



## **Application Notes for Configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0**

### **Abstract**

These Application Notes describe the procedure for configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 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.

CenturyLink SIP Trunk service provides PSTN access via SIP trunks between the enterprise and CenturyLink'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 an IP Telephony Node.....	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 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 the Avaya SBCE .....	30
5.5.2.	Administer Virtual D-Channel.....	32
5.5.3.	Administer Virtual Super-Loop .....	36
5.5.4.	Administer Virtual SIP Routes .....	37
5.5.5.	Administer Virtual Trunks.....	40
5.5.6.	Administer Calling Line Identification Entries.....	43
5.5.7.	Enable External Trunk to Trunk Transfer.....	45
5.6.	Administer Dialing Plans .....	45
5.6.1.	Define ESN Access Codes and Parameters (ESN) .....	45
5.6.2.	Associate NPA and SPN call to ESN Access Code 1 .....	46
5.6.3.	Digit Manipulation Block Index (DMI).....	47
5.6.4.	Route List Block (RLB).....	49
5.6.5.	Inbound Digit Translation.....	50
5.6.6.	Outbound Call - Special Number Configuration. ....	52
5.6.7.	Outbound Call - Numbering Plan Area Code (NPA) .....	54
5.7.	Administer Phone.....	54
5.7.1.	Phone creation.....	54
5.7.2.	Enable Privacy for Phone.....	55
5.7.3.	Enable Call Forward for the Phone.....	56

5.7.4.	Enable Call Waiting for the Phone .....	61
6.	Configure the Avaya Session Border Controller for Enterprise. ....	62
6.1.	Log in the Avaya SBCE .....	62
6.2.	Global Profiles.....	62
6.2.1.	Server Interworking Avaya-CS1000.....	62
6.2.2.	Server Interworking SP-General.....	64
6.2.3.	Routing Profiles .....	65
6.2.4.	Server Configuration.....	66
6.2.5.	Topology Hiding .....	69
6.2.6.	Signaling Manipulation.....	71
6.3.	Domain Policies .....	73
6.3.1.	Create Application Rules .....	73
6.3.2.	Media Rules .....	74
6.3.3.	Signaling Rules .....	75
6.3.4.	End Point Policy Groups.....	76
6.4.	Device Specific Settings.....	78
6.4.1.	Network Management.....	78
6.4.2.	Media Interface .....	80
6.4.3.	Signaling Interface.....	80
6.4.4.	End Point Flows.....	82
7.	CenturyLink SIP Trunk Service Configuration .....	85
8.	Verification Steps.....	85
8.1.	General .....	85
8.2.	Verify Call Establishment on the CS1000 Call Server .....	86
8.3.	Protocol Traces.....	88
9.	Conclusion .....	90
10.	References.....	91

# 1. Introduction

These Application Notes provide the procedure for configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 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 CenturyLink and Avaya Communication Server 1000E.

In the sample configuration, the Avaya solution consists of a Communication Server 1000E Rel. 7.6 (hereafter referred to as CS1000), Avaya Session Border Controller for Enterprise Rel. 6.2 (hereafter referred to as the Avaya SBCE), and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE.

## 2. General Test Approach and Test Results

The CS1000 system was connected to the Avaya SBCE via the Local Area Network (LAN). The Avaya SBCE was connected to CenturyLink's network via the public internet. Various call types were made from the CS1000 to CenturyLink and vice versa to verify interoperability between the CS1000 and CenturyLink.

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

### 2.1. Interoperability Compliance Testing

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

- Incoming calls from the PSTN were routed to DID numbers assigned by CenturyLink. 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 CenturyLink'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 voice mail off).
- Proper response when calling busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711 u-law/20ms, G.711 a-law/20ms and G.729/20ms with Voice Activity Detection (VAD) disabled.
- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- Call Pilot Voice Mail Server (Hosted in the CS1000).

- Outbound Toll-Free calls to Interactive Voice Response systems (IVR).
- Inbound Toll-Free.
- Local Calls and long distance calls.
- Operator assisted calls (0 and 0+10).
- Emergency calls (911).
- Directory Assistance calls (411).
- 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 CenturyLink SIP Trunk Service with the CS1000 solution was completed successfully with the following observations/limitations.

- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and CenturyLink when there is no call re-direction involved. However, when calls are re-directed to the PSTN at the CS1000 extension, the Caller ID will not properly reflect the true originator of the call. 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. The CS1000 is not sending UPDATE or re-INVITE to update the true connected Calling Party. This is a CS1000 known issue.
- **CS1000 phone holds/retrieves an outbound call:** If a CS1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed; instead the access code of the trunk route (ACOD) is displayed. Also, the trunk route (ACOD), instead of the Caller ID of the extension that originated the call, is displayed during some call transfer scenarios. These are CS1000 known issues.
- **PSTN to CS1000 calls with Privacy enabled:** Calls from the PSTN to the CS1000 with Privacy enabled (Calling Party Name/Number Block) will display the access code of the trunk route (ACOD) instead of **Anonymous**. This is a CS1000 known issue.
- **Conversion of History-Info to Diversion Header:** CenturyLink supports Diversion Header for call re-direction, Signaling Manipulation rules (SigMa script) were added to the Avaya SBCE to convert History-Info messages sent by the CS1000 to Diversion Header. Refer to **Section 6.2.6**.
- **SIP Header Optimization:** SIP header rules were implemented in the Avaya SBCE 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.

- Items not supported or not tested included the following:
  - International calls were not tested.

## 2.3. Support

For support on CenturyLink systems, visit the corporate web page at:

<http://www.CenturyLink.com/>

### 3. Reference Configuration

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

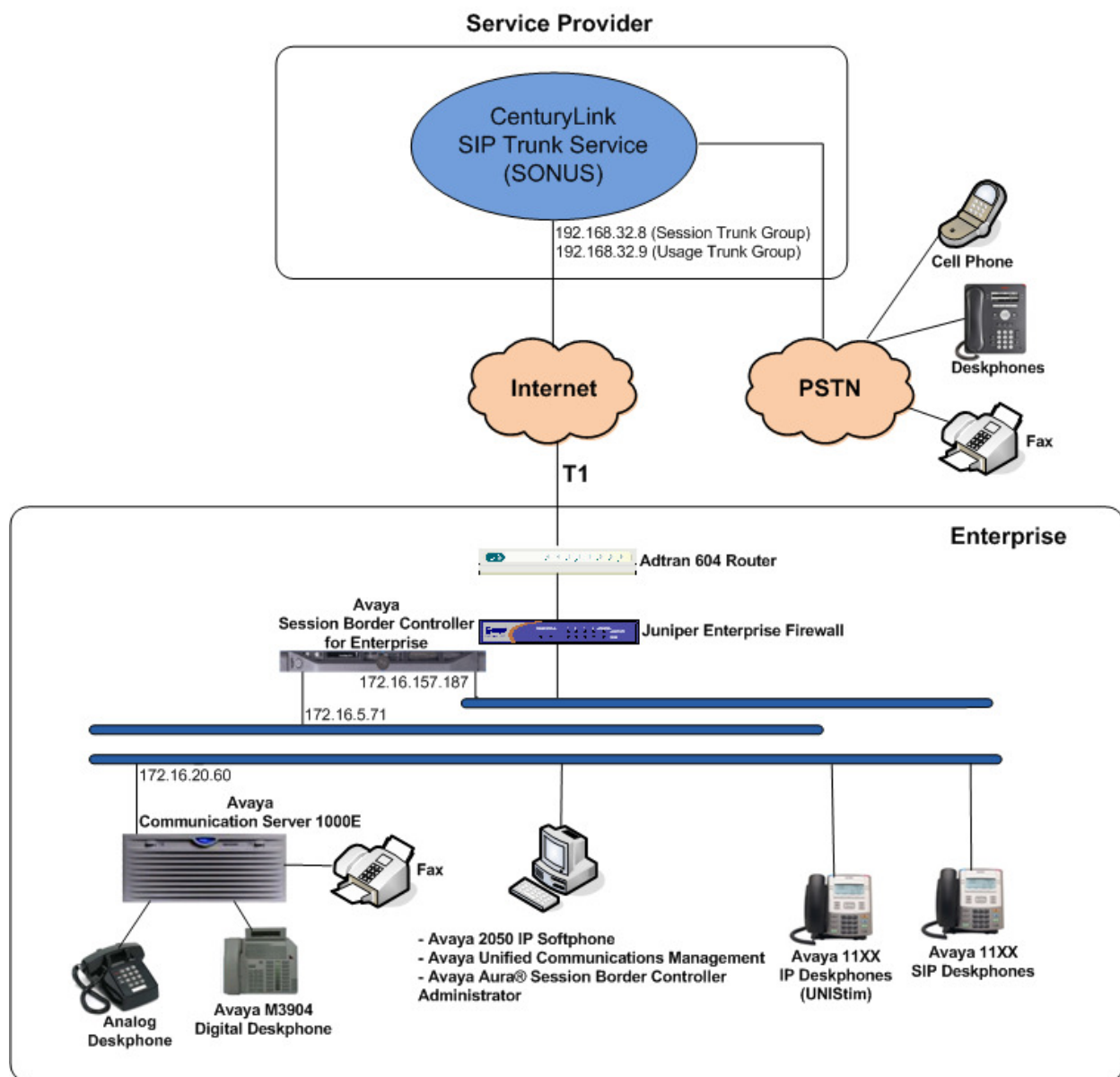
The Avaya components used to create the simulated customer site included:

- Avaya Communication Server 1000E (CS1000E).
- DELL R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 1100-Series IP Deskphones (UniStim).
- Avaya 1100-Series Deskphones (SIP).
- 2050 Avaya IP Softphone.
- Avaya M3904 Digital Deskphones.
- Analog Deskphones.
- 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 CenturyLink across the public IP network is UDP. The transport protocol between the Avaya SBCE and the CS1000 across the enterprise IP network is UDP.

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

For inbound calls, the calls flowed from CenturyLink to the Avaya SBCE, then to the CS1000. Once the call arrived at the CS1000, 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 the Avaya SBCE for egress to CenturyLink.



**Figure 1: CenturyLink 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.	RELEASE 7 ISSUE 65 P +  DepList 1: core Issue: 01(created: 2013-05-28 04:19:50 (est))  Signaling Server: 7.65.16.00 <b>(Service Pack 2)</b>  **See Service Updates & Patches below**
Avaya Call Pilot 202i	Call Pilot Manager Version: 05.00.41.156
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.0.Q48
Avaya Deskphones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.4 Service Pack 1 (Build 067)
Lucent Analog Phone	N/A
Fax Machines	N/A
<b>CenturyLink:</b>	
<b>Equipment</b>	<b>Release/Version</b>
SONUS SBC9000	V07.03.07F017

## **Signaling Server Service Updates & Patches:**

### **CS1000 Linux SU's included in Service Pack 2:**

cs1000-linuxbase-7.65.16.21-04.i386.000  
cs1000-patchWeb-7.65.16.21-04.i386.000  
cs1000-dmWeb-7.65.16.21-01.i386.000  
cs1000-snmp-7.65.16.00-01.i686.000  
cs1000-oam-logging-7.65.16.01-01.i386.000  
cs1000-cs1000WebService\_6-0-7.65.16.21-00.i386.000  
cs1000-sps-7.65.16.21-01.i386.000  
cs1000-pd-7.65.16.21-00.i386.000  
cs1000-shared-carrrdtct-7.65.16.21-01.i386.000  
cs1000-shared-tpselect-7.65.16.21-01.i386.000  
cs1000-emWebLocal\_6-0-7.65.16.21-01.i386.000  
cs1000-dbcom-7.65.16.21-00.i386.000  
cs1000-csmWeb-7.65.16.21-05.i386.000  
cs1000-shared-xmsg-7.65.16.21-00.i386.000  
cs1000-vtrk-7.65.16.21-29.i386.000  
cs1000-tps-7.65.16.21-05.i386.000  
cs1000-mscAnnc-7.65.16.21-02.i386.001  
cs1000-mscAttn-7.65.16.21-04.i386.001  
cs1000-mscConf-7.65.16.21-02.i386.001  
cs1000-mscMusc-7.65.16.21-02.i386.001  
cs1000-mscTone-7.65.16.21-03.i386.001  
cs1000-bcc-7.65.16.21-21.i386.000  
cs1000-Jboss-Quantum-7.65.16.21-3.i386.000  
cs1000-emWeb\_6-0-7.65.16.21-06.i386.000  
cs1000-cs-7.65.P.100-01.i386.001

