



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

---

# **Application Notes for Configuring CenturyLink BroadWorks SIP Trunk service with Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and Avaya Session Border Controller for Enterprise Release 4.0.5Q02 - Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) Trunking between CenturyLink BroadWorks SIP Trunk service and Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1, Avaya Session Border Controller for Enterprise Release 4.0.5Q02.

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 in both directions with various Avaya endpoints.

The CenturyLink BroadWorks SIP Trunk service provides PSTN access via a SIP trunk between the enterprise and the CenturyLink 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 1000 .....	11
5.1.	Log in to the CS1000 System.....	11
5.1.1.	Log in to Unified Communications Management (UCM) and Element Manager .....	11
5.1.2.	Log in to the Call Server Command Line Interface (CLI) .....	13
5.2.	Administer a IP Telephony Node.....	13
5.2.1.	Obtain Node IP address .....	13
5.2.2.	Administer TPS.....	14
5.2.3.	Administer Quality of Service (QoS) .....	15
5.2.4.	Synchronize the New Configuration .....	16
5.3.	Administer Voice Codec.....	17
5.3.1.	Enable Voice Codec, IP Telephony Node.....	17
5.3.2.	Enable Voice Codec on Media Gateways .....	19
5.4.	Administer Zones and Bandwidth.....	20
5.4.1.	Create a zone for IP phones (zone 5).....	20
5.4.2.	Create a zone for virtual SIP trunk (zone 4) .....	22
5.5.	Administer SIP Trunk Gateway .....	22
5.5.1.	Integrated Services Digital Network (ISDN).....	22
5.5.2.	Administer the SIP Trunk Gateway to Session Manager .....	24
5.5.3.	Administer Virtual D-Channel.....	26
5.5.4.	Administer Virtual Super-Loop .....	30
5.5.5.	Administer Virtual SIP Routes .....	30
5.5.6.	Administer Virtual Trunks .....	33
5.5.7.	Administer Calling Line Identification Entries.....	35
5.5.8.	Enable External Trunk to Trunk Transferring .....	36
5.6.	Administer Dialing Plans.....	37
5.6.1.	Define ESN Access Codes and Parameters (ESN).....	37
5.6.2.	Associate NPA and SPN call to ESN Access Code 1 .....	38
5.6.3.	Digit Manipulation Block (DMI).....	38
5.6.4.	Route List Block (RLB) .....	39
5.6.5.	Inbound Call Digit Translation .....	40
5.6.6.	Outbound Call - Special Number Configuration. ....	41
5.6.7.	Outbound Call - Numbering Plan Area Code (NPA) .....	43
5.7.	Administer Phone.....	43
5.7.1.	Phone creation.....	43
5.7.2.	Enable Privacy for Phone.....	45

5.7.3.	Enable Call Forward for the Phone .....	46
5.7.4.	Enable Call Waiting for the Phone .....	48
6.	Configure the Avaya Aura® Session Manager .....	50
6.1.	System Manager Login and Navigation .....	50
6.2.	Specify SIP Domains .....	52
6.3.	Add Location .....	52
6.4.	Add Adaptation Module .....	53
6.5.	Add SIP Entities .....	55
6.6.	Add Entity Links .....	58
6.7.	Add Routing Policies .....	60
6.8.	Add Dial Patterns .....	62
6.9.	Add/View Avaya Aura® Session Manager .....	66
7.	Configure the Avaya Session Border Controller for Enterprise .....	68
7.1.	Provisioning Script .....	68
7.2.	Install Device .....	71
7.3.	Global Profiles .....	74
7.3.1.	Server Interworking .....	74
7.3.2.	Routing Profiles .....	76
7.3.3.	Server Configuration .....	79
7.3.4.	Topology Hiding .....	84
7.3.5.	Signaling Manipulation .....	86
7.4.	Domain Policies .....	89
7.4.1.	Media Rules .....	89
7.4.2.	Signaling Rules .....	89
7.4.3.	End Point Policy Groups .....	92
7.5.	Device Specific Settings .....	94
7.5.1.	Network Management .....	94
7.5.2.	Media Interface .....	95
7.5.3.	Signaling Interface .....	97
7.5.4.	End Point Flows .....	99
8.	CenturyLink BroadWorks SIP Trunk Service Configuration .....	103
9.	Verification Steps .....	104
9.1.	General .....	104
9.2.	Verify Call Establishment on the CS1000 Call Server .....	104
9.3.	Protocol Traces .....	105
10.	Conclusion .....	108
11.	References .....	109

# 1. Introduction

This document provides the steps to configure Session Initiation Protocol (SIP) Trunking between Avaya Communication Server 1000 and the CenturyLink BroadWorks SIP Trunk service (hereafter referred to as CenturyLink or CenturyLink system). During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between the CenturyLink system and the Avaya CS1000.

In the sample configuration, the Avaya CS1000 solution consists of a CS1000 Rel. 7.5 (hereafter referred to as CS1000) , Avaya Aura® Session Manager Rel. 6.1 (hereafter referred to as Avaya Aura® Session Manager), Avaya Session Border Controller for Enterprise Rel. 4.0.5Q02 (hereafter referred to as Avaya SBCE) , and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE or Avaya Aura® Session Manager.

## 2. General Test Approach and Test Results

The CS1000 system was connected to an Avaya SBCE via SIP trunks to the Avaya Aura® Session Manager. The Avaya SBCE was connected to the CenturyLink system via a SIP trunk. Various call types were made from the CS1000 to the CenturyLink system and vice versa to ensure interoperability between the CS1000 and the CenturyLink system.

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 testing was to verify that the CS1000 can interoperate with the CenturyLink system. The following interoperability areas were covered.

- Static IP.
- Incoming calls from the PSTN were routed to the DID numbers assigned by CenturyLink. Incoming PSTN calls were terminated to the following end points: Avaya 1100 Series 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 the CenturyLink BroadWorks network to the various PSTN destinations.
- 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 (w/voice mail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.

- Codec G.711u with VAD disabled. (CenturyLink only supports Codec G.711u).
- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- CallPilot Voice Mail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with IVR (Interactive Voice Response systems).
- International calls.
- Calls to special numbers (411, 711, 911, Operator (0), 0+10 digits Operator Assisted calls, etc.).
- 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.
- G.711u fax pass-through support (inbound and outbound) (CenturyLink does not support T.38)
- Long duration calls (one hour).
- Early Media transmission

## 2.2. Test Results

Interoperability testing of CenturyLink BroadWorks SIP Trunk Service with the Avaya CS1000 solution was completed successfully with the following observations/limitations.

- **Calling Name and Calling Number Delivery to PSTN:** On outbound calls from the CS1000 to the PSTN the “Calling Name” is not delivered to the PSTN phone (is not displayed), only the “Calling Number” is delivered (is displayed).
- **Calling Name Blocking:** In the CS1000, the “Calling Name” can be blocked/restricted from being displayed at the PSTN extension. With this setting enabled on the CS1000 extension, the CS1000 will send the “Calling Number” in the “From” header of the INVITE message and will set the Privacy to “user” (Privacy: user) in the same INVITE message. The expected result is the display of only the number and not the name. The actual result is the blocking of the number. Since the name was never delivered to the PSTN, as indicated above, neither the name nor the number are displayed at the PSTN extension with Calling Name restriction enabled on the CS1000 extension.
- **Blind Transfer of calls from the CS1000 to the PSTN:** Blind Transfers of calls from the CS1000 to the PSTN were failing with the BroadWorks switch sending a “500 Server Internal Error” in response to the UPDATE sent to the BroadWorks switch by the CS1000. The problem is that the CS1000 sends an UPDATE to the BroadWorks switch “before” the completion of the initial INVITE transaction, with this INVITE containing an offer. Per **RFC3311** an UPDATE cannot be sent with an offer unless the callee has generated an answer in a reliable provisional response. The INVITE needs to be answered by the CS1000 with a PRACK “before” sending the UPDATE. The solution to this problem is to apply patch **p30224\_1.ntl** to the CS1000 Signaling Server (Linux) and

to upgrade the Signaling Server to the latest **VTRK** SU version. Version cs1000-vtrk-7.50.17.16-34.i386.000.ntl was used in the Avaya lab during testing. Also, testing was done with Plug-In **201 enabled** and Plug-In **501 disabled**. For the information on how to obtain and how to apply the patch please visit <http://support.avaya.com>

