



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

---

# **Application Notes for Configuring Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0**

## **Abstract**

These Application Notes describe the procedure for configuring Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls were placed to and from the PSTN with various Avaya endpoints.

Hawaiian Telecom SIP Trunk service provides PSTN access via SIP trunks between the enterprise and Hawaiian Telecom's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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 .....	7
4.	Equipment and Software Validated .....	9
5.	Configure Avaya Communication Server 1000E .....	12
5.1.	Login to the CS1000 System .....	12
5.1.1.	Login to Unified Communications Management (UCM) and Element Manager .....	12
5.1.2.	Login to the Call Server Command Line Interface (CLI).....	15
5.2.	Administer a Node IP Telephony .....	16
5.2.1.	Obtain Node IP address .....	16
5.2.2.	Administer Terminal Proxy Server .....	17
5.2.3.	Administer Quality of Service (QoS) .....	18
5.2.4.	Synchronize the New Configuration.....	19
5.3.	Administer Voice Codec.....	20
5.3.1.	Enable Voice Codec, Node IP Telephony. ....	20
5.3.2.	Enable Voice Codec on Media Gateways.....	23
5.4.	Administer Zones and Bandwidth .....	25
5.4.1.	Create a zone for IP phones (zones 1 and 5).....	25
5.4.2.	Create a zone for virtual SIP trunks (zone 4).....	27
5.5.	Administer SIP Trunk Gateway.....	28
5.5.1.	Administer the SIP Trunk Gateway to Session Manager .....	30
5.5.2.	Administer Virtual D-Channel.....	32
5.5.3.	Administer Virtual Super-Loop .....	36
5.5.4.	Administer Virtual SIP Routes .....	36
5.5.5.	Administer Virtual Trunks.....	39
5.5.6.	Administer Calling Line Identification Entries.....	41
5.5.7.	Enable External Trunk to Trunk Transferring .....	43
5.6.	Administer Dialing Plans.....	43
5.6.1.	Define ESN Access Codes and Parameters (ESN) .....	43
5.6.2.	Associate NPA and SPN call to ESN Access Code 1 .....	44
5.6.3.	Digit Manipulation Block Index (DMI).....	45
5.6.4.	Route List Block (RLB).....	46
5.6.5.	Inbound Call Digit Translation .....	49
5.6.6.	Outbound Call - Special Number Configuration. ....	50
5.6.7.	Outbound Call - Numbering Plan Area Code (NPA) .....	52
5.7.	Administer Phone.....	52
5.7.1.	Phone creation.....	52
5.7.2.	Enable Privacy for Phone.....	54
5.7.3.	Enable Call Forward for the Phone.....	55

5.7.4.	Enable Call Waiting for the Phone .....	58
6.	Configure Session Manager .....	59
6.1.	System Manager Login and Navigation .....	60
6.2.	Specify SIP Domains .....	61
6.3.	Add Location .....	62
6.4.	Add Adaptation Module .....	62
6.5.	Add SIP Entities.....	66
6.6.	Add Entity Links.....	70
6.7.	Add Routing Policies .....	72
6.8.	Add Dial Patterns.....	73
6.9.	Add/View Session Manager .....	75
7.	Configure the Avaya Session Border Controller for Enterprise (Avaya SBCE).....	76
7.1.	Log in Avaya SBCE.....	76
7.2.	Global Profiles .....	77
7.2.1.	Server Interworking Avaya-SM.....	77
7.2.2.	Server Interworking SP-General.....	78
7.2.3.	Routing Profiles .....	79
7.2.4.	Server Configuration.....	81
7.2.5.	Topology Hiding .....	84
7.2.6.	Signaling Manipulation.....	86
7.3.	Domain Policies .....	88
7.3.1.	Create Application Rules .....	88
7.3.2.	Media Rules .....	89
7.3.3.	Signaling Rules .....	90
7.3.4.	End Point Policy Groups.....	92
7.4.	Device Specific Settings .....	94
7.4.1.	Network Management.....	94
7.4.2.	Media Interface .....	95
7.4.3.	Signaling Interface .....	96
7.4.4.	End Point Flows.....	97
8.	Hawaiian Telecom SIP Trunk Service Configuration .....	100
9.	Verification Steps.....	100
9.1.	General.....	100
9.2.	Verify Call Establishment on the CS1000 Call Server.....	101
9.3.	Protocol Traces .....	102
10.	Conclusion .....	104
11.	References.....	105

# 1. Introduction

These Application Notes provide the procedure for configuring Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2. During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between the Hawaiian Telecom network and Avaya Communication Server 1000E.

In the sample configuration, the Avaya solution consists of a Communication Server 1000E Rel. 7.5 (hereafter referred to as CS1000), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.2 (hereafter referred to as Avaya SBCE), and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE or Session Manager.

## 2. General Test Approach and Test Results

The CS1000 system was connected to the Avaya SBCE via SIP trunks to Session Manager. The Avaya SBCE was connected to the Hawaiian Telecom network via SIP trunks. Various call types were made from the CS1000 to Hawaiian Telecom's network and vice versa to verify interoperability between the CS1000 and the Hawaiian Telecom network.

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 for 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

The focus of this test was to verify that the CS1000 can interoperate with the Hawaiian Telecom network. The following interoperability areas were covered:

- SIP trunk registration with the service provider
- Incoming calls from the PSTN were routed to DID numbers assigned by Hawaiian Telecom. Incoming PSTN calls were terminated to the following Avaya Endpoints: Avaya 1100 Series IP Telephones (SIP), Avaya 1100 Series IP Telephones (UniStim), Avaya M3904 Digital Telephones, Avaya 2050 IP Softphone, Analog Telephones and Fax machines.
- Outgoing calls to the PSTN were routed via Hawaiian Telecom's network.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect during normal active call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voicemail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codecs G.711u, G.711a and G.729 with Voice Activity Detection (VAD) disabled.

- Voicemail and DTMF tone support in both directions (RFC2833) (Leaving voicemail, retrieving voicemail, etc.).
- CallPilot Voicemail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with Interactive Voice Response systems (IVR).
- International calls.
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Call Park.
- Consultative Call transfers.
- Station Conference.
- T.38 fax support.
- G.711u fax pass-through support.
- Long duration calls (one hour).
- Early Media transmission.

## 2.2. Test Results

Interoperability testing of Hawaiian Telecom SIP Trunk Service with the CS1000 solution was completed successfully with the following observations/limitations.

- **Calling Name and Calling Number Delivery to PSTN:** On outbound calls from the CS1000 to the PSTN the “Calling Name” is not delivered to the PSTN phone (is not displayed), only the “Calling Number” is delivered (is displayed).
- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and the Hawaiian Telecom network when there is no call re-direction involved. However, when a call is re-directed to the PSTN at the CS1000 extension, the Caller ID will not properly reflect the true originator of the call. In normal conditions if a call is re-directed at the CS1000 to a PSTN extension, the Caller ID displayed at the PSTN extension will be of the extension doing the re-direction (i.e., transferee) and not the Caller ID of the extension that originated the call.
- **T.38 Fax:** T.38 fax from the CS1000 to the PSTN (outbound) is not supported by Hawaiian Telecom; Hawaiian Telecom only supports T.38 fax from the PSTN to the CS1000 (inbound). Fax calls from the CS1000 to the PSTN (outbound) defaulted to G.711 pass-through. G.711 pass-through for fax was successfully tested in both directions (CS1000 → PSTN and PSTN → CS1000).
- **SIP Header Optimization:** SIP header rules were implemented in Avaya SBCE and in Session Manager to streamline the SIP header and remove any unnecessary parts. The following headers were removed: X\_nt\_e164\_clid, Alert-Info if they were present in the INVITE. Also the multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-nt-esn5-frag-hex, and x-nt-epid-frag were stripped out. These particular headers and MIME have no real use in the service provider network. If an issue is being investigated on the service provider network, the presence of these headers may add unnecessary confusion.

- **Calls to Busy Numbers:** Hawaiian Telecom's network is not sending "486 Busy Here" for calls from the CS1000 to Busy PSTN numbers. Since Busy Tone is heard by the user this observation is considered non critical.
- **Displays on Held Calls:** If a CS1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed, instead the access code for the trunk route (ACOD) is displayed. This is a Communication Server 1000 known issue.
- **Items not supported or not tested included the following:**
  - Off-net call forwarding was not tested with the History-Info method. Testing was done with an Adaptation in Session Manager to convert History-Info to Diversion header.
  - Inbound toll-free calls.
  - 0, 0+10, 911

## 2.3. Support

For support on Hawaiian Telecom systems, call:

Toll Free at: 1-808-643-0944 or visit the corporate Web page at:

<https://www.hawaiiantel.com/business/Business.aspx>

### 3. Reference Configuration

**Figure 1** below illustrates the test configuration used. The test configuration simulates an enterprise site with the Avaya components connected to Hawaiian Telecom's SIP Trunk Service through the Public Internet.

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

- Avaya Communication Server 1000E (CS1000E).
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise.
- Avaya 1100-Series IP Telephones (UniStim).
- Avaya 1100-Series Telephones (SIP).
- 2050 Avaya IP Softphone.
- Avaya M3904 Digital telephones.
- Analog Telephones.
- Fax machines.
- Desktop with administration interfaces.

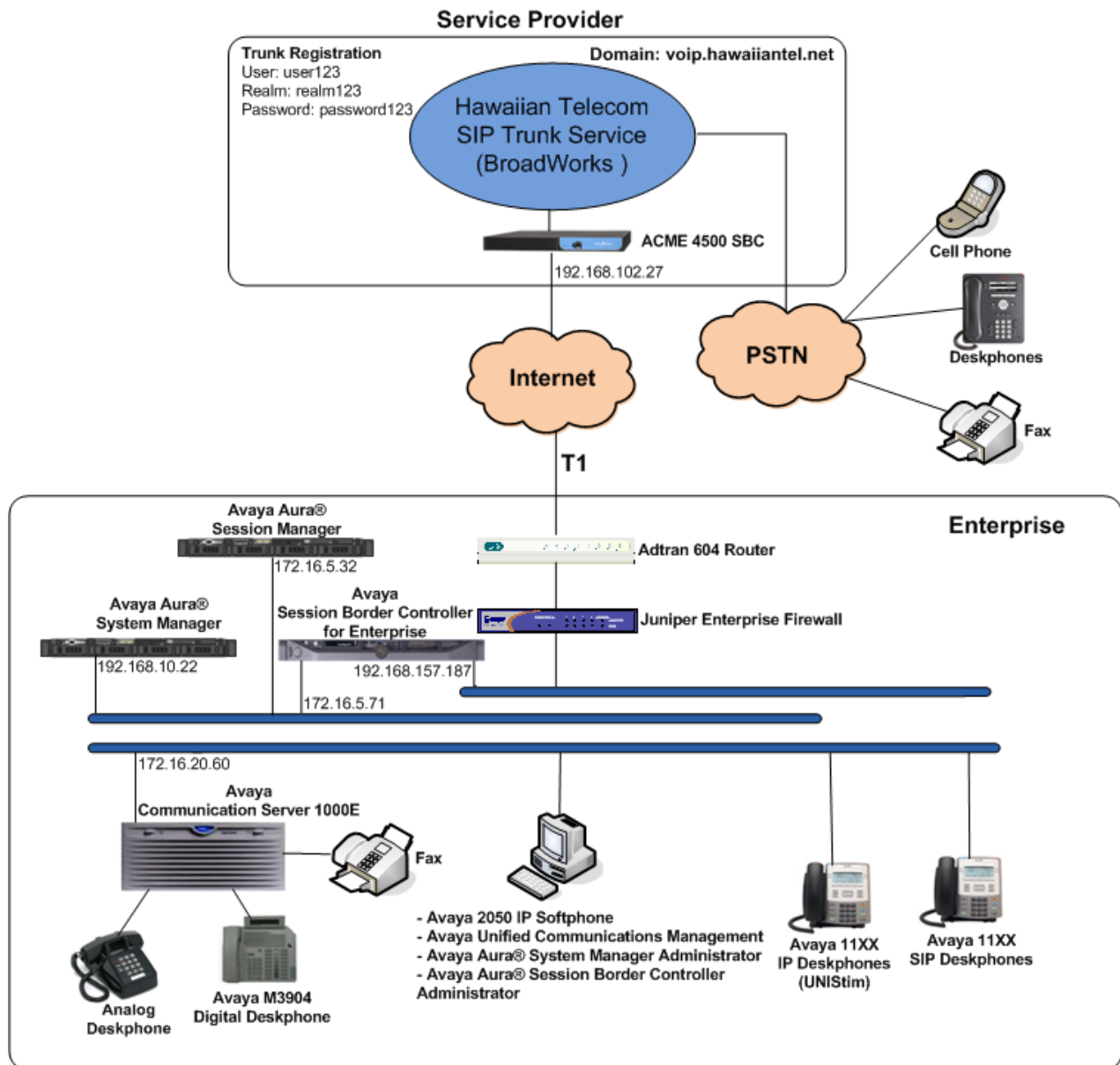
Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Hawaiian Telecom across the public IP network is SIP over UDP. The transport protocol between the Avaya SBCE and Session Manager across the enterprise IP network is SIP over TCP. The transport protocol between Session Manager and the CS1000 across the enterprise IP network is SIP over TLS. For ease of troubleshooting during testing, the compliance test was conducted with the Transport Method set to UDP between Session Manager and the CS1000.

For security reasons, any actual public IP addresses used in the configuration have been masked. Similarly, any references to real routable DID and PSTN numbers have also been masked to numbers that cannot be routed by the PSTN.

One SIP trunk group was created between the CS1000 and Session Manager to carry the traffic to and from the service provider (two-way trunk group).

For inbound calls, the calls flowed from Hawaiian Telecom's network to the Avaya SBCE and then to Session Manager. Session Manager used the configured dial patterns and routing policies to determine the recipient (in this case the CS1000) and on which link to send the call. Once the call arrived at the CS1000, further incoming call treatment, such as incoming digit translations and class of service restrictions were performed.

Outbound calls to the PSTN were first processed by the CS1000 for outbound treatment through the Electronic Switched Network and class of service restrictions. Once the CS1000 selected the proper SIP trunk; the call was routed to Session Manager. Session Manager once again used the configured dial patterns, adaptations, and routing policies to determine the route to the Avaya SBCE for egress to Hawaiian Telecom's network.



**Figure 1: Hawaiian Telecom SIP Trunk service with Avaya CS1000E**



## 4. Equipment and Software Validated

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

<b>Avaya:</b>	
<b>Equipment</b>	<b>Release/Version</b>
Avaya Communication Server 1000E running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	Call Server: 7.50 Q + DepList 1: core Issue: 01 ( <b>created: 2013-03-19 16:44:12 (est)</b> )  Signaling Server: 7.50.17.00  **See Service Updates & Patches below**
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1 (6.3.1.0.631004)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1 Build No. 6.3.0.8.5682-6.3.8.859 Software Update Rev. No. 6.3.1.9.1212
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.0.Q36
Avaya Deskphones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.02.0062
Lucent Analog Phone	N/A
Fax Machines	N/A
<b>Hawaiian Telecom:</b>	
<b>Equipment</b>	<b>Release/Version</b>
BroadWorks	17 SP3
ACME Session Border Controller (4500)	SCX 6.2.0 MR11

### Signaling Server Service Updates & Patches:

**Note:** The **VTRK** SU version should be “cs1000-vtrk-7.50.17.16-**20**.i386.000.ntl” or higher on all Signaling Servers to ensure proper operation of blind transfer feature. Patch **p30224\_1** is required if problems with **SIP UPDATE** are observed during Call Redirection scenarios. Patch **p27159\_1** is required for T.38 fax support.

#### SUs:

avaya-cs1000-cnd-4.0.20-00.i386.000  
cs1000-dbcom-7.50.17.16-1.i386.000

```

ipsec-tools-0.6.5-14.el5.3_avaya_1.i386.000
cs1000-shared-pbx-7.50.17.16-1.i386.000
cs1000-kcv-7.50.17.16-1.i386.000
cs1000-baseWeb-7.50.17.16-2.i386.000
cs1000-ipsec-7.50.17.16-1.i386.000
cs1000-linuxbase-7.50.17.16-15.i386.000
cs1000-patchWeb-7.50.17.16-11.i386.000
cs1000-ncs-7.50.17.16-1.i386.000|Start:ncs
spiritAgent-6.1-1.0.0.108.208.i386.000
cs1000-dmWeb-7.50.17.16-7.i386.000
cs1000-Jboss-Quantum-7.50.17.16-33.i386.000
cs1000-sps-7.50.17.16-12.i386.000
cs1000-cs1000WebService_6-0-7.50.17.16-1.i386.000
tzdata-2011h-2.el5.i386.000
cs1000-csoneksvrmgr-7.50.17.16-1.i386.000
cs1000-csmWeb-7.50.17.16-6.i386.000
cs1000-emWeb_6-0-7.50.17.16-34.i386.000
cs1000-tps-7.50.17.16-29.i386.000
cs1000-ftpkg-7.50.17.16-12.i386.000
cs1000-pd-7.50.17.16-2.i386.000
cs1000-EmCentralLogic-7.50.17.16-2.i386.000
cs1000-bcc-7.50.17.16-87.i386.000
cs1000-mscAttn-7.50.17.16-6.i386.000
cs1000-mscAnnc-7.50.17.16-16.i386.000
cs1000-emWebLocal_6-0-7.50.17.16-3.i386.000
cs1000-mscConf-7.50.17.16-4.i386.000
cs1000-mscMusc-7.50.17.16-17.i386.000
cs1000-mscTone-7.50.17.16-4.i386.000
cs1000-vtrk-7.50.17.16-168.i386.000
#####
Patches:
p30224_1
p27159_1
p31484_1
#####

```

## **Loadware:**

LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 11

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	Q01981776	ISS1:1OF1	udtcab17	09/04/2013	udtcab17.lw
01	Q01820502	ISS1:1OF1	MGCMAB01	13/02/2012	MGCMAB01.LW
02	WI00998702	ISS1:1OF1	MGCCCD03	09/04/2013	MGCCCD03.LW
05	wi00839337	ISS1:1OF1	DSP1AB06	08/02/2012	DSP1AB06.LW
06	wi00839337	ISS1:1OF1	DSP2AB06	08/02/2012	DSP2AB06.LW
07	wi00839337	ISS1:1OF1	DSP3AB06	08/02/2012	DSP3AB06.LW
08	wi00839337	ISS1:1OF1	DSP4AB06	08/02/2012	DSP4AB06.LW
09	wi00839337	ISS1:1OF1	DSP5AB06	08/02/2012	DSP5AB06.LW
10	wi00946113	ISS1:1OF1	MGCBBA15	08/02/2012	MGCBBA15.LW
11			mgcfaa19	08/02/2012	MGCFAA19.LD
12	wi00946109	ISS1:1OF1	MGCABA15	08/02/2012	MGCABA15.L

In addition to applying the latest Call Server patches, Signaling Server Service updates and patches listed above, the following procedure should be followed to ensure proper operation of Call Transfers from the CS1000 to the PSTN.

**Enable Plug-Ins 201 and 501** as follows:

Login to the **Unified Communications Management (UCM) and Element Manager** as described in **Section 5.1.1**, go to **System → Software → Plug-ins**, select **plug-in 201** and click the **Enable** button, the status will change to **Enabled**; do the same for **plug-in 501**.

ENABLED PLUGINS : 2

PLUGIN	STATUS	PRS/CR_NUM	MPLR_NUM	DESCRIPTION
<b>201</b>	<b>ENABLED</b>	Q00424053	MPLR08139	PI:Cant XFER OUTG TRK TO OUTG TRK
<b>501</b>	<b>ENABLED</b>	Q02138637	MPLR30070	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end

## 5. Configure Avaya Communication Server 1000E

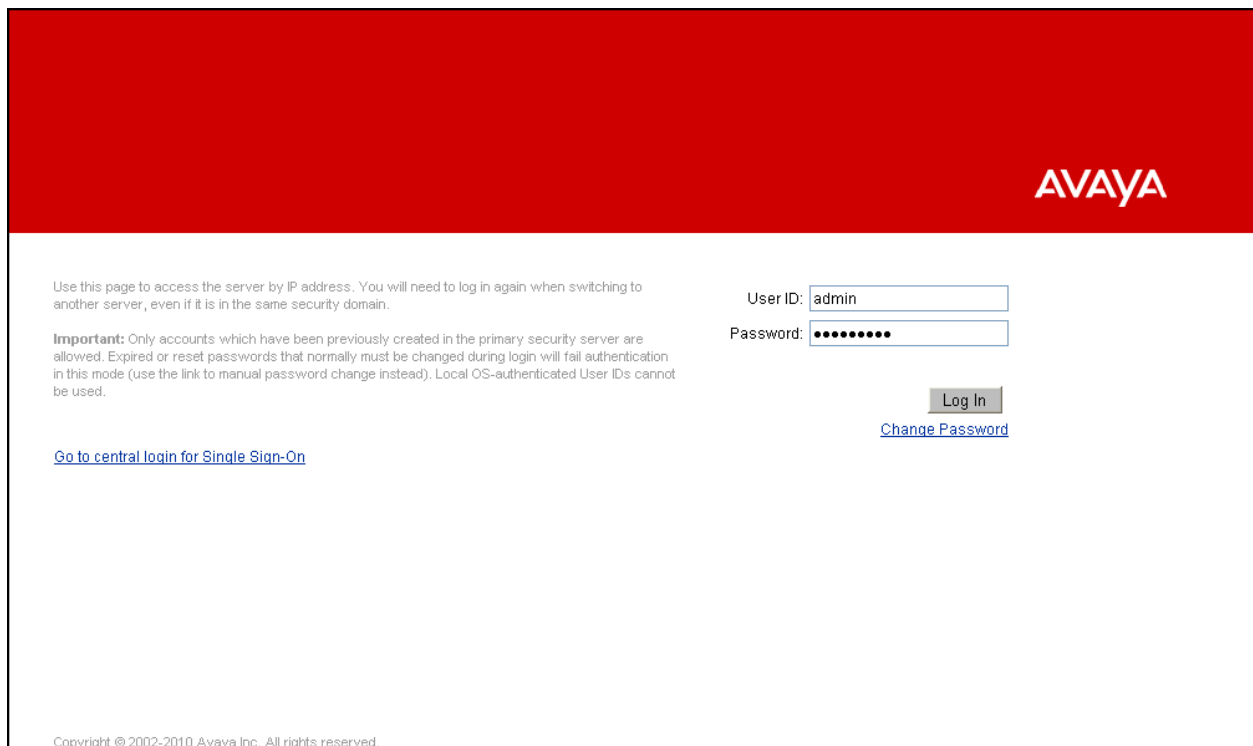
These Application Notes assume that the basic configuration of the CS1000 has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11**.

The procedures shown below describe the configuration details of the CS1000 with SIP trunks to the Hawaiian Telecom network.

### 5.1. Login to the CS1000 System

#### 5.1.1. Login to Unified Communications Management (UCM) and Element Manager

Open an instance of a web browser and connect to the UCM GUI at the following address: <http://<UCM IP address>> Log in using an appropriate Username and Password.

The image shows the Avaya UCM login page. It has a red header with the 'AVAYA' logo in white. Below the header, there is a login form. On the left, there is a paragraph of text: 'Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.' Below this is an 'Important' note: '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.' Below the important note is a link: 'Go to central login for Single Sign-On'. On the right side of the page, there are two input fields: 'User ID:' with the value 'admin' and 'Password:' with a masked password '••••••••'. Below these fields is a 'Log In' button and a link 'Change Password'. At the bottom left, there is a copyright notice: 'Copyright © 2002-2010 Avaya Inc. All rights reserved.'

The **Unified Communications Management** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in the red box shown below.

**AVAYA**

Avaya Unified Communications Management

[Help](#) | [Logout](#)

- Network
  - Elements
    - CS 1000 Services
      - IPSec
      - Patches
      - SNMP Profiles
      - Secure FTP Token
    - Software Deployment
  - User Services
    - Administrative Users
    - External Authentication
    - Password
  - Security
    - Roles
    - Policies
    - Certificates
    - Active Sessions
  - Tools
    - Logs
    - Data

Host Name: 172.16.20.60    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
1 <input type="checkbox"/>	EM on cs1k	CS1000	7.5	172.16.21.61	New element.
2 <input type="checkbox"/>	cs1k.avaya.lab.com (primary)	Linux Base	7.5	172.16.20.61	Base OS element.
3 <input type="checkbox"/>	MGC	Media Gateway Controller	7.5	172.16.21.62	Media Gateway Controller

Copyright 2002-2010 Avaya Inc. All rights reserved.

The CS1000 Element Manager **System Overview** page is displayed as shown below.

**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

**- Phones**

- Templates
- Reports
- Views
- Lists
- Properties
- Migration

**- Tools**

- + Backup and Restore
- Date and Time
- + Logs and reports

**- Security**

- + Passwords
- + Policies
- + Login Options

Managing: **172.16.21.61** Username: admin  
System Overview

### System Overview

IP Address: 172.16.21.61  
Type: Avaya Communication Server 1000E CPMG128 Linux  
Version: 4421  
Release: 750 Q +

Copyright © 2002-2012 Avaya Inc. All rights reserved.

### 5.1.2. Login to the Call Server Command Line Interface (CLI)

Using Putty, login to the Signaling Server with the admin account. Run the command “cslogin” and “logi” with the appropriate admin account and password, as shown below.

```
===== PUTTY log 2012.03.26 11:44:22 =====
login as: admin

                Avaya Inc. Linux Base 7.50
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@172.16.20.60's password:
Last login: Mon Mar 26 12:15:09 2012 from 172.16.5.250
[]0;admin@cs1k:~>[]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authenticating

TTY 15 SCH MTC BUG OSN 12:18
OVL111 IDLE 0
>logi
USERID? admin
PASS?
.
TTY #15 LOGGED IN ADMIN 12:18 26/3/2012

>
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only to
authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.

OVL000
>
```

## 5.2. Administer a Node IP Telephony

This section describes how to configure a Node IP Telephony on the CS1000.

### 5.2.1. Obtain Node IP address

These Application Notes assume that the basic configuration has already been done and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 1006) in the CS1000 IP network to work with the Hawaiian Telecom network.

Select **System** → **IP Network** → **Nodes: Servers, Media Cards**. Following is the display of the **IP Telephony Nodes** page. Then click on the Node ID of the CS1000 Element (i.e., 1006).

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.81 Username: admin  
System > IP Network > IP Telephony Nodes

**IP Telephony Nodes**  
Click the Node ID to view or edit its properties.

Print | Refresh

<input type="checkbox"/> Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 1006	1	SIP Line, LTPS, IP Media Services, Gateway (SIPGw)	-	172.16.20.60		Synchronized

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



The **Node Details** screen is displayed below with the IP address of the CS1000 node. 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 “172.16.20.60”. This IP address will be needed when configuring Session Manager with a SIP Entity for the Avaya CS1000 in **Section 6.5**.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))

Node ID: 1006 \* (0-9999)

Call server IP address: 172.16.21.61 \* TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

**Embedded LAN (ELAN)** Gateway IP address: 172.16.21.254 \* Subnet mask: 255.255.255.0 \*

**Telephony LAN (TLAN)** Node IPv4 address: 172.16.20.60 \* Subnet mask: 255.255.255.0 \*

Node IPv6 address:

\* Required Value. [Save] [Cancel]

**Associated Signaling Servers & Cards**

Select to add [Add] [Remove] [Make Leader] [Print] [Refresh]

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

## 5.2.2. Administer Terminal Proxy Server

Continue from **Section 5.2.1**. On the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown below.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))

Subnet mask: 255.255.255.0 \* Node IPv6 address:

**IP Telephony Node Properties**

- Voice Gateway (V/GW) and Coders
- 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]

**Associated Signaling Servers & Cards**

Select to add [Add] [Remove] [Make Leader] [Print] [Refresh]

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

The **UNISim Line Terminal Proxy Server (LTPS) Configuration Details** screen is displayed below. Check the **Enable proxy service on this node** check box and then click **Save**.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > UNISim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 1006 - 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  
Options: ☐ Client authentication  
☐ Periodic re-keying

**Network Connect Server**

Primary network connect server (TL & M) IP address: 0.0.0.0

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

Save Cancel

Copyright © 2002-2012 Avaya Inc. All rights reserved.

### 5.2.3. Administer Quality of Service (QoS)

Continue from **Section 5.2.2**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown below.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway (SIPGw))

Subnet mask: 255.255.255.0 \* Node IPv6 address:

**IP Telephony Node Properties**

- Voice Gateway (VGW) and Coders
- 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

**Associated Signaling Servers & Cards**

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

The **Quality of Service (QoS)** screen shown below will be displayed. Accept the default Diffserv values. Click the **Save** button.

**AVAYA** CS1000 Element Manager Help | Logout

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > Quality of Service (QoS)

Node ID: 1006 - Quality of Service (QoS)

**Diffserv Codepoint (DSCP)**

Enable Avaya automatic QoS: ☐

Control packets: 40 (0-63)  
Voice packets: 46 (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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

#### 5.2.4. Synchronize the New Configuration

Continue from **Section 5.2.3**, return to the **Node Details** page shown below and click on the **Save** button. The **Node Saved** screen is displayed (not shown). Click on the **Transfer Now** button (not shown). The **Synchronize Configuration Files** screen is displayed (not shown). Check the **Signaling Server** check box and click on the **Start Sync** button (not shown). When the synchronization completes, check the **Signaling Server** check box and click on the **Restart Applications** (not shown).

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

Managing: Network Services - User Name: admin  
System > IP Network > IP Telephony Nodes > Node Details

**Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))**

Node ID:  \* (0-9999)

Call server IP address:  \*

TLAN address type: ☒ IPv4 only  
☐ IPv4 and IPv6

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

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

\* Required Value. Save Cancel

**Associated Signaling Servers & Cards**

Select to add    Print | Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

## 5.3. Administer Voice Codec

This section describes how to configure Voice Codecs on the CS1000.

### 5.3.1. Enable Voice Codec, Node IP Telephony.

Select **IP Network** → **Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of the CS1000 system (not shown). The **Node Details** screen is displayed. On the **Node Details** page shown below, click on **Voice Gateway (VGW) and Codecs**.

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

Managing: Network Services - User Name: admin  
System > IP Network > IP Telephony Nodes > Node Details

**Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))**

Subnet mask:  \*

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

**Associated Signaling Servers & Cards**

Select to add    Print | Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

The **Voice Gateway (VGW) and Codec** screen is displayed below. Hawaiian Telecom supports **G711u**, **G.711a** and **G.729** Codecs with **Voice Activity Detection (VAD)** disabled.

The values for the **G711** Voice Codec is shown below, ensure that **Voice Activity Detection (VAD)** is unchecked.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > VGW and Codecs

Node ID: 1006 - Voice Gateway (VGW) and Codecs

General | Voice Codes | Fax

☒ V.21 Fax tone detection  
☐ R factor calculation

**Voice Codes**

Codec G711: ☒ Enabled (required)  
Voice payload size: 20 (milliseconds per frame)  
Voice playback (jitter buffer) delay: 40 80 (milliseconds)  
Nominal Maximum  
Maximum delay may be automatically adjusted based on nominal settings.  
☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled  
Voice payload size: 20 (milliseconds per frame)  
Voice playback (jitter buffer) delay: 40 80 (milliseconds)  
Nominal Maximum  
Maximum delay may be automatically adjusted based on nominal settings.

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

The values for the **G729** Voice Codec are shown below; ensure that **Codec G729** is checked and **Voice Activity Detection (VAD)** is unchecked as shown below.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > VGW and Codecs

Node ID: 1006 - Voice Gateway (VGW) and Codecs

General | Voice Codes | Fax

Codec G729: ☒ Enabled  
Voice payload size: 20 (milliseconds per frame)  
Voice playback (jitter buffer) delay: 40 80 (milliseconds)  
Nominal Maximum  
Maximum delay may be automatically adjusted based on nominal settings.  
☐ Voice Activity Detection (VAD)

Codec G723.1: ☐ Enabled  
Voice payload size: 30 (milliseconds per frame)  
Voice playback (jitter buffer) delay: 60 120 (milliseconds)  
Nominal Maximum  
Maximum delay may be automatically adjusted based on nominal settings.  
Coding rate: 5.3 (kbps)

**Fax**  
Codec name: T.38 FAX

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

For Fax over IP, **T.38** was used as the default and **G.711u pass-through** was set as fallback. **T.38** with payload size **30ms** was chosen as the default codec for fax. During the testing **T.38** fax transport worked successfully for fax calls from the PSTN to the CS1000 (inbound), for fax calls from the CS1000 to the PSTN (outbound), calls defaulted to **G.711u pass-through** (Refer to Section 2.2).

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > VGW and Codecs

**Node ID: 1006 - Voice Gateway (VGW) and Codecs**

General | Voice Codecs | Fax

Codec G723.1: ☐ Enabled  
Voice payload size: 30 (milliseconds per frame)  
Voice playout (jitter buffer) delay: 60 120 (milliseconds)  
Nominal Maximum  
Maximum delay may be automatically adjusted based on nominal settings.  
Coding rate: 5.3 (kbps)

**Fax**

Codec name: T.38 FAX  
Maximum rate: 14400 (bps)  
Fax TCF method: 2  
Fax playout nominal delay: 100 (0 - 300 milliseconds)  
FAX no activity timeout: 20 (10 - 32000 milliseconds)  
Packet size: 30 (bps)

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

Scroll to the top of the page and ensure that **Modem/Fax Pass Through** and **V.21** are checked.

AVAYA CS1000 Element Manager

Managing: 172.16.21.81 Username: admin

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

Node ID: 1006 - 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 (squench 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 (jitter buffer) delay: 40 (milliseconds)

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

Save Cancel

Click on **Save** and **Synchronize** as described in **Section 5.2.4**.

### 5.3.2. Enable Voice Codec on Media Gateways.

From the left menu of the Element Manager page, select the **IP Network** → **Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on the **IPMG** (not shown) and the **IPMG Property Configuration** page is displayed (not shown). Click **next** (not shown) and scroll down to the Codec **G711**, uncheck **VAD** for codec **G711**. Check Codec **G729A** and uncheck **VAD** for codec **G729A** as shown below. Scroll down to the bottom of the page and click **Save** (not shown).

AVAYA CS1000 Element Manager

Help | Logout

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

Dialing and Numbering Plans

Phones

Tools

Security

Codec name: G711

Voice payload size: 20 (ms/frame)

Voice playout (jitter buffer) nominal delay: 40

Modifications may cause changes to dependent settings

Voice playout (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 playout (jitter buffer) nominal delay: 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay: 80

Modifications may cause changes to dependent settings

VAD ☐

+ Codec: G723.1 Select ☐

+ Codec: T38 FAX Select ☒

+ QoS

+ Media Based CLID

+ Call Server LAN

Embedded LAN (ELAN) configuration

For Fax over IP, **T.38** was used as the default and **G.711u pass-through** was set as fallback. During the testing, **T.38** fax transport worked successfully for fax calls from the PSTN to the CS1000 (inbound), but for fax calls from the CS1000 to the PSTN (outbound), calls defaulted to **G.711u pass-through** (Refer to **Section 2.2**).

Under **VGW and IP phone codec profile** ensure that **Enable V.21 FAX tone detection** and **Enable modem fax pass through mode** are checked. T.38 with payload size **30ms** was chosen.

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

**- 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
  - + Dialing and Numbering Plans
  - + Phones
  - + Tools
  - + Security

**- 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 (squelch 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: G.711 ☒ Select

+ Codec: G.729A ☒ Select



## 5.4. Administer Zones and Bandwidth

This section describes the steps to create bandwidth zones to be used by IP sets and SIP Trunks: **zones 1 and 5** are used by IP sets and **zone 4** is used by SIP Trunks.

### 5.4.1. Create a zone for IP phones (zones 1 and 5)

The following figures show how to configure a zone for IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference. Select **IP Network** → **Zones** from the left pane, then click on **Bandwidth Zones** as shown below.

The screenshot displays the Avaya CS1000 Element Manager web interface. On the left, a navigation pane lists various system components, with 'Zones' selected under the 'IP Network' category. The main content area is titled 'Zones' and provides a brief overview: 'Zones are used to group related information for either bandwidth or dial plan numbering purposes.' Two sub-sections are visible: 'Bandwidth Zones', which is highlighted with a red rectangular box and described as being used for alternate routing and bandwidth management, and 'Numbering Zones', described as being used to route calls through a centralized call server. The top of the interface includes the Avaya logo, the product name 'CS1000 Element Manager', and user session details: 'Managing: 172.16.21.61 Username: admin System > IP Network > Zones'. The bottom of the page shows a copyright notice: 'Copyright © 2002-2012 Avaya Inc. All rights reserved.'

Click **Add** (not shown), select the values shown below and click on the **Save** button.

- **INTRA\_STGY**: Bandwidth configuration for local calls, select **Best Quality (BQ)**.
- **INTER\_STGY**: Bandwidth configuration for calls over the trunk, select **Best Quality (BQ)**.
- **ZBRN**: Select **MO** (**MO** is used for IP phones).

**Note:** **BQ** will use **G711** as first choice and **G729** as second choice. **BB**, or **Best Bandwidth**, will use **G729** as first choice and **G711** as second choice.

The values for **Zone 5** are shown below; **G711** will be used as first choice and **G729** as second choice.

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 menu 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', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The main content area is titled 'Zone Basic Property and Bandwidth Management'. It features a table with two columns: 'Input Description' and 'Input Value'. The table contains the following configuration details for Zone 5:

Input Description	Input Value
Zone Number (ZONE)	5 (1 - 8000)
Intrazone Bandwidth (INTRA_BW)	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY)	Best Quality (BQ)
Interzone Bandwidth (INTER_BW)	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY)	Best Quality (BQ)
Resource Type (RES_TYPE)	Shared (SHARED)
Zone Intent (ZBRN)	MO (MO)
Description (ZDES)	

Below the table, there is a note: '\* Required value.' and two buttons: 'Save' and 'Cancel'. The footer of the page indicates 'Copyright © 2002-2012 Avaya Inc. All rights reserved.'

The values for **Zone 1** are shown below; **G729** will be used as first choice and **G711** as second choice.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System > IP Network > Zones > Bandwidth Zones > Bandwidth Zones 1 > Edit Bandwidth Zone > Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	1 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	IPPHONES_G729_FIRST

Submit Refresh Cancel

Copyright © 2002-2012 Avaya Inc. All rights reserved.

## 5.4.2. Create a zone for virtual SIP trunks (zone 4)

This section describes how to create a zone for the Virtual SIP Trunks. The difference is in the **Zone Intent (ZBRN)** field. For **ZBRN** select **VTRK** for virtual trunk and **Best Quality (BQ)** for both **INTRA\_STGY** and **INTER\_STGY** as shown below, and then click on the **Save** button. For Hawaiian Telecom **Zone 4** was created for the Virtual SIP Trunks.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System > IP Network > Zones > Bandwidth Zones > Bandwidth Zones 4 > Edit Bandwidth Zone > Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	4 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	VTRKZONE_G711_FIRST

Submit Refresh Cancel

Copyright © 2002-2012 Avaya Inc. All rights reserved.

## 5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP IP connection between the SIP Signaling Gateway (SSG) and Session Manager.

Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options: UCM Network Services, Home, Links, Virtual Terminals, System, Customers (highlighted), Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Customers' and displays a table with columns: Customer Number, Total Routes, and Total Trunks. The table contains one row with Customer Number 00, Total Routes 3, and Total Trunks 17. The number 00 in the Customer Number column is highlighted with a red box. Above the table are buttons for 'Add...' and 'Delete', and a 'Refresh' link. The top of the page shows the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. Below the title, it says 'Managing: 172.16.21.61 Username: admin' and 'Customers'.

Customer Number	Total Routes	Total Trunks
00	3	17

The **Customer 00 Details** page will appear. Select the **Feature Packages** option from this page.

The screenshot shows the AVAYA CS1000 Element Manager interface for the 'Customer Details' page. The left sidebar is the same as in the previous screenshot, with 'Customers' highlighted. The main content area is titled 'Customer Details' and contains a list of links: Basic Configuration, Application Module Link, Attendant, Call Detail Recording, Call Party Name Display, Call Redirection, Centralized Attendant Service, Controlled Class of Service, Features, Feature Packages (highlighted with a red box), Flexible Feature Codes, Intercept Treatments, ISDN and ESN Networking, Listed Directory Numbers, Media Services Properties, Mobile Service Directory Numbers, Multi-Party Operations, Night Service, Recorded Overflow Announcement, and SIP Line Service. The top of the page shows the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. Below the title, it says 'Managing: 172.16.21.61 Username: admin' and 'Customers > Customer 00 > Customer Details'.

The screen is updated with a list of **Feature Packages** populated. Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network (ISDN)** check box, and retain the default values for all remaining fields as shown below. Scroll down to the bottom of the screen and click on the **Save** button (not shown).

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

Help | Logout

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- + System
- **Customers**
- + Routes and Trunks
- + Dialing and Numbering Plans
- + Phones
- + Tools
- + Security

**Integrated Services Digital Network**
**Package: 145**

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier:  (1 - 16383)

- Private network identifier:  (1 - 16383)

- Node DN:

Multi-location business group:  (0 - 65535)

Business sub group consult-only:  (0 - 65535)

Prefix 1:

Prefix 2:

Home number plan area code :  (200 - 999)

Prefix for central office :  (100 - 9999)

Local steering code:

Calling number type: CLID feature displays the set's Prime DN

Redirection count for ISDN calls:

CLID information for incoming/outgoing calls: No manipulation is done

Public service telephone networks: ☐

**Network Attendant Service**
**Package: 159**

**Flexible Numbering Plan**
**Package: 160**

**Trunk Failure Monitor**
**Package: 182**

Copyright © 2002-2012 Avaya Inc. All rights reserved.

HG; Reviewed:  
SPOC 1/17/2014

Solution & Interoperability Test Lab Application Notes  
©2013 Avaya Inc. All Rights Reserved.

29 of 106  
HTCS1KSMASBCE

### 5.5.1. Administer the SIP Trunk Gateway to Session Manager

Select **IP Network** → **Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of this CS1000 system. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below. The parameters (highlighted in red boxes) are filled in to match values entered for the SIP Entity Link in Session Manager (these are shown in **Section 6.6**).

- **Vtrk gateway application:** SIP Gateway (SIPGw).
- **SIP domain name:** voip.hawaiiintel.net
- **Local SIP port:** 5085.
- **Gateway endpoint name:** CS1KGateway.
- **Application node ID:** 1006.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar shows a navigation tree with categories like UCM Network Services, Links, System, and Interfaces. The main content area is titled 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details'. It features a 'General' tab and a 'Virtual Trunk Network Health Monitor' section. The 'General' section contains several input fields, some of which are highlighted with red boxes: 'Vtrk gateway application' (set to 'SIP Gateway (SIPGw)'), 'SIP domain name' (set to 'voip.hawaiiintel.net'), 'Local SIP port' (set to '5085'), 'Gateway endpoint name' (set to 'CS1KGateway'), and 'Application node ID' (set to '1006'). The 'Virtual Trunk Network Health Monitor' section includes a checkbox for 'Monitor IP addresses' and a list of 'Monitor addresses'. At the bottom, there are 'Save' and 'Cancel' buttons.

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in the red box) for the specified fields, and retain the default values for the remaining fields as shown below.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | **SIP Gateway Settings** | SIP Gateway Services

**Proxy Or Redirect Server:**

**Proxy Server Route 1:**

Primary TLAN IP address: 172.16.5.32  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5085 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration  
☐ Primary CDS proxy

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

Port: 5060 (1 - 65535)

Transport protocol: UDP

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

On the same page shown above, scroll down to the **SIP URI Map** section.

Under the **Public E.164 Domain Names**, for:

- **National:** leave this SIP URI field as blank.
- **Subscriber:** leave this SIP URI field as blank.
- **Special Number:** leave this SIP URI field as blank.
- **Unknown:** leave this SIP URI field as blank.

Under the **Private E.164 Domain Names**, for:

- **UDP:** leave this SIP URI field as blank.
- **CDP:** leave this SIP URI field as blank.
- **Special Number:** leave this SIP URI field as blank.
- **Vacant number:** leave this SIP URI field as blank.
- **Unknown:** leave this SIP URI field as blank.

Note: These fields are shown with no entries (blank) for the Avaya DevConnect lab configuration; it is possible that customer installations may have domain names configured here.

Then click on the **Save** button.

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

---

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

**Node ID: 1006 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

**SIP URI Map:**

Public E.164 domain names		Private domain names	
National:	<input type="text"/>	UDP:	<input type="text"/>
Subscriber:	<input type="text"/>	CDP:	<input type="text"/>
Special number:	<input type="text"/>	Special number:	<input type="text"/>
Unknown:	<input type="text"/>	Vacant number:	<input type="text"/>
		Unknown:	<input type="text"/>

**SIP Gateway Services**

**SIP Converged Desktop:** ☒ Enable CD service

Service DN:  Used for making VTRK call from agent.

Converged telephone call forward DN:

RAN route for announce:  (route number 0 - 511)

Wait time before RAN queue:  (-1 - 32767 msec)

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

Copyright © 2002-2012 Avaya Inc. All rights reserved.

## 5.5.2. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown below. Click on the **to Add** button.

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

---

Managing: 172.16.21.61 Username: admin  
Routes and Trunks » D-Channels

**D-Channels**

**Maintenance**

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

**Configuration**

Choose a D-Channel Number:  and type:

Channel	Type	Card Type	Description	Action
Channel: 0	Type: DCH	Card Type: DCIP	Description: VoIP	<input type="button" value="Edit"/>
Channel: 96	Type: DCH	Card Type: DCIP	Description: SIPL_DCH	<input type="button" value="Edit"/>

Copyright © 2002-2012 Avaya Inc. All rights reserved.



The **D-Channels 0 Property Configuration** screen is displayed next as shown below (D-Channel 0 was added for testing). Enter the following values for the specified fields:

- **D channel Card Type (CTYP):** D-Channel is over IP (DCIP).
- **Designator (DES):** A descriptive name.
- **Interface type for D-channel (IFC):** Meridian Meridian1 (SL1).
- **Meridian 1 node type:** Slave to the controller (USR).
- **Release ID of the switch at the far end (RLS):** 25.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
Routes and Trunks > D-Channels > D-Channels 0 Property Configuration

### D-Channels 0 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
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:	<a href="#">more PRI</a>
Secondary PRI2 loops:	
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 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

**+ Basic options (BSCOPT)**

Copyright © 2002-2012 Avaya Inc. All rights reserved.

On the same page scroll down and enter the following values for the specified fields:

- **Advanced options (ADVOPT):** check **Network Attendant Service Allowed**.

Retain the default values for the remaining fields.

**AVAYA CS1000 Element Manager** Help | Logout

**- UCM Network Services**

- + Home
- + Links
- + System
- Customers
  - Routes and Trunks
    - **D-Channels**
    - Digital Trunk Interface
- + Dialing and Numbering Plans
- + Phones
- + Tools
- + Security

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: [more PRI](#)

Secondary PRI2 loops:

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 Range: 1 - 4000

Signalling server resource capacity: 3700 Range: 0 - 3700

**+ Basic options (BSCOPT)**

**- Advanced options (ADVOPT)**

- Layer 3 call control message count per 5 second time interval: 300 Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms: 1
- Map channel number to timeslots on a PRI2 loop: ☒

**- H323 Overlap Signaling Settings (H323)**

- Overlap Receiving: ☐
- Overlap Sending: ☐
- Overlap Timer:
- Multilocation Business Group Allowed: ☐
- **Network Attendant Service Allowed: ☒**

**+ - Link Access Protocol for D-channel (LAPD)**

Copyright © 2002-2012 Avaya Inc. All rights reserved.

Click on **Basic Options (BSCOPT)** and click on the **Edit** button for the **Remote Capabilities** attribute as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, D-Channels, Digital Trunk Interface, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Basic options (BSCOPT)' and contains several configuration sections: 'Change protocol timer value (TIMR)', 'Advanced options (ADVOPT)', 'H323 Overlap Signaling Settings (H323)', 'Link Access Protocol for D-channel (LAPD)', and 'Feature Packages'. The 'Remote Capabilities' section is highlighted with a red box, and the 'Edit' button is also highlighted with a red box.

The **Remote Capabilities Configuration** page will appear. Then check **ND2** and **MWI** (if mailboxes are present on the CS1K Call Pilot) checkboxes as shown below.

Click on the **Return – Remote Capabilities** button (not shown).  
Click on the **Submit** button (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, D-Channels, Digital Trunk Interface, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Remote Capabilities Configuration' and contains a list of checkboxes for various features. The 'Message waiting interworking with DMS-100 (MWI)' and 'Network name display method 2 (ND2)' checkboxes are checked and highlighted with red boxes.

### 5.5.3. Administer Virtual Super-Loop

Select **System** → **Core Equipment** → **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click the **Add** button to create a new one. In this example, Superloop 8 is one of the Superloops that was added and used.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System > Core Equipment > Superloops

**Superloops**

Buttons: Add... Delete Refresh

Superloop Number	Superloop Type
1 4	IPMG
2 8	Virtual
3 12	Virtual
4 16	Phantom
5 48	Virtual
6 52	Virtual

### 5.5.4. Administer Virtual SIP Routes

Select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown below.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
Routes and Trunks > Routes and Trunks

**Routes and Trunks**

+ Customer: 0 Total routes: 3 Total trunks: 17 Add route

The **Customer 0, Route 0 Property Configuration** screen is displayed next. Scroll down until the **Basic Configuration** Section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown below.

- **Route Number (ROUT):** Select an available route number.
- **Designator field for trunk (DES):** A descriptive text.
- **Trunk Type (TKTP):** **TIE trunk data block (TIE).**
- **Incoming and Outgoing trunk (ICOG):** **Incoming and Outgoing (IAO).**
- **Access Code for the trunk route (ACOD):** An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter **4** (created in Section 5.4.2).
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number **1006** (created in Section 5.2.1).
- Select **SIP** (SIP) from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
- **Mode of operation (MODE):** Route uses **ISDN Signalling Link (ISLD).**
- **D channel number (DCH):** **D-Channel number 0** (created in Section 5.5.2).
- **Interface type for route (IFC):** **Meridian M1 (SL1).**

**AVAYA** CS1000 Element Manager Help | Logout

Managing: 17216.4151 Username: admin  
Routes and Trunks > Routes and Trunks > Customer 0, Route 0 Property Configuration

### Customer 0, Route 0 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE): RDB  
Customer number (CUST): 00  
Route number (ROUT): 0  
Designator field for trunk (DES): SERVICE PROVIDE  
Trunk type (TKTP): TIE  
Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)  
Access code for the trunk route (ACOD): 7916

Trunk type M911P (M911P): ☐

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

- Zone for codec selection and bandwidth management (ZONE): 00004 (0 - 8000)  
- Node ID of signaling server of this route (NODE): 1006 (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 (0 - 254)  
- Interface type for route (IFC): Meridian M1 (SL1)

Copyright © 2002-2012 Avaya Inc. All rights reserved.

- **Network calling name allowed (NCNA):** Check box.
- **Network call redirection (NCRD):** Check box.
- **Insert ESN access code (INAC):** Check box.

**AVAYA CS1000 Element Manager**

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Phones

Tools

Security

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

Network calling name allowed (NCNA): ☒

Network call redirection (NCRD): ☒

Trunk route optimization (TRO): ☐

Recognition of DTI2 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): ☐

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

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

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

Basic Route Options

Network Options

General Options

Advanced Configurations

Submit Refresh Delete Cancel

- In **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below. The IDC is discussed in **Section Error!** Reference source not found..

**AVAYA CS1000 Element Manager**

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Phones

Tools

Security

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

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

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

Basic Route Options

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

Billing number required (BLN): ☐

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): ☐

Network Options

General Options

Advanced Configurations

Submit Refresh Delete Cancel

Copyright © 2002-2012 Avaya Inc. All rights reserved.

- In **Advance Configurations** (not shown); check **Music-on-hold** to enable music on hold on the route. Input **Music route number 1** in the box as shown below. The CS1000 system is pre-configured with route 1 as a music route.

Click on the **Submit** button (not shown).

**AVAYA CS1000 Element Manager**

Help | Logout

Home local number (HLCU) :   
Home national number (HNTN) :   
In-band automatic number identification route (IANI) : ☐  
Incoming identifier send (ICIS) : ☒  
Internal/external definition (IDEF) : Use network info (NET)   
Identify originating party (IDOP) : ☐  
Insert (INST) :   
Manual outgoing trunk route (MANO) : ☐  
Manual route (MNL) : ☐  
Music on-hold (MUS) : ☒  
- Music route number (MRT) : 1 (0 - 511)  
Outgoing identifier send (OGIS) : ☒  
Off-hook timer delay (OHTD) : ☐  
Outpulsing route (OPR) : ☐  
Pseudo answer (PANS) : ☒  
Periodic clearing signal (PECL) : ☐  
Privacy indicator ignored (PII) : ☐  
Auxiliary application (AUXP) : ☐  
Protocol selection (PSEL) : DM-DM Protocol Selection (DMDM)   
Preference trunk usage threshold (PTUT) : 0 (0 - 510)  
Port type at far end (PTYF) : Analog TIE trunks (ATT)   
Route traffic information in ACD Reports (RACD) : ☐  
Radio paging route (RPA) : ☐

Copyright © 2002-2012 Avaya Inc. All rights reserved.

### 5.5.5. Administer Virtual Trunks

Continue from **Section 5.5.4**, after clicking on **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, **Route 0** has been added. Click on **Add trunk** button next to the newly added route **0** as shown below.

**AVAYA CS1000 Element Manager**

Help | Logout

Managing: 172.16.21.61 Username: admin  
Routes and Trunks > Routes and Trunks

**Routes and Trunks**

Customer	Total routes	Total trunks		
- Customer: 0	Total routes: 3	Total trunks: 17	<input type="button" value="Add route"/>	
+ Route: 0	Type: TIE	Description: SERVICE PROVIDER	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 1	Type: IMUS	Description: MUSIC	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
+ Route: 96	Type: TIE	Description: SIPL_ROUTE	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>

The **Customer 0, Route 0, Trunk 1 Property Configuration** screen is displayed as shown below. Enter the following values for the specified fields and retain default values for the remaining fields. The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown below.

- The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 11 trunks were created.
- **Trunk data block (TYPE): IP Trunk (IPTI).**
- **Terminal Number (TN):** Available terminal number (created in **Section 5.5.3**).
- **Designator field for trunk (DES):** A descriptive text.
- **Extended Trunk (XTRK): Virtual trunk (VTRK).**
- **Member number (RTMB):** Current route number and starting member.
- **Start arrangement Incoming (STRI): Immediate (IMM).**
- **Start arrangement Outgoing (STRO): Immediate (IMM).**
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level.
- **Channel ID for this trunk (CHID):** An available starting channel ID.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
Routes and Trunks > Routes and Trunks > Customer 0, Route 0, Trunk 1 Property Configuration

### Customer 0, Route 0, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:  \*

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

- Advanced Trunk Configurations



Click on **Edit Class of Service** (shown on previous screen), For **Media Security** select **Media Security Never (MSNV)**, for **Restriction Level** select **Unrestricted (UNR)**. Use default for remaining values. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown).

AVAYA CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Customers

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Phones

Tools

Security

Busy Tone Supervised COT:

Calling party Denied (CND)

Central Office Ringback:

Centrex Switchhook Flash:

Centrex Switchhook Flash Denied (THFD)

Dial Pulse:

DTR PAD value:

Echo Canceling:

Echo Canceling Denied (ECD)

Hong Kong DTI:

Loop Break Supervised COT:

Make-break ratio for dial pulse:

10 pulses per second (P10)

Manual Incoming:

Manual Incoming Denied (MID)

Media Security:

Media Security Never (MSNV)

Network Hook Flash Over M911P:

Polarity:

Priority:

Low Priority (LPR)

Restriction level:

Unrestricted (UNR)

Reversed Ear Piece:

Reversed Ear Piece denied (REP)

Short or long line:

Transmission Class of Service:

Non-Transmission Compensated (NTC)

Warning Tone:

Warning Tone Allowed (WTA)

Reversed Ear Piece:

Reversed Ear Piece denied (REP)

ARF Supervised COT:

Copyright © 2002-2012 Avaya Inc. All rights reserved.

## 5.5.6. Administer Calling Line Identification Entries

Select **Customers** → **00** → **ISDN and ESN Networking** (Not shown). Click on **Calling Line Identification Entries** as shown below.

AVAYA CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Customers

Routes and Trunks

Dialing and Numbering Plans

Phones

Tools

Security

General Properties

Flexible trunk to trunk connection option:

Connections restricted

Flexible orbiting prevention timer:

6

Country code:

1 (0 - 9999)

Code for processing the called number

National access code:

1

International access code:

011

Options:

☒ Transfer on ringing of supervised external trunks

☒ Connection of supervised external trunks

Network option:

Coordinated dialing plan routing

Integrated services digital network:

☒

Microsoft converged office dialing plan:

Private dialing plan

Private dialing plan for non-DID users:

☐ Coordinated dialing plan

☐ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

No manipulation is done

Size:

256 (0 - 4000)

Country code:

1 (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Copyright © 2002-2012 Avaya Inc. All rights reserved.

Click on **Add** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager web interface. The top navigation bar includes the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. The left sidebar contains a tree view with categories like 'UCM Network Services', 'Home', 'Links', 'System', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The main content area is titled 'Calling Line Identification Entries'. It features a 'Search for CLID' section with input fields for 'Start range' and 'End range', and a 'Search' button. Below this is a table for 'Calling Line Identification Entries' with an 'Add...' button highlighted by a red rectangle and a 'Delete' button. A 'Refresh' button is located at the bottom right of the table area.

Add entry **0** as shown below.

- **National Code:** Input the three digit area code prefix of the DID number assigned by the service provider, in this case **808**.
- **Local Code:** input the seven digit number of the DID assigned by Service Provider, in this case it is **5551234**.
- **Calling Party Name Display:** Uncheck the **Roman characters** box.

Repeat for each of the DID numbers to be assigned to extensions in the CS1000.

The screenshot shows the 'Edit Calling Line Identification 0' page in the AVAYA CS1000 Element Manager. The top navigation bar and left sidebar are consistent with the previous screenshot. The main content area is titled 'Edit Calling Line Identification 0'. It contains several sections: 'General Properties' with fields for 'National Code' (808) and 'Local Code' (5551234), both highlighted with a red rectangle; 'Local Steering Code' and 'Use DN as DID' (set to NO); 'Emergency Services Access' with 'Emergency Local Code' and 'Emergency Options' (including 'Home national number for emergency services access calls' and 'Append the originating directory number for emergency services access calls'); and 'Calling Party Name Display' with a 'Roman characters' checkbox. The bottom of the page includes a copyright notice: 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

### 5.5.7. Enable External Trunk to Trunk Transferring

This section shows how to enable the External Trunk to Trunk Transferring feature which is a mandatory configuration to make call transfers and conferences work properly over a SIP trunk.

- Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail)
- Allow External Trunk to Trunk Transferring for **Customer Data Block** by using **LD 15**.

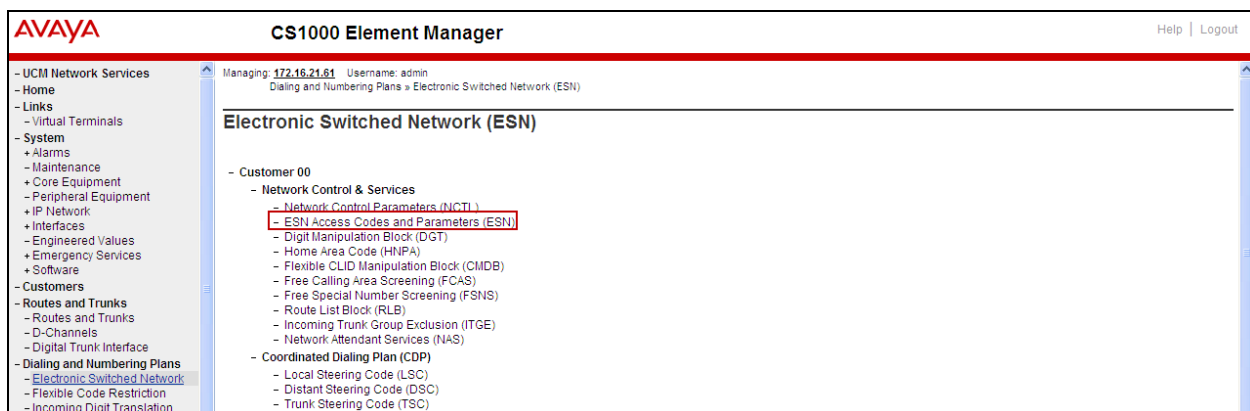
```
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101   USED U P: 371282 939078   TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....
```

## 5.6. Administer Dialing Plans

This section describes how to administer dialing plans on the CS1000.

### 5.6.1. Define ESN Access Codes and Parameters (ESN)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **ESN Access Code and Parameters (ESN)** as shown below.



In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** as shown below. Click **Submit** (not shown).

**AVAYA CS1000 Element Manager** Help | Logout

**ESN Access Codes and Basic Parameters**

**General Properties**

NARS/BARS Access Code 1:

NARS Access Code 2:

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

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time:  (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

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

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

**Limits**

Maximum number of Digit Manipulation tables:  (0 - 2000)

Maximum number of Route Lists:  (0 - 2000)

Maximum number of CLID manipulation tables:  (1 - 256)

Maximum number of Supplemental Digit restriction blocks:  (0 - 1500)

Maximum number of Incoming Trunk Group exclusion tables:  (0 - 255)

Maximum number of Free Calling area screening tables:  (0 - 255)

Copyright © 2002-2012 Avaya Inc. All rights reserved.

### 5.6.2. Associate NPA and SPN call to ESN Access Code 1

Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail).

In **LD 15**, change Customer Net\_Data Block by disabling NPA and SPN to be associated to Access Code 2 (AC2). It means Access Code 1 will be used for NPA and SPN calls.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35717857   USED U P: 8241949 920063   TOT: 44879869
DISK SPACE NEEDED: 1697 KBYTES
REQ: chg
TYPE: net_data
CUST 0
OPT
AC2 xn timer xspn
FNP
CLID
ISDN
...
```

Verify Customer Net\_Data Block by using **LD 21**

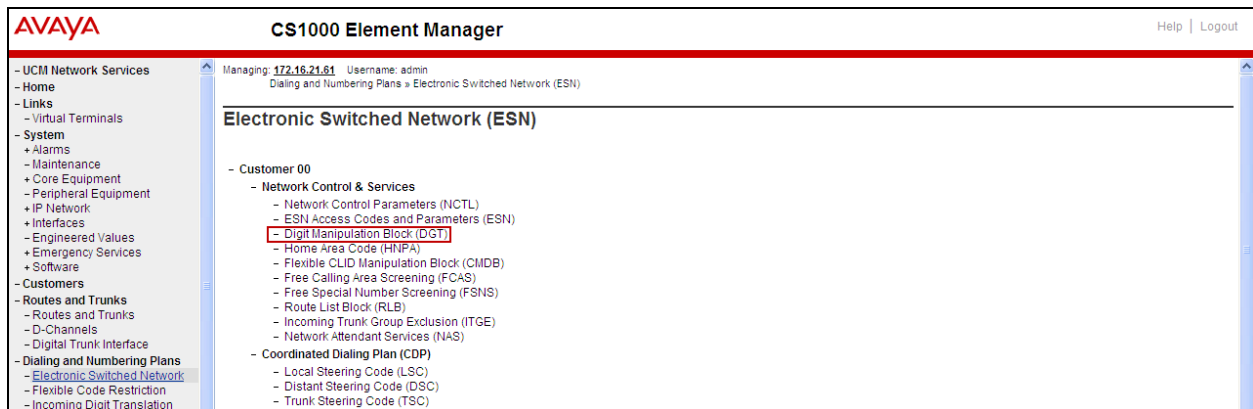
```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTA
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
...
```

### 5.6.3. Digit Manipulation Block Index (DMI)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Digit Manipulation Block (DGT)** as shown below.



In the **Please choose the Digit Manipulation Block Index** drop-down field, select an available DMI from the list and click **to Add** as shown below.

In the example shown below **Digit Manipulation Block Index 1** was previously added.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main content area is titled 'Digit Manipulation Block List'. It shows a list of existing blocks: 'Digit Manipulation Block Index -- 1' and 'Digit Manipulation Block Index -- 2', each with an 'Edit' link. Above the list, there is a dropdown menu labeled 'Please choose the' with 'Digit Manipulation Block Index 3' selected, and a 'to Add' button.

Enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits**, and then click **Submit** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface with the 'Digit Manipulation Block' configuration form. The form includes fields for 'Digit Manipulation Index numbers' (set to 1), 'Number of leading digits to be deleted' (set to 0, with a range of 0 - 19), 'Insert' (empty text field), 'IP Special Number' (checkbox), and 'Call Type to be used by the manipulated digits' (set to NPA (NPA)). At the bottom, there are buttons for 'Submit', 'Refresh', 'Delete', and 'Cancel'.

#### 5.6.4. Route List Block (RLB)

This section shows how to add a RLB associated with the DMI created in **Section 5.6.3**. Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown below.

AVAYA

CS1000 Element Manager

Help | Logout

Managing: 172.16.21.81 Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

Customer 00

Network Control & Services

Network Control Parameters (NCTL)

ESN Access Codes and Parameters (ESN)

Digit Manipulation Block (DGT)

Home Area Code (HNPA)

Flexible CLID Manipulation Block (CMDB)

Free Calling Area Screening (FCAS)

Free Special Number Screening (FSNS)

Route List Block (RLB)

Incoming Trunk Group Exclusion (ITGE)

Network Attendant Services (NAS)

Coordinated Dialing Plan (CDP)

Local Steering Code (LSC)

Distant Steering Code (DSC)

Trunk Steering Code (TSC)

Select an available value in the **Please enter a route list index** field and click on the “to Add” button as shown below.

In the example shown below **Route List Block Index 1** was previously added.

AVAYA

CS1000 Element Manager

Help | Logout

Managing: 172.16.21.81 Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index  (0 - 1999) to Add

Route List Block Index -- 1 Edit

Route List Block Index -- 2 Edit

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Submit** button (not shown).

- **Digit Manipulation Index (DMI): 1** (created in **Section 5.6.3**).
- **Route number (ROUT): 0** (created in **Section 5.5.4**).

**AVAYA CS1000 Element Manager** Help | Logout

**General Properties**

Entry Number for the Route List:

**Indexes**

Time of Day Schedule:

Facility Restriction Level:  (0 - 7)

**Digit Manipulation Index: 1**

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

Free Calling Area Screening Index:

Free Special Number Screening Index:

Business Network Extension Route: ☐

Incoming CLID Table:  (0 - 255)

**Options**

Local Termination entry: ☐

**Route Number: 0**

Skip Conventional Signaling: ☐

Display Originator's Information: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

Strategy on Congestion:

- QSIG Alternate Routing Causes:

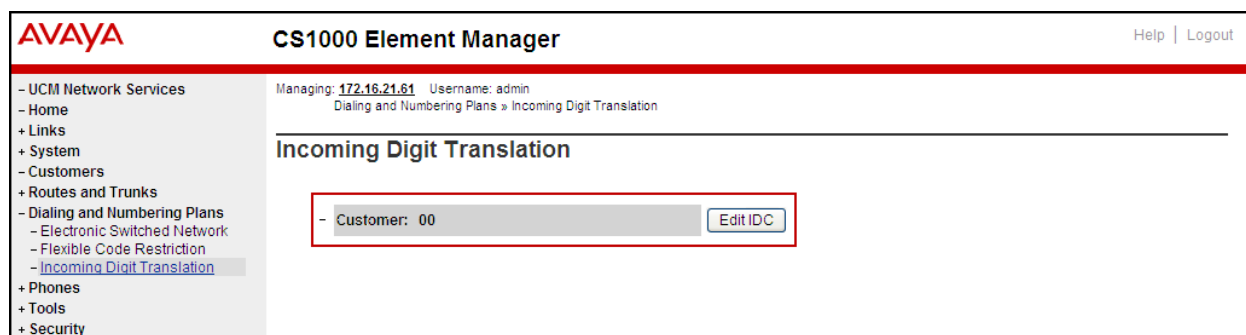
Copyright © 2002-2012 Avaya Inc. All rights reserved.



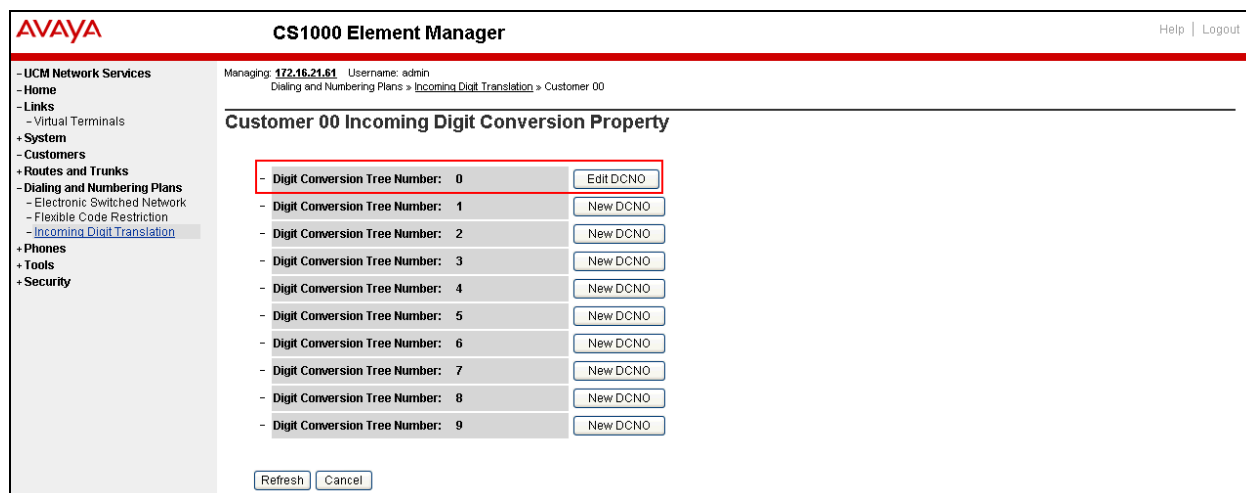
### 5.6.5. Inbound Call Digit Translation

This section describes the steps for receiving calls from the PSTN via Hawaiian Telecom's network.

Select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown below.



Click on **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCNO) 0** was created as shown below.



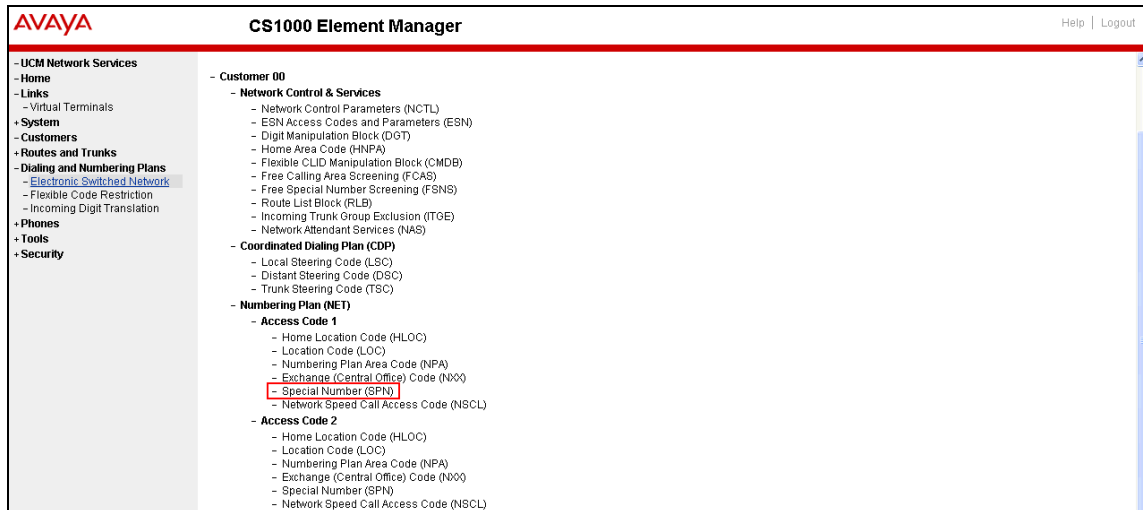
Details of the **DCNO** configuration are shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 system extension number. This **DCNO** has been assigned to route 0 as shown in **Section 5.5.4**

In the following configuration, the incoming call from PSTN with the prefix **8085551234** will be translated to the CS1000 extension number **8000**.

### 5.6.6. Outbound Call - Special Number Configuration.

There are special numbers which are configured to be used for this testing such as **0** to reach the Service Provider operator, **0+10** digits to reach the Service Provider operator assistant, **011** prefix for international calls, **1** for national long distance calls, **411**, **911**, **711** and so on. Calls to special numbers shown here are for reference only and may not have been tested for various reasons. Refer to **Items not supported or not tested** in **Section 2.2**.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Special Number (SPN)** as shown below.



Enter **SPN** and then click on the “**to Add**” button.

#### Special Number: 0

- **Flexible length: 0** (flexible, unlimited and accept the character # to ending dial number).
- **CallType: NONE.**
- **Route list index: 1**, created in **Section 5.6.4.**

#### Special Number: 011

- **Flexible length: 15.**
- **CallType: NONE.**
- **Route list index: 1**, created in **Section 5.6.4.**

#### Special Number: 1

- **Flexible length: 0** (flexible, unlimited and accept the character # to ending dial number).
- **CallType: NATL.**
- **Route list index: 1**, created in **Section 5.6.4.**

#### Special Number: 411

- **Flexible length: 3.**
- **CallType: None.**
- **Route list index: 1**, created in **Section 5.6.4.**

#### Special Number: 711

- **Flexible length: 3.**
- **CallType: None.**
- **Route list index: 1**, created in **Section 5.6.4.**

#### Special Number: 911

- **Flexible length: 3.**
- **CallType: None.**
- **Route list index: 1**, created in **Section 5.6.4.**

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

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Numbering Plan (NET) > Access Code 1 > Special Number List

### Special Number List

Please enter a Special Number

- Special Number -- 0	<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: 1	
- Special Number -- 011	<input type="button" value="Edit"/>
Flexible length: 15 Inhibit time-out handler: NO Type of call that is defined by the special number: NONE Route list index: 1	
- Special Number -- 1	<input type="button" value="Edit"/>
Flexible length: 0 Type of call that is defined by the special number: NATL Route list index: 1	
+ Special Number -- 326	<input type="button" value="Edit"/>
- Special Number -- 411	<input type="button" value="Edit"/>
Flexible length: 3 Inhibit time-out handler: NO Type of call that is defined by the special number: NONE Route list index: 1	
- Special Number -- 611	<input type="button" value="Edit"/>
Flexible length: 3 Inhibit time-out handler: NO Type of call that is defined by the special number: NONE Route list index: 1	

Copyright © 2002-2013 Avaya Inc. All rights reserved.

### 5.6.7. Outbound Call - Numbering Plan Area Code (NPA)

The **Numbering Plan Area Code (NPA)** was not used for Outbound Calls. The **Special Number 1** defined above in **Section 5.6.6** allows the user to dial any Numbering Plan Area Code (NPA) when dialing **9+1**.

## 5.7. Administer Phone

This section describes the addition of the CS1000 extension used during the testing.

### 5.7.1. Phone creation

Refer to **Section 5.5.3** to create a virtual super-loop - **8** used for IP phone.  
Refer to **Section 5.4.1** to create a bandwidth zone - **5** for IP phone.

For CS1000 FAX over IP Support recommendation refer to the Avaya Product Support Notice (PSN) referred to in **Section 11** [16], including the **Analog Station provisioning for T.38** section and **Minimum Vintage Loadware Recommendation** for MGC.

Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail).  
Create an IP phone using **Unified Communications Management (UCM)** or **LD 11**.

```

REQ: prt
TYPE: 1110
TN
CUST
TEN
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES 8001
TN 008 0 00 01 VIRTUAL
TYPE 1110
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00005
CUR_ZONE 00005
MRT
ERL 0
ECL 0
FDN
TGAR 0
LDN NO
NCOS 5
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW
SFLT NO
CAC_CIS 0
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHA FICD NAID DNAA BUZZ
UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRD
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
MSNV FRA PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO 0
EFD
HUNT
EHT
LHK 0
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 8001 1 MARP
CPND
CPND_LANG ROMAN
NAME Avaya, 1110_uni
XPLN 14
DISPLAY_FMT FIRST, LAST
ANIE 0
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16 MWK 8056
17 TRN
18 AO6
19 CFW 12
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27

```

### 5.7.2. Enable Privacy for Phone

This section shows how to enable or disable Privacy for a phone by changing its class of service (CLS); changes can be made by using **Unified Communications Management (UCM)** or **LD 11**. By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately. The privacy for a single call can be done by configuring per-call blocking and a corresponding dialing sequence, for example \*67. The resulting SIP privacy setting will be the same in either case.

To hide display name, set CLS to **namd**. The CS1000 will include “Privacy:user” in the SIP message header before sending to the Service Provider.

```
REQ: chg
TYPE: 1110
TN 8 0 0 1
ECHG yes
ITEM cls namd
ITEM [ ]
```

To hide display number, set CLS to **ddgd**. The CS1000 will include “Privacy:id” in SIP message header before sending to Service Provider.

```
REQ: chg
TYPE: 1110
TN 8 0 0 1
ECHG yes
ITEM cls ddgd
ITEM [ ]
```

To hide display name and number, set CLS to **namd, ddgd**. The CS1000 will include “Privacy:id, user” in SIP message header before sending to Service Provider.

```
REQ: chg
TYPE: 1110
TN 8 0 0 1
ECHG yes
ITEM cls namd ddgd
ITEM [ ]
```

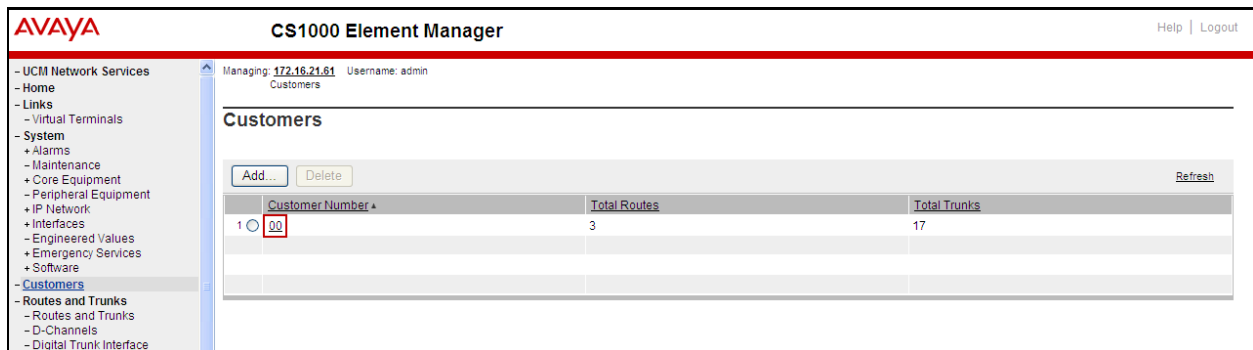
To allow display name and number, set CLS to **nama, ddga**. The CS1000 will send header “Privacy:none” to Service Provider.

```
REQ: chg
TYPE: 1110
TN 8 0 0 1
ECHG yes
ITEM cls nama ddga
ITEM [ ]
```

### 5.7.3. Enable Call Forward for the Phone

This section shows how to configure the Call Forward feature at the system level and phone level.

Select **Customers** from the left pane to display the **Customers** screen as shown below. Select **Customer 00** as shown below.



AVAYA CS1000 Element Manager

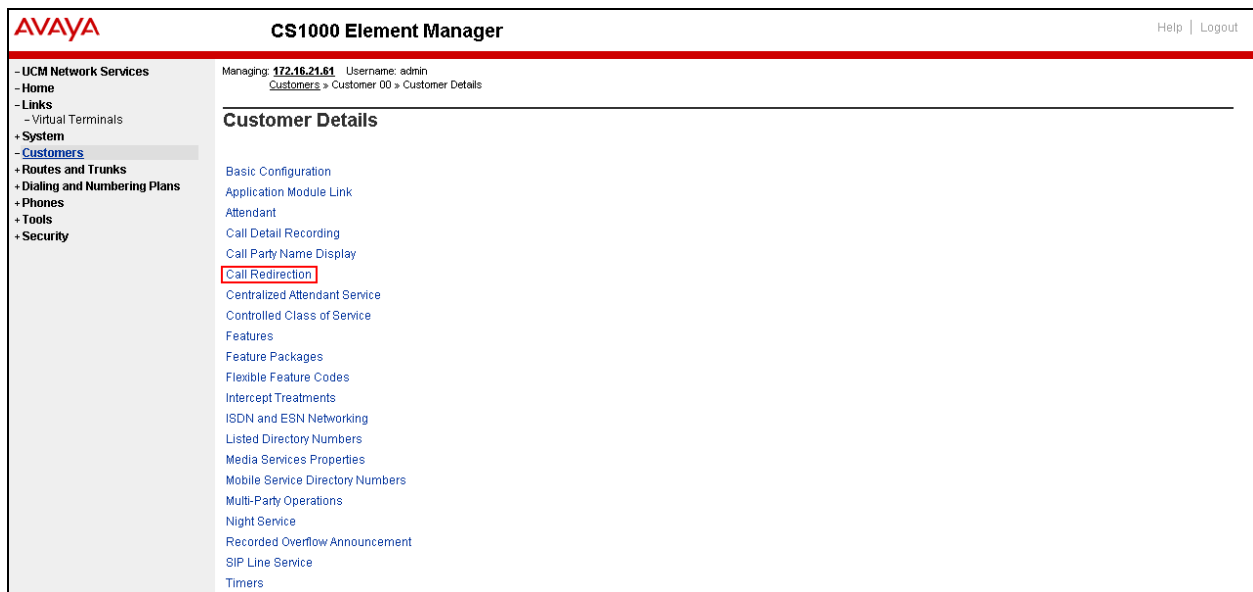
Managing: 172.16.21.61 Username: admin

Customers

Add... Delete Refresh

Customer Number	Total Routes	Total Trunks
1 00	3	17

Select **Call Redirection** as shown below.



AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

Customers > Customer 00 > Customer Details

Customer Details

- Basic Configuration
- Application Module Link
- Attendant
- Call Detail Recording
- Call Party Name Display
- Call Redirection
- Centralized Attendant Service
- Controlled Class of Service
- Features
- Feature Packages
- Flexible Feature Codes
- Intercept Treatments
- ISDN and ESN Networking
- Listed Directory Numbers
- Media Services Properties
- Mobile Service Directory Numbers
- Multi-Party Operations
- Night Service
- Recorded Overflow Announcement
- SIP Line Service
- Timers

The **Call Redirection** page is displayed as shown below.

Set the following fields:

- **Total redirection count limit: 0** (unlimited).
- **Call Forward: Originating.**
- **Number of normal ringing cycles for CFNA: 4.**

Click on **Save** (not shown)

AVAYA CS1000 Element Manager

Help | Logout

Do not disturb hunting: ☐

Total redirection count limit: 0

Options: ☐ Call forward reminder tone for 500/2500 sets  
☐ CFNA treatment for call waiting calls on a DN  
☐ DID call to second degree busy treatment  
☒ Message center  
☒ Prevention of reciprocal call forward

Call forward: ☒ Originating  
☐ Forwarding

Number of normal ringing cycles for CFNA

Option 0: 4  
Option 1: 4  
Option 2: 4

Number of distinctive ringing cycles for CFNA

Option 0: 4  
Option 1: 4  
Option 2: 4

Calls routed to message center

Copyright © 2002-2012 Avaya Inc. All rights reserved.

Enable **Call Forward All Calls (CFAC)** for the phone over the SIP trunk by using **LD 11**. Change its CLS to **CXFA** and then program the forward number on the phone set. The following is the configuration of a phone that has CFAC enabled. The phone was forwarded to the PSTN number **919195551212**.

```
REQ: prt
TYPE: 2050pc
TN 8003
CLS UNR FBA WTA LPR MTD FNA HTA TOD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRO
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD
```

**19 CFW 12 919195551212**



Enable **Call Forward Busy (CFB)** for the phone over the SIP trunk by using **LD 11**. Change its CLS to **FBA**, **HTA** and then program the forward number as **HUNT**. The following is the configuration of a phone that has CFB enabled. The phone was CFB to the PSTN number **919195551212**.

```
REQ: prt
TYPE: 2050pc
TN 8003
....
CLS UNR FBA WTA LPR MTD HTA TOD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRD
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSF NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD
CPND LANG ENG
RCO 0
EFD 8004
HUNT 919195551212
....
```

Enable **Call Forward No Answer (CFNA)** for the phone over the SIP trunk by using **LD 11**. Change its CLS to **FNA**, **SFA** and then program the forward number as **FDN**. The following is the configuration of a phone that has CFNA enabled. The phone was CFNA to the PSTN number **919195551234**.

```
REQ: prt
TYPE: 2050pc
TN 8003
....
FDN 919195551234
....
CLS UNR FBA WTA LPR MTD FNA HTA TOD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRD
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSF NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD
....
```

#### 5.7.4. Enable Call Waiting for the Phone

This section shows how to configure the **Call Waiting** feature at the phone level.

To configure the Call Waiting feature for the phone by using **LD 11**, change the CLS to **HTD**, **SWA** and add **CWT** to a key as shown below.

```
REQ: prt
TYPE: 2050pc
TN 8003
....
CLS UNR FBA WTA LPR MTD FNA HTD TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWA LND CNDA
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRD
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD
....
02 CWT
....
```

## 6. Configure Session Manager

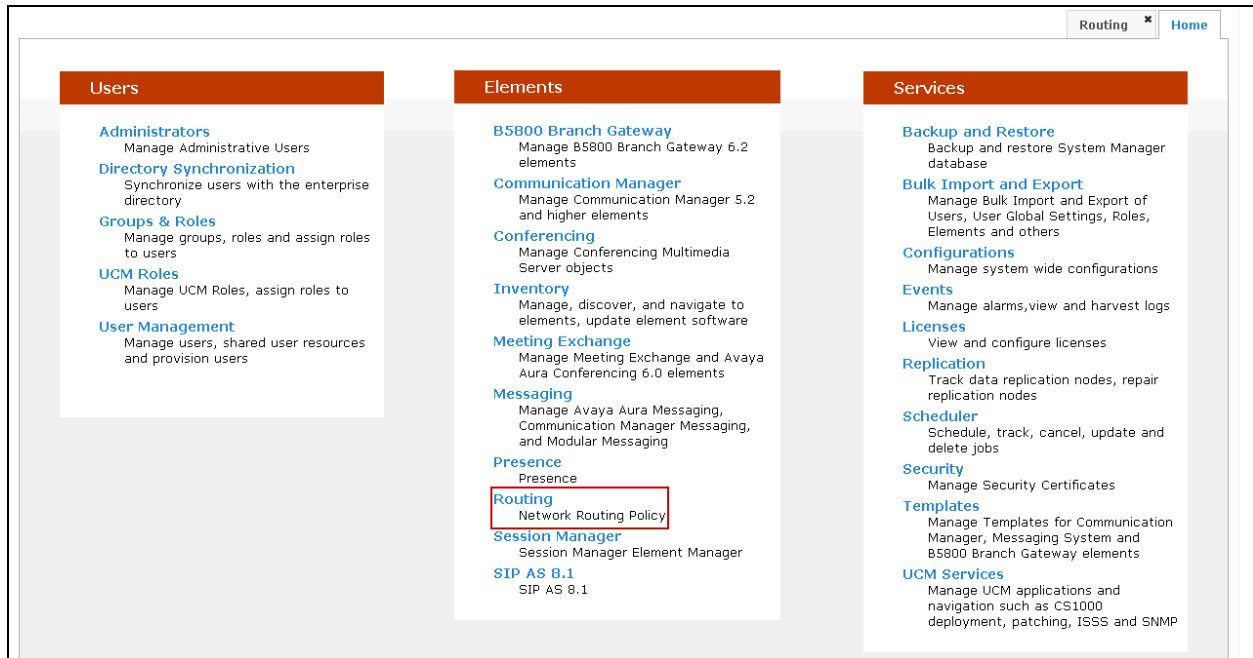
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location(s) that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to the CS1000, Avaya SBCE and Session Manager itself.
- 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.
- Regular Expressions, which also can be used to route calls.
- Session Manager, corresponding to the Session Manager Server to be managed by Avaya Aura® System Manager.

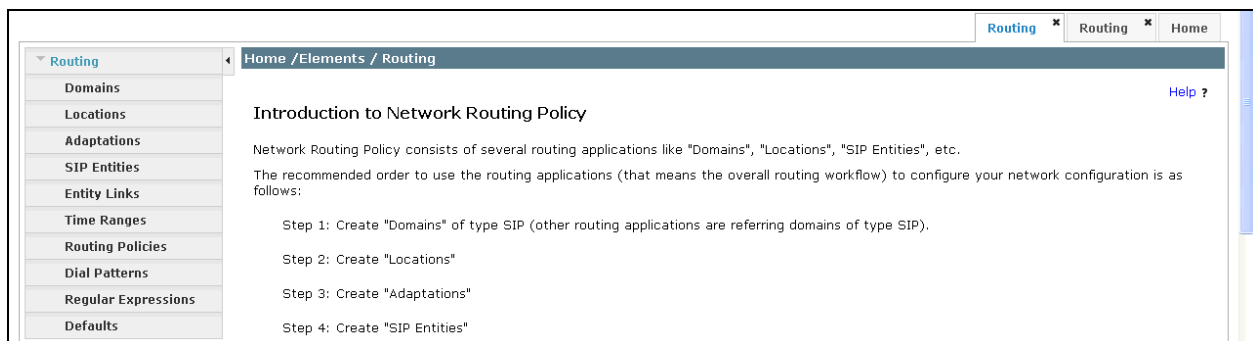
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

## 6.1. System Manager Login and Navigation

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



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.



## 6.2. Specify SIP Domains

Create a SIP domain for which Session Manager will need to be aware in order to route calls. For the compliance test, the domain **voip.hawaiiintel.net** was added.

To add a domain Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), 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 Hawaiian Telecom domain.

The screenshot shows a web application interface for 'Domain Management'. On the left is a navigation pane with 'Routing' expanded and 'Domains' selected. The main area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb are 'Commit' and 'Cancel' buttons. A table with one item is displayed, with columns 'Name', 'Type', and 'Notes'. The 'Name' column contains 'voip.hawaiiintel.net', the 'Type' column contains 'sip', and the 'Notes' column is empty. Below the table are another 'Commit' and 'Cancel' buttons.

Name	Type	Notes
voip.hawaiiintel.net	sip	

### 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).

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

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of the **HG Lab** location, which includes all equipment on the **172.16.5.x** and **172.16.20.x** subnets including the CS1000, Avaya SBCE and Session Manager. Click **Commit** to save.

The screenshot displays the 'Add Location' configuration page. The left navigation pane shows 'Routing' expanded, with 'Locations' selected. The main content area has a breadcrumb 'Home / Elements / Routing / Locations' and a 'Help ?' link. The 'Location Details' section includes 'Commit' and 'Cancel' buttons. The 'General' section contains a 'Name' field with the value 'HG Lab' and a 'Notes' field with the value 'Simulated Enterprise Customer (C...'. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec', 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and a checked box for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Location Pattern' section has 'Add' and 'Remove' buttons, a '2 Items' count, and a 'Refresh' button. Below this is a table with two rows, each representing an IP address pattern: '172.16.5.\*' and '172.16.20.\*'. The 'Commit' button is highlighted at the bottom right.

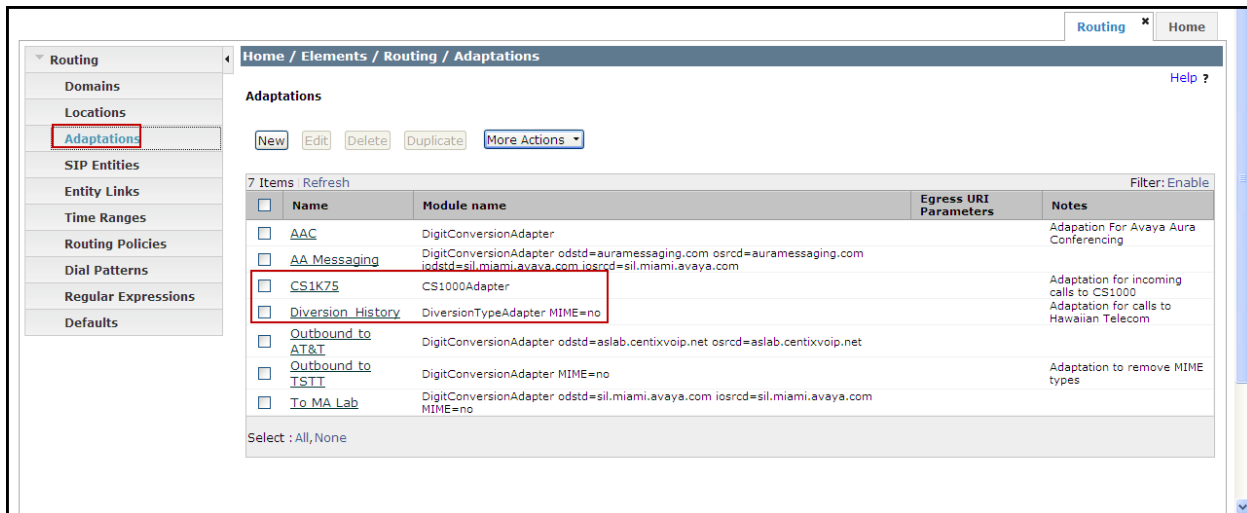
IP Address Pattern	Notes
172.16.5.*	
172.16.20.*	

### 6.4. Add Adaptation Module

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic module and can modify other headers to permit interoperability with third party SIP products.

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 a portion of the list of adaptations in the sample configuration.

The adaptations named **CS1K75** and **Diversion\_History** were created and used during the compliance test.



The screenshot displays the Avaya Aura Configuration Manager interface. On the left, a navigation pane shows the 'Routing' section expanded, with 'Adaptations' highlighted. The main content area shows the 'Adaptations' list. At the top, there are buttons for 'New', 'Edit', 'Delete', 'Duplicate', and a 'More Actions' dropdown. Below this is a table with 7 items. The table has columns for 'Name', 'Module name', 'Egress URI Parameters', and 'Notes'. The rows for 'CS1K75' and 'Diversion\_History' are highlighted with a red box. The 'CS1K75' row shows a module name of 'CS1000Adapter' and a note about adaptation for incoming calls to CS1000. The 'Diversion\_History' row shows a module name of 'DiversionTypeAdapter' and a note about adaptation for calls to Hawaiian Telecom. Other rows include 'AAC', 'AA Messaging', 'Outbound to AT&T', 'Outbound to TSTT', and 'To MA Lab'.

Name	Module name	Egress URI Parameters	Notes
AAC	DigitConversionAdapter		Adaptation For Avaya Aura Conferencing
AA Messaging	DigitConversionAdapter	odstd=auramessaging.com osrcd=auramessaging.com idstd=sil.miami.avaya.com iosrcd=sil.miami.avaya.com	
CS1K75	CS1000Adapter		Adaptation for incoming calls to CS1000
Diversion_History	DiversionTypeAdapter	MIME=no	Adaptation for calls to Hawaiian Telecom
Outbound to AT&T	DigitConversionAdapter	odstd=aslab.centixvoip.net osrcd=aslab.centixvoip.net	
Outbound to TSTT	DigitConversionAdapter	MIME=no	Adaptation to remove MIME types
To MA Lab	DigitConversionAdapter	odstd=sil.miami.avaya.com iosrcd=sil.miami.avaya.com MIME=no	

Select : All, None

Settings for **CS1K75** Adaptation:

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **CS1000Adapter**.

Click **Commit** to save.

The **CS1K75** adaptation shown below will later be assigned to the **CS1K7.5** SIP entity.

The screenshot shows a web interface for configuring adaptations. On the left is a navigation menu with 'Routing' expanded and 'Adaptations' selected. The main area is titled 'Home / Elements / Routing / Adaptations' and contains 'Adaptation Details' for 'CS1K75'. The 'General' section has fields for 'Adaptation name' (CS1K75), 'Module name' (CS1000Adapter), 'Module parameter', and 'Egress URI Parameters'. A 'Notes' field contains 'Adaptation for incoming calls to C'. Below are sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM', each with an 'Add' button and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The interface includes 'Commit' and 'Cancel' buttons at the top and bottom right.



## Settings for **Diversion\_History** Adaptation:

The adapter named **Diversion\_History** will later be assigned to the Avaya SBCE SIP entity for calls to Hawaiian Telecom. This adaptation uses the **DiversionTypeAdapter** to convert the History-Info header to a Diversion header. The Module parameter **MIME=no** will remove MIME types inserted by the CS1000 which are not used for call processing and should not be sent to Hawaiian Telecom.

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DiversionTypeAdapter**.
- **Module parameter:** Enter **MIME=no**

Click **Commit** to save.

The **Diversion\_History** adaptation shown below will later be assigned to the **HG ASBCE** SIP entity.

The screenshot displays the Avaya Management System (AMS) interface for configuring an adaptation. The left sidebar shows the navigation menu with 'Adaptations' highlighted. The main content area is titled 'Home / Elements / Routing / Adaptations' and includes a 'Commit' button and a 'Cancel' button. The 'General' section is active, showing the following fields:

- Adaptation name:** Diversion\_History
- Module name:** DiversionTypeAdapter (selected from a dropdown)
- Module parameter:** MIME=no
- Egress URI Parameters:** (empty field)
- Notes:** Adaptation for calls to Hawaiian T

Below the 'General' section, there are two sections for digit conversion:

- Digit Conversion for Incoming Calls to SM:** Includes an 'Add' button, a 'Remove' button, and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The table currently shows 0 items.
- Digit Conversion for Outgoing Calls from SM:** Includes an 'Add' button, a 'Remove' button, and a table with the same columns as the incoming section. The table currently shows 0 items.

At the bottom right of the interface, there are 'Commit' and 'Cancel' buttons.

## 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 the CS1000 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 interface that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for the CS1000 and Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** defined in **Section 6.4**.
- **Location:** Select one of the locations defined in **Section 6.3**.
- **Time Zone:** Select the time zone to which the entity belongs.

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.

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

Click **Commit** to save.

For the compliance test, only two Ports were used:

- **5060** with **TCP** for connecting to Avaya SBCE.
- **5085** with **UDP** for connecting to the CS1000.

The following screen shows the addition of Session Manager. The IP address of the Session Manager Security Module Interface is entered for **FQDN or IP Address**.

Routing
Home

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

Home / Elements / Routing / SIP Entities
Help ?

Commit
Cancel

**SIP Entity Details**

**General**

**\* Name:** HG Session Manager

**\* FQDN or IP Address:** 172.16.5.32

**Type:** Session Manager

**Notes:** HG Session Manager

**Location:** HG Lab

**Outbound Proxy:**

**Time Zone:** America/New\_York

**Credential name:**

**SIP Link Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

**Port**

**TCP Failover port:**

**TLS Failover port:**

Add Remove

9 Items	Refresh	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>		5060	TCP	voip.hawaiiantel.net	
<input type="checkbox"/>		5085	UDP	voip.hawaiiantel.net	

Select : All, None

**SIP Responses to an OPTIONS Request**

Add Remove

0 Items	Refresh	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
---------	---------	-------------------------------	---------------------	-------

Commit
Cancel

A separate SIP entity for the CS1000 is required in order to send SIP service provider traffic. The following screen shows the addition of the CS1000 SIP entity.

For the compliance testing, the following values were used:

- **Name:** Enter a descriptive name.
- The **FQDN or IP Address** field is set to the TLAN IP address of the CS1000 Signaling Gateway (Node IP address), refer to **Section 5.2.1**.
- For Adaptation select the **CS1K75** adaptation defined in **Section 6.4**.
- For Location select the **HG Lab** location defined in **Section 6.3**.

The screenshot displays the 'SIP Entity Details' configuration page. The left sidebar shows a navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. A red box highlights the following fields:

- Name:** CS1K7.5
- FQDN or IP Address:** 172.16.20.60
- Type:** Other
- Notes:** CS1000 Rel. 7.5
- Adaptation:** CS1K75
- Location:** HG Lab
- Time Zone:** America/New\_York

Below these fields, there are several other options:

- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty dropdown)

At the bottom, the **SIP Link Monitoring** section shows a dropdown set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

A separate SIP entity for the Avaya SBCE is required in order to route calls to the service provider. The following screen shows the addition of Avaya SBCE SIP entity.

For the compliance test the following values were used:

- **Name:** Enter a descriptive name.
- The **FQDN or IP Address** field is set to the IP address of the private network interface of the Avaya SBCE (see **Figure 1**).
- For Adaptation select the **Diversion\_History** adaptation defined in **Section 6.4**.
- For Location select the **HG Lab** location defined **Section 6.3**.

Routing \* Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

Help ?

Routing

Domains

Locations

Adaptations

**SIP Entities**

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

**General**

\* Name: HG ASBCE

\* FQDN or IP Address: 172.16.5.71

Type: Other

Notes: HG ASBCE

Adaptation: Diversion\_History

Location: HG Lab

Time Zone: America/New\_York

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

## 6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the CS1000 and the other 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 Session Manager entity configured in **Section 6.5**.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol defined in **Section 6.5**.
- **Port:** Port number on which Session Manager will receive SIP requests. This must match the port defined in **Section 6.5**.
- **SIP Entity 2:** Select the name of the other system. For the CS1000 and Avaya SBCE, select the CS1000 or Avaya SBCE SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the CS1000 will receive SIP requests. For the CS1000 this must match the port defined under **SIP Gateway Settings** tab, under **Proxy or Redirect Server** in **Section 5.5.1**. For the Avaya SBCE this must match the port defined under **Server Configuration** in **Section 7.2.4**.
- **Connection Policy:** Select **Trusted** from the pull-down menu.

Click **Commit** to save.

The following screen illustrates the Entity Link to the CS1000.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*HG SM to CS1K75	*HG Session Manager	UDP	*5085	*CS1K7.5	*5085	Trusted	<input type="checkbox"/>	

The following screen illustrates the Entity Link to the Avaya SBCE.

The screenshot shows the 'Entity Links' configuration page. The left sidebar contains a menu with 'Entity Links' highlighted. The main area shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service, and Notes. The single row shows a link from 'HG SM' to 'HG ASBCE' with a 'Trusted' connection policy.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* HG SM to HG ASBCE	* HG Session Manager	TCP	* 5060	* HG ASBCE	* 5060	Trusted	<input type="checkbox"/>	

The following screen shows the list of Entity Links. Note that only the highlighted links were created for the compliance test, and are the relevant links for these Application Notes.

The screenshot shows the 'Entity Links' list page. The left sidebar contains a menu with 'Entity Links' highlighted. The main area shows a table with 17 items. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service, and Notes. Several rows are highlighted in red, including 'HG SM to CS1K75', 'HG SM to HG AA-SBC', and 'HG SM to HG ASBCE'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
AAC	HG Session Manager	TCP	5060	AAC	5060	Trusted	<input type="checkbox"/>	AAC Entity Link
HG SM to CM Trk 2	HG Session Manager	TCP	5070	HG CM Trunk 2	5070	Trusted	<input type="checkbox"/>	
HG SM to CS1K75	HG Session Manager	UDP	5085	CS1K7.5	5085	Trusted	<input type="checkbox"/>	
HG SM to HG AA-SBC	HG Session Manager	TCP	5060	HG AA-SBC	5060	Trusted	<input type="checkbox"/>	
HG SM to HG ASBCE	HG Session Manager	TCP	5060	HG ASBCE	5060	Trusted	<input type="checkbox"/>	

## 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 were added for this compliance test: One for the CS1000 and one for the 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 following screen is displayed.

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**. 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 screen shows the Routing Policy for the CS1000.

The screenshot displays the 'Routing Policy Details' page for a policy named 'To CS1K75'. The left navigation pane shows 'Routing Policies' selected. The main content area has two sections: 'General' and 'SIP Entity as Destination'. In the 'General' section, the 'Name' field is 'To CS1K75', 'Disabled' is unchecked, 'Retries' is '0', and 'Notes' is 'Inbound Calls to CS1K75'. In the 'SIP Entity as Destination' section, there is a 'Select' button and a table with one entry.

Name	FQDN or IP Address	Type	Notes
CS1K7.5	172.16.20.60	Other	CS1000 Rel. 7.5



The following screen shows the Routing Policy for the Avaya SBCE.

Routing Policy Details

General

\* Name: HG ASBCE

Disabled: ☐

\* Retries: 0

Notes: Outbound calls via ASBCE

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
HG ASBCE	172.16.5.71	Other	HG ASBCE

## 6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were configured to route calls from the CS1000 to Hawaiian Telecom 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 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 configured in **Section 6.2** used in the matching 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.

The example shown below is for dial pattern **1** for the North American Numbering Plan area prefix, which have a destination domain of **voip.hawaiiintel.net**, Originating Location Name of **HG Lab**, and uses Routing Policy **HG ASBCE**.

**Dial Pattern Details**

**General**

\* Pattern: 1  
 \* Min: 1  
 \* Max: 11

Emergency Call: ☐  
 Emergency Priority: 1  
 Emergency Type:   
 SIP Domain: voip.hawaiiintel.net  
 Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K <sub>0</sub> )	HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE

Select : All, None

The next example shown below is for dial pattern **80** to route inbound calls to DID numbers provided by Hawaiian Telecom (DID numbers assigned to extensions in the CS1000), which have a destination domain of **-ALL-**, Originating Location Name of **-ALL-**, and uses Routing Policy **To CS1K75**. Note that **-ALL-** is being used for the SIP Domain and the Originating Location Name since pattern **80** is being shared with other domain and originating locations being used by other test activities in the lab.

**Dial Pattern Details**

**General**

\* Pattern: 80  
 \* Min: 2  
 \* Max: 36

Emergency Call: ☐  
 Emergency Priority: 1  
 Emergency Type:   
 SIP Domain: -ALL-  
 Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any originating location	To CS1K75		<input type="checkbox"/>	CS1K7.5	Inbound Calls to CS1K75

Select : All, None

The same procedure should be followed to add other required dial patterns.

## 6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was done as part of the initial Session Manager installation. To add 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 Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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.

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 the IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager above.
- **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 Session Manager. The screen below shows the Session Manager values used for the compliance test.

Session Manager Administration

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |

Expand All | Collapse All

General

SIP Entity Name: HG Session Manager

Description: Lab-HG SM

Management Access Point Host Name/IP: 172.16.5.31

Direct Routing to Endpoints: Enable

Security Module

SIP Entity IP Address: 172.16.5.32

Network Mask: 255.255.255.0

Default Gateway: 172.16.5.254

Call Control PHB: 46

QOS Priority: 6

Speed & Duplex: Auto

VLAN ID: .

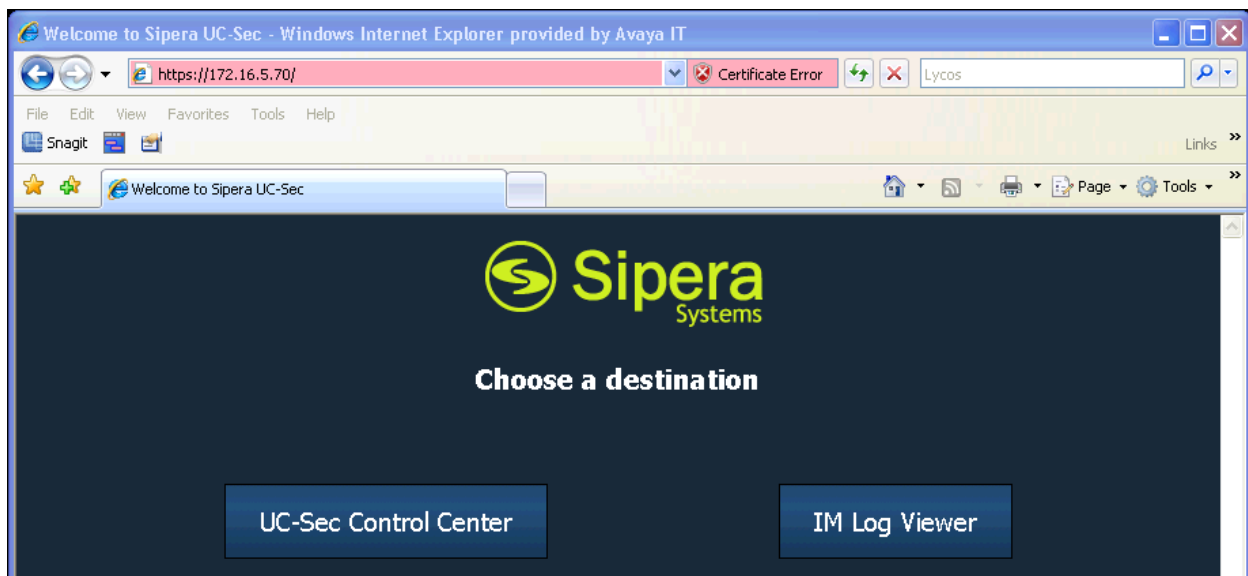
## 7. Configure the Avaya Session Border Controller for Enterprise (Avaya SBCE).

This section describes the required configuration of the Avaya SBCE to connect to Hawaiian Telecom's SIP Trunk service.

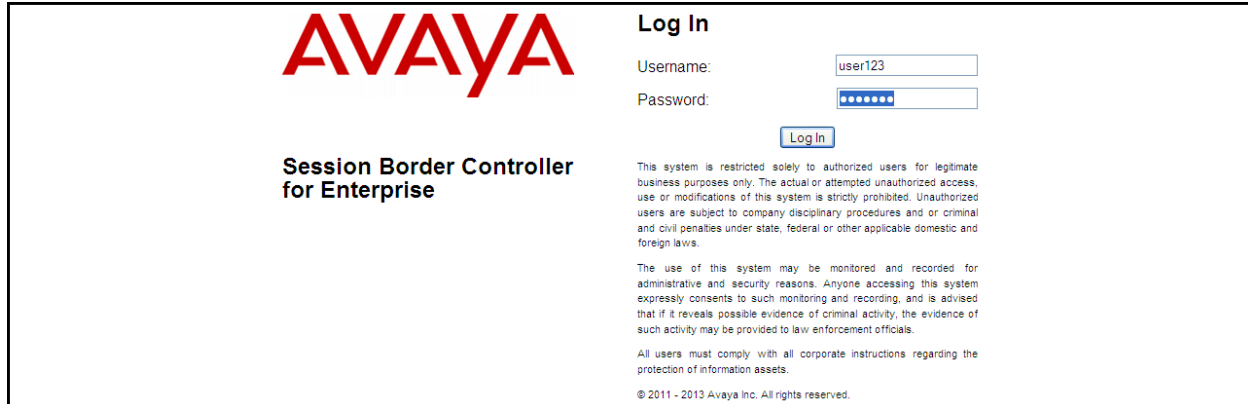
It is assumed that the Avaya SBCE is provisioned and ready to be used on the IP network. The configuration shown here is accomplished using the Avaya SBCE web interface.

### 7.1. Log in Avaya SBCE

Access the web interface by typing "https://x.x.x.x" (where x.x.x.x is the management IP address of the Avaya SBCE)



Select **UC-Sec Control Center** and enter the **Username** and **password**.

The image shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, there is a "Log In" section. It includes a "Username:" label with a text input field containing "user123", and a "Password:" label with a password input field showing masked characters. Below the password field is a blue "Log In" button. To the right of the login fields, there is a disclaimer: "This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws." Below this is another disclaimer: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." At the bottom, it states: "All users must comply with all corporate instructions regarding the protection of information assets." and "© 2011 - 2013 Avaya Inc. All rights reserved."

## 7.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters that affect all the devices under the UC-Sec control Center.

### 7.2.1. Server Interworking Avaya-SM

Interworking Profile features are configured to facilitate interoperability of implementations between enterprise SIP-enabled solutions and different SIP trunk service providers.

Several profiles have already been pre-defined and are populated in the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or “cloned”, and then modified to meet specific requirements for the enterprise SIP-enabled solution.

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone** (not shown).

Enter the new profile name in the **Clone Name** field, the name of **Avaya-SM** was chosen in this example. Click **Finish**.

For the newly created **Avaya-SM** profile, click **Edit** (not shown) at the bottom of the General tab

- Verify that for **Hold Support**, **RFC2543** is selected.
- Verify that **T.38 Support** is selected.
- Click **Next**.
- Leave other fields with their default values.
- Click **Finish** on the **Privacy and DTMF** tab (not shown).

The following screen capture shows the newly added **Avaya-SM** Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The 'Global Profiles' section is expanded, and 'Server Interworking' is selected. The main area is titled 'Interworking Profiles: Avaya-SM' and contains a list of profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, **Avaya-SM** (highlighted), and SP-General. An 'Add' button is at the top. The 'Avaya-SM' profile is selected, showing its configuration tabs: General, Timers, URI Manipulation, Header Manipulation, and Advanced. The 'General' tab is active, showing a table of settings. The 'Hold Support' setting is set to 'RFC2543'. The 'T.38 Support' setting is set to 'Yes'. The 'Privacy' section shows 'Privacy Enabled' set to 'No' and a 'User Name' field.

General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	

### 7.2.2. Server Interworking SP-General

A second Server Interworking profile named **SP-General** was created for the Service Provider.

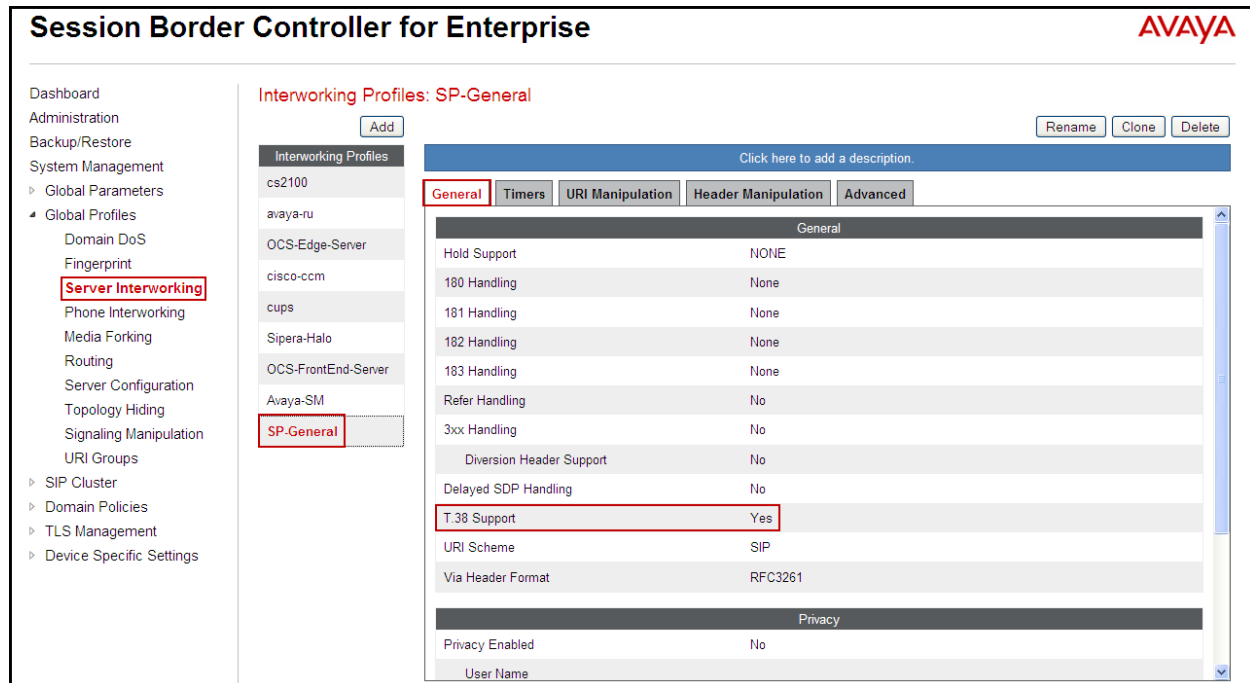
On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **Add**.

Enter the new profile name (not shown), the name of **SP-General** was chosen in this example. Accept the default values for all fields by clicking **Next** and then click **Finish**.

For the newly created **SP-General** profile, click **Edit** (not shown) at the bottom of the General tab.

- Select **T.38 Support**
- Click **Next**.
- Leave other fields with their default values.
- Click **Finish** on the **Privacy and DTMF** tab.

The following screen capture shows the newly added **SP-General** Profile.



### 7.2.3. Routing Profiles

Routing Profiles define a specific set of routing criteria that are used, in conjunction with other types of domain policies, to determine the route that SIP packets should follow to arrive at their intended destination.

Two Routing Profiles were created in the test configuration; one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are sent to the Service Provider SIP trunk.

To create the inbound route, from the **Global Profiles** menu on the left-hand side:

- Select the **Routing** tab.
- Select **Add Profile**.
- Enter Profile Name: **Route\_to\_SM**.
- Click **Next**.

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.32** (Session Manager IP address).
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport: TCP**.
- Click **Finish**.

The following screen shows the newly added **Route\_to\_SM** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Routing' highlighted. The main content area is titled 'Routing Profiles: Route\_to\_SM'. It features a list of routing profiles on the left: 'default', 'Route\_to\_SM' (highlighted), 'Route\_to\_SP', and 'Route\_to\_CM'. The 'Route\_to\_SM' profile is selected, and its configuration is shown on the right. The configuration includes a table with the following data:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	172.16.5.32	---

The 'View' and 'Edit' buttons are visible next to the table entry.

Similarly, for the outbound route:

- Select **Add Profile**.
- Enter Profile Name: **Route\_to\_SP**
- Click **Next**.
- **Next Hop Server 1: 192.168.102.27** (Service Provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport: UDP**.
- Click **Finish**.

The following screen capture shows the newly added **Route\_to\_SP** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Routing' highlighted. The main content area is titled 'Routing Profiles: Route\_to\_SP'. It features a list of routing profiles on the left: 'default', 'Route\_to\_SM', 'Route\_to\_SP' (highlighted), and 'Route\_to\_CM'. The 'Route\_to\_SP' profile is selected, and its configuration is shown on the right. The configuration includes a table with the following data:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	192.168.102.27	---

The 'View' and 'Edit' buttons are visible next to the table entry.



## 7.2.4. Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (Session Manager) and the Trunk Server or SIP Proxy at the service provider's network.

To add the profile for the Call Server, from the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration**. Click **Add Profile** and enter the profile name: **Session Manager**.

On the **Add Server Configuration Profile** Tab:

- Select **Call Server** for **Server Type**.
- **IP Address: 172.16.5.32** (IP Address of Session Manager Security Module).
- **Supported Transports: Check TCP**.
- **TCP Port: 5060**.
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

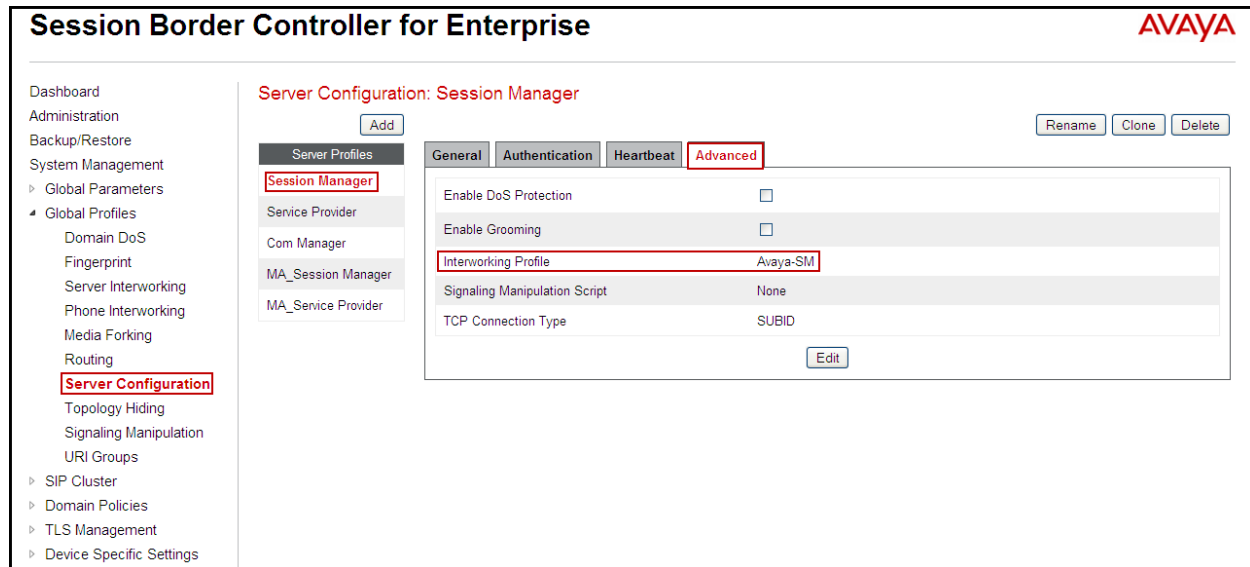
The following screen capture shows the **General** tab of the newly added **Session Manager** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The main title is "Session Border Controller for Enterprise" with the Avaya logo in the top right. The left navigation pane includes sections like Dashboard, Administration, System Management, Global Parameters, Global Profiles (with "Server Configuration" selected), SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Server Configuration: Session Manager" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. Below this are tabs for "General", "Authentication", "Heartbeat", and "Advanced". The "General" tab is active, showing a table with the following configuration:

Server Type	Call Server
IP Addresses / FQDNs	172.16.5.32
Supported Transports	TCP
TCP Port	5060

An "Edit" button is located at the bottom right of the configuration table.

The following screen capture shows the **Advanced** tab of the added **Session Manager** Profile.



To add the profile for the Trunk Server, from the **Server Configuration** screen, click **Add Profile** and enter the profile name: **Service Provider**.

On the **Add Server Configuration Profile** Tab:

- Select **Trunk Server** for **Server Type**.
- **IP Address: 192.168.102.27** (service provider's SIP Proxy IP address).
- **Supported Transports: Check UDP.**
- **UDP Port: 5060.**
- Click **Next**.
- Select **Enable Authentication**.
- Enter the **user name** provided by Hawaiian Telecom in the **User Name** field.
- Enter the **realm** provided by Hawaiian Telecom in the **Realm** field.
- Enter the **password** provided by Hawaiian Telecom in the **Password** field.
- Re-enter the password provided by Hawaiian Telecom in the **Confirm Password** field
- Click **Next** to continue.
- Select **Enable Heartbeat**.
- Select **Register** under **Method**.
- Enter **frequency** for registration challenges (Value of **60** seconds was used in the compliance testing).
- Enter the **From URI** information (i.e., **8085551234@192.168.157.187**)  
Explanation of values used in the compliance testing:
  - **8085551234** is the pilot user provided by Hawaiian Telecom for registration purpose.
  - **192.168.157.187** is the outside IP address assigned to the Avaya SBCE.
- Enter the **To URI** information (i.e., **8085551234@hawaiiantel.net**).
  - **8085551234** is the pilot user provided by Hawaiian Telecom for registration purpose.
  - **Hawaiiantel.net** is the domain name provided by Hawaiian Telecom.

- Click **Next** to continue.
- On the **Advanced** tab, select **SP General** from the **Interworking Profile** drop down menu.  
Leave other fields with their default values for now, a **Signaling Manipulation** Script will be assigned later.
- Click **Finish**.

The following screen capture shows the **General** tab of the **Service Provider** Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, and System Management. The 'Server Configuration' section is expanded, and 'Service Provider' is selected. The main area shows the 'Server Configuration: Service Provider' page with tabs for General, Authentication, Heartbeat, and Advanced. The 'General' tab is active, showing a table with the following data:

Field	Value
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.102.27
Supported Transports	UDP
UDP Port	5060

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible at the top right of the configuration area.

The following screen capture shows the **Authentication** tab of the **Service Provider** Profile.

This screenshot shows the same 'Session Border Controller for Enterprise' interface, but with the 'Authentication' tab selected. The configuration table is as follows:

Field	Value
Enable Authentication	<input checked="" type="checkbox"/>
User Name	8085551234
Realm	Realm123

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

The following screen capture shows the **Heartbeat** tab of the **Service Provider** Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Global Profiles. The 'Server Configuration' option is highlighted. The main area is titled 'Server Configuration: Service Provider' and contains tabs for General, Authentication, Heartbeat, and Advanced. The 'Heartbeat' tab is active, showing a table of heartbeat settings. The 'Enable Heartbeat' checkbox is checked. The table lists the Method as REGISTER, Frequency as 60 seconds, From URI as 8085551234@192.168.157.187, and To URI as 8085551234@voip.hawaiiantel.net. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

Server Configuration: Service Provider	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER
Frequency	60 seconds
From URI	8085551234@192.168.157.187
To URI	8085551234@voip.hawaiiantel.net

The following screen capture shows the **Advanced** tab of the **Service Provider** Profile.

This screenshot shows the 'Advanced' tab of the 'Service Provider' profile in the same interface. The 'Advanced' tab is selected, displaying a table of advanced settings. The 'Enable DoS Protection' and 'Enable Grooming' checkboxes are unchecked. The 'Interworking Profile' is set to 'SP-General', which is highlighted with a red box. The 'Signaling Manipulation Script' is set to 'None', and the 'UDP Connection Type' is set to 'SUBID'. The 'Edit' button is at the bottom right.

Server Configuration: Service Provider	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
UDP Connection Type	SUBID

## 7.2.5. Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in SIP headers like To, From, Request-URI, Via, Record-Route and SDP to the IP addresses or domains expected by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the Enterprise to the public network.

To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on the **default** profile and select **Clone Profile**.
- Enter the **Profile Name: Session\_Manager**.
- Click **Finish**.

The following screen capture shows the newly added **Session\_Manager** Profile. Note that for Session Manager no values were overwritten (default).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and SIP Cluster. Under Global Profiles, 'Topology Hiding' is selected. The main area is titled 'Topology Hiding Profiles: Session\_Manager'. It shows a list of profiles: 'default', 'cisco\_th\_profile', 'Session\_Manager' (highlighted), 'Service\_Provider', and 'Com Manager'. An 'Add' button is above the list. Below the list, the 'Session\_Manager' profile is expanded, showing a table of Topology Hiding rules. The table has columns: Header, Criteria, Replace Action, and Overwrite Value. The rules are: Request-Line (IP/Domain, Auto, ---), Record-Route (IP/Domain, Auto, ---), From (IP/Domain, Auto, ---), To (IP/Domain, Auto, ---), SDP (IP/Domain, Auto, ---), and Via (IP/Domain, Auto, ---). An 'Edit' button is at the bottom of the table.

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

To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

- Click on the **default** profile and select **Clone Profile**
- Enter the **Profile Name: Service\_Provider**.
- Click **Finish**.
- Click **Edit** on the newly added **Service\_Provider** Topology Hiding profile.
- For the **From** header, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**voip.hawaiiintel.net**) under **Overwrite Value**.
- For the **To** header, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**voip.hawaiiintel.net**) under **Overwrite Value**.

- For the **Request-Line**, choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**voip.hawaiiintel.net**) under **Overwrite Value**.
- Click **Finish**.

The following screen capture shows the newly added **Service\_Provider** Profile.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ Domain DoS  
‣ Fingerprint  
‣ Server Interworking  
‣ Phone Interworking  
‣ Media Forking  
‣ Routing  
‣ Server Configuration  
**Topology Hiding**  
‣ Signaling Manipulation  
‣ URI Groups  
‣ SIP Cluster  
‣ Domain Policies  
‣ TLS Management  
‣ Device Specific Settings

**Topology Hiding Profiles: Service\_Provider**

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

Click here to add a description.

**Topology Hiding**

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

[Edit](#)

## 7.2.6. Signaling Manipulation

The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation, or SigMa Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For the test configuration, the Editor was used to create the script needed to handle the header manipulation described below.

From the **Global Profiles** menu on the left panel (not shown), select **Signaling Manipulation** (not shown). Click on **Add Script** (not shown) to open the SigMa Editor screen (not shown).

- For the **Title**, enter **Remove\_Unwanted\_Headers**.
- Enter the script as shown on the screen below.
- click **Save**

## Signaling Manipulation Editor

AVAYA

Title Remove\_Unwanted\_Headers
Save

```

1 within session "ALL"
2 {
3   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
4   {
5
6     // Remove unwanted Headers
7
8     remove(%HEADERS["Alert-Info"][1]);
9     remove(%HEADERS["x-nt-e164-clid"][1]);
10    remove(%HEADERS["History-info"][1]);
11
12    // Remove unwanted mimes from the body.
13
14    // The SBC will not remove the SDP MIME, so "x-nt-mcdn-frag-hex" = %BODY[1]
15    // After "x-nt-mcdn-frag-hex" is removed, "x-nt-esn5-frag-hex" moves up one...
16    // So the same command removes "x-nt-esn5-frag-hex".
17    // And so on (e.g., "x-nt-epid-frag-hex").
18
19    remove(%BODY[1]);
20    remove(%BODY[1]);
21    remove(%BODY[1]);
22  }
23 }
24
25

```

The following screen capture shows the added **Remove\_Unwanted\_Headers** Script.

## Session Border Controller for Enterprise

AVAYA

- Dashboard
- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
    - Domain DoS
    - Fingerprint
    - Server Interworking
    - Phone Interworking
    - Media Forking
    - Routing
    - Server Configuration
    - Topology Hiding
    - Signaling Manipulation**
    - URI Groups
  - SIP Cluster
  - Domain Policies
  - TLS Management
  - Device Specific Settings

### Signaling Manipulation Scripts: Remove\_Unwanted\_Headers

Upload
Add

Download
Clone
Delete

Signaling Manipulation Scripts
Click here to add a description.

Remove\_Replace H...
Signaling Manipulation

```

within session "ALL"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {

    // Remove unwanted Headers

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

    // Remove unwanted mimes from the body.

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

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

```

Edit

After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 7.2.4**.

Go to **Global Profiles** → **Server Configuration** → **Service Provider** → **Advanced** tab → **Edit**. Select **Remove\_Unwanted\_Headers** from the drop down menu on the **Signaling Manipulation Script** field. Click **Finish** to save and exit.

HG; Reviewed:  
SPOC 1/17/2014

Solution & Interoperability Test Lab Application Notes  
©2013 Avaya Inc. All Rights Reserved.

87 of 106  
HTCS1KSMASBCE

**Edit Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

**Signaling Manipulation Script** Remove\_Unwanted\_Headers

UDP Connection Type SUBID PORTID MAPPING

**Finish**

The following screen capture shows the **Advanced** tab of the previously added **Service Provider** Profile with the **Signaling Manipulation Script** assigned.

**Session Border Controller for Enterprise**

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

**Server Configuration: Service Provider**

**Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

**Signaling Manipulation Script** Remove\_Unwanted\_Headers

UDP Connection Type SUBID

**Edit**

## 7.3. Domain Policies

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

### 7.3.1. Create Application Rules

Application Rules defines which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: Voice, video, and/or Instant Messaging (IM). In



addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select **default** Rule (not shown)
- Select **Clone Rule** button (not shown)
- **Name:** **new\_default**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to the recommended values. The value of **1000** was used in the sample configuration.
- Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Domain Policies', and 'Application Rules' is selected. The main content area is titled 'Application Rules: 1000 Sessions'. It features a list of application rules on the left, with '1000 Sessions' highlighted. The main table displays the configuration for the 'Voice' application type, showing 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint' both set to 1000. The 'Video' and 'IM' application types are also listed but have their respective checkboxes unchecked. Below the table, there is a 'Miscellaneous' section with 'CDR Support' set to 'None' and 'RTCP Keep-Alive' set to 'No'. An 'Edit' button is located at the bottom right of the configuration area.

### 7.3.2. Media Rules

For the compliance test, the **default-low-med** Media Rule was used.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Domain Policies', and 'Media Rules' is selected. The main content area is titled 'Media Rules: default-low-med'. It features a list of media rules on the left, with 'default-low-med' highlighted. The main content area displays a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below the warning, there are tabs for 'Media NAT', 'Media Encryption', 'Media Anomaly', 'Media Silencing', and 'Media QoS'. The 'Media NAT' tab is active, showing a text input field for 'Media NAT' with the placeholder text 'Learn Media IP dynamically'. An 'Edit' button is located at the bottom right of the configuration area.

### 7.3.3. Signaling Rules

Signaling Rules define the actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow control of the Quality of Service of the signaling packets.

The Alert-Info, P-Location and P-Charging-Vector headers are sent in SIP messages from Session Manager to the Avaya SBCE, and then to the Service Provider's network. These headers should not be exposed outside of the enterprise. For simplicity, these headers were removed (blocked) from both requests and responses for both inbound and outbound calls.

A Signaling Rule was created, to be later applied in the direction of the Enterprise or the Service Provider. To create a rule to block the Alert-Info, P-Location and P-Charging-Vector headers coming from Session Manager, and from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** Signaling Rules.
- Click on **Clone Rule**.
- Enter a name: **Remove Headers**.
- Click **Finish**.

Select the **Request Headers** tab of the newly created Signaling Rule.

To add the Alert-Info header:

- Select **Add in Header Control**.
- **Header Name: Alert-Info**.
- **Method Name: INVITE**.
- **Header Criteria: Forbidden**.
- **Presence Action: Remove Header**.
- Click **Finish**.

To add the P-Location header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name: P-Location**.
- **Method Name: INVITE**.
- **Header Criteria: Forbidden**.
- **Presence Action: Remove Header**.
- Click **Finish**.

To add the P-Charging-Vector header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name: P-Charging-Vector**.
- **Method Name: INVITE**.

- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**
- 

The following screen capture shows the **Request Headers** tab of the **Remove Headers** Signaling Rule.

**Session Border Controller for Enterprise** AVAYA

**Signaling Rules: Remove Headers**

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Click here to add a description.

Tabs: General, Requests, Responses, **Request Headers**, Response Headers, Signaling QoS

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Select the **Response Headers** tab.

To add the Alert-Info header:

- Select **Add in Header Control.**
- **Header Name: Alert-Info.**
- **Response Code: 200.**
- **Method Name: INVITE.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the P-Location header:

- Select **Add in Header Control.**
- Check the **Proprietary Request Header** box.
- **Header Name: P-Location.**
- **Response Code: 200.**
- **Method Name: INVITE.**
- **Header Criteria: Forbidden.**
- **Presence Action: Remove Header.**
- Click **Finish.**

To add the P-Charging-Vector header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box.
- **Header Name: P-Charging-Vector**.
- **Response Code: 200**.
- **Method Name: INVITE**.
- **Header Criteria: Forbidden**.
- **Presence Action: Remove Header**.
- Click **Finish**.

The following screen capture shows the **Response Headers** tab of the **Service Provider** Signaling Rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Signaling Rules' highlighted. The main content area is titled 'Signaling Rules: Remove Headers' and includes an 'Add' button and a 'Filter By Device...' dropdown. Below this, there are tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers' (which is selected), and 'Signaling QoS'. The 'Response Headers' tab contains a table with three rows of header information. The table has columns for Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, Direction, and Edit/Delete links. The three rows are: 1. Alert-Info, 200, ALL, Forbidden, Remove Header, No, IN; 2. P-Charging-Vector, 200, ALL, Forbidden, Remove Header, Yes, IN; 3. P-Location, 200, ALL, Forbidden, Remove Header, Yes, IN. Above the table, there are buttons for 'Add In Header Control' and 'Add Out Header Control'.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

### 7.3.4. End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the Enterprise, from the **Domain Policies** menu, select **End Point Policy Groups**. Select **Add Group**.

- **Group Name: Enterprise**.
- **Application Rule: 1000 Sessions**.
- **Border Rule: default**.
- **Media Rule: default-low-med**.
- **Security Rule: default-low**.
- **Signaling Rule: Remove Headers**.
- **Time of Day: default**.
- Click **Finish**.

The following screen capture shows the newly added **Enterprise** End Point Policy Group.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
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  
‣ TLS Management  
‣ Device Specific Settings

**Policy Groups: Enterprise**

Filter By Device...

Click here to add a description.

Hover over a row to see its description.

**Policy Group**

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	1000 Sessions	default	default-low-med	default-low	Remove Headers	default	Edit Clone

**Enterprise**

Service Provider

Similarly, to create an End Point Policy Group for the Service Provider SIP Trunk, select **Add Group**.

- **Group Name: Service Provider.**
- **Application Rule: 1000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: default.**
- **Time of Day: default.**
- **Click Finish.**

The following screen capture shows the newly added **Service Provider** End Point Policy Group.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
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  
‣ TLS Management  
‣ Device Specific Settings

**Policy Groups: Service Provider**

Filter By Device...

Click here to add a description.

Hover over a row to see its description.

**Policy Group**

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	1000 Sessions	default	default-low-med	default-low	default	default	Edit Clone

**Enterprise**

**Service Provider**

## 7.4. Device Specific Settings

The **Device Specific Settings** allow the management of various device-specific parameters, which determine how a particular device will function when deployed in the network. Specific server parameters, like network and interface settings, as well as call flows, etc. are defined here.

### 7.4.1. Network Management

The network information should have been previously completed. To verify the network configuration, from the **Device Specific Settings** menu on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

**Session Border Controller for Enterprise** AVAYA

**Network Management: Sipera**

Devices **Network Configuration** Interface Configuration

Sipera

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**.

Changes will not take effect until the interface is updated.

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.192 B2 Netmask:

Add Save Clear

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
192.168.157.187		192.168.157.129	B1	Delete

In the event that changes need to be made to the network configuration information, they could be entered here.

On the Interface Configuration tab, click the **Toggle** control for interfaces **A1** and **B1** to change the status to **Enabled**. It should be noted that the default state for all interfaces is **disabled** so it is important to perform this step or the Avaya SBCE will not be able to communicate on any of its interfaces.

# Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings

Network Management

Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting

## Network Management: Sipera

Devices

Sipera

Network Configuration

Interface Configuration

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

## 7.4.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private and Public interfaces of the Avaya SBCE, the port range of 35000 to 40000 was used.

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**

- Select **Add Media Interface**.
- **Name: Private**.
- **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000**.
- Click **Finish**.
- Select **Add Media Interface**.
- **Name: Public**.
- **IP Address: 192.168.157.187** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000**.
- Click **Finish**.

The following screen capture shows the added **Media Interfaces**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left-hand navigation menu includes options like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. Under Device Specific Settings, the Media Interface option is highlighted. The main content area is titled 'Media Interface: Sipera'. It features a table with columns for Name, Media IP, and Port Range. The table lists four media interfaces: Private, Public, MA\_Private\_med, and MA\_Public\_med. The Private and Public interfaces are highlighted with a red border. A warning message at the top states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add' button is located at the top right of the table.

Name	Media IP	Port Range	Edit	Delete
Private	172.16.5.71	35000 - 40000	Edit	Delete
Public	192.168.157.187	35000 - 40000	Edit	Delete
MA_Private_med	172.16.5.73	35000 - 40000	Edit	Delete
MA_Public_med	192.168.157.143	35000 - 40000	Edit	Delete

### 7.4.3. Signaling Interface

To create the Signaling Interface toward Session Manager, from the **Device Specific Settings** menu on the left hand side, select **Signaling Interface**

- Select **Add Signaling Interface**:
- **Name: Private.**
- **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port: 5060.**
- Click **Finish.**
- Select **Add Signaling Interface**:
- **Name: Public**
- **IP Address: 192.168.157.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**



The following screen capture shows the newly added **Signaling Interfaces**.

**Session Border Controller for Enterprise**
AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
**Signaling Interface**
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting

**Signaling Interface: Sipera**

Devices
**Sipera**

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private	172.16.5.71	5060	---	---	None	Edit Delete
Public	192.168.157.187	---	5060	---	None	Edit Delete

#### 7.4.4. End Point Flows

When a packet is received by the UC-Sec, 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.

The **End-Point Flows** define certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, then the **Server Flows** tab. Click **Add Flow**.

- **Name:** SIP\_Trunk\_Flow.

HG; Reviewed:  
SPOC 1/17/2014

Solution & Interoperability Test Lab Application Notes  
©2013 Avaya Inc. All Rights Reserved.

97 of 106  
HTCS1KSMASBCE

- **Server Configuration: Service Provider.**
- **URI Group: \***
- **Transport: \***
- **Remote Subnet: \***
- **Received Interface: Private.**
- **Signaling Interface: Public.**
- **Media Interface: Public.**
- **End Point Policy Group: Service Provider.**
- **Routing Profile: Route\_to\_SM** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service\_Provider.**
- **File Transfer Profile: None.**
- Click **Finish**.

View Flow: SIP_Trunk_Flow		X	
Criteria		Profile	
Flow Name	SIP_Trunk_Flow	Signaling Interface	Public
Server Configuration	Service Provider	Media Interface	Public
URI Group	*	End Point Policy Group	Service Provider
Transport	*	Routing Profile	Route_to_SM
Remote Subnet	*	Topology Hiding Profile	Service_Provider
Received Interface	Private	File Transfer Profile	None

To create the call flow toward Session Manager, click **Add Flow**.

- **Name: Session\_Manager\_Flow.**
- **Server Configuration: Session Manager.**
- **URI Group: \***
- **Transport: \***
- **Remote Subnet: \***
- **Received Interface: Public**
- **Signaling Interface: Private.**
- **Media Interface: Private.**
- **End Point Policy Group: Enterprise.**
- **Routing Profile: Route\_to\_SP** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Session\_Manager.**
- **File Transfer Profile: None.**
- Click **Finish**.

View Flow: Session_Manager_Flow		X	
Criteria		Profile	
Flow Name	Session_Manager_Flow	Signaling Interface	Private
Server Configuration	Session Manager	Media Interface	Private
URI Group	*	End Point Policy Group	Enterprise
Transport	*	Routing Profile	Route_to_SP
Remote Subnet	*	Topology Hiding Profile	Session_Manager
Received Interface	Public	File Transfer Profile	None

The following screen capture shows the added **End Point Flows**.

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
**End Point Flows**
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting

End Point Flows: Sipera

Devices

Sipera

Subscriber Flows

Server Flows

Click here to add a row description.

Add

Server Configuration: Service Provider

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SIP_Trunk_Flow	*	Private	Public	Service Provider	Route_to_SM	View Clone Edit Delete

Server Configuration: Session Manager

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Session_Manager_Flow	*	Public	Private	Enterprise	Route_to_SP	View Clone Edit Delete

## 8. Hawaiian Telecom SIP Trunk Service Configuration

To use Hawaiian Telecom SIP Trunk service, a customer must request the service from Hawaiian Telecom using their sales processes. The process can be started by contacting Hawaiian Telecom via the corporate web site at:

<https://www.hawaiiantel.com/business/Business.aspx> or by calling: 1-808-643-0944 and requesting information.

During the signup process, Hawaiian Telecom will require that the customer provide the public IP address used to reach the Avaya SBCE at the edge of the enterprise. Hawaiian Telecom will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, SIP Trunk Registration information, etc. This information is used to complete the CS1000, Session Manager, and Avaya SBCE configuration discussed in the previous sections.

## 9. Verification Steps

The following steps may be used to verify the configuration.

### 9.1. General

Place an inbound/outbound call to/from a PSTN phone to/from an internal CS1000 phone, answer the call, and verify that two-way speech path exists. Check call display number to ensure the correct information was sent/received. Perform hold/retrieve on calls. Verify the call remains stable for several minutes and disconnects properly.

## 9.2. Verify Call Establishment on the CS1000 Call Server

### Active Call Trace (LD 80).

The following is an example of one of the commands available on the CS1000 to trace the extension (DN) when the call is in progress and/or idle. The call scenario involved the CS1000 extension 8000 calling a PSTN phone number (7861234567).

- Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail)
- Login to the Overlay command prompt, issue the command **LD 80** and then **trac 0 8000**.
- After the call is released, issue the command **trac 0 8000** again to see if the DN is released back to an idle state.

Below is the actual output of the Call Server Command Line mode when extension 8000 is in an active call:

Note that IP addresses and telephone numbers have been masked for security reasons.

```
>ld 80
TRA000
.trac 0 8000

ACTIVE   VTN 008 0 00 00

ORIG     VTN 008 0 00 00  KEY 0   SCR MARP  CUST 0   DN 8000  TYPE 1165
SIGNALLING ENCRYPTION: INSEC
FAR-END SIP SIGNALLING IP: 172.16.21.61
FAR-END MEDIA ENDPOINT IP: 172.16.20.32  PORT: 5200
FAR-END VendorID: Not available
TERM     VTN 048 0 00 10  VTRK IPTI  RMBR  0 11 OUTGOING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 172.16.5.71
FAR-END MEDIA ENDPOINT IP: 172.16.5.71  PORT: 35032
FAR-END VendorID: AVAYA-SM-6.3.1.0.631004
MEDIA PROFILE: CODEC G.729A NO-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT 101   TXPT 101   DIAL DN 91786[REDACTED]
MAIN_PM   ESTD
TALKSLOT  ORIG 12    TERM 17    JUNCTOR  ORIGO  TERMO
EES_DATA:
NONE
QUEU  NONE
CALL ID 0 309

----  ISDN ISL CALL (TERM)  ----
CALL REF # = 395
BEARER CAP = VOICE
HLC =
CALL STATE = 10      ACTIVE
CALLING NO = 808[REDACTED]  NUM_PLAN:E164  TON:NATIONAL  ESN:NPA
CALLED NO  = 1786[REDACTED]  NUM_PLAN:E164  TON:NATIONAL  ESN:NPA
```

The following screen shows an example after the call on 8000 has been released.

```
.trac 0 8000  
  
IDLE VTN 008 0 00 00   MARP
```

The following screen shows an example after the call has been released, It shows that there are no trunks busy.

```
>ld 32  
NPRO00  
.stat 48 0  
012 UNIT(S) IDLE  
000 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY
```

### 9.3. Protocol Traces

Wireshark was used to verify the following information for each call:

- RequestURI: verify the request number and SIP domain.
- From: verify the display name and display number.
- To: verify the display name and display number.
- Diversion: verify the name, number and reason code.
- P-Asserted-Identity: verify the display name and display number.
- Privacy: verify the “user, id” masking.
- Connection Information: verify IP addresses.
- Time Description: verify session timeout of far end endpoint.
- Media Description: verify audio port, codec, and DTMF event description.
- Media Attribute: verify specific audio port, codec, ptime, and send/ receive ability.
- DTMF event and fax attributes.

The following screen shows an example of a typical capture for a call made from an 1165 Deskphone (DID: 8085551234) on the CS1000 to a PSTN number (7865551234).

The screenshot displays a Wireshark packet capture on a D-Link PCI Fast Ethernet Adapter. The filter is set to 'sip'. The packet list shows a sequence of SIP messages:

No.	Time	Source	Destination	Protocol	Length	Info
32	9.034832	192.168.1.107	192.168.1.27	SIP/SDF	109	Request: INVITE sip:1786[redacted]@voip.hawaiiantel.net;use
33	9.167217	192.168.1.27	192.168.1.107	SIP	406	Status: 100 Trying
47	12.050601	192.168.1.27	192.168.1.107	SIP/SDF	1068	Status: 183 Session Progress   , with session descriptio
49	12.065750	192.168.1.107	192.168.1.27	SIP	1180	Request: OPTIONS sip:+1786[redacted]:5060;tra
50	12.067300	192.168.1.107	192.168.1.27	SIP	910	Request: PRACK sip:+1786[redacted]:5060;trans
60	12.200124	192.168.1.27	192.168.1.107	SIP	788	Status: 200 OK
62	12.203593	192.168.1.27	192.168.1.107	SIP	519	Status: 200 OK
246	13.949642	192.168.1.27	192.168.1.107	SIP/SDF	1059	Status: 200 OK   , with session description
248	13.964179	192.168.1.107	192.168.1.27	SIP	1127	Request: ACK sip:+1786[redacted]:5060;transpo
641	17.765245	192.168.1.27	192.168.1.107	SIP	636	Request: BYE sip:808[redacted]:5060;transpor
643	17.776408	192.168.1.107	192.168.1.27	SIP	741	Status: 200 OK

The packet details pane for Frame 32 (109 bytes) shows the following SIP INVITE structure:

- Session Initiation Protocol (INVITE)
- Request-Line: INVITE sip:1786[redacted]@voip.hawaiiantel.net;user=phone SIP/2.0
- Message Header
  - From: "Avaya 1165\_Uni" <sip:808[redacted]@voip.hawaiiantel.net;user=phone>;tag=2e37710-3c1410ac-13dd-55013-12c9a8-4d167681
  - To: <sip:1786[redacted]@voip.hawaiiantel.net;user=phone>
  - CSeq: 1 INVITE
  - Call-ID: 2e88e50-3c1410ac-13dd-55013-12c9a8-1398d0b3-12c9a8
  - Contact: <sip:808[redacted]:5060;transport=udp;user=phone;gsid=8b782d90-cd46-11e2-9b33-78e3b51bf2d0>
  - Record-Route: <sip:192.168.1.107:5060;ipcs-line=95;lr;transport=udp>
  - Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE
  - Supported: 100rel, x-nortel-sipvc, replaces
  - User-Agent: Nortel CS1000 SIP GW release\_7.0 version\_sslinux-7.50.17 AVAYA-SM-6.3.1.0.631004
  - Max-Forwards: 65
  - Via: SIP/2.0/UDP 192.168.1.107:5060;branch=z9hG4bK-s1632-000509876152-1--s1632-
  - Privacy: none
  - P-Asserted-Identity: "Avaya 1165\_Uni" <sip:808[redacted]@voip.hawaiiantel.net;user=phone>
  - History-Info: <sip:1786[redacted]@voip.hawaiiantel.net;user=phone>;index=1.1
  - Remote-Party-ID: "Avaya 1165\_Uni" <sip:808[redacted]@voip.hawaiiantel.net;user=phone>;party=calling;screen=no;privacy=off
  - Content-Type: application/sdp
  - D-V-Mac<30b>-Td< 7 1

## 10. Conclusion

These Application Notes describe the procedures necessary to Configure Hawaiian Telecom SIP Trunk service with Avaya Communication Server 1000E Release 7.5, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 as shown in **Figure 1**.

Hawaiian Telecom SIP Trunk service passed compliance testing with the observation/limitations noted in **Section 2.2**.



## 11. References

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

- [1] *Network Routing Service Fundamentals*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.
- [2] *IP Peer Networking Installation and Commissioning*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010
- [3] *Communication Server 1000E Overview*, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011
- [4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011
- [5] *Communication Server 1000 Dialing Plans Reference*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010
- [6] *Product Compatibility Reference*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011
- [7] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, February 2011.
- [8] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
- [9] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [10] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473.
- [11] *Administering Avaya Aura® Session Manager*, November 2010, Document Number 03-603324.
- [12] *Sipera Systems E-SBC 1U Installation Guide*. Release 4.0.5. November 2011.
- [13] *Sipera Systems E-SBC Administration Guide*. Release 4.0.5. November 2011.
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15] *RFC 2833 RTP Payload for DTMF Digits*, Telephony Tones and Telephony Signals, <http://www.ietf.org/>
- [16] *Avaya Product Support Notice – PSN003460u – Configuring FAX over IP in CS 1000: An Overview*.

---

**©2013 Avaya Inc. All Rights Reserved.**

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

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