#####

Patches:

#####

**Loadware:**

INSTALLED LOADWARE PEPS : 5

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	wi01057886	ISS1:1OF1	DSP1AB07	09/08/2013	DSP1AB07.LW
01	wi01057886	ISS1:1OF1	DSP2AB07	09/08/2013	DSP2AB07.LW
02	wi01057886	ISS1:1OF1	DSP3AB07	09/08/2013	DSP3AB07.LW
03	wi01057886	ISS1:1OF1	DSP4AB07	09/08/2013	DSP4AB07.LW
04	wi01057886	ISS1:1OF1	DSP5AB07	09/08/2013	DSP5AB07.LW

## 5. Configure Avaya Communication Server 1000E

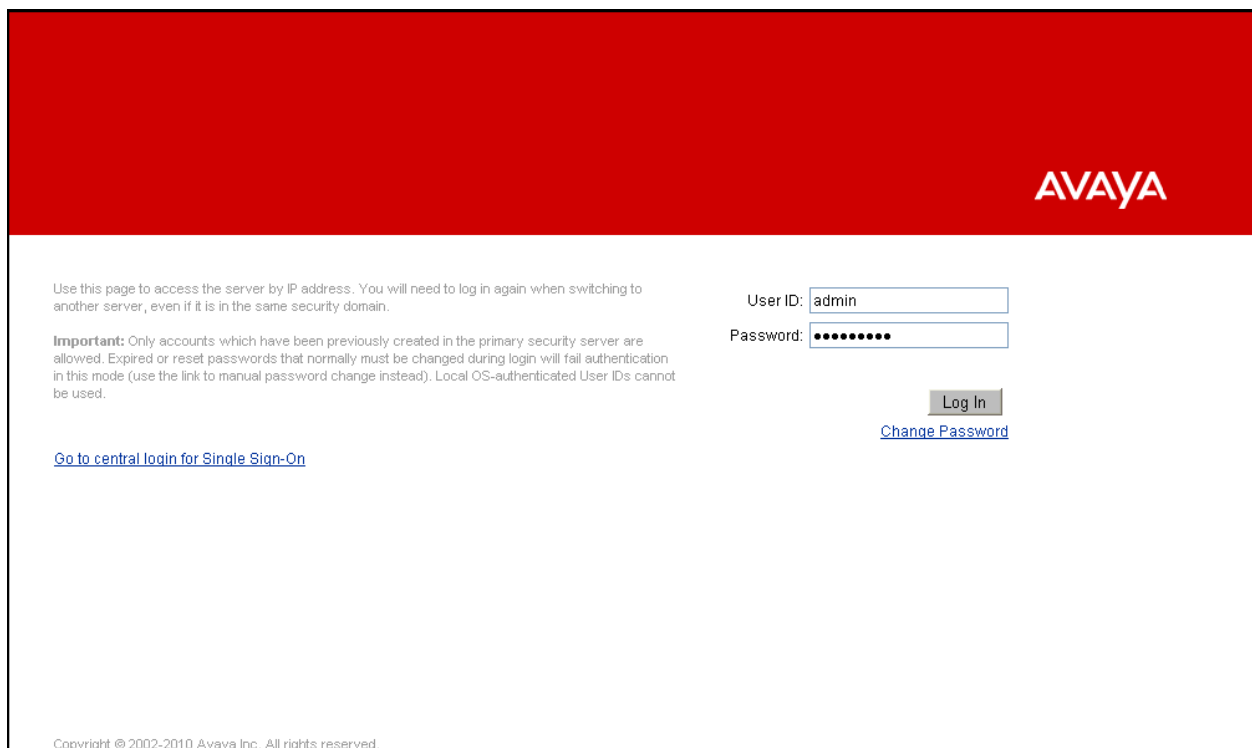
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 10**.

The procedures shown below describe the configuration details of the CS1000 with SIP trunks to the CenturyLink's 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.



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

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

User ID:

Password:

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

[Change Password](#)

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.

The screenshot displays the Avaya Unified Communications Management web interface. The left sidebar contains a navigation menu with categories: 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), and Tools (Logs, Data). The main content area is titled 'Avaya Unified Communications Management' and includes a header with 'Host Name: 172.16.20.60', 'Software Version: 02.30.0066.00(6406)', and 'User Name admin'. Below the header, the 'Elements' section contains a search bar and a table of registered elements. The table has columns for 'Element Name', 'Element Type', 'Release', 'Address', and 'Description'. The first row, 'EM on cs1k', is highlighted with a red box. Below the table are 'Add...', 'Edit...', and 'Delete' buttons. The footer of the interface shows the copyright notice: 'Copyright 2002-2012 Avaya Inc. All rights reserved.'

	Element Name	Element Type	Release	Address	Description
1	EM on cs1k	CS1000	7.6	172.16.21.61	New element.
2	cs1k.avaya.lab.com (primary)	Linux Base	7.6	172.16.20.61	Base OS element.
3	172.16.21.62	Media Gateway Controller	7.6	172.16.21.62	New element.

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

The screenshot displays the Avaya CS1000 Element Manager web interface. At the top, the Avaya logo is on the left, the title 'CS1000 Element Manager' is in the center, and 'Help | Logout' is on the right. A red horizontal bar separates the header from the main content. Below the header, a navigation sidebar on the left lists various system components: UCM Network Services, Home, Links, System (with sub-items like Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, and Interfaces), Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'System Overview' and contains a box with system details: IP Address: 172.16.21.61, Type: Avaya Communication Server 1000E CPMG128 Linux, Version: 4421, and Release: 765 P. At the bottom of the page, a copyright notice reads 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

AVAYA CS1000 Element Manager Help | Logout

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: 765 P +

Copyright © 2002-2013 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.

```
login as: admin

                Avaya Inc. Linux Base  7.65
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: Wed Aug 28 15:59:22 2013 from 172.16.5.250
[admin@cs1k ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without aut
hentic
ting

TTY 14 SCH MTC BUG OSN    10:44
OVL111 IDLE    0
>logi
USERID? admin
PASS?
.
TTY #14 LOGGED IN ADMIN 10:44  29/8/2
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.
013

>
```

## 5.2. Administer an IP Telephony Node

This section describes how to configure an IP Telephony Node 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 CenturyLink.

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

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

Buttons: Add... Import... Export... Delete Print | Refresh

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1006	1	SIP Line, LTPS, IP Media Services, Gateway ( SIPGw )	-	172.16.20.60	-	Synchronized

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

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



The **Node Details** screen is displayed below with the IP address of the CS1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate with other components for call processing.

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 \*

Telephone 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
cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), 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.

## 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.

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 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 [Add] [Remove] [Make Leader] [Print] [Refresh]

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), 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 © 2002-2013 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**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'Nodes: Servers, Media Cards' highlighted. The main content area is titled 'Node ID: 1006 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details'. It features a 'Firmware' section with fields for IP address (0.0.0.0), Full file path (download/firmware), Server Account/User ID, and Password. A 'DTLS' section has a 'DTLS policy' dropdown set to 'Off' and options for 'Client authentication' and 'Periodic re-keying'. A 'Network Connect Server' section shows the 'Primary network connect server (TL) IP address' as 0.0.0.0. A red box highlights the 'UNISim Line Terminal Proxy Server: ☒ Enable proxy service on this node' checkbox. At the bottom, there are 'Save' and 'Cancel' buttons and a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

### 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.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'Nodes: Servers, Media Cards' highlighted. The main content area is titled 'Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))'. It features a 'Subnet mask' field set to 255.255.255.0 and a 'Node IPv6 address' field. Below these is the 'IP Telephony Node Properties' section, which includes a list of links: 'Voice Gateway (V/GW) and Codecs', 'Quality of Service (QoS)', 'LAN', 'SNTP', 'Numbering Zones', and 'MCDN Alternative Routing Treatment (MALT) Causes'. The 'Quality of Service (QoS)' link is highlighted with a red box. To the right is the 'Applications (click to edit configuration)' section, which includes links for 'SIP Line', 'Terminal Proxy Server (TPS)', 'Gateway (SIPGw)', 'Personal Directories (PD)', 'Presence Publisher', and 'IP Media Services'. At the bottom, there are 'Save' and 'Cancel' buttons and a note: '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'. Below this is the 'Associated Signaling Servers & Cards' section, which includes a table with columns for 'Hostname', 'Type', 'Deployed Applications', 'ELAN IP', 'TLAN IPv4', and 'Role'. The table contains one entry: 'cs1k', 'Signaling\_Server', 'SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services', '172.16.21.61', '172.16.20.61', and 'Leader'.

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

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

AVAYA CS1000 Element Manager

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

## 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** (not shown). The **Synchronize Configuration Files** screen is displayed (not shown). Check the Signaling Server check box and click on the **Start Sync** (not shown). When the synchronization completes, check the Signaling Server check box and click on the **Restart Applications** (not shown).

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 (SIPH323), 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

Copyright © 2002-2013 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**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards (highlighted), 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 "Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))". It includes fields for Subnet mask (255.255.255.0) and Node IPv6 address. Below these are two lists of properties and applications:

- IP Telephony Node Properties:**
  - Voice Gateway (VGW) and Codecs (highlighted)
  - 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

Below the lists is a section titled "Associated Signaling Servers & Cards" with a table of associated servers. The table has columns for Hostname, Type, Deployed Applications, ELAN IP, TLAN IPv4, and Role. One server is listed: cs1k, Signaling\_Server, SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services, 172.16.21.61, 172.16.20.61, Leader.

At the bottom, there is a note: "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".

The **Voice Gateway (VGW) and Codec** screen is displayed below. CenturyLink supports codecs **G711u**, **G.711a** and **G.729** with **Voice Activity Detection (VAD)** disabled. Enable codec **G.729** by checking the box.

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

AVAYA CS1000 Element Manager

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

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.

Codec G729: ☒ Enabled  
Voice payload size: 20 (milliseconds per frame)

\* 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 **Voice Activity Detection (VAD)** is unchecked.

AVAYA CS1000 Element Manager

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

Voice Codes

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 default and **G.711u pass-through** as fallback. **T.38** with payload size **30ms** was chosen as default codec for fax. During the testing, **T.38** fax transport worked successfully for fax calls made from the PSTN to the CS1000 (inbound) and for CS1000 to the PSTN (outbound). **G.711u fax pass-through** was also tested successfully.

The screenshot displays the Avaya CS1000 Element Manager web interface. The top header shows the Avaya logo and the title 'CS1000 Element Manager'. A navigation sidebar on the left lists various system components, with 'Nodes: Servers: Media Cards' highlighted. The main content area is titled 'Node ID: 1006 - Voice Gateway (VGW) and Codecs'. It features a tabbed interface with 'General', 'Voice Codecs', and 'Fax' tabs. The 'Fax' tab is active, showing configuration for 'Codec G723.1' (disabled) and 'Voice payload size: 30 (milliseconds per frame)'. The 'Voice payout (jitter buffer) delay' is set to 60 milliseconds. The 'Coding rate' is 5.3 kbps. The 'Fax' section includes a 'Codec name' dropdown set to 'T.38 FAX', a 'Maximum rate' dropdown set to '14400 (bps)', a 'Fax TCF method' dropdown set to '2', a 'Fax payout nominal delay' input field set to '100 (0 - 300 milliseconds)', a 'FAX no activity timeout' input field set to '20 (10 - 32000 milliseconds)', and a 'Packet size' dropdown set to '30 (ms)'. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are 'Save' and 'Cancel' buttons at the bottom right.

Ensure that **Modem/Fax Pass Through** and **V.21 Fax tone detection** are checked.