- **SIP Diversion Header for call re-direction:** CenturyLink does not support History-Info, instead requires SIP Diversion Header for calls that are re-directed at the CS1000. Session Manager was used to convert History-Info to SIP Diversion Header. This can be accomplished by using adaptation modules in Session Manager.
- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and the CenturyLink network when there is no call re-direction involved. However, when a call is re-directed to the PSTN at the CS1000 extension, the Caller ID will not properly reflect the true originator of the call. In normal conditions if a call is re-directed at the CS1000 to a PSTN extension, the Caller ID displayed at the PSTN extension will be of the extension doing the re-direction (i.e., transfer) and not the Caller ID of the extension that originated the call. On the CenturyLink network, the PAI header is used to authenticate the call during call redirection scenarios. When a call is re-directed, the PAI header will be populated with the information of the extension that is doing the call redirection.
- **Routing Profiles:** When configuring Routing Profiles in the Avaya SBCE (**Section 7.3.2**), the selection of **Use Next Hop for In Dialog Messages** should **not** be checked. In the current software release of the Avaya SBCE (Release **4.0.5Q02**), when this field is not checked, messaging problems with the SIP **BYE** method were observed in between the Avaya SBCE and Avaya Aura® Session Manager. In order to correct this problem in the current software release of the Avaya SBCE (Release **4.0.5Q02**) patch **ipcs-bin-mvista\_debug\_20120413150346-2.i386.rpm** must be applied to the Avaya SBCE. The fix will be included in the next software release of the Avaya SBCE (Release **4.0.5Q09**). For the information on how to obtain and how to apply the patch please contact Avaya SBCE support at: **866-861-3113 toll free or +1 214-269-2424**.
- **SIP Header Optimization:** SIP header rules were implemented in the Avaya SBCE and in Session Manager to streamline the SIP header and remove any unnecessary parts. The following headers were removed: X\_nt\_e164\_clid, Alert-Info and History-info if it is present in the INVITE. Also the multipart MIME SDP, which included 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.

## 2.3. Support

For technical support on CenturyLink system, please contact CenturyLink technical support at: Toll Free: 1-877-290-5458

<http://www.centurylink.com/Pages/Support/>

### 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 BroadWorks SIP Trunk Service through the public Internet.

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

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

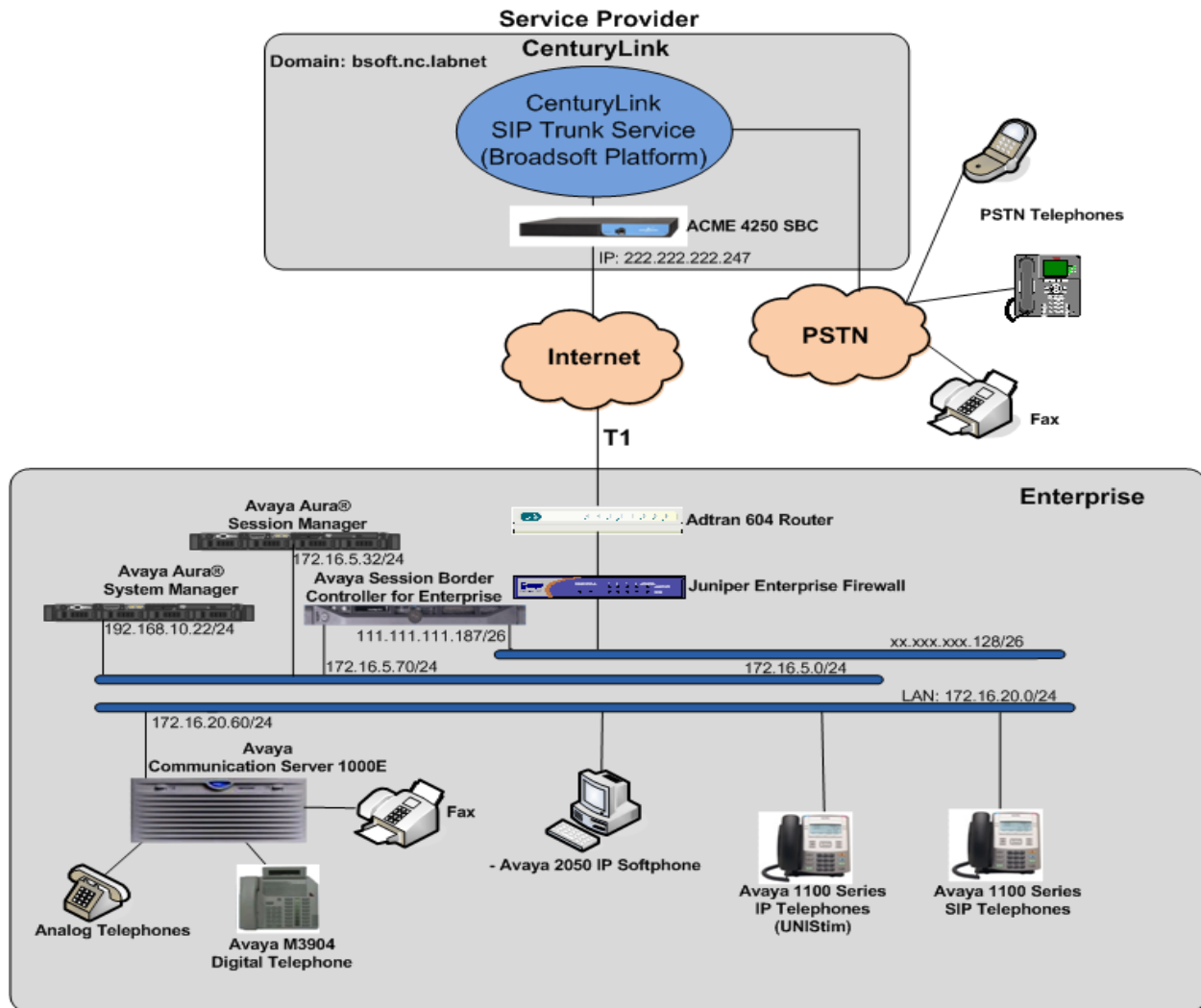
Located at the edge of the enterprise is the Avaya Session Border Controller for Enterprise (Avaya SBCE). It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya 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 SIP over UDP. The transport protocol between the Avaya SBCE and Avaya Aura® Session Manager across the enterprise IP network is SIP over TCP. The transport protocol between Avaya Aura® Session Manager and the CS1000 across the enterprise IP network is SIP over TLS. For ease of troubleshooting during testing, the compliance test was conducted with the Transport Method set to UDP between Avaya Aura® Session Manager and the CS1000.

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

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

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

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



**Figure 1: CenturyLink BroadWorks SIP Trunk service and Avaya CS1000E**



## 4. Equipment and Software Validated

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

<b>Avaya:</b>	
<b>Equipment</b>	<b>Release/Version</b>
Avaya Communication Server 1000E running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	Call Server: 7.50 Q + DepList 1: core Issue: 01 (created: 2012-01-10 16:47:54 (est))  Signaling Server: 7.50.17.00 **See Service Updates & Patches below**
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.1 service pack 5 (ASM 6.1.5.0.615006)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.1 Service Pack 5 Build No. 6.1.0.0.7345-6.1.5.502
Avaya Session Border Controller for Enterprise (Avaya SBCE)	4.0.5Q02
Avaya Phones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Lucent Analog Phone	--
Fax Machines	--
<b>CenturyLink:</b>	
<b>Equipment</b>	<b>Release/Version</b>
BroadWorks Broadsoft	17 sp2
Sonus NBS	B07.02.07 F004
Sonus GSX	B07.02.07 F004
Acme Packet Net-Net 4250 Session Border Controller	SC6.1.0 MR-5 GA (Built 704)

### Signaling Server Service Updates & Patches:

#####

#### SUs:

cs1000-patchWeb-7.50.17.16-4.i386.000  
cs1000-baseWeb-7.50.17.16-1.i386.001  
ipsec-tools-0.6.5-14.el5.3\_avaya\_1.i386.000  
cs1000-dbcom-7.50.17-02.i386.000  
cs1000-shared-pbx-7.50.17.16-1.i386.000  
cs1000-kec-7.50.17.16-1.i386.000  
cs1000-ipsec-7.50.17.16-1.i386.000  
cs1000-linuxbase-7.50.17.16-6.i386.000

spiritAgent-6.1-1.0.0.108.208.i386.000  
cs1000-EmCentralLogic-7.50.17.16-1.i386.000  
cs1000-csmWeb-7.50.17.16-3.i386.000  
cs1000-mscAnnc-7.50.17.16-1.i386.000  
cs1000-mscTone-7.50.17.16-1.i386.000  
cs1000-mscMusc-7.50.17.16-2.i386.000  
cs1000-dmWeb-7.50.17.16-2.i386.000  
tzdata-2011h-2.el5.i386.000  
cs1000-Jboss-Quantum-7.50.17.16-10.i386.000  
cs1000-sps-7.50.17.16-2.i386.000  
cs1000-tps-7.50.17.16-11.i386.000  
cs1000-ftpkg-7.50.17.16-7.i386.000  
cs1000-bcc-7.50.17.16-46.i386.000  
**cs1000-vtrk-7.50.17.16-34.i386.000**  
cs1000-emWeb\_6-0-7.50.17.16-16.i386.000  
#####

**Patches:**

**p30224\_1**

#####

**Note:** The **VTRK** SU version should be “cs1000-vtrk-7.50.17.16-**15**.i386.000.ntl” or higher on all Signaling Servers to ensure proper operation of the blind transfer feature. Patch **p30224\_1** is also required if problems with SIP **UPDATE** are observed during Call Redirection scenarios.

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

**Enable Plug-In 201** and ensure Plug-In **501** is **disabled** as follows:

Log in to the **Unified Communications Management (UCM) and Element Manager** as described in **Section 5.1.1**. Go to **System → Software → Plug-ins**, select **plug-in 201** and click the **Enable** button. The status will change to **Enabled**. Verify the status for **plug-in 501** shows **Disabled**.

## 5. Configure Avaya Communication Server 1000

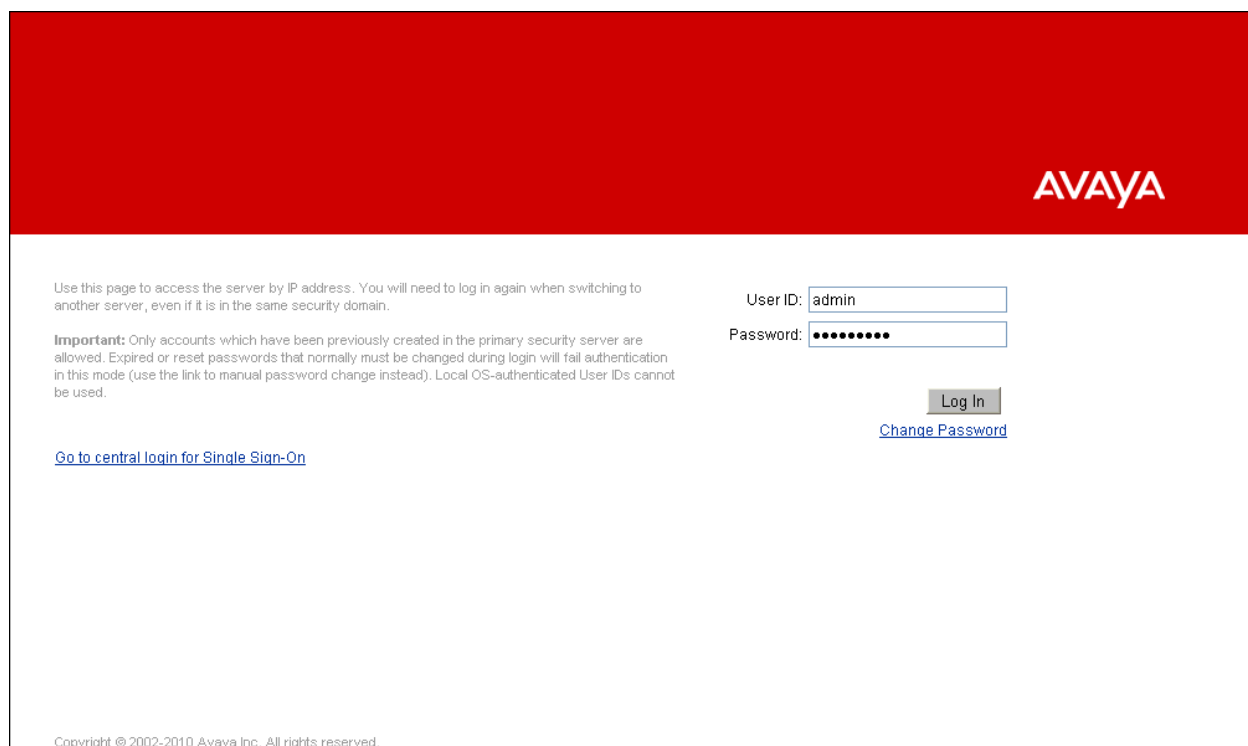
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11**.

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

### 5.1. Log in to the CS1000 System

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

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

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

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

**AVAYA** Avaya Unified Communications Management [Help](#) | [Logout](#)

Host Name: 172.16.20.60 Software Version: 02.20.0017.00(4713) User Name admin

### Elements

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

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	<b>EM on cs1k</b>	CS1000	7.5	172.16.21.61	New element.
<input type="checkbox"/>	cs1k.avaya.lab.com (primary)	Linux Base	7.5	172.16.20.61	Base OS element.
<input type="checkbox"/>	MGC	Media Gateway Controller	7.5	172.16.21.62	Media Gateway Controller

Copyright 2002-2010 Avaya Inc. All rights reserved.

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

**AVAYA** CS1000 Element Manager [Help](#) | [Logout](#)

Managing: 172.16.21.61 Username: admin  
System Overview

### System Overview

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

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

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

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

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

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

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

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

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

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

OVL000
>
```

## 5.2. Administer a IP Telephony Node

This section describes how to configure a 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 CS1000 IP network to work with the CenturyLink system.

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

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

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.

Print | Refresh

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

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

**Left Navigation Menu:**

- 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

The **Node Details** screen is displayed as shown 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.

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

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

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

Node ID:  \* (0-9999)

Call server IP address:  \*

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

**Embedded LAN (ELAN)**

Gateway IP address:  \*

Subnet mask:  \*

**Telephony LAN (TLAN)**

Node IPv4 address:  \*

Subnet mask:  \*

Node IPv6 address:

\* Required Value. Save Cancel

**Associated Signaling Servers & Cards**

Print | Refresh

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

Show: ☐ IPv6 address

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

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

## 5.2.2. Administer TPS

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

**AVAYA CS1000 Element Manager** Help | Logout

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

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

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

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

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

\* Required Value. Save Cancel

**Associated Signaling Servers & Cards**

Select to add Add Remove Make Leader Print Refresh

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

Show: ☐ IPv6 address

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

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

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

**AVAYA CS1000 Element Manager** Help | Logout

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

**Node ID: 1006 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details**

Firmware | DTLS | Network Connect Server

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

**Firmware**

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

**DTLS**

DTLS policy: Off

Options: ☐ Client authentication  
☐ Periodic re-keying

**Network Connect Server**

Primary network connect server (TLAN IP address): 0.0.0.0

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

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

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

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

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

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

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

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

**IP Telephony Node Properties**

- Voice Gateway (VGVW) 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
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

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

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

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

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

**Node ID: 1006 - Quality of Service (QoS)**

**Diffserv Codepoint (DSCP)**

Enable Avaya automatic QoS: ☐

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

VLAN tagging: ☐ 802.1Q support

802.1Q bits value (802.1P): 5 (0-7)

\* Required Value. Save Cancel

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

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

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



**AVAYA CS1000 Element Manager**

Help | Logout

Managing-Element-Manager-User-Interface-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
cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

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

## 5.3. Administer Voice Codec

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

Select **IP Network** → **Nodes: Servers, Media Cards** Configuration from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed. On the **Node Details** page shown below, click on **Voice Gateway (VGW) and Codecs**.

**AVAYA CS1000 Element Manager**

Help | Logout

Managing-Element-Manager-User-Interface-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 \*

Subnet mask: 255.255.255.0 \*

Node IPv6 address: \*

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

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

\* Required Value.

**Save** **Cancel**

**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, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

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

The **Voice Gateway (VGW) and Codecs** screen will be displayed as shown below. The CenturyLink system only supports **G711u** with **VAD** disabled. The CenturyLink system does not

support **G729**. Ensure that for **G711** the **Voice Activity Detection (VAD)** is unchecked; uncheck Codec **G729** checkboxes as shown below. Click on **Save** and **Synchronize** as described in **Section 5.2.4**.

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

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

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

General | **Voice Codes** | Fax

**Voice Codes**

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

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

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

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

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

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

**AVAYA** CS1000 Element Manager Help | Logout

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

**- Codec G711** Select ☒

Codec name **G711**

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

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

Modifications may cause changes to dependent settings

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

Modifications may cause changes to dependent settings

**VAD** ☐

**+ Codec G729A** Select ☐

**+ Codec G723.1** Select ☐

**+ Codec T38 FAX** Select ☒

**+ QoS**

**+ Media Based CLID**

**- Call Server LAN**

**Embedded LAN (ELAN) configuration**

Primary call server IP address **172.16.21.61**

Primary call server hostname **Primary\_CS**

Signaling port **15000**

Broadcast port **15001** (1024 - 65535)

**Telephony LAN (TLAN) configuration**

Signaling port **5000**

Voice port **5200** (1024 - 65535)

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

For Fax over IP, CenturyLink does not support **T.38**, only **G.711u pass-through**. G.711 was chosen as the default codec. Ensure that **Enable V.21 FAX tone detection** is unchecked, and that **Enable modem fax pass through mode** is checked. This configuration enables G.711 pass through codec for fax.

**AVAYA CS1000 Element Manager** Help | Logout

**- UCM Network Services**

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

**- VGW and IP phone codec profile**

**Enable echo canceller** ☒

Echo canceller tail delay  (milliseconds)

**Enable dynamic attenuation** ☒

Voice activity detection threshold  (0 - 4 DBM)

Idle noise level  (0 - 1 DBM)

R factor calculation ☐

DTMF tone detection ☒

Enable low latency mode ☐

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

**Enable modem/fax pass through mode** ☒

**Enable V.21 FAX tone detection** ☐

Fax TCF method

FAX maximum rate  (bps)

FAX playout nominal delay  (0 - 300 milliseconds)

FAX no activity timeout  (10 - 32000 milliseconds)

FAX packet size

**- Codec**  **Select** ☒

Codec name G711

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

## 5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: **zone 5** for IP sets and **zone 4** for IP SIP Trunk.

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

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

Managing: **172.16.21.61** Username: admin  
System > IP Network > Zones

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

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

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

**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

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

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

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

**Note:** **BQ** will use **G711** as first choice and **G729** as second choice. **BB** will use **G729** as first choice and **G711** as second choice.

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

Managing: **172.16.21.61** Username: admin  
System > IP Network > Zones > **Bandwidth Zones** > 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 - 100000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 100000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

\* Required value.

**Save** **Cancel**

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

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

Follow **Section 5.4.1** to create a zone for the Virtual Trunk. 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 Trunk.

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

## 5.5. Administer SIP Trunk Gateway

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

### 5.5.1. Integrated Services Digital Network (ISDN)

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.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
Customers

### Customers

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

	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.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
Customers » Customer 00 » Customer Details

### Customer Details

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

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

The screen is updated with a list of **Feature Packages** populated on the CS1000. Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network (ISDN)** checkbox, and retain the default values for all remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

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

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

**- Integrated Services Digital Network** **Package: 145**  
 + Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier:  (1 - 16383)  
 - Private network identifier:  (1 - 16383)

- Node DN:

Multi-location business group:  (0 - 65535)  
 Business sub group consult-only:  (0 - 65535)  
 Prefix 1:   
 Prefix 2:   
 Home number plan area code:  (200 - 999)  
 Prefix for central office:  (100 - 9999)  
 Local steering code:   
 Calling number type: CLID feature displays the set's Prime DN   
 Redirection count for ISDN calls:   
 CLID information for incoming/outgoing calls: No manipulation is done   
 Public service telephone networks: ☐

**+ Network Attendant Service** **Package: 159**  
**+ Flexible Numbering Plan** **Package: 160**  
**+ Trunk Failure Monitor** **Package: 182**

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

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

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

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

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

- Vtrk gateway application: **SIP Gateway (SIPGw)**
- SIP domain name: bsoft.nc.labnet
- Local SIP port: 5085
- Gateway endpoint name: CS1KGateway
- Application node ID: 1006

The domain for CenturyLink (bsoft.nc.labnet) may change during installations.



**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

Vtrk gateway application: ☒ Enable gateway service on this node

**General**

Vtrk gateway application: SIP Gateway (SIPGw) \*

SIP domain name: bsoft.nc.labnet \*

Local SIP port: 5085 \* (1 - 65535)

Gateway endpoint name: CS1KGateway \*

Gateway password: \*

Application node ID: 1006 \* (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ☒ IPv4 ☐ IPv6

**Virtual Trunk Network Health Monitor**

☐ Monitor IP addresses (listed below)  
Information will be captured for the IP addresses listed below.

Monitor IP:  Add

Monitor addresses:  Remove

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

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

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

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

---

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

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

General | SIP Gateway Settings | SIP Gateway Services

**Proxy Or Redirect Server:**

**Proxy Server Route 1:**

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

Port: 5085 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration ☐ Primary CDS proxy

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

Port: 5060 (1 - 65535)

Transport protocol: UDP

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

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

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

Under the **Public E.164 domain names**:

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

Under the **Private domain names**:

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

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

Then click on the **Save** button.

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 services and tools. The main content area is titled 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details'. It features a tabbed interface with 'General', 'SIP Gateway Settings', and 'SIP Gateway Services'. The 'SIP URI Map' section is highlighted with a red box and contains two columns of input fields for Public E.164 and Private domain names. Below this, the 'SIP Gateway Services' section includes a checkbox for 'SIP Converged Desktop' and several text input fields for service parameters. At the bottom, there are 'Save' and 'Cancel' buttons and a copyright notice.

AVAYA CS1000 Element Manager

Help | Logout

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

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

**SIP URI Map:**

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

**SIP Gateway Services**

SIP Converged Desktop: ☒ Enable CD service

Service DN:  Used for making VTRK call from agent.

Converged telephone call forward DN:

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

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

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

Save Cancel

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

### 5.5.3. 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

- UCM Network Services
- Home
+ Links
+ 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 » 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: 1 and type: DCH to Add

- Channel: 0	Type: DCH	Card Type: DCIP	Description: VoIP	Edit
- Channel: 96	Type: DCH	Card Type: DCIP	Description: SIPL_DCH	Edit

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

The D-Channels 0 Property Configuration screen is displayed next as shown below (D-Channel 0 was added for the 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**

HG; Reviewed:  
SPOC 6/21/2012

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

27 of 110  
CTLCS1KSMSBCE

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

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

### D-Channels 0 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300=102 basic protocol (ETS)
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

**+ Basic options (BSCOPT)**

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

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

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

Retain the default values for the remaining fields.

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

User: Integrated Services Signaling Link Dedicated (ISLD)

Interface type for D-channel: Meridian Meridian1 (SL1)

Country: ETS 300=102 basic protocol (ETS)

D-Channel PRI loop number:

Primary Rate Interface:

Secondary PRI2 loops:

Meridian 1 node type: Slave to the controller (USR)

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000

Signalling server resource capacity: 3700 Range: 0 - 3700

**+ Basic options (BSCOPT)**

**- Advanced options (ADVOPT)**

- Layer 3 call control message count per 5 second time interval: 300 Range: 60 - 350

- Number of Status Enquiry Messages sent within 128 ms: 1

- Map channel number to timeslots on a PRI2 loop: ☒

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

- Overlap Receiving: ☐

- Overlap Sending: ☐

--Overlap Timer:

- Multilocation Business Group Allowed: ☐

**- Network Attendant Service Allowed: ☒**

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

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

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

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

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

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Remote Capabilities Configuration'. It contains a list of checkboxes for various features. The 'Message waiting interworking with DMS-100 (MWI)' and 'Network name display method 2 (ND2)' checkboxes are highlighted with red boxes.

### 5.5.4. Administer Virtual Super-Loop

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

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

### 5.5.5. 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.

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

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 5.5.3)
  - **Interface type for route (IFC):** Meridian M1 (SL1)

**AVAYA** CS1000 Element Manager Help | Logout

Managing: 172.16.21.61 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):   
 Customer number (CUST):   
 Route number (ROUT):   
 Designator field for trunk (DES):   
 Trunk type (TKTP):   
 Incoming and outgoing trunk (ICOG):   
 Access code for the trunk route (ACOD):   
 Trunk type M911P (M911P): ☐

The route is for a virtual trunk route (VTRK): ☒  
 - Zone for codec selection and bandwidth management (ZONE):  (0 - 8000)  
 - Node ID of signaling server of this route (NODE):  (0 - 9999)  
 - Protocol ID for the route (PCID):   
 - Print correlation ID in CDR for the route (CRID): ☐

Integrated services digital network option (ISDN): ☒  
 - Mode of operation (MODE):   
 - D channel number (DCH):  (0 - 254)  
 - Interface type for route (IFC):

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

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

**AVAYA** CS1000 Element Manager Help | Logout

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

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

- 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)** box and **Incoming DID digit conversion on this route (IDC)** box, 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
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Software
- Customers
- Routes and Trunks
  - **Routes and Trunks**
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore
  - Date and Time
  - + Logs and reports
- Security
  - + Passwords

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

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

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

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

**- Basic Route Options**

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

Billing number required (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

- Click on **Advance Configurations**; check **Music-on-hold** to enable music on hold on the route. Input music route 1 to the boxes as shown below. The CS1000 system has been pre-configured with route 1 as a music route.

Click on the **Submit** 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

Home local number (HLCN) :

Home national number (HNTN) :

In-band automatic number identification route (IANI) : ☐

Incoming identifier send (ICIS) : ☒

Internal/external definition (IDEF) : Use network info (NET)

Identify originating party (IDOP) : ☐

Insert (INST) :

Manual outgoing trunk route (MANO) : ☐

Manual route (MNL) : ☐

Music on-hold (MUS) : ☒

Music route number (MRT) :  (0 - 511)

Outgoing identifier send (OGIS) : ☒

Off-hook timer delay (OHTD) : ☐

Outpulsing route (OPR) : ☐

Pseudo answer (PANS) : ☒

Periodic clearing signal (PECL) : ☐

Privacy indicator ignored (PII) : ☐

Auxiliary application (AUXP) : ☐

Protocol selection (PSEL) : DM-DM Protocol Selection (DMDM)

Preference trunk usage threshold (PTUT) :  (0 - 510)

Port type at far end (PTYP) : Analog TIE trunks (ATT)

Route traffic information in ACD Reports (RACD) : ☐

Radio paging route (RPA) : ☐

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

### 5.5.6. Administer Virtual Trunks

Continue on **Section 5.5.5** after click **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, Route 0 was being added. Click on the **Add trunk** button next to the newly added route 0 as shown below.

**AVAYA CS1000 Element Manager**

Help | Logout

Managing: 122.16.21.61 Username: admin  
Routes and Trunks > Routes and Trunks

**Routes and Trunks**

Customer	Route	Type	Description	Edit	Add trunk
0	0	TIE	SERVICE PROVIDER	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
0	1	IMUS	MUSIC	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>
0	96	TIE	SIPL_ROUTE	<input type="button" value="Edit"/>	<input type="button" value="Add trunk"/>

The **Customer 00, 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. Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown below.

- The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 11 trunks were created.
- **Trunk data block (TYPE): IP Trunk (IPTI)**
- **Terminal Number (TN):** Available terminal number (created in **Section 5.5.4**)
- **Designator field for trunk (DES):** A descriptive text
- **Extended Trunk (XTRK): Virtual trunk (VTRK)**

- **Member number (RTMB):** Current route number and starting member
- **Start arrangement Incoming (STRI): Immediate (IMM)**
- **Start arrangement Outgoing (STRO): Immediate (IMM)**
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level
- **Channel ID for this trunk (CHID):** An available starting channel ID

**AVAYA CS1000 Element Manager** Help | Logout

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

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

**- Basic Configuration**

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

**+ Advanced Trunk Configurations**

Save Delete Cancel

Click on **Edit** button next to **Class of Service**. For **Media Security**, select **Media Security Never (MSNV)**. For **Restriction Level**, enter **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

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

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

**- Basic Configuration**

**+ Advanced Trunk Configurations**

- Media Security:

- Restriction level:

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

### 5.5.7. Administer Calling Line Identification Entries

Select **Customers** → **00** → **ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is divided into two sections: 'General Properties' and 'Calling Line Identification'. The 'General Properties' section includes fields for 'Flexible trunk to trunk connection option' (set to 'Connections restricted'), 'Flexible orbiting prevention timer' (set to 6), 'Country code' (set to 1), 'National access code' (set to 1), and 'International access code' (set to 011). There are also checkboxes for 'Options' (Transfer on ringing of supervised external trunks, Connection of supervised external trunks) and 'Network option' (Coordinated dialing plan routing). The 'Calling Line Identification' section includes a dropdown for 'Information for incoming/outgoing calls' (set to 'No manipulation is done'), 'Size' (set to 256), and 'Country code' (set to 1). A red box highlights the 'Calling Line Identification Entries' link at the bottom of the 'Calling Line Identification' section.

Click on **Add** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface, specifically the 'Calling Line Identification Entries' section. The top navigation bar shows the path: Managing: 172.16.21.61 Username: admin Customers > Customer 00 > Customer Details > ISDN and ESN Networking > Calling Line Identification Entries. The main content area has a search bar for CLID with 'Start range' and 'End range' fields, and a 'Search' button. Below the search bar, there is a table for 'Calling Line Identification Entries'. At the bottom of the table, there are two buttons: 'Add...' and 'Delete'. The 'Add...' button is highlighted with a red box.

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 318.
- **Local Code**: Input the seven digit number of the DID assigned by the service provider, in this case it is 5551234.
- **Calling Party Name Display**: Uncheck for **Roman characters**.

Repeat for each one 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

### Edit Calling Line Identification 0

#### General Properties

National Code: 318 (0 - 999999)  
Code for national home number

Local Code: 5551234 (1-12 digits)  
Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID: NO

#### 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

Expected Length:

Display Format: First name, Last name

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

### 5.5.8. Enable External Trunk to Trunk Transferring

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 a SIP trunk.

Log in to the Call Server CLI (please refer to **Section 5.1.2** for more detail)

Allow External Trunk to Trunk Transferring for **Customer Data Block** by using LD 15.

```

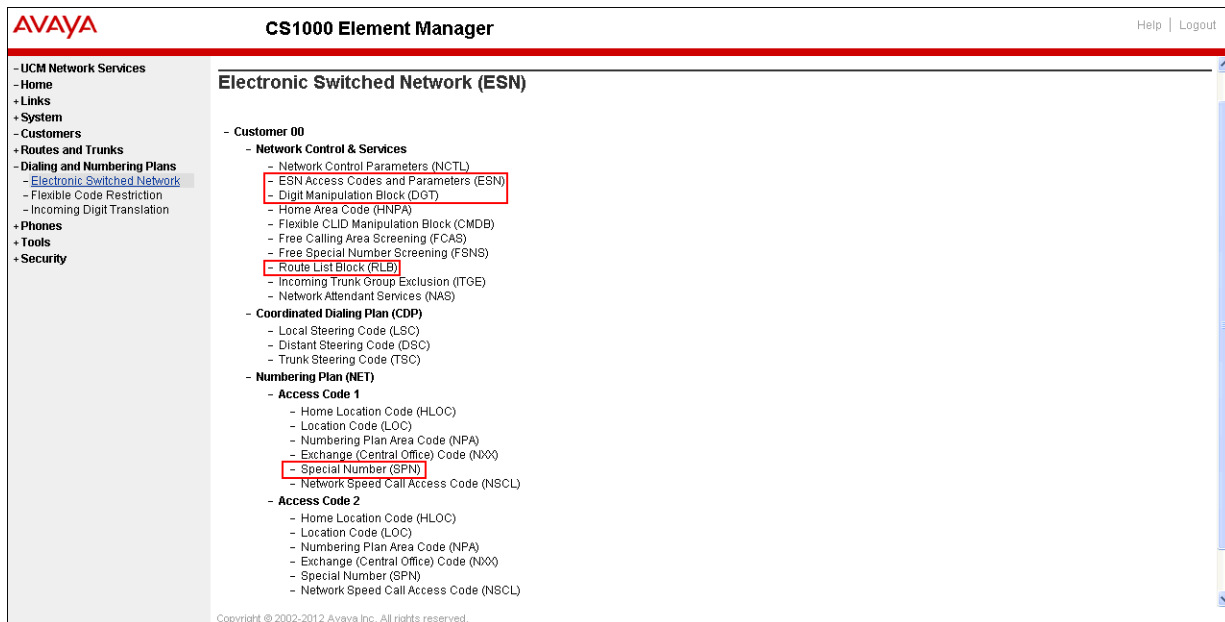
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101   USED U P: 371282 939078   TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....

```

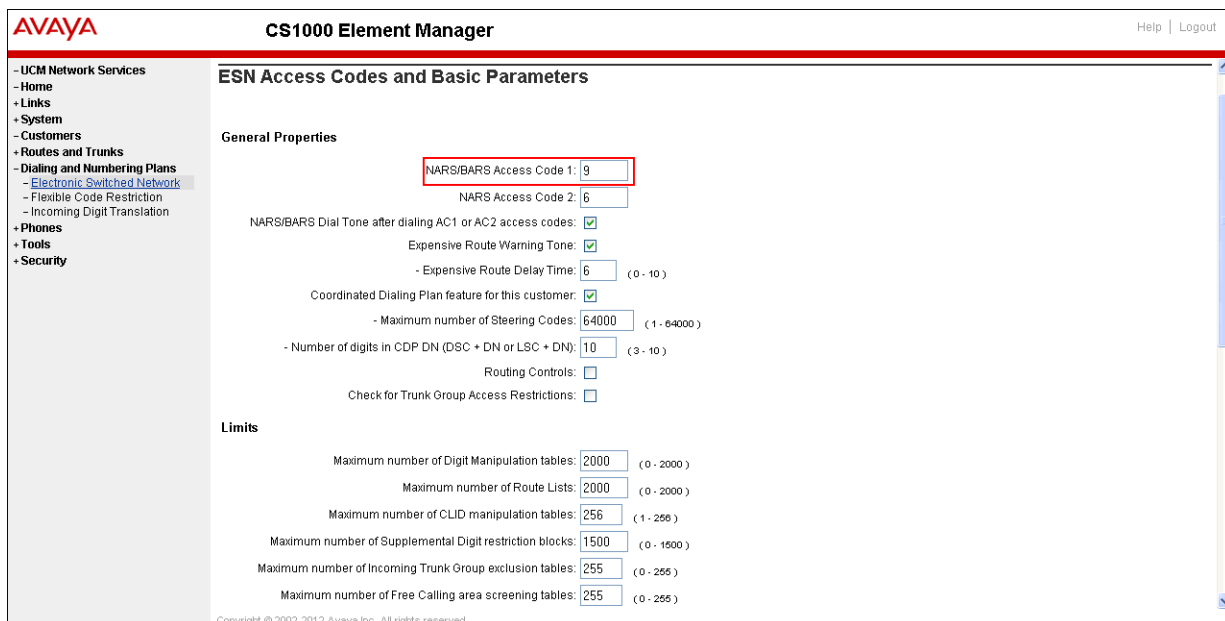
## 5.6. Administer Dialing Plans

### 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).



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

Log in 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. 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 (DMI)

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

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

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

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.

#### 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 index 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.

- **Route Number (ROUT): 0** (created in **Section 5.5.5**)
- **Digit Manipulation Index (DMI): 1** (created in **Section 5.6.3**)

**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

**General Properties**

Entry Number for the Route List:

**Indexes**

Time of Day Schedule:  ▼

Facility Restriction Level:  (0 - 7)

**Digit Manipulation Index: 1** ▼

ISL D-Channel Down Digit Manipulation Index:  (0 - 1000)

Free Calling Area Screening Index:  ▼

Free Special Number Screening Index:  ▼

Business Network Extension Route: ☐

Incoming CLID Table:  (0 - 255)

**Options**

Local Termination entry: ☐

**Route Number: 0** ▼

Skip Conventional Signaling: ☐

Display Originator's Information: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

Strategy on Congestion: No Reroute (NRR) ▼

- QSIG Alternate Routing Causes: QSIG Alternate Routing Cause 1 ▼

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

### 5.6.5. Inbound Call Digit Translation

This section describes the steps for receiving the calls from PSTN via the CenturyLink system. Select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown below.

**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: **172.16.21.61** Username: admin  
Dialing and Numbering Plans > Incoming Digit Translation

**Incoming Digit Translation**

- Customer: **00** Edit IDC

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



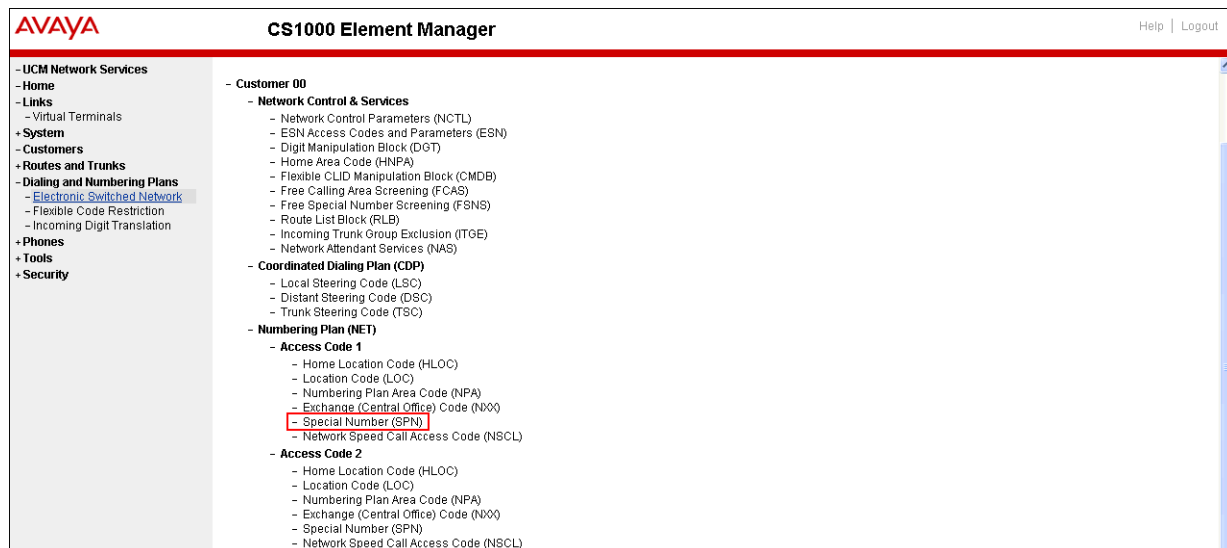
Detail configuration of the **DCNO** is shown below. The **Incoming Digits** can be mapped to the **Converted Digits** which would be the CS1000 system extension number. This **DCNO** has been assigned to route 0 as shown in **Section 5.5.5**.

In the following configuration, the incoming call from PSTN with the prefix 3185551234 will be translated to the CS1000 extension number 8005.

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

There are special numbers which have been configured to be used for this testing such as **0** to reach the 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**, **711** and so on.

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



Enter **SPN** and then click on the “**to Add**” button. Special numbers that were used for the testing are shown below.

#### Special Number: 0

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

#### Special Number: 011

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

#### Special Number: 1

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

#### Special Number: 411

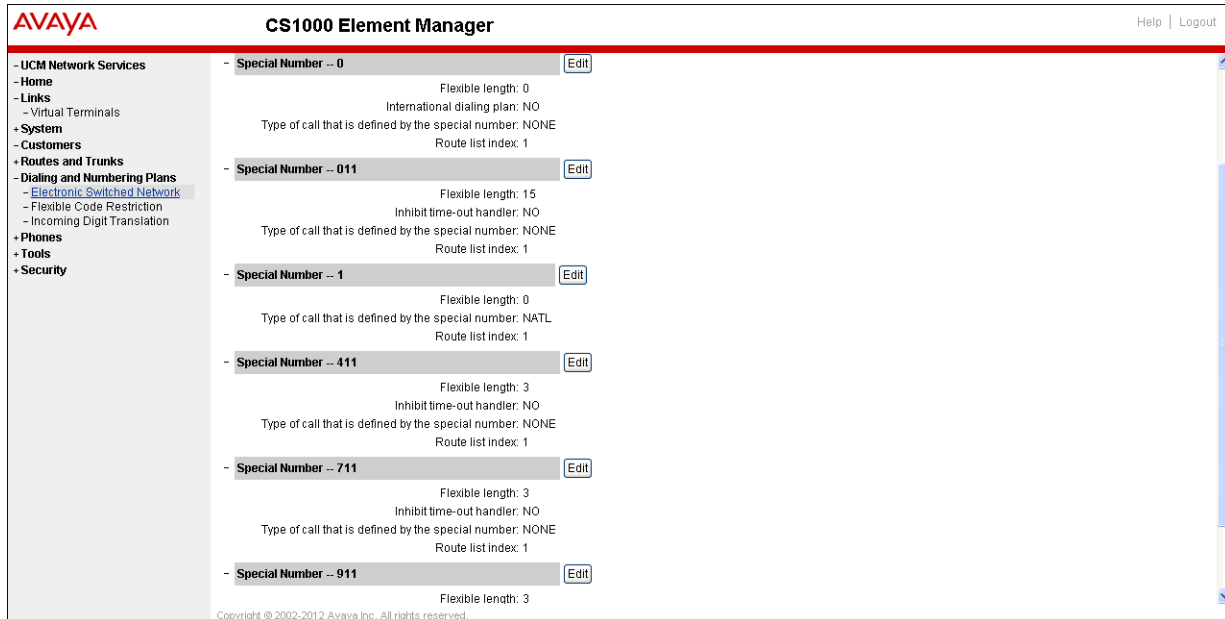
- **Flexible length:** 3
- **CallType:** None
- **Route list index:** 1, created in **Section 5.6.4**

#### Special Number: 711

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

### Special Number: 911

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



### 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 under **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 extensions used during the testing.

### 5.7.1. Phone creation

Refer to **Section 5.5.4** 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.

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

Create an IP phone using **Unified Communications Management (UCM)** or **LD 11**.

```

REQ: prt
TYPE: 1110
TN
CUST
TEN
DATE
PAGE
DES
MODEL_NAME
EMULATED
DES 8001
TN 008 0 00 01 VIRTUAL
TYPE 1110
CDEN 80
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00005
CUR_ZONE 00005
MRT
ERL 0
ECL 0
FDN
TGAR 0
LDN NO
NCOS 5
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW
SFLT NO
CAC_CIS 0
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRGL
POD SLKD CCSD SWD LND CNDA
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
ICDA CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHA FICD NAID DNAA BUZZ
UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
MSNV FRA PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
RCO 0
EFD
HUNT
EHT
LHK 0
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 8001 1 MARP
CPND
CPND_LANG ROMAN
NAME Avaya, 1110_Un1
XPLN 14
DISPLAY_FMT FIRST, LAST
ANIE 0
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16 Mwk 8056
17 TRN
18 AO6
19 CFW 12
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27

```

### 5.7.2. Enable Privacy for Phone

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

To hide display name, set CLS to **namd**. 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**. 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**. 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 ☐
```

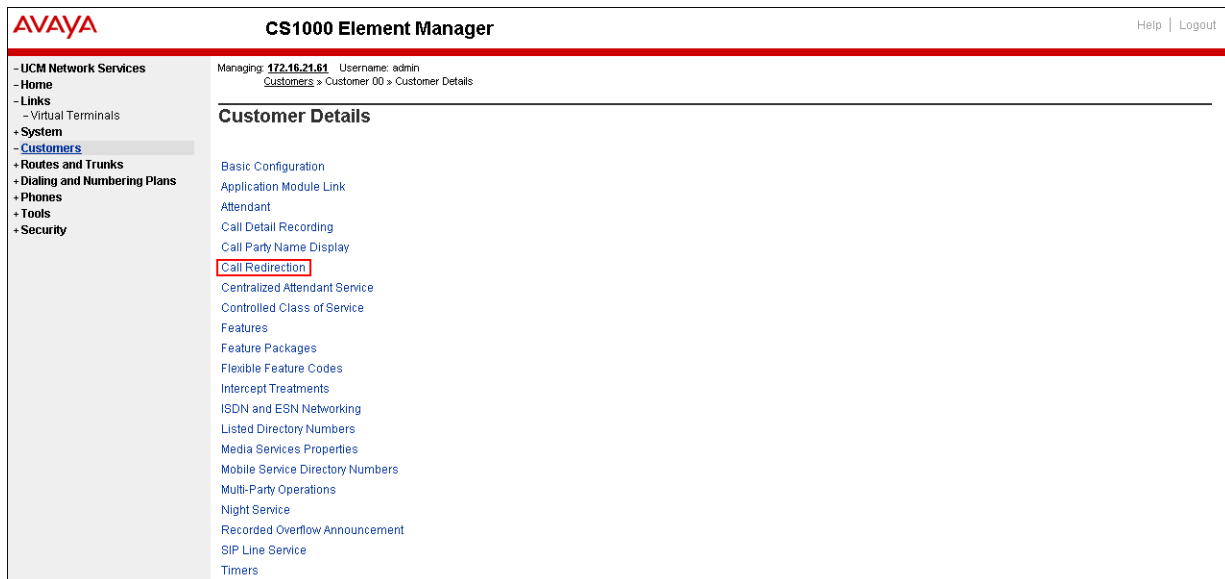
To allow display name and number, set CLS to **nama, ddga**. CS1000 will send header “Privacy:none” to Service Provider.

```
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 **Customer** → **00** → **Call Redirection**. 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

UCM Network Services

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

Redirection Holidays

Do not disturb hunting: ☐

Total redirection count limit: 0

Options:

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

Call forward: ☒ Originating ☐ Forwarding

Number of normal ringing cycles for CFNA

Option 0: 4

Option 1: 4

Option 2: 4

Number of distinctive ringing cycles for CFNA

Option 0: 4

Option 1: 4

Option 2: 4

Calls routed to message center

No answer DID calls: ☐

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

```
REQ: prt
TYPE: 2050pc
TN 8003
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRD
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSO NOVQ VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCB
.....
19 CFW 12 919195551212
```

Enable **Call Forward Busy (CFB)** for the phone over the SIP trunk by using **LD 11**, change its CLS to **FBA**, **HTA** 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 HTA TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC 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
.....

```

Enable **Call Forward No Answer (CFNA)** for the phone over SIP trunk by using **LD 11**, change its 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 TDD 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 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
.....

```

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

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

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



REQ: prt  
TYPE: 2050pc  
TN 8003

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

....  
**02 CWT**  
....

## 6. Configure the Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to the Avaya CS1000, the Avaya SBCE and Avaya Aura® Session Manager itself.
- Entity Links, which define the SIP trunk parameters used by Avaya Aura® Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Regular Expressions, which also can be used to route calls
- Avaya Aura® Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager.

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

### 6.1. System Manager Login and Navigation

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

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Home

Users

Administrators

Manage Administrative Users

Groups & Roles

Manage groups, roles and assign roles to users

Subscribers

Manage users and shared resources associated with CS1000, including LDAP/file import and export

Synchronize and Import

Synchronize users with the enterprise directory, import users from file

UCM Roles

Manage UCM Roles, assign roles to users

User Management

Manage users, shared user resources and provision users

Elements

Application Management

Manage applications and application certificates

Communication Manager

Manage Communication Manager objects

Conferencing

Conferencing

Inventory

Manage, discover, and navigate to elements, update element software

Messaging

Manage Messaging System objects

Presence

Presence

Routing

Network Routing Policy

Session Manager

Session Manager Element Manager

SIP AS 8.1

SIP AS 8.1

Services

Backup and Restore

Backup and restore System Manager database

Configurations

Manage system wide configurations

Events

Manage alarms, view and harvest logs

Licenses

View and configure licenses

Replication

Track data replication nodes, repair replication nodes

Scheduler

Schedule, track, cancel, update and delete jobs

Security

Manage Security Certificates

Templates

Manage Templates for Communication Manager and Messaging System objects

UCM Services

Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

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

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing x Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home /Elements / Routing

Introduction to Network Routing Policy

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

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

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

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

HG; Reviewed:  
SPOC 6/21/2012

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

51 of 110  
CTLCS1KSMSBCE

## 6.2. Specify SIP Domains

Create a SIP domain for each domain for which Avaya Aura® Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain:

**avaya.lab.com** and the domain for CenturyLink: **bsoft.nc.labnet**.

The domain for CenturyLink (bsoft.nc.labnet) may change during installations.

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

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

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

The screenshot shows the Avaya Aura® System Manager 6.1 web interface. The top header includes the Avaya logo, the product name, and user information. The left navigation pane shows a tree structure with 'Routing' expanded and 'Domains' selected. The main content area is titled 'Domain Management' and contains a table with one entry. The entry has a red asterisk next to the name 'bsoft.nc.labnet', a type of 'sip', and a note of 'CenturyLink'. There are 'Commit' and 'Cancel' buttons at the bottom right of the table area.

Name	Type	Default	Notes
* bsoft.nc.labnet	sip	<input type="checkbox"/>	CenturyLink

## 6.3. Add Location

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

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

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

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

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

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

**AVAYA** Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

**Routing** Home

**Home /Elements / Routing / Locations- Location Details**

**Location Details** Commit Cancel Help ?

**General**

\* Name:

Notes:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

**Per-Call Bandwidth Parameters**

Maximum Multimedia Bandwidth (Intra-Location):  Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):  Kbit/Sec

Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

**Location Pattern**

2 Items  Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 172.16.20.*	<input type="text"/>
<input type="checkbox"/>	* 172.16.5.*	<input type="text"/>

Select : All, None

\* Input Required Commit Cancel

## 6.4. Add Adaptation Module

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

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed. The following screen shows a portion of the list of adaptations in the sample configuration.

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing | Home

Home /Elements / Routing / Adaptations- Adaptations

Adaptations

Edit New Duplicate Delete More Actions

5 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	AAC	DigitConversionAdapter		Adaptation For Avaya Aura Conferencing
<input type="checkbox"/>	Acme Out/In	DigitConversionAdapter odstd=avayalab2.com losrcd=sil.miami.avaya.com		
<input type="checkbox"/>	CS1K75	CS1000Adapter		Adaptation for outgoing calls to CS1000
<input type="checkbox"/>	Diversion_History	DiversionTypeAdapter MIME=no		Adaptation for calls to CenturyLink
<input type="checkbox"/>	Outbound to AT&T	DigitConversionAdapter odstd=aslab.centrixvoip.net osrcd=aslab.centrixvoip.net		

Select : All, None

Settings for CS1K75 Adaptation:

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

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

Click **Commit** to save.

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing | Home

Home /Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

Commit Cancel

General

\* Adaptation name: CS1K75

Module name: CS1000Adapter

Module parameter:

Egress URI Parameters:

Notes: Adaptation for outgoing calls to C

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

Add Remove

0 Items Refresh Filter: Enable

Settings for **Diversion\_History** Adaptation:

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

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

- **Module Name:** Enter **DiversionTypeAdapter**.
- **Module parameter:** Enter **MIME=no**.

Click **Commit** to save.

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

## 6.5. Add SIP Entities

A SIP Entity must be added for Avaya Aura® Session Manager and for each SIP telephony system connected to it which includes Avaya CS1000 and the Avaya SBCE. Navigate to **Routing** → **SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for Avaya CS1000 and the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** defined previously.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

To define the ports used by Avaya Aura® Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

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

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

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

For the compliance test, only two Ports were used:

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

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.

**AVAYA** Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

**Routing** Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

**SIP Entity Details** Help ?

**General** Commit Cancel

\* Name: HG Session Manager

\* FQDN or IP Address: 172.16.5.32

Type: Session Manager

Notes: HG Session Manager

Location: HG Lab

Outbound Proxy:

Time Zone: America/New\_York

Credential name:

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

**Port** Add Remove

8 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avaya.lab.com	
<input type="checkbox"/>	5060	TCP	avaya.lab.com	
<input type="checkbox"/>	5061	TLS	avaya.lab.com	
<input type="checkbox"/>	5062	TCP	avaya.lab.com	
<input type="checkbox"/>	5070	TCP	avaya.lab.com	
<input type="checkbox"/>	5080	TCP	avaya.lab.com	
<input type="checkbox"/>	5085	UDP	avaya.lab.com	
<input type="checkbox"/>	5086	TCP	avaya.lab.com	

Select : All, None

\* Input Required Commit Cancel



The following screen shows the addition of the Avaya CS1000 SIP entity.

A separate SIP entity for the Avaya CS1000, other than the one created for Avaya Aura® Session Manager during installation, is required in order to send SIP service provider traffic.

For the compliance test the following values were used:

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

The screenshot displays the Avaya Aura® System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura® System Manager 6.1", and links for "Help | About | Change Password | Log off admin". A breadcrumb trail shows the path: "Home /Elements / Routing / SIP Entities- SIP Entity Details". The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "SIP Entity Details" and has a "General" tab selected. It contains several form fields: "Name" (CS1K7.5), "FQDN or IP Address" (172.16.20.60), "Type" (Other), "Notes" (CS1000 Rel. 7.5), "Adaptation" (CS1K75), "Location" (HG Lab), and "Time Zone" (America/New\_York). There is an unchecked checkbox for "Override Port & Transport with DNS SRV". Below these are fields for "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), and "Call Detail Recording" (none). A section titled "SIP Link Monitoring" includes a dropdown for "SIP Link Monitoring" (Link Monitoring Disabled), and three fields for monitoring intervals: "Proactive Monitoring Interval (in seconds)" (900), "Reactive Monitoring Interval (in seconds)" (120), and "Number of Retries" (1). "Commit" and "Cancel" buttons are located at the top right of the form area.

The following screen shows the addition of the Avaya SBCE SIP entity.

For the compliance test the following values were used:

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

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields and values:

- Name:** HG ASBCE
- FQDN or IP Address:** 172.16.5.71
- Type:** Other (dropdown)
- Notes:** HG ASBCE
- Adaptation:** Diversion\_History (dropdown)
- Location:** HG Lab (dropdown)
- Time Zone:** America/New\_York (dropdown)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown)
- SIP Link Monitoring:** Link Monitoring Disabled (dropdown)
- Proactive Monitoring Interval (in seconds):** 900
- Reactive Monitoring Interval (in seconds):** 120
- Number of Retries:** 1

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

## 6.6. Add Entity Links

A SIP trunk between Avaya Aura® Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the Avaya CS1000 and one to the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Avaya Aura® Session Manager.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol defined under **SIP Entities** in **Section 6.5**
- **Port:** Port number on which Session Manager will receive SIP requests. This must match the port defined under **SIP Entities** in **Section 6.5**

- **SIP Entity 2:** Select the name of the other system. For the Avaya CS1000 and Avaya SBCE, select the CS1000 or the Avaya SBCE SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the far-end is listening on. For the Avaya CS1000 this must match the port defined under **SIP Gateway Settings** tab, under **Proxy or Redirect Server** in **Section 5.5.2**. For the Avaya SBCE this must match the port defined under Server Configuration in **Section 7.3.3**
- **Connection Policy:** Select **Trusted** from the pull-down menu (not shown).

Click **Commit** to save.

It should be noted that in a customer environment the Entity Links to the Avaya CS1000 and to the Avaya SBCE may be configured with a protocol other than the ones shown on the sample configuration. For the compliance test, TCP was used to the Avaya SBCE and UDP was used to the CS1000 to aid in troubleshooting. The protocol and ports defined here must match the values used on the Avaya CS1000 and the Avaya SBCE.

The following screens illustrate the Entity Link between Avaya Aura® Session Manager and the Avaya CS1000.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Entity Links- Entity Links

Entity Links

Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* HG SM to CS1K75	* HG Session Manager	UDP	* 5085	* CS1K7.5	* 5085	Trusted	

\* Input Required

Commit Cancel

The following screens illustrate the Entity Link between Avaya Aura® Session Manager and the Avaya SBCE.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* HG SM to HG ASBCE	* HG Session Manager	TCP	* 5060	* HG ASBCE	* 5060	Trusted	

\* Input Required

Commit Cancel

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Entity Links

Edit New Duplicate Delete More Actions

15 Items | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
AAC	HG Session Manager	TCP	5060	AAC	5060	Trusted	AAC Entity Link
HG-SM to ACME	HG Session Manager	TCP	5060	HG-ACME	5060	Trusted	HG-ACME Entity Link
HG SM to CS1K75	HG Session Manager	UDP	5085	CS1K7.5	5085	Trusted	
HG SM to HG AA-SBC	HG Session Manager	TCP	5060	HG AA-SBC	5060	Trusted	
HG SM to HG ASBCE	HG Session Manager	TCP	5060	HG ASBCE	5060	Trusted	
HG SM to HG CM Trunk 1	HG Session Manager	TCP	5080	HG CM Trunk 1	5080	Trusted	
HG SM to HG CM Trunk 2	HG Session Manager	TCP	5070	HG CM Trunk 2	5070	Trusted	
SM to AA-Messaging	MA_Session Manager	TCP	5060	AA-Messaging	5060	Trusted	
SM to AA-SBC	MA_Session Manager	TCP	5060	MA_AA-SