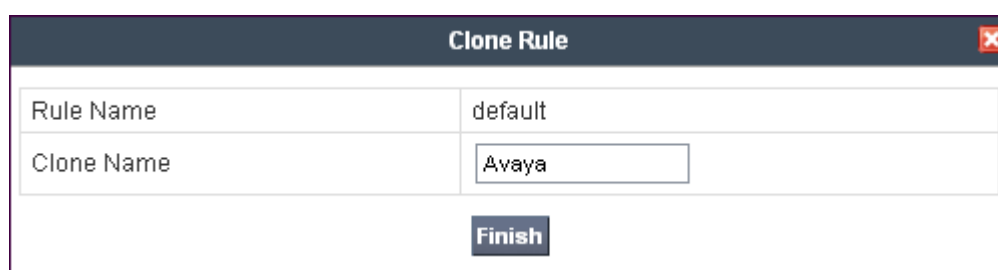
Solution & Interoperability Test Lab Application Notes  
©2012 Avaya Inc. All Rights Reserved.

82 of 103  
CBTCS1K75SM62

## 7.7. Signaling Rule

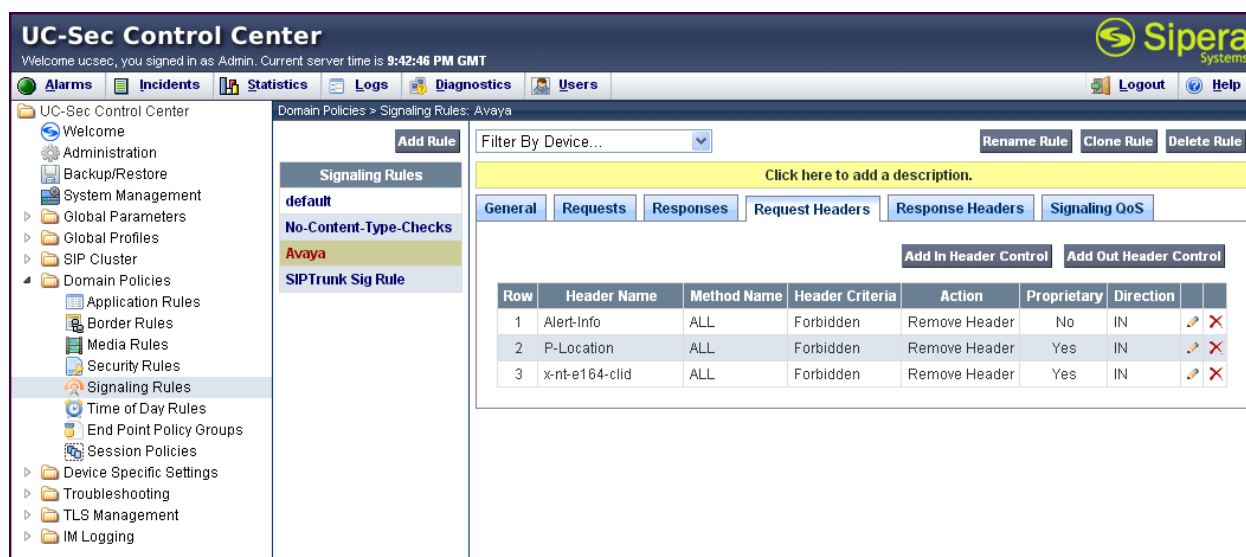
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined 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 remove unnecessary SIP headers and 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** (not shown). Enter a descriptive name for the new rule and click **Finish**.



The image shows a 'Clone Rule' dialog box. It has a title bar with a close button. Inside, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'Avaya'. Below these fields is a 'Finish' button.

In the sample configuration, signaling rule **Avaya** was created for Session Manager to prevent certain headers in the SIP messages sent from the CS1000E and Session Manager from being propagated to Cincinnati Bell. Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE or UPDATE message. The following screen shows the **Alert-Info**, **P-Location**, and **x-nt-e164-clid** headers removed during the compliance test.



The image shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, SIP Cluster, Domain Policies, and Signaling Rules. The main area displays the 'Signaling Rules' for the 'Avaya' rule. It includes tabs for General, Requests, Responses, Request Headers, Response Headers, and Signaling QoS. The 'Request Headers' tab is active, showing a table of headers to be removed.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	
2	P-Location	ALL	Forbidden	Remove Header	Yes	IN	
3	x-nt-e164-clid	ALL	Forbidden	Remove Header	Yes	IN	

Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Profiles, SIP Cluster, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies, Device Specific Settings, Troubleshooting, TLS Management, and IM Logging. The main area is titled 'Domain Policies > Signaling Rules: Avaya'. It includes an 'Add Rule' button, a 'Filter By Device...' dropdown, and buttons for 'Rename Rule', 'Clone Rule', and 'Delete Rule'. Below these is a yellow bar with the text 'Click here to add a description.' and tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'Response Headers' tab is active, showing a table with columns: Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, and Direction. The table contains two rows of data.

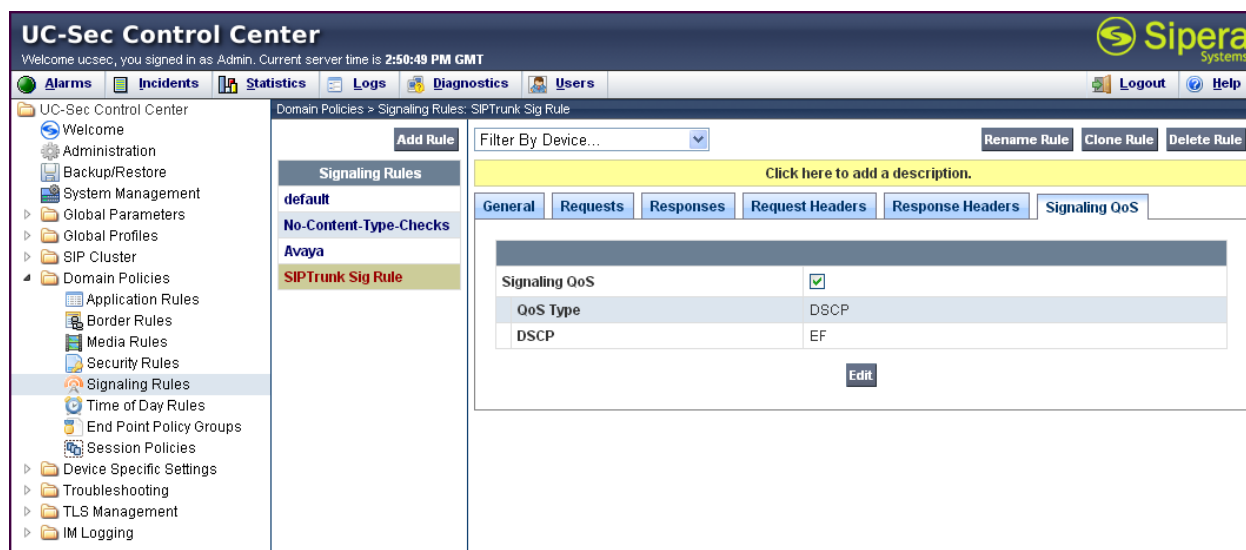
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction
1	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN
2	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN

On the **Signaling QoS** tab select the proper Quality of Service (QoS). The 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 signaling. The following screen shows the QoS values used for compliance testing.

The screenshot shows the UC-Sec Control Center interface. The left sidebar is the same as in the previous screenshot. The main area is titled 'Domain Policies > Signaling Rules: Avaya'. It includes an 'Add Rule' button, a 'Filter By Device...' dropdown, and buttons for 'Rename Rule', 'Clone Rule', and 'Delete Rule'. Below these is a yellow bar with the text 'Click here to add a description.' and tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'Signaling QoS' tab is active, showing a table with columns: Signaling QoS, QoS Type, and DSCP. The table contains two rows of data.

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

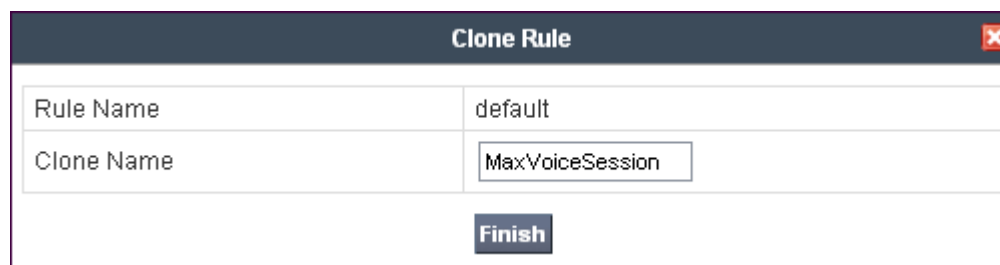
A separate signaling rule **SIPTrunk Sig Rule** was created for Cincinnati Bell eVantage IP Service by cloning the **default** signaling rule and changing the **Signaling QoS** parameters as shown below.



## 7.8. 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** (not shown). Enter a descriptive name for the new rule and click **Finish**.



Modify the rule by clicking the **Edit** button. 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 shows the UC-Sec Control Center interface. The left sidebar lists various configuration areas, with 'Domain Policies' expanded and 'Application Rules' selected. The main panel displays the 'MaxVoiceSession' rule configuration. It includes a table for application types and a miscellaneous section.

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.

## 7.9. 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 7.12**. Create a separate Endpoint Policy Group for the enterprise and the Cincinnati Bell eVantage IP Service.

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 for Endpoint Policy Groups. The left sidebar shows 'Domain Policies' expanded and 'End Point Policy Groups' selected. The main panel displays a list of existing policy groups and a table for the 'default-low' group.

**Policy Groups**

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc

**default-low**

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default	default	default-low-med	default-low	default	default	

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

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. Under 'Domain Policies', 'Enterprise\_DomPolicy' is selected. The main area displays 'Domain Policy for Avaya equipment'. A table lists policy groups with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and actions. The row for 'Enterprise\_DomPolicy' shows: Order 1, Application MaxVoiceSession, Border default, Media New-Low-Med, Security default-low, Signaling Avaya, Time of Day default.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	MaxVoiceSession	default	New-Low-Med	default-low	Avaya	default	

The following screen shows **SIP Trunk\_DomPolicy** created for Cincinnati Bell. Set the **Application**, **Media**, and **Signaling** rules to the one previously created for Cincinnati Bell. 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 is the same as the previous screenshot. Under 'Domain Policies', 'SIP Trunk\_DomPolicy' is selected. The main area displays 'Domain Policy for SIP Trunk Service Provider'. A table lists policy groups with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and actions. The row for 'SIP Trunk\_DomPolicy' shows: Order 1, Application MaxVoiceSession, Border default, Media New-Low-Med, Security default-high, Signaling SIPTrunk Sig Rule, Time of Day default.

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	MaxVoiceSession	default	New-Low-Med	default-high	SIPTrunk Sig Rule	default	



## 7.10. 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 includes a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of existing media interfaces.

Name	Media IP	Port Range		
Media_Inside	10.64.19.100	2048 - 5059		
Media_Outside_92	192.168.62.92	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 devices. The 'Updates' tab is active, and a red circle highlights the 'Restart' icon (a power button with a circular arrow) in the action column for the 'ASBCE' device.

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



## 7.11. 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.

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 2:39:33 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  
Policy Settings

Device Specific Settings > Signaling Interface: ASBCE

UC-Sec Devices  
ASBCE

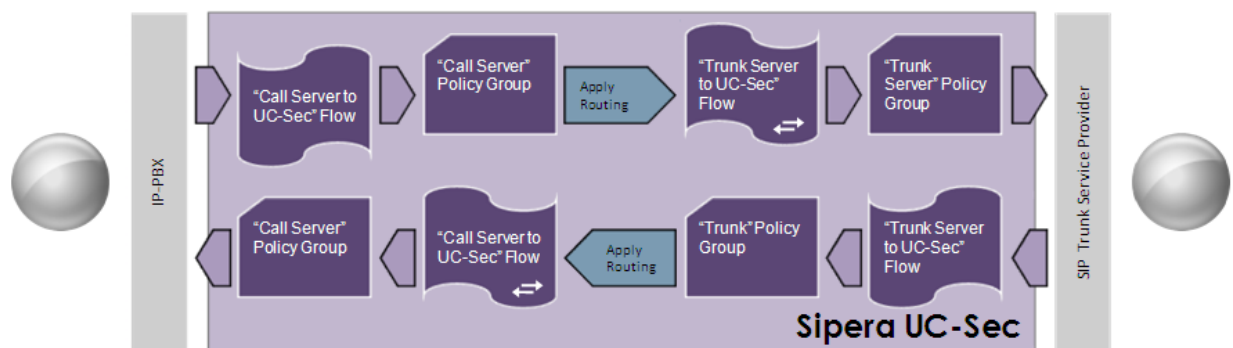
Signaling Interface

Add Signaling Interface

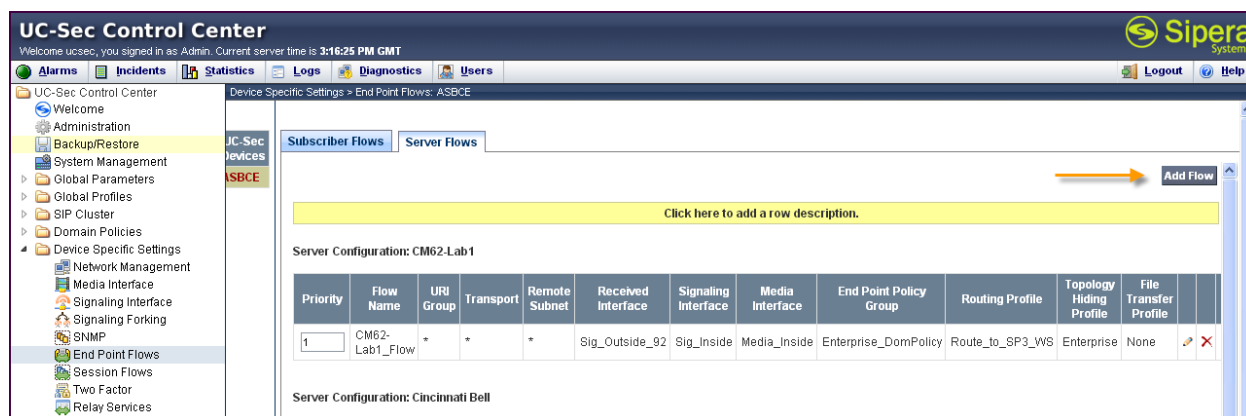
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Inside	10.64.19.100	5060	5060	---	None	
Sig_Outside_92	192.168.62.92	5060	5060	---	None	
Inside_TLS	10.64.19.100	---	---	5061	Avaya_tls_server	
Outside_TLS_92	192.168.62.92	---	---	5061	Avaya_tls_server	

## 7.12. 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 Avaya SBCE to secure a SIP Trunk call.



Create a Server Flow for Session Manager and Cincinnati Bell eVantage IP Service. 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 7.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 7.11** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.11** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.10** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy created in **Section 7.9** assigned to the Server Configuration.
- **Routing Profile:** Select the profile created in **Section 7.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile created in **Section 7.3** to apply toward the Server Configuration.

Click **Finish** to save and exit.

The following screen shows the Sever Flow for Cincinnati Bell eVantage IP Service:

**Edit Flow: CBT\_Flow**

Criteria	
Flow Name	CBT_Flow
Server Configuration	Cincinnati Bell
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside_92
Media Interface	Media_Outside_92
End Point Policy Group	SIP Trunk_DomPolicy
Routing Profile	Route_to_SM62-Lab1
Topology Hiding Profile	CBT SIP Trunk
File Transfer Profile	None

Finish

The following screen shows the Sever Flow for Session Manager:

**Edit Flow: SM62-Lab1-Flow**

Criteria	
Flow Name	SM62-Lab1-Flow
Server Configuration	SM62-Lab1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_92
Signaling Interface	Sig_Inside
Media Interface	Media_Inside
End Point Policy Group	Enterprise_DomPolicy
Routing Profile	Route_to_CBT
Topology Hiding Profile	Enterprise
File Transfer Profile	None

Finish

## 8. Cincinnati Bell eVantage IP Service Configuration

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

## 9. Verification

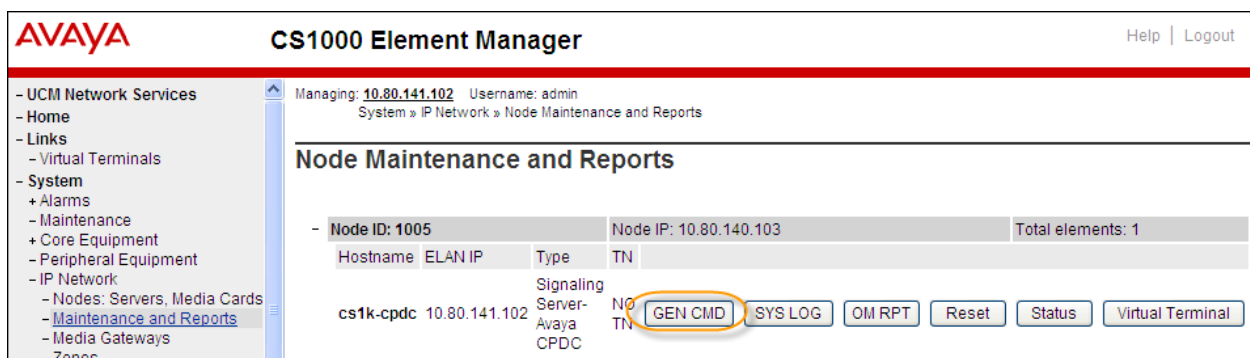
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

### 9.1. Avaya Communication Server 1000E Verification

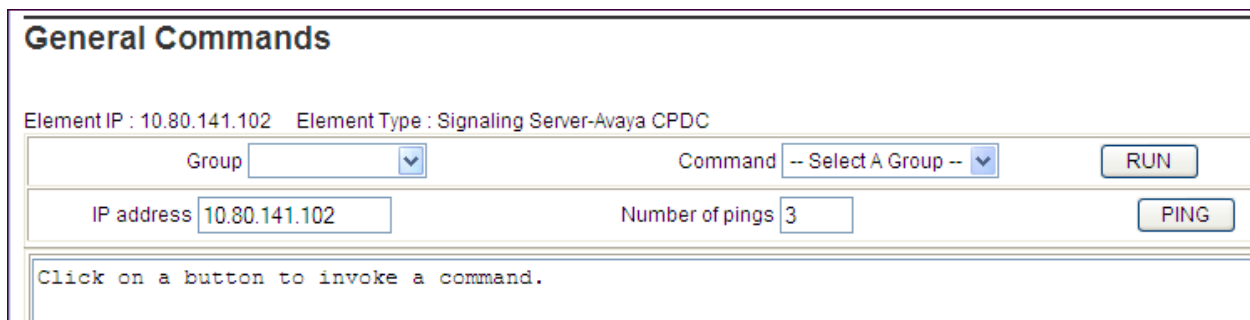
This section illustrates sample verifications that may be performed using the Avaya CS1000E Element Manager GUI.

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

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



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



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

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

### General Commands

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

Group Sip
Command SIPGwShow
Sip
RUN

IP address 10.80.141.102
Number of pings 3
PING

```

SIPNPM Status           : Active
Primary Proxy IP address : 10.64.19.150
Primary Proxy port       : 5060
Primary Proxy Transport  : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port     : 5060
Secondary Proxy Transport : TCP
Primary Proxy2 IP address : 10.64.19.250
Primary Proxy2 port      : 5060
Primary Proxy2 Transport : TCP
Active Proxy            : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 32 / 32
Stack version           : 5.5.0.13
TLS Security Policy      : Security Disabled

```

The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**. At the time this screen was captured, the SIP telephone with DN 7108 was involved in an active call with the Cincinnati Bell eVantage IP Service.

### General Commands

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

Group SipLine
Command sigSetShowAll
RUN

IP address 10.80.141.102
Number of pings 3
PING

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

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

### General Commands

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

Group Iset Command isetShow Range 0 500 RUN

IP address 10.80.141.102 Number of pings 3 PING

Set Information

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

Total sets = 2

### 9.1.2. System Maintenance Commands

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

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

## CS1000 Element Manager

Help | Logout

Managing: 10.80.141.102    Username: admin  
System » Maintenance

### Maintenance

☒ Select by Overlay    ☐ Select by Functionality

<Select by Overlay>

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

<Select Group>

- D-Channel Diagnostics
- MSDL Diagnostics
- TMDI Diagnostics

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

### D-Channel Diagnostics

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

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

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



## 9.2. Avaya Aura® Session Manager Verification

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

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

The screenshot shows the 'Call Routing Test' page in the Avaya System Manager. The breadcrumb trail at the top is 'Home / Elements / Session Manager / System Tools / Call Routing Test'. The page title is 'Call Routing Test'. Below the title is a description: 'This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.' The main section is 'SIP INVITE Parameters', which contains several input fields and dropdown menus: 'Called Party URI' (17205551997@avayalab.com), 'Calling Party URI' (5135555180@avayalab.com), 'Day Of Week' (Tuesday), 'Time (UTC)' (18:34), 'Called Session Manager Instance' (DenverSM), 'Calling Party Address' (10.80.140.103), 'Session Manager Listen Port' (5060), and 'Transport Protocol' (TCP). There is an 'Execute Test' button. Below the parameters section is the 'Routing Decisions' section, which displays the result: 'Route < sip:17205551997@avayalab.com > to SIP Entity Loc19-ASBCE (10.64.19.100). Terminating Location is Loc19-ASBCE.'

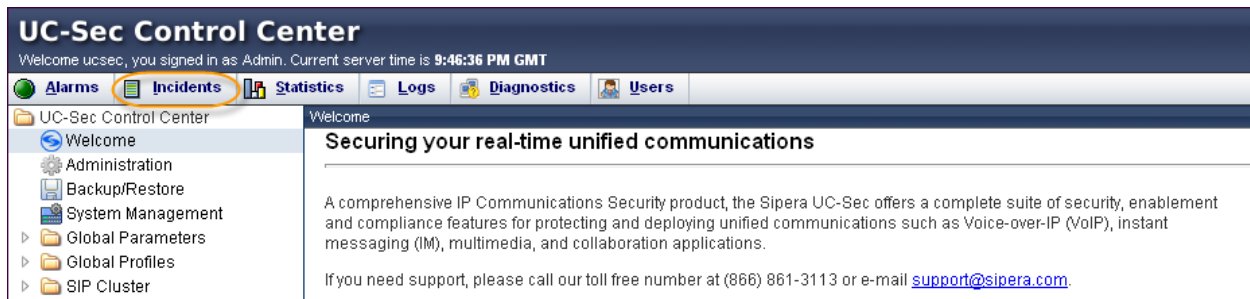
2. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
3. Verify that endpoints at the enterprise site can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

## 9.3. Avaya Session Border Controller for Enterprise Verification

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

### 9.3.1. 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:

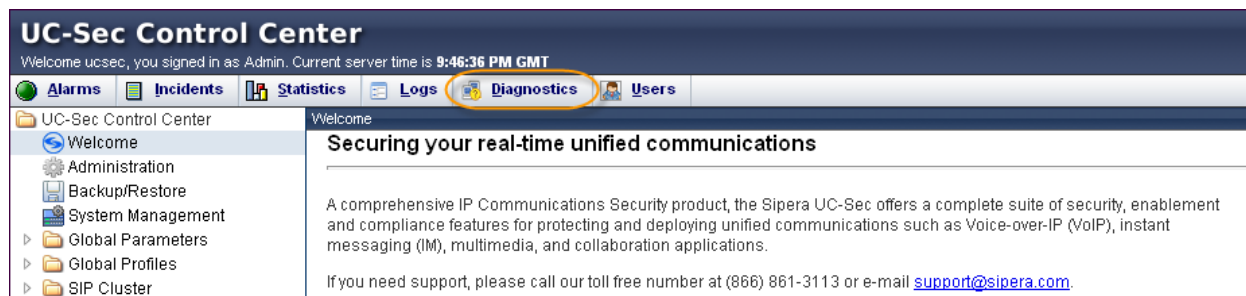
Displaying results 1 to 15 out of 102.

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

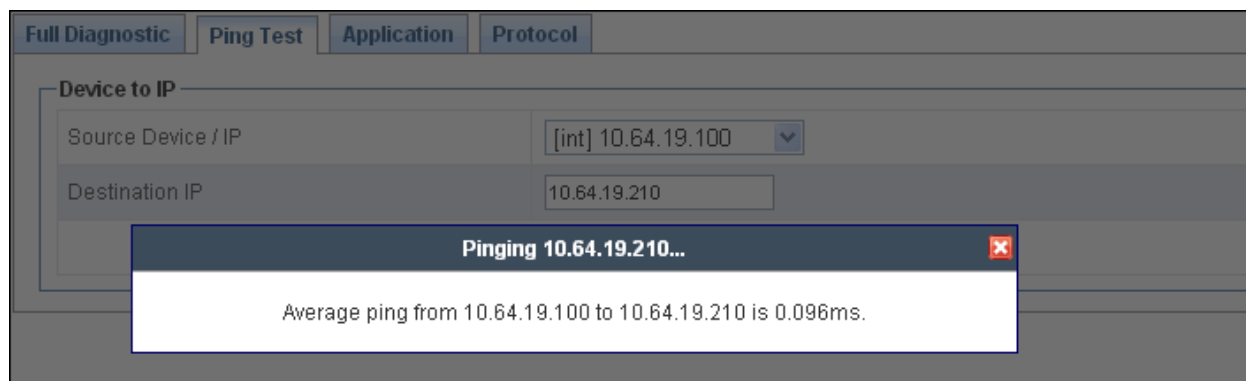
<< 1 2 3 4 5 >>

### 9.3.2. 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 Session Manager from the internal signaling interface of the Avaya SBCE.



### 9.3.3. 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 **1000**. The **Capture Filename** **CBT-A1.pcap** will be created once the **Start Capture** button is pressed.

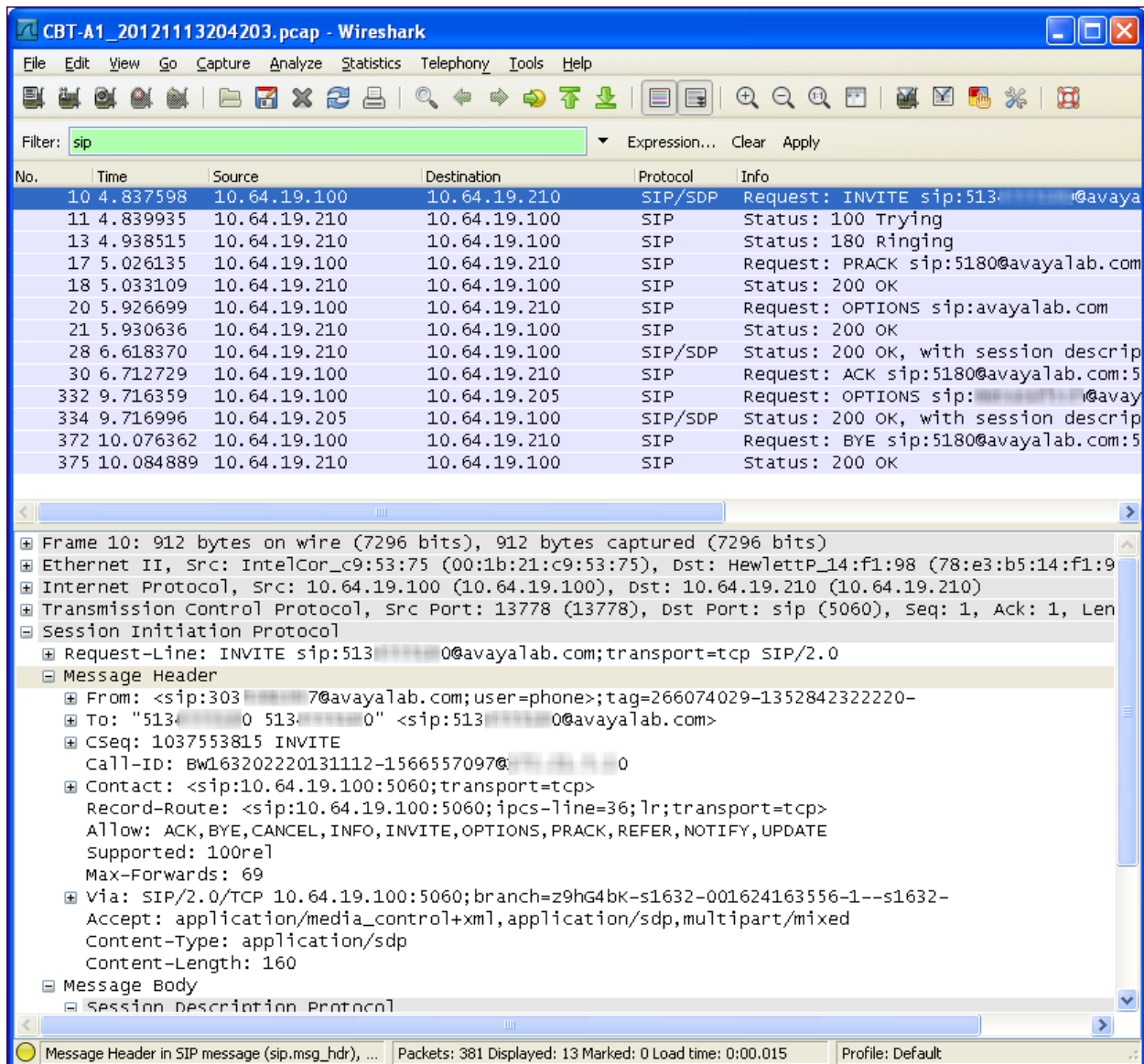
The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Profiles, SIP Cluster, Domain Policies, Device Specific Settings, Troubleshooting, and IM Logging. The 'Troubleshooting' category is expanded, showing 'Trace Settings' as the selected option. The main content area is titled 'Troubleshooting > Trace Settings: ASBCE'. It features a 'UC-Sec Devices' list with 'ASBCE' selected. Below this, there are tabs for 'Packet Trace', 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, displaying the 'Packet Capture Configuration' form. The form includes fields for 'Currently capturing' (No), 'Interface' (A1), 'Local Address (ip:port)' (All), 'Remote Address (\*, \*, port, ip, ip:port)' (\*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (1000), and 'Capture Filename' (CBT-A1.pcap). A 'Start Capture' button and a 'Clear' button are at the bottom of the form.

The following screen shows a completed packet capture.

The screenshot shows the UC-Sec Control Center interface with the 'Captures' tab selected. The 'UC-Sec Devices' list still shows 'ASBCE' selected. The 'Captures' tab displays a table of completed captures. A 'Refresh' button is located at the top right of the table. The table has columns for 'File Name', 'File Size (bytes)', and 'Last Modified'. One capture is listed: 'CBT-A1\_20121113204203.pcap' with a file size of 90,112 bytes and a last modified time of November 13, 2012 8:42:14 PM GMT. A red 'X' icon is visible in the rightmost column of the table row.

File Name	File Size (bytes)	Last Modified
<a href="#">CBT-A1_20121113204203.pcap</a>	90,112	November 13, 2012 8:42:14 PM GMT

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



## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise to the Cincinnati Bell eVantage IP Service. The Cincinnati Bell eVantage IP Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The Cincinnati Bell eVantage IP Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

## 11. Additional References

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

- [1] *Avaya Communication Server 1000E Installation and Commissioning*, November 2010, Document Number NN43041-310.
- [2] *Feature Listing Reference Avaya Communication Server 1000*, November 2010, Document Number NN43001-111, 05.01.
- [3] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [4] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, Document Number NN43001-125, 03.09 October 2011
- [5] *Installing and Configuring Avaya Aura® System Platform, Release 6.2.0*, March 2012.
- [6] *Administering Avaya Aura® System Platform, Release 6.2.0*, February 2012.
- [7] *Implementing Avaya Aura® System Manager*, Release 6.2, March 2012
- [8] *Installing Service Packs for Avaya Aura® Session Manager*, February 2012, Document Number 03-603863
- [9] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473.
- [10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315, 05.18 January 2012
- [11] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Document Number NN43170-600, Standard 04.02 December 2011

---

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

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

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