AVAYA CS1000 Element Manager

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

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)

Signalling options: ☒ DTMF tone detection

☐ Low latency mode

☒ Remove DTMF delay (squell 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 80 (milliseconds)

\* Required Value.

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

Save Cancel

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

Click on **Save** and Synchronize the new configuration 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 **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), 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

FAX no activity timeout: 20 (10 - 32000 milliseconds)

FAX packet size: 30

Codec G711 Select ☒

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 ☐

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

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.

The screenshot shows the Avaya CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Links, System, and Media Gateways. The 'Media Gateways' section is expanded, and the 'VGW and IP phone codec profile' is selected. The main configuration area contains various settings for fax and voice services. Key settings highlighted with red boxes include: 'Enable V.21 FAX tone detection' (checked), 'Enable modem/fax pass through mode' (checked), and 'FAX packet size' (set to 30). Other visible settings include 'Enable echo canceller' (checked), 'Echo canceller tail delay' (128 ms), 'Enable dynamic attenuation' (checked), 'Voice activity detection threshold' (1), 'Idle noise level' (0), 'R factor calculation' (unchecked), 'DTMF tone detection' (checked), 'Enable low latency mode' (unchecked), 'Remove DTMF delay' (checked), 'Fax TCF method' (2), 'FAX maximum rate' (14400 bps), 'FAX playout nominal delay' (100 ms), 'FAX no activity timeout' (20 ms), and '+ Codec G711' (selected). The footer shows the copyright notice: 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

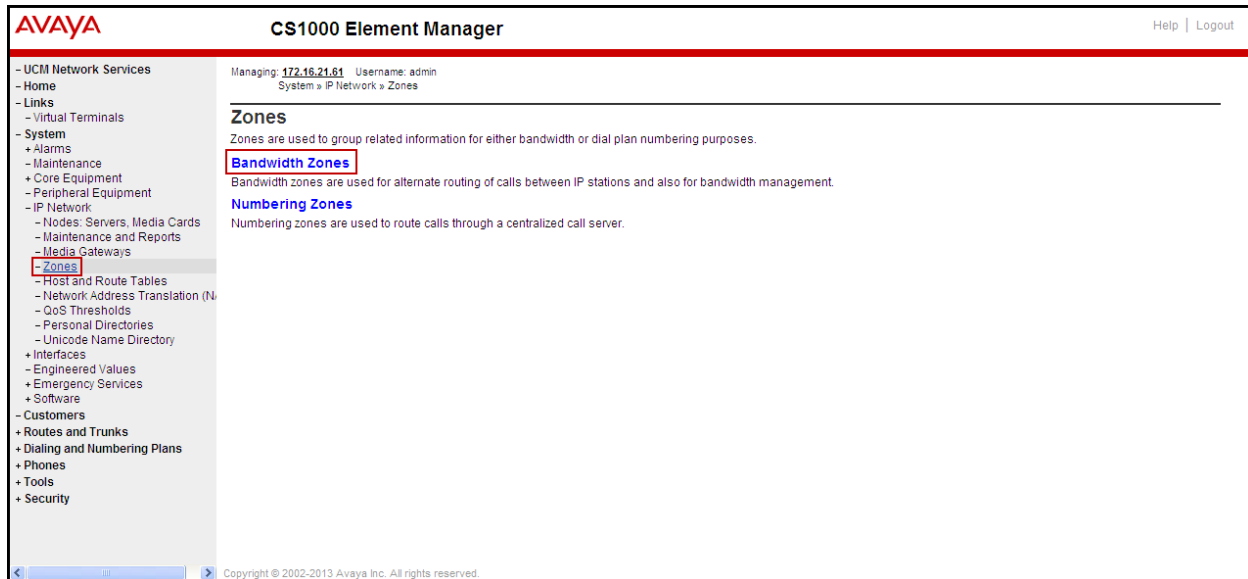


## 5.4. Administer Zones and Bandwidth

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

### 5.4.1. Create a zone for IP phones (zones 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, click on the **Bandwidth Zones** as shown below.



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 the calls over trunk, select **Best Quality (BQ)**.
- **ZBRN**: Select **MO** (**MO** is used for IP phones).

The values for Zone 5 are shown below; **G711** will be used for local and for calls over the trunk.

Managing: 172.16.21.81 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 5 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

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):	IPPHONES_G711
Location Name (ZNAME):	
Reserved BW Block Size (RESERVED_BW_SIZE):	0 ( 200 - 9999999 )

Submit Refresh Cancel

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

Follow Section 5.4.1 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 CenturyLink, Zone 4 was created for the Virtual SIP Trunks.

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 © 2002-2013 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 the Avaya SBCE.

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. Above the table are buttons for 'Add...' and 'Delete', and a 'Refresh' button. The top of the page shows the AVAYA logo, 'CS1000 Element Manager', and 'Help | Logout' link. The top right corner shows 'Managing: 172.16.21.61 Username: admin Customers'.

Customer Number	Total Routes	Total Trunks
1 00	3	17

The **Customer 00** Edit 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 the previous screenshot, with 'Customers' highlighted. The main content area is titled 'Customer Details' and lists various configuration options: 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), 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, and Timers. The top of the page shows the AVAYA logo, 'CS1000 Element Manager', and 'Help | Logout' link. The top right corner shows 'Managing: 172.16.21.61 Username: admin 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 (not shown). 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** (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:

Redirection count for ISDN calls:

CLID information for incoming/outgoing calls:

Public service telephone networks: ☐

+ Network Attendant Service Package: 159

+ Flexible Numbering Plan Package: 160

+ Trunk Failure Monitor Package: 182

+ Radio Paging Package: 187

+ Commonwealth of Independent States -Trunk Package: 221

+ Called Party Control on Internal Calls Package: 310

+ M3900 Product Enhancement Package: 386

+ IP Media Services Package: 422

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

### 5.5.1. Administer the SIP Trunk Gateway to the Avaya SBCE

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 **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.

- **Vtrk gateway application: SIP Gateway (SIPGw).**
- **SIP domain name: avaya.lab.com**
- **Local SIP port: 5060.**
- **Gateway endpoint name: CS1KGateway.**
- **Application node ID: 1006.**

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards (highlighted in red), Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), CoS 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 displays the 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details' screen. The 'General' tab is selected, and the 'Vtrk gateway application' is set to 'SIP Gateway (SIPGw)'. The 'SIP domain name' is 'avaya.lab.com', 'Local SIP port' is '5060', 'Gateway endpoint name' is 'CS1KGateway', and 'Application node ID' is '1006'. The 'Virtual Trunk Network Health Monitor' section is also visible, showing a checkbox for 'Monitor IP addresses (listed below)' and a list of 'Monitor addresses'.

Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the values highlighted in red boxes for the Primary TLAN, and Secondary TLAN if one exist, retain the default values for the remaining fields as shown below. For the compliance testing only the Primary TLAN was configured, values shown correspond to the IP address, Port, and Transport of the inside (private side) IP address of the Avaya SBCE.

The screenshot displays the Avaya CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories like 'UCM Network Services', 'System', 'IP Network', and 'Tools'. The 'Nodes, Servers, Media Cards' link is highlighted. The main content area shows the configuration for 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details'. The 'SIP Gateway Settings' tab is selected. Under the 'Proxy Or Redirect Server' section, 'Proxy Server Route 1' is configured. The 'Primary TLAN IP address' is 172.16.5.71, 'Port' is 5060, and 'Transport protocol' is UDP. The 'Secondary TLAN IP address' is 0.0.0.0, 'Port' is 5060, and 'Transport protocol' is UDP. The 'Options' section has 'Support registration' and 'Primary CDS proxy' unchecked. At the bottom, there are 'Save' and 'Cancel' buttons and a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

On the same page shown above, scroll down to the **SIP URI Map** section. The entries shown below were used during the compliance testing:

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

- **National:** blank.
- **Subscriber:** blank.
- **Special Number:** PublicSpecial.
- **Unknown:** PublicUnknown.

Under the **Private Domain Names**, for:

- **UDP:** udp.
- **CDP:** cdp.udp.
- **Special Number:** PrivateSpecial.
- **Vacant number:** PrivateUnknown.
- **Unknown:** UnknowUnknown.

**Note:** The SIP URI Map entries shown above were used during the compliance testing; the values shown are default values.

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" value="udp"/>
Subscriber:	<input type="text"/>	CDP:	<input type="text" value="cdp.udp"/>
Special number:	<input type="text" value="PublicSpecial"/>	Special number:	<input type="text" value="PrivateSpecial"/>
Unknown:	<input type="text" value="PublicUnknown"/>	Vacant number:	<input type="text" value="PrivateUnknown"/>
		Unknown:	<input type="text" value="UnknownUnknown"/>

**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.

## 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 **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: 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"/>



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

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 \(BSCOPT\)](#)  
[+ Advanced options \(ADVOPT\)](#)  
[+ Feature Packages](#)

Copyright © 2002-2013 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

**- 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:	<input type="button" value="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
<b>+ Basic options (BSCOPT)</b>	
<b>- Advanced options (ADVOPT)</b>	
- 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:	<input checked="" type="checkbox"/>
<b>+ H323 Overlap Signaling Settings (H323)</b>	
--Overlap Timer:	<input type="button" value="more"/>
- Multilocation Business Group Allowed:	<input type="checkbox"/>
- Network Attendant Service Allowed:	<input checked="" type="checkbox"/>
<b>+ - Link Access Protocol for D-channel (LAPD)</b>	

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

Click on the **Basic Options (BSCOPT)** and click on the **Edit** button for the **Remote Capabilities** attribute 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
  - + Phones
  - + Tools
  - + Security

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 Signalling 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 Signalling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700
Primary D-channel for a backup DCH:	Range: 0 - 254
- PINX customer number:	
- Progress signal:	
- Calling Line Identification:	
- Output request Buffers:	32
- D-channel transmission Rate:	56 kb/s when LCMT is AMI (56K)
- Channel Negotiation option:	No alternative acceptable, exclusive. (1)
- Remote Capabilities:	<a href="#">Edit</a>
- B channel Service messaging:	<input type="checkbox"/>

- Basic options (BSCOPT)

+ - Change protocol timer value (TMR)

+ Advanced options (ADVOPT)

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

The **Remote Capabilities Configuration** page will appear, check **MWI** and **ND2** (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).

**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
  - + Phones
  - + Tools
  - + Security

Call completion on busy for QSIG and EuroISDN BRI (CCBS) ☐

Call completion on no response using integer value (CCNI) ☐

Call completion on no response using object identifier (CCNO) ☐

Call completion to no reply for QSIG and EuroISDN BRI (CCNR) ☐

Network call park (CPK) ☐

Connected line identification presentation (COLP) ☐

Call transfer integer (CTI) ☐

Call transfer object (CTO) ☐

Diversion info. is sent using integer value (DV1I) ☐

Diversion info. is sent using object identifier (DV1O) ☐

Rerouting requests processed using integer value (DV2I) ☐

Rerouting requests processed using object identifier (DV2O) ☐

Diversion info. sent. rerouting requests processed (DV3I) ☐

EuroISDN - div. info sent. rerouting req. processed (DV3O) ☐

Call transfer notification and invocation to EuroISDN (ECTO) ☐

Malicious call identification (MCID) ☐

MCDN QSIG conversion (MQC) ☐

Remote D-channel is on a MSDL card (MSL) ☐

**Message waiting interworking with DMS-100 (MWI) ☒**

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

**Network name display method 2 (ND2) ☒**

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

### 5.5.3. Administer Virtual Super-Loop

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

**AVAYA CS1000 Element Manager** Help | Logout

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

**Superloops**

Add... Delete Refresh

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

Left sidebar menu:

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Loops
  - **Superloops**
  - MSDL/MISF Cards
  - Conference/TDS/Multifrequency
  - Tone Senders and Detectors
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Software
- Customers
  - + Routes and Trunks
  - Routes and Trunks
  - + Dialing and Numbering Plans
  - + Phones
  - + Tools
  - + Security

## 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.



The **Customer 0**, New **Route 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).
- **Network calling name allowed (NCNA):** Check box.
- **Network call redirection (NCRD):** Check box.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.51 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 signalling 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): ☐  
 - Enable Shared Bandwidth Management for the route (SBWM): ☐  
 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)  
 - Private network identifier (PNI): 00001 (0 - 32700)  
 - Network calling name allowed (NCNA): ☒  
 - Network call redirection (NCRD): ☒  
 - Trunk route optimization (TRO): ☐

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

- **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

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

Enable Shared Bandwidth Management for the route (SBWM): ☐

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)

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

- Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** (created in Section 5.6.5) for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown below.

**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

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

Basic Route Options

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

Billing number required (BILN): ☐

Call detail recording (CDR): ☐

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

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

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

Display external dialed digits (DEXT): ☐

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

Process notification networked calls (PNNC): ☐

Network Options

General Options

Advanced Configurations

Submit Refresh Delete Cancel

### 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 being added. Click on **Add trunk** button next to the newly added route 0 as shown below.

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

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

+ Route: 0

Type: TIE

Description: SERVICE PROVIDER

Edit

Add trunk

+ Route: 1

Type: IMUS

Description: MUSIC

Edit

Add trunk

+ Route: 96

Type: TIE

Description: SIPL\_ROUTE

Edit

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 the 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 basic trunk configuration page. Click on the **Edit** button as shown below.

Note: 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 (use virtual super-loop 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.

The screenshot shows the Avaya CS1000 Element Manager interface. The main title is "CS1000 Element Manager". The breadcrumb trail is "Managing: 172.16.21.61 Username: admin Routes and Trunks > Routes and Trunks > Customer 0, Route 0, Trunk 1 Property Configuration". The page title is "Customer 0, Route 0, Trunk 1 Property Configuration". The left sidebar shows a navigation menu with "Routes and Trunks" highlighted. The main content area is divided into two sections: "Basic Configuration" and "Advanced Trunk Configurations". The "Basic Configuration" section contains the following fields:

- 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:

The "Advanced Trunk Configurations" section is currently empty. At the bottom right, there are buttons for "Save", "Delete", and "Cancel".

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
  - Routes and Trunks
  - D-Channels
  - Digital Trunk Interface
- + Dialing and Numbering Plans
- + Phones
- + Tools
- + Security

**Analog Semi-Permanent Connections** **Analog Semi-Permanent Connections Denied (AR CD)**

- ARF Supervised COT: [Dropdown]
- Barring: [Dropdown]
- Battery Supervised COT: [Dropdown]
- Busy Tone Supervised COT: [Dropdown]
- Calling party: Calling party Denied (CND) [Dropdown]
- Central Office Ringback: [Dropdown]
- Centrex Switchhook Flash: Centrex Switchhook Flash Denied (THFD) [Dropdown]
- Dial Pulse: Dial Pulse (DIP) [Dropdown]
- DTR PAD value: [Dropdown]
- Echo Cancelling: Echo Cancelling Denied (ECD) [Dropdown]
- Hong Kong DTI: [Dropdown]
- Loop Break Supervised COT: [Dropdown]
- Make-break ratio for dial pulse: 10 pulses per second (P10) [Dropdown]
- Manual Incoming: Manual Incoming Denied (MID) [Dropdown]
- Media Security: Media Security Never (MSNV) [Dropdown]
- Network Hook Flash Over M911P: [Dropdown]
- Polarity: [Dropdown]
- Priority: Low Priority (LPR) [Dropdown]
- Restriction level: Unrestricted (UNR) [Dropdown]
- Reversed Ear Piece: Reversed Ear Piece denied (XREP) [Dropdown]
- Short or long line: [Dropdown]
- Transmission Class of Service: Non-Transmission Compensated (NTC) [Dropdown]
- Warning Tone: Warning Tone Allowed (WTA) [Dropdown]
- Reversed Ear Piece denied (XREP) [Dropdown]
- ARF Supervised COT: [Dropdown]

**Return Class of Service** **Cancel**

Copyright © 2002-2013 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.

The screenshot shows the 'General Properties' page in the AVAYA CS1000 Element Manager. The left sidebar contains a navigation tree with 'Customers' selected. The main content area is divided into 'General Properties' and 'Calling Line Identification'. The 'Calling Line Identification' section is highlighted with a red box and contains the following fields:

- Flexible trunk to trunk connection option:
- Flexible orbiting prevention timer:
- Country code:  (0 - 9999)
- Code for processing the called number:
- National access code:
- International access code:
- 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 for non-DID users: ☐ Coordinated dialing plan, ☐ Uniform dialing plan
- Information for incoming/outgoing calls:
- Size:  (0 - 4000)
- Country code:  (0 - 9999)
- Code displayed as part of calling number:
- [Calling Line Identification Entries](#)

Click on **Add** as shown below.

The screenshot shows the 'Calling Line Identification Entries' page in the AVAYA CS1000 Element Manager. The left sidebar contains a navigation tree with 'Customers' selected. The main content area is divided into 'Calling Line Identification Entries' and 'Search for CLID'. The 'Calling Line Identification Entries' section is highlighted with a red box and contains the following fields:

- Start range:
- End range:
- 'End range' should not exceed the CLID size specified
- 
- 
- 

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 720.
- **Local Code:** input the seven digit number of the DID assigned by Service Provider, in this case it is 3621234.
- **Calling Party Name Display:** Uncheck for **Roman characters**.

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

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

Managing: 172.16.21.61 Username: admin  
[Customers](#) » [Customer 00](#) » [Customer Details](#) » [ISDN and ESN Networking](#) » [Calling Line Identification Entries](#) » Edit Calling Line Identification 0

### Edit Calling Line Identification 0

General Properties

National Code:  (0 - 999999)  
Code for national home number  
 Local Code:  (1-12 digits)  
Code for home local number or listed DN  
 Local Steering Code:   
(1-7 digits)  
 Use DN as DID:

Emergency Services Access

Emergency Local Code:   
(1-12 digits)  
Code for home local number during Emergency calls  
 Emergency Options: ☐ Home national number for emergency services access calls  
☒ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☐  
 CPND Name:   
First name, last name

### 5.5.7. Enable External Trunk to Trunk Transfer

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

- Login into 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.

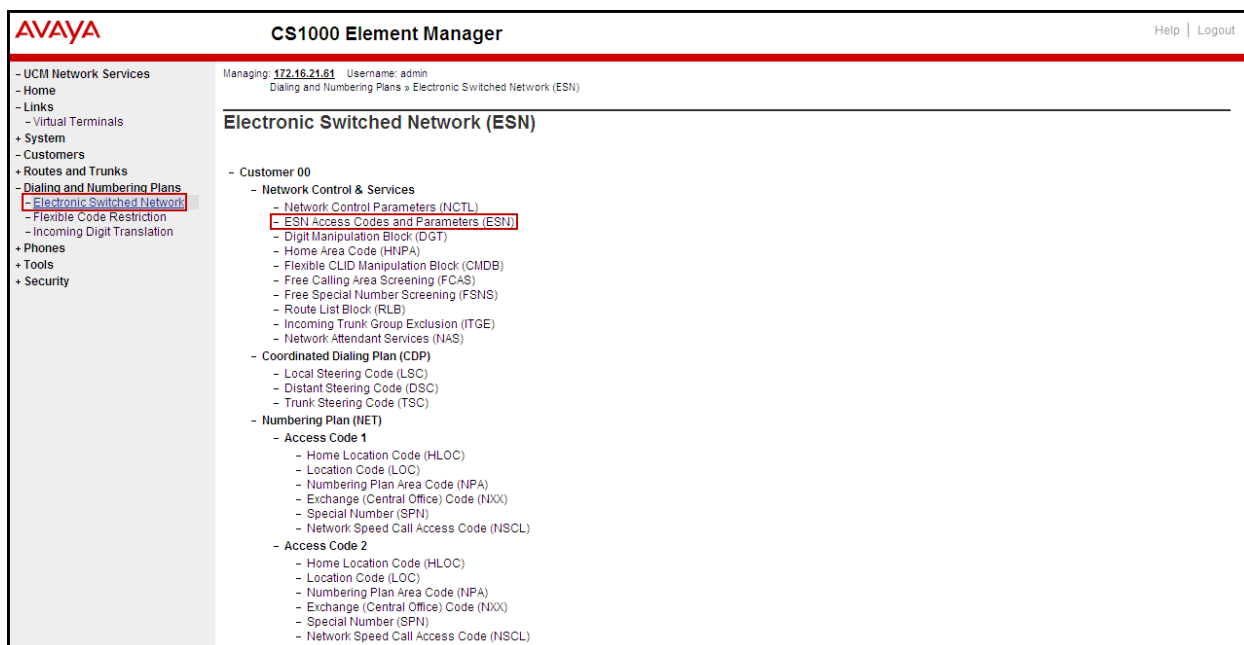
```
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101   USED U P: 371282 939078   TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....
```

## 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).

**Note:** BARS and NARS access codes are customer defined; any one or two digit code can be used, provided there is no conflict with any other part of the dial plan.

### 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 xnpa 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.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top header includes the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. Below the header, the interface is divided into a left sidebar and a main content area. The sidebar contains a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks, Dialing and Numbering Plans (expanded), Electronic Switched Network (selected), Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area displays the 'Electronic Switched Network (ESN)' configuration for 'Customer 00'. It includes a 'Managing' section with the IP address '172.16.21.81' and username 'admin', and a breadcrumb trail 'Dialing and Numbering Plans > Electronic Switched Network (ESN)'. The configuration is organized into several sections: 'Network Control & Services' (containing Network Control Parameters (NCTL), ESN Access Codes and Parameters (ESN), Digit Manipulation Block (DGT) - highlighted, 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), and Network Attendant Services (NAS)), 'Coordinated Dialing Plan (CDP)' (containing Local Steering Code (LSC), Distant Steering Code (DSC), and Trunk Steering Code (TSC)), and 'Numbering Plan (NET)' (containing Access Code 1 and Access Code 2, each with Home Location Code (HLOC), Location Code (LOC), Numbering Plan Area Code (NPA), Exchange (Central Office) Code (NXX), Special Number (SPN), and Network Speed Call Access Code (NSCL)).

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, Virtual Terminals, 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" button. Above the list, there is a dropdown menu labeled "Please choose the" with "Digit Manipulation Block Index 3" selected, and a "to Add" button.

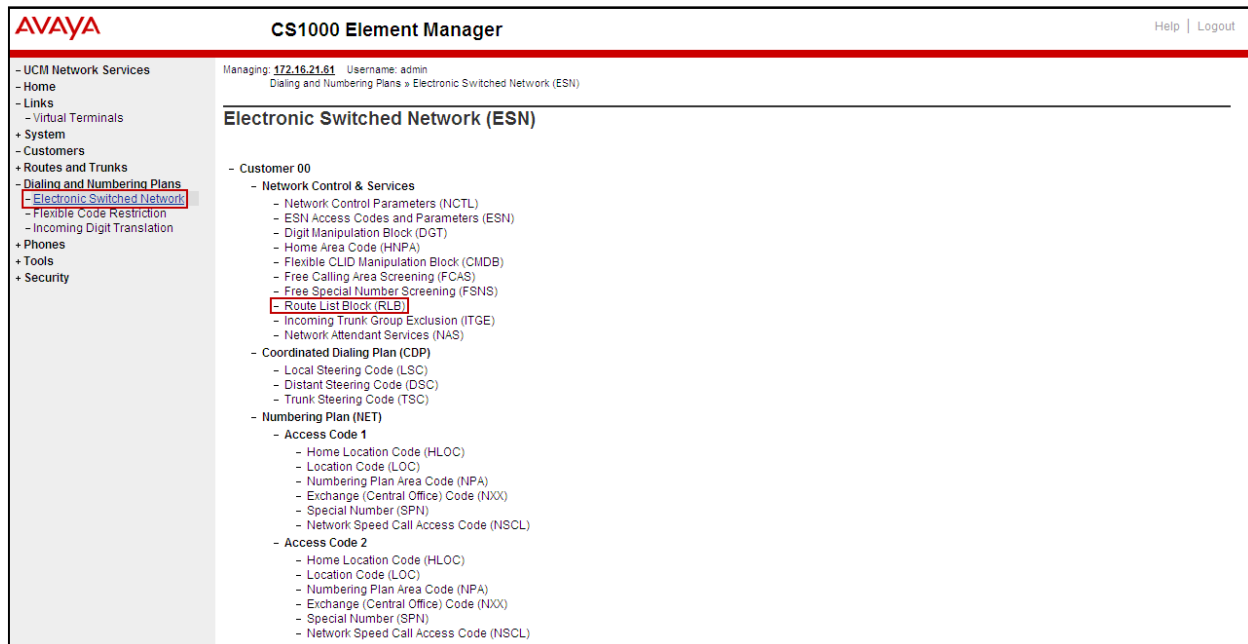
Enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** and then click **Submit** as shown below.

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), "IP Special Number" (checkbox), and "Call Type to be used by the manipulated digits" (set to NPA (NPA)). At the bottom right, there are buttons for "Submit", "Refresh", "Delete", and "Cancel".



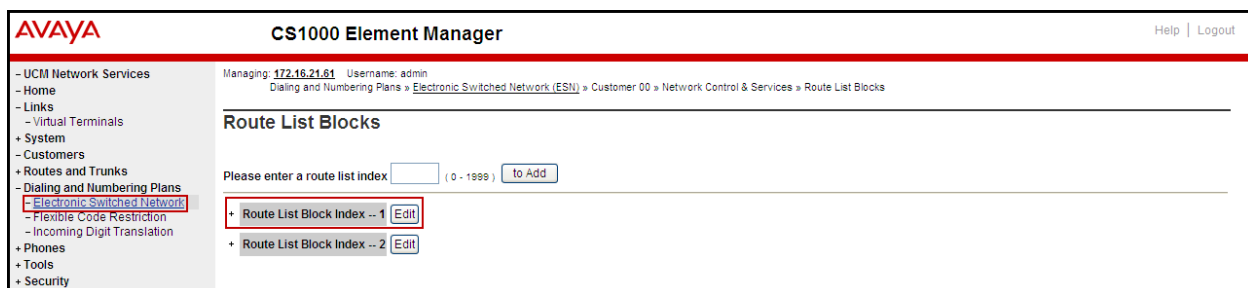
#### 5.6.4. Route List Block (RLB)

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.



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

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



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.

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

The screenshot shows the 'CS1000 Element Manager' interface. On the left is a navigation tree with 'Dialing and Numbering Plans' expanded, and 'Incoming Digit Translation' selected. The main area is titled 'Route List Block Index: 1'. It contains two sections: 'General Properties' and 'Indexes'. Under 'Indexes', 'Digit Manipulation Index' is set to 1. Under 'Options', 'Route Number' is set to 0. Other fields like 'Entry Number for the Route List' are set to 0. The bottom of the page shows a copyright notice for Avaya Inc. 2002-2013.

### 5.6.5. Inbound Digit Translation

This section describes the steps for mapping DID numbers to extensions in the CS1000.

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

The screenshot shows the 'Incoming Digit Translation' screen in the 'CS1000 Element Manager'. The left navigation pane shows 'Incoming Digit Translation' selected. The main area displays 'Managing: 172.16.21.81 Username: admin' and 'Dialing and Numbering Plans > Incoming Digit Translation'. Below this, the 'Incoming Digit Translation' section shows a 'Customer' field with the value '00' and an 'Edit IDC' button.

Click on **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number (DCN0) 0** was created 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

- Electronic Switched Network

- Flexible Code Restriction

- Incoming Digit Translation

+ Phones

+ Tools

+ Security

Managing: 172.16.21.81 Username: admin  
Dialing and Numbering Plans > Incoming Digit Translation > Customer 00

Customer 00 Incoming Digit Conversion Property

- Digit Conversion Tree Number: 0	Edit DCNO
- Digit Conversion Tree Number: 1	New DCNO
- Digit Conversion Tree Number: 2	New DCNO
- Digit Conversion Tree Number: 3	New DCNO
- Digit Conversion Tree Number: 4	New DCNO
- Digit Conversion Tree Number: 5	New DCNO
- Digit Conversion Tree Number: 6	New DCNO
- Digit Conversion Tree Number: 7	New DCNO
- Digit Conversion Tree Number: 8	New DCNO
- Digit Conversion Tree Number: 9	New DCNO

Refresh

Cancel

Detail configuration of the **DCNO** is 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 7203621234 will be translated to the CS1000 extension number 8000.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top header displays the AVAYA logo and the title 'CS1000 Element Manager'. Below the header, there is a navigation sidebar on the left with various links. The main content area is titled 'Add Incoming Digits'. It contains several input fields and checkboxes. The 'Incoming Digits' field is set to '7203621234'. The 'Converted digits' field is set to '8000'. There is a checkbox for 'Force storage or removal of data'. Below this, there is a section for 'CPND language' with a checkbox for 'Roman characters' which is checked. The 'CPND Name' field is set to 'Avaya 1165'. There is also a 'Display format' dropdown menu set to 'First name, Last name'. The interface is in English and shows a user logged in as 'admin'.

### 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 Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international call, **1** for national long distance call, **411**, **911** and so on. Calls to special numbers shown here are for reference only and may not have been tested for various reasons. Refer to section **Items not supported or not tested** in **Section 2.2**.

Note that for the compliance testing, “1” was added to the Special Number list and was used for national long distance, if the customer prefers, the **Numbering Plan Area Code (NPA)** could be use instead.

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 on the next screen.

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

Managing: 172.16.21.61 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)
  - Numbering Plan (NET)
    - Access Code 1
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)
      - Special Number (SPN)
      - Network Speed Call Access Code (NSCL)
    - Access Code 2
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)
      - Special Number (SPN)
      - Network Speed Call Access Code (NSCL)

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

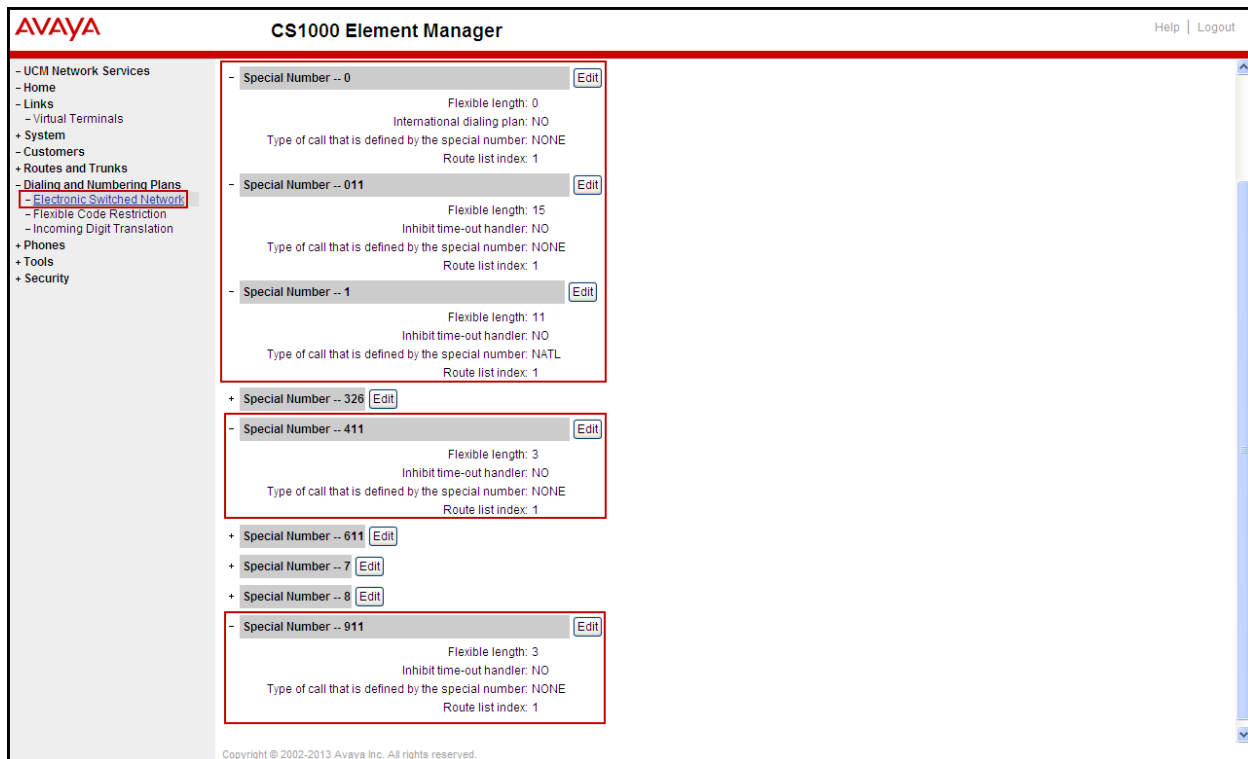
- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number).
- **CallType:** NATL.
- **Route list index:** 1, created in **Section 5.6.4.**

#### Special Number: 411

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

#### Special Number: 911

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



### 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) listed in **Section 10** [7], 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**.

Not all fields are shown in the example below; some of the fields have been cut out for brevity.

```
>ld 11
REQ: prt
TYPE: 1165
DES 8000
TN 008 0 00 00 VIRTUAL
TYPE 1165
CDEN 8D
CTYP XDLC
CUST 0
CFG_ZONE 00005
CUR_ZONE 00005
TGAR 0
LDN NO
NCOS 5
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDD
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD 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 EXRO
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 VMSA
CPND_LANG ENG
RCO 0
EFD 91786331
HUNT 91786331
EHT 91786331
DNDR 0
KEY 00 SCR 8000 0 MARP
CPND
CPND_LANG ROMAN
NAME Avaya, 1165_Uni
XPLN 14
DISPLAY_FMT FIRST, LAST
ANIE 0
01 CWT
02
31
```

## 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.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane has 'Customers' selected. The main area displays a table of customers. The first row shows 'Customer Number' 00, 'Total Routes' 3, and 'Total Trunks' 17. The '00' is highlighted with a red box.

Customer Number	Total Routes	Total Trunks
00	3	17

Select **Call Redirection** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface with 'Customer Details' selected. The left navigation pane has 'Customers' selected. The main area displays a list of configuration options. 'Call Redirection' is highlighted with a red box.

- 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 ring cycle of CFNA: 4.**

Click on **Save** (not shown)

**AVAYA** CS1000 Element Manager Help | Logout

**Navigation:**

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

**Redirection Holidays**

Do not disturb hunting: ☐

Total redirection count limit:

**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:

Option 1:

Option 2:

**Number of distinctive ringing cycles for CFNA**

Option 0:

Option 1:

Option 2:

**Calls routed to message center**

No answer DID calls: ☐

No answer non-DID calls: ☐

DID calls to busy telephones: ☐

**Buttons:**

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

To enable **Call Forward All Call (CFAC)** for the phone over the SIP trunk by using **LD 11**, change its CLS to **CFXA** then program the forward number on the phone set. Following is the configuration of a phone that has CFAC enabled, the phone 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 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
.....
19 CFW 12 919195551212

```

To enable **Call Forward Busy (CFB)** for the phone over the SIP trunk by using **LD 11**, change its CLS to **FBA**, **HTA** then program the forward number as **HUNT**. Following is the configuration of a phone that has CFB enabled; the phone is CFB 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 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
CPND LANG ENG
RCO 0
EFD 8004
HUNT 919195551212
.....

```

To enable **Call Forward No Answer (CFNA)** for the phone over SIP trunk by using **LD 11**, change CLS to **FNA**, **SFA** then program the forward number as **FDN**. Following is the configuration of a phone that has CFNA enabled; the phone is 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 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
....
```

### 5.7.4. Enable Call Waiting for the Phone

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

To configure 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 the Avaya Session Border Controller for Enterprise.

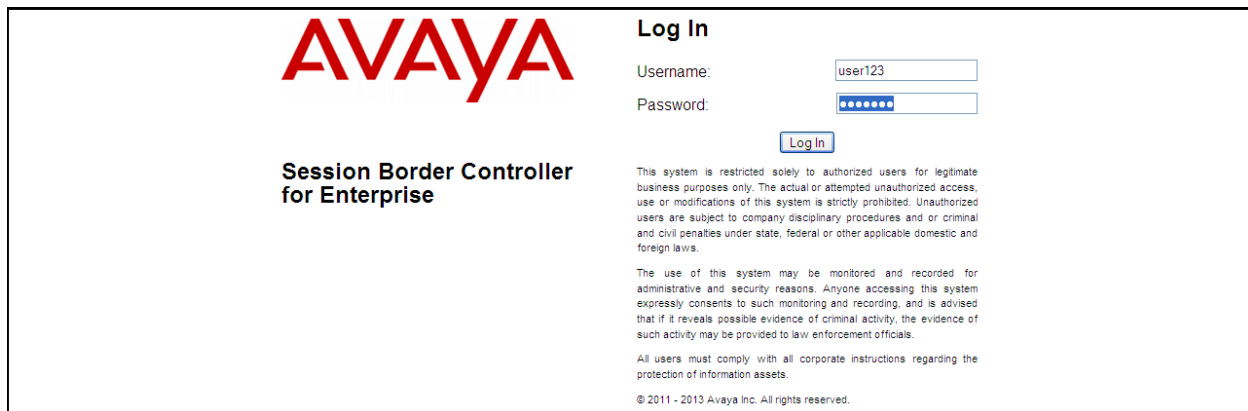
This section describes the required configuration of the Avaya SBCE to connect to CenturyLink SIP Trunk service.

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.

### 6.1. Log in the Avaya SBCE

Access the web interface by typing “<https://x.x.x.x/sbc/>” (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password**.

The image shows the login page of 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, under the heading "Log In", there are input fields for "Username:" (containing "user123") and "Password:" (masked with dots). A "Log In" button is positioned below the password field. To the right of the login fields, there is a block of disclaimer text: "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." followed by a paragraph about monitoring and a final note: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom right, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

### 6.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all devices.

#### 6.2.1. Server Interworking Avaya-CS1000

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

Several profiles have been already pre-defined and they populate 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 Profile**.

Enter the new profile name in the **Clone Name** field, the name of **Avaya-CS1000** was chosen in this example. Click **Finish**.

For the newly created **Avaya-CS1000** profile, click **Edit** (not shown) at the bottom of the General tab

- Verify that for **Hold Support**, **RFC2543** is selected.
- Check **T.38 Support**.
- Click **Next**.
- Click **Finish** on the **Privacy and DTMF** tab.
- Leave other fields with their default values.

The following screen capture shows the newly added **Avaya-CS1000** 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 Interworking' option is highlighted. The main area is titled 'Interworking Profiles: Avaya-CS1000' and includes an 'Add' button and action buttons (Rename, Clone, Delete). A list of profiles is shown, with 'Avaya-CS1000' selected. The configuration for this profile is displayed in a tabbed interface with tabs for General, Timers, URI Manipulation, Header Manipulation, and Advanced. The 'General' tab is active, showing settings for Hold Support (RFC2543), 180-183 Handling (None), Refer Handling (No), 3xx Handling (No), Diversion Header Support (No), Delayed SDP Handling (No), T.38 Support (Yes), URI Scheme (SIP), and Via Header Format (RFC3261). Below this, the 'Privacy' section shows Privacy Enabled (No), User Name, P-Asserted-Identity (No), P-Preferred-Identity (No), and Privacy Header. The 'DTMF' section shows DTMF Support (None). An 'Edit' button is at the bottom right of the configuration area.

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	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

## 6.2.2. 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.

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left navigation pane shows the 'Global Profiles' section expanded, with 'Server Interworking' highlighted. The main content area shows the 'Interworking Profiles: SP-General' configuration page. The 'General' tab is active, displaying a list of configuration parameters. The 'T.38 Support' parameter is highlighted with a red box and set to 'Yes'. The 'Privacy' and 'DTMF' tabs are also visible.

General	
Hold Support	NONE
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	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None



### 6.2.3. 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 the CS1000 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\_CS1000**.
- Click **Next**.

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.20.60** (Node IP address of the CS1000).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish**.

The following screen shows the newly added **Route\_to\_CS1000** Profile.

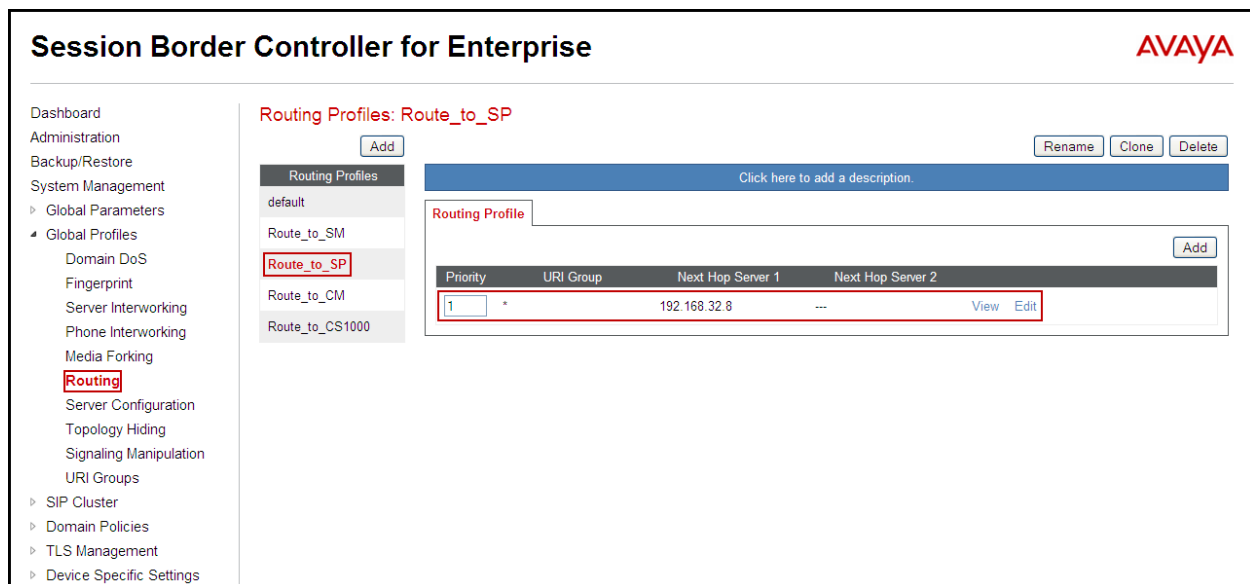
The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu is expanded to the 'Routing' tab. Under 'Global Profiles', the 'Routing' sub-tab is selected. The main content area shows the configuration for the 'Route\_to\_CS1000' profile. A table lists the routing profiles, with 'Route\_to\_CS1000' highlighted. Below the table, the configuration details for the selected profile are shown, including a table with columns for Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The 'Priority' is set to 1, and 'Next Hop Server 1' is set to 172.16.20.60.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	*	172.16.20.60	---

Similarly, for the outbound route:

- Select **Add Profile**.
- Enter Profile Name: **Route\_to\_SP**
- Click **Next**.
- **Next Hop Server 1: 192.168.32.8** (IP address for CenturyLink **SESSION** Trunk Group).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish**.

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



## 6.2.4. Server Configuration

Server Profiles should be created for the Avaya SBCE's two peers, the Call Server (CS1000) 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: **CS1000**.

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

- Select Server Type: **Call Server**.
- **IP Address: 172.16.20.60** (Node IP address of the CS1000).
- **Supported Transports: Check UDP**.
- **UDP Port: 5060** (This port must match the far end (CS1000) local port number defined in **Section 5.5.1**).
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.

- On the **Advanced** tab, select **Avaya-CS1000** 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 **CS1000** Profile.

The screenshot shows the 'Session Border Controller for Enterprise' interface. On the left is a navigation menu with 'Server Configuration' highlighted. The main area is titled 'Server Configuration: CS1000' and has 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	172.16.20.60
Supported Transports	UDP
UDP Port	5060

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

The following screen capture shows the **Advanced** tab of the added **CS1000** Profile.

The screenshot shows the 'Session Border Controller for Enterprise' interface with the 'Advanced' tab selected. The configuration table is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya-CS1000
Signaling Manipulation Script	None
UDP Connection Type	SUBID

The 'Interworking Profile' is highlighted with a red box. Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

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 Server Type: **Trunk Server**.
- **IP Addresses: 192.168.32.8, 192.168.32.9**
  - **192.168.32.8** (IP address for CenturyLink **SESSION** Trunk Group).
  - **192.168.32.9** (IP address for CenturyLink **USAGE** Trunk Group).
- **Supported Transports: Check UDP**.
- **UDP Port: 5060**.
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **SP-General** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**, a Signaling Manipulation Script will be assigned latter.
- Click **Finish**.

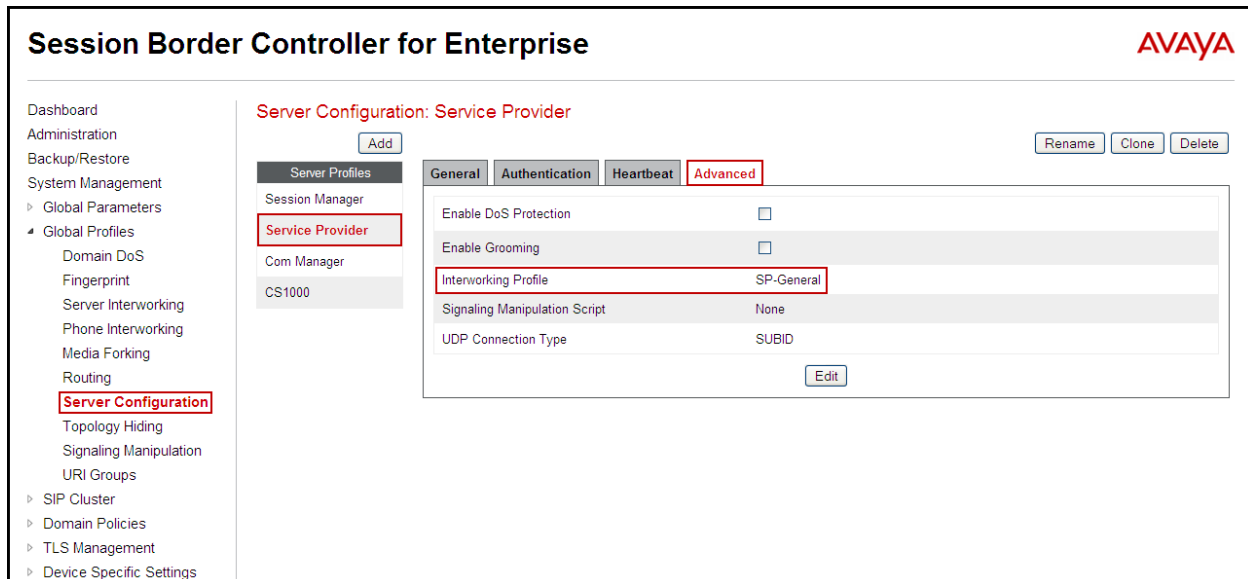
The following screen capture shows the **General** tab of the **Service Provider** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Server Configuration: Service Provider' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a table with the following configuration details:

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.32.8, 192.168.32.9
Supported Transports	UDP
UDP 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 **Service Provider** Profile.



### 6.2.5. 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 names.

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 **default** profile and select **Clone Profile**.
- Enter the **Profile Name: CS1000**.
- Click **Finish**.

The following screen capture shows the newly added **CS1000** Profile. Note that for the CS1000 profile no values were overwritten (default).



## 6.2.6. 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.

The Signaling Manipulation Script shown below is needed to convert History Info to Diversion Header, also to remove unwanted headers and MIME types.

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).

- On the **Title** enter a name, the name of **CenturyLink\_1** was chosen in this example.
- Enter the script as shown on the screen below (The script can be copied from Appendix A).
- Click **Save**.

**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: CenturyLink\_1**

Upload Add Download Clone Delete

Click here to add a description.

**Signaling Manipulation**

```
within session "All"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    if (%HEADERS["History-Info"][1].regex_match("reason")) then
    {
      %HEADERS["Diversion"][1] = "sip:dummy@dummy.com";
      %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-Info"][1].URI.SCHEME;
      %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
      %HEADERS["Diversion"][1].URI.HOST = %HEADERS["History-Info"][1].URI.HOST;
      %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-Info"][1].URI.PORT;

      %HEADERS["Diversion"][1].URI.PARA/MS["reason"] = "unconditional";
      %HEADERS["Diversion"][1].URI.PARA/MS["counter"] = "1";
      %HEADERS["Diversion"][1].URI.PARA/MS["privacy"] = "off";
    }

    %HEADERS["Content-Type"][1].regex_replace("multipart/mixed;boundary=unique-boundary-1","application/sdp");

    // The SBC will not remove the SDP MIME, so "x-nt-mcdn-frag-hex" = %BODY[1] // After "x-nt-mcdn-frag-hex" is rem
    // So the same command removes "x-nt-ens5-frag-hex".
    // And so on (e.g., "x-nt-epid-frag-hex").

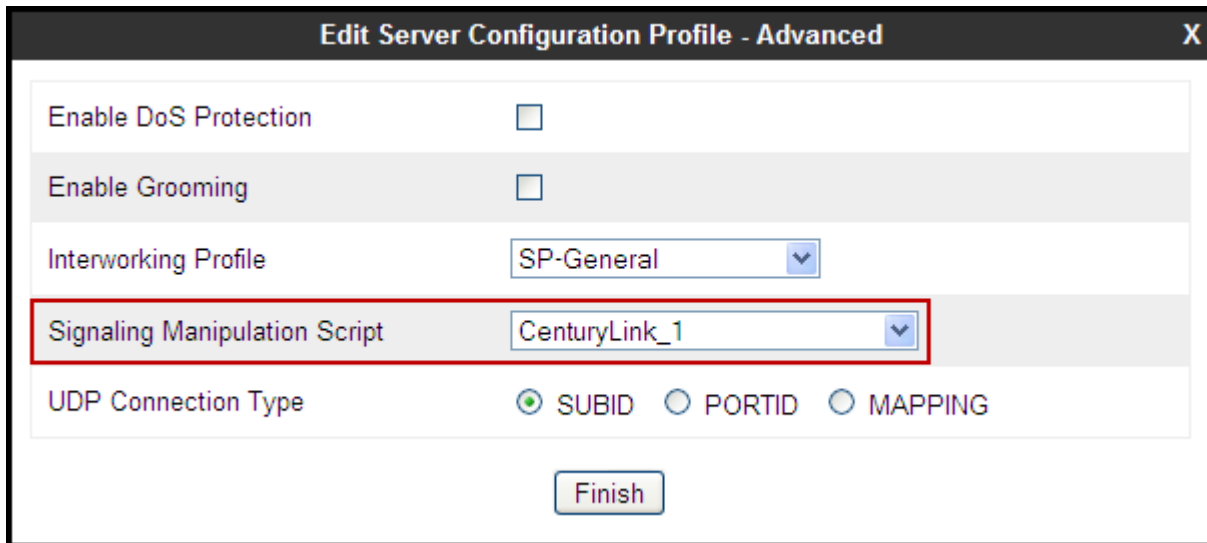
    remove(%BODY[1]);
    remove(%BODY[1]);

    // Remove unwanted Headers
    remove(%HEADERS["History-Info"][3]);
    remove(%HEADERS["History-Info"][2]);
    remove(%HEADERS["History-Info"][1]);
    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["x-nt-e164-clid"][1]);
    remove(%HEADERS["P-AV-Message-Id"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["Av-Global-Session-ID"][1]);
    remove(%HEADERS["P-Location"][1]);
    remove(%HEADERS["Remote-Party-ID"][1]);
  }
}
```

Edit

After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 6.2.4**.

Go to **Global Profiles** → **Server Configuration** → **Service Provider** → **Advanced** tab → **Edit**. Select **CenturyLink\_1** from the drop down menu on the **Signaling Manipulation Script** field. Click **Finish** to save and exit.



**Edit Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

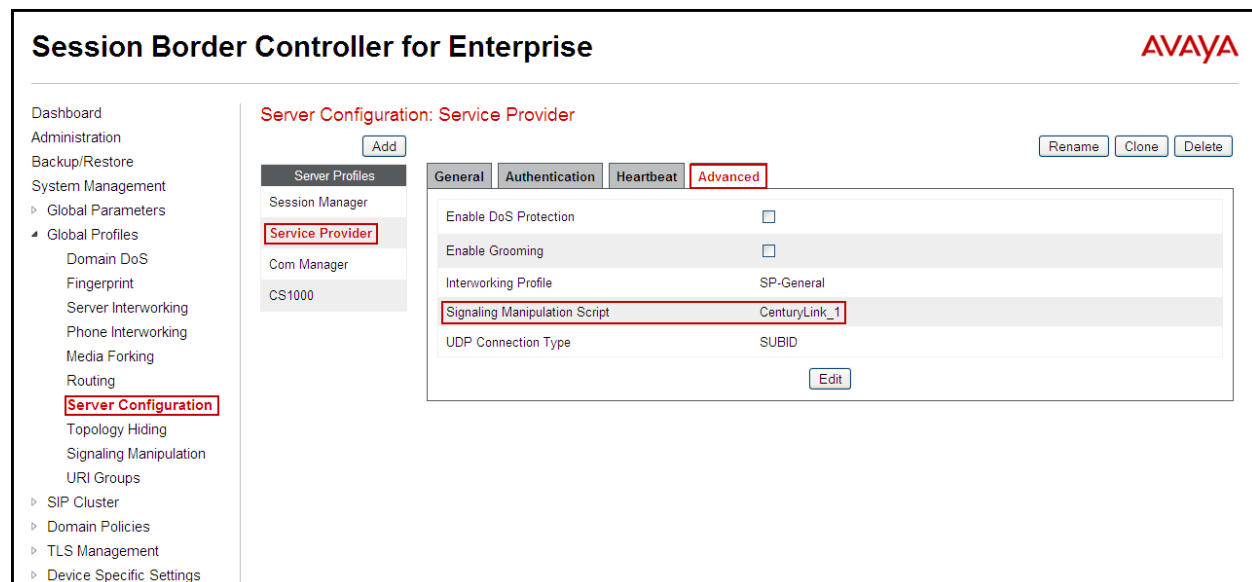
Interworking Profile SP-General

**Signaling Manipulation Script** CenturyLink\_1

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** 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

**Server Configuration: Service Provider**

**Server Profiles**  
Session Manager  
**Service Provider**  
Com Manager  
CS1000

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

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

**Signaling Manipulation Script** CenturyLink\_1

UDP Connection Type SUBID

**Edit**

**Rename** **Clone** **Delete**



## 6.3. 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.

### 6.3.1. 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 defines 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: **1000 Sessions**
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **1000** was used in the sample configuration.
- Click Finish (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, and TLS Management. Under Domain Policies, 'Application Rules' is selected and highlighted. The main content area is titled 'Application Rules: 1000 Sessions' and features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. A list of application rules is shown, with '1000 Sessions' selected. The table below details the configuration for the 'Voice' application type.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Below the table, a 'Miscellaneous' section includes 'CDR Support' (None) and 'RTCP Keep-Alive' (No). An 'Edit' button is located at the bottom right of the configuration area.

## 6.3.2. Media Rules

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. Under 'Domain Policies', 'Media Rules' is highlighted. The main content area is titled 'Media Rules: default-low-med'. It features a list of media rules on the left: 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', and 'avaya-low-med-enc'. The 'default-low-med' rule is selected. To the right of the list, there is a warning banner stating 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' Below this, there are tabs for 'Media NAT', 'Media Encryption', 'Media Anomaly', 'Media Silencing', and 'Media QoS'. The 'Media NAT' tab is active, showing a configuration field for 'Media NAT' with the value 'Learn Media IP dynamically' and an 'Edit' button. The Avaya logo is in the top right corner.

### 6.3.3. 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 the control of the Quality of Service of the signaling packets.

For the compliance test **default** Signaling Rule was used. The removal of unwanted headers is accomplished by Signaling Manipulation rules defined in **Section 6.2.6**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies (expanded), Application Rules, Border Rules, Media Rules, Security Rules, **Signaling Rules** (highlighted), Time of Day Rules, End Point Policy Groups, Session Policies, TLS Management, and Device Specific Settings. The main content area is titled "Signaling Rules: default" and includes an "Add" button and a "Filter By Device..." dropdown. A warning banner states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, there are tabs for "General", "Requests", "Responses", "Request Headers", "Response Headers", and "Signaling QoS". The "General" tab is active, showing settings for Inbound and Outbound traffic. The Inbound section includes: Requests (Allow), Non-2XX Final Responses (Allow), Optional Request Headers (Allow), and Optional Response Headers (Allow). The Outbound section includes: Requests (Allow), Non-2XX Final Responses (Allow), Optional Request Headers (Allow), and Optional Response Headers (Allow). The Content-Type Policy section includes: "Enable Content-Type Checks" (checked), "Action" (Allow), "Multipart Action" (Allow), and "Exception List". An "Edit" button is located at the bottom right of the Content-Type Policy section.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy	
Enable Content-Type Checks	<input checked="" type="checkbox"/>
Action	Allow
Multipart Action	Allow
Exception List	Exception List

### 6.3.4. 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: default.**
- **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**

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	<input type="button" value="Edit"/> <input type="button" value="Clone"/>

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

Add

Filter By Device...

Rename

Delete

Policy Groups

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Add

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

Service Provider

HG; Reviewed:  
SPOC 12/4/2013

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

77 of 94  
CLCS1K76ASBCE62

## 6.4. 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.

### 6.4.1. Network Management

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

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

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Network Management' highlighted under 'Device Specific Settings'. The main content area is titled 'Network Management: Sipera' and has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A red box highlights the 'Sipera' device name in the sidebar and the 'Network Configuration' tab. An orange warning banner states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, a blue banner says: 'Changes will not take effect until the interface is updated.' The configuration section includes fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.192), and 'B2 Netmask'. There are 'Add', 'Save', and 'Clear' buttons. A table lists IP configurations with columns for IP Address, Public IP, Gateway, and Interface. The first two rows are highlighted with a red box.

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
172.16.157.187		172.16.157.129	B1	Delete
			B1	Delete
		64.197.157.129	B1	Delete
172.16.5.72		172.16.5.254	A1	Delete

On the Interface Configuration tab, click the **Toggle State** 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

### 6.4.2. Media Interface

Media Interfaces were created to adjust the port range that the Avaya SBCE will advertise as the listening ports. On the Private and Public interfaces of the Avaya SBCE ports range 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.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward the CS1000).
- **Port Range: 35000-40000.**
- Click **Finish.**
- Select **Add Media Interface.**
- **Name: Public.**
- Select **IP Address: 172.16.157.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

The following screen capture shows the added **Media 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

**Media Interface: Sipera**

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range	Edit	Delete
Private	172.16.5.71	35000 - 40000	Edit	Delete
Public	172.16.157.187	35000 - 40000	Edit	Delete

### 6.4.3. Signaling Interface

To create the Signaling Interface toward the CS1000, from the **Device Specific** menu on the left hand side, select **Signaling Interface**

- Select **Add Signaling Interface:**
- **Name: Private.**



- Select **IP Address: 172.16.5.71** (Inside or private IP Address of the Avaya SBCE , toward the CS1000)
- **UDP Port: 5060.**
- **Click Finish.**

To create the Signaling Interface toward the Service Provider, from the **Device Specific** menu on the left hand side, select **Signaling Interface**

- Select **Add Signaling Interface:**
- **Name: Public**
- Select **IP Address: 172.16.157.187** (Outside or public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- **Click Finish.**

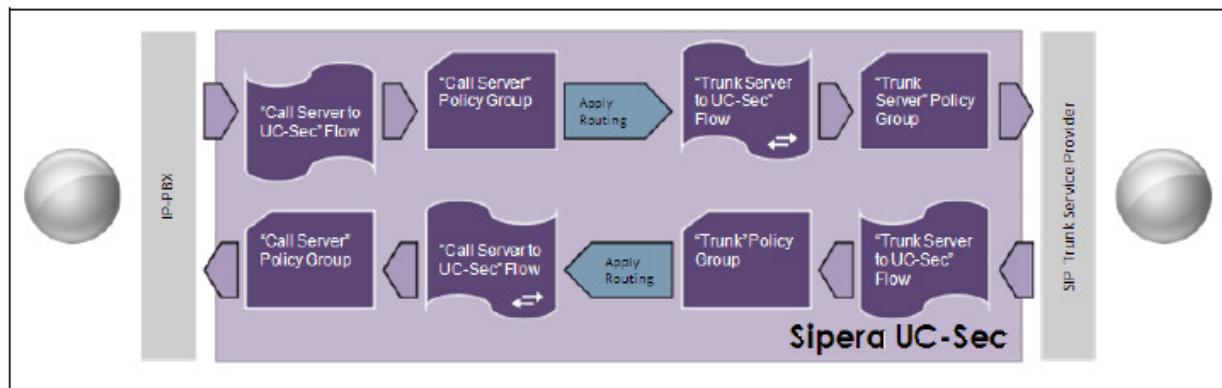
The following screen capture shows the newly added **Signaling Interfaces**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Device Specific Settings', where 'Signaling Interface' is highlighted. The main content area is titled 'Signaling Interface: Sipera'. It features a tabbed interface with 'Devices' and 'Signaling Interface' tabs. The 'Signaling Interface' tab contains a table listing the configured interfaces. The table has columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. Two interfaces are listed: 'Private' with IP 172.16.5.71 and 'Public' with IP 172.16.157.187, both using UDP port 5060 and no TLS profile. Each row has 'Edit' and 'Delete' links. An 'Add' button is located at the top right of the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private	172.16.5.71	---	5060	---	None	Edit Delete
Public	172.16.157.187	---	5060	---	None	Edit Delete

#### 6.4.4. End Point Flows

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



The **End-Point Flows** defines 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**, tab **Server Flows**. Click **Add Flow**.

- **Name:** SIP\_Trunk\_Flow.
- **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\_CS1000 (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	
<b>Criteria</b>		<b>Profile</b>	
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_CS1000
Remote Subnet	*	Topology Hiding Profile	Service_Provider
Received Interface	Private	File Transfer Profile	None

To create the call flow toward the CS1000, click **Add Flow**.

- **Name: CS1000\_Flow.**
- **Server Configuration: CS1000.**
- **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: CS1000.**
- **File Transfer Profile: None.**
- Click **Finish**.

View Flow: CS1000_Flow		X	
<b>Criteria</b>		<b>Profile</b>	
Flow Name	CS1000_Flow	Signaling Interface	Private
Server Configuration	CS1000	Media Interface	Private
URI Group	*	End Point Policy Group	Enterprise
Transport	*	Routing Profile	Route_to_SP
Remote Subnet	*	Topology Hiding Profile	CS1000
Received Interface	Public	File Transfer Profile	None

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

## 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

End Point Flows: Sipera

Devices

Sipera

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: CS1000

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	CS1000_Flow	*	Public	Private	Enterprise	Route_to_SP	View Clone Edit Delete

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_CS1000	View Clone Edit Delete

## 7. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk service, a customer must request the service from CenturyLink using their sales processes. The process can be started by contacting CenturyLink via the corporate web site at: <http://www.CenturyLink.com/>

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

## 8. Verification Steps

The following steps may be used to verify the configuration.

### 8.1. General

Place an inbound/outbound call to/from to 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 or received. Perform hold/retrieve on calls. Verify the call remains stable for several minutes and disconnect properly.

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

### Active Call Trace (LD 80).

Following is an example of one of the commands available on the CS1000 to trace the extension (DN) when the call is active or idle. The call scenario involved the CS1000 extension 8000 calling a PSTN phone number (7863311234).

- 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** while the call is active.
- After call is released, issue command **trac 0 8000** again to see if the DN is released back to idle state.

The screen on the next page shows the actual output of the Call Server Command Line mode when the 8000 is in an active call:

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

The following screen shows an example of an active call on extension 8000.

```
>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: 172.16.20.154 PORT: 5200
FAR-END SIP SIGNALLING IP: 172.16.21.61
FAR-END MEDIA ENDPOINT IP: 172.16.20.154 PORT: 5200
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: 35010
FAR-END VendorID: AVAYA-SM-6.3.2.0.632023
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 91786331
MAIN_PM ESTD
TALKSLOT ORIG 10 TERM 15 JUNCTOR ORIGO TERMO
EES_DATA:
NONE
QUEUE NONE
CALL ID 0 489

----- ISDN ISL CALL (TERM) -----
CALL REF # = 395
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 8000 NUM_PLAN:E164 TON:NATIONAL ESN:NPA
CALLED NO = 1786331 NUM_PLAN:E164 TON:NATIONAL ESN:NPA
```

The following screen shows an example after the call on extension 8000 was released.

```
.trac 0 8000

IDLE VTN 008 0 00 00 MARP
```

The following screen shows an example after the call was 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
```

### 8.3. 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 and 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, DTMF event description.
- Media Attribute: verify specific audio port, codec, ptime, 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: 7203621234) on the CS1000 to a PSTN number (7863311234).

The image shows a Wireshark network capture of a SIP call. The top pane displays a list of captured packets, and the bottom pane shows the detailed view of a selected packet (Frame 41).

No.	Time	Source	Destination	Protocol	Length	Info
41	8.502745	.157.187	.32.8	SIP/SDP	1198	Request: INVITE sip:1786331@.32.8;user=phone
42	8.553136	.32.8	.157.187	SIP	405	Status: 100 Trying
63	11.918188	.32.8	.157.187	SIP/SDP	926	Status: 180 Ringing
64	11.923951	.157.187	.32.8	SIP	803	Request: OPTIONS sip:1786331@.32.8:5060
65	11.925484	.157.187	.32.8	SIP	748	Request: PRACK sip:1786331@.32.8:5060
69	11.971927	.32.8	.157.187	SIP	718	Status: 200 OK
70	11.974195	.32.8	.157.187	SIP	473	Status: 200 OK
326	14.363089	.32.8	.157.187	SIP/SDP	995	Status: 200 OK
329	14.368093	.157.187	.32.8	SIP	752	Request: ACK sip:1786331@.32.8:5060
1950	29.823160	.157.187	.32.8	SIP	723	Request: BYE sip:1786331@.32.8:5060
1956	29.876033	.32.8	.157.187	SIP	471	Status: 200 OK

**Frame 41: 1198 bytes on wire (9584 bits), 1198 bytes captured (9584 bits)**

- Ethernet II, Src: IntelCor\_cb:79:91 (00:1b:21:cb:79:91), Dst: Adtran\_30:cd:78 (00:a0:c8:30:cd:78)
- Internet Protocol Version 4, Src: .157.187 (.157.187), Dst: .32.8 (.32.8)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol (INVITE)
  - Request-Line: INVITE sip:1786331@.32.8;user=phone SIP/2.0
  - Method: INVITE
  - Request-URI: sip:1786331@.32.8;user=phone
  - [Resent Packet: False]
  - Message Header
    - From: "Avaya 1120" <sip:720362@.157.187:5060;user=phone>;tag=396db10-3c1410ac-13c4-55013-15aa1-f34cfe8-15aa1
    - To: <sip:1786331@.32.8;user=phone>
    - CSeq: 1 INVITE
    - Call-ID: f3c11c072231c74478ed043f39999638
    - Contact: <sip:720362@.157.187:5060;transport=udp;user=phone>
    - Record-Route: <sip:157.187:5060;ipcs-line=1790;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-7.65.16.21
    - Max-Forwards: 19
    - Via: SIP/2.0/UDP .157.187:5060;branch=z9hG4bK-s1632-001587970584-1--s1632-Privacy: none
    - P-Asserted-Identity: "Avaya 1120" <sip:720362@.157.187:5060;user=phone>
    - Content-Type: application/sdp
    - Content-Length: 275
  - Message Body
    - Session Description Protocol
      - Session Description Protocol version (v): 0
      - Owner/Creator, Session Id (o): - 441 1 IN IP4 .157.187
      - Session Name (s): -
      - Connection Information (c): IN IP4 .157.187
      - Time Description, active time (t): 0 0
      - Media Description, name and address (m): audio 35232 RTP/AVP 0 8 18 101 111
      - Connection Information (c): IN IP4 .157.187
      - Media Attribute (a): fmtp:18 annexb=no
      - Media Attribute (a): rtpmap:101 telephone-event/8000
      - Media Attribute (a): fmtp:101 0-15
      - Media Attribute (a): rtpmap:111 X-nt-inforeq/8000
      - Media Attribute (a): ptime:20
      - Media Attribute (a): sendrecv
      - Data (8 bytes)

## 9. Conclusion

These Application Notes describe the procedures necessary to Configuring CenturyLink SIP Trunk service with Avaya Communication Server 1000E Release 7.6 and Avaya Session Border Controller for Enterprise Release 6.2 as shown in **Figure 1**.

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

## 10. References

This section references the documentation relevant to these Application Notes.

Product documentation for the Avaya Communication Server 1000E, including the following, is available at:

<http://support.avaya.com/>

- [1] Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013.
- [2] IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013.
- [3] Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013.
- [4] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.
- [5] Dialing Plans Reference, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.
- [6] Product Compatibility Reference, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013.
- [7] Avaya Product Support Notice – PSN003460u – Configuring FAX over IP in CS 1000: An Overview.
- [8] Communication Server 1000 Release 7.6 & Service Pack 2 Release Notes, Issue 1.1 July 2013.

Product documentation for the Avaya SBCE, including the following, is available at:

<http://support.avaya.com/>

- [9] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, May 2013.
- [10] Installing Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, June 20 2013.
- [11] Upgrading Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, July 2013.

Other resources:

- [12] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>
- [13] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>

## Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE, **Section 6.2.6:**

```
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {
        if (%HEADERS["History-Info"][1].regex_match("reason")) then
        {

            %HEADERS["Diversion"][1] = "sip:dummy@dummy.com";

            %HEADERS["Diversion"][1].URI.SCHEME = %HEADERS["History-
Info"][1].URI.SCHEME;
            %HEADERS["Diversion"][1].URI.USER = %HEADERS["History-
Info"][1].URI.USER;
            %HEADERS["Diversion"][1].URI.HOST = %HEADERS["History-
Info"][1].URI.HOST;
            %HEADERS["Diversion"][1].URI.PORT = %HEADERS["History-
Info"][1].URI.PORT;

            %HEADERS["Diversion"][1].URI.PARAMS["reason"] = "unconditional";
            %HEADERS["Diversion"][1].URI.PARAMS["counter"] = "1";
            %HEADERS["Diversion"][1].URI.PARAMS["privacy"] = "off";
        }

        %HEADERS["Content-Type"][1].regex_replace("multipart/mixed;boundary=unique-
boundary-1","application/sdp");

// 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 unwanted Headers
        remove(%HEADERS["History-Info"][3]);
        remove(%HEADERS["History-Info"][2]);
        remove(%HEADERS["History-Info"][1]);
    }
}
```

```
remove(%HEADERS["Alert-Info"][1]);
remove(%HEADERS["x-nt-e164-clid"][1]);
remove(%HEADERS["P-AV-Message-Id"][1]);
remove(%HEADERS["P-Charging-Vector"][1]);
remove(%HEADERS["Av-Global-Session-ID"][1]);
remove(%HEADERS["P-Location"][1]);
remove(%HEADERS["Remote-Party-ID"][1]);
    }
}
```

---

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

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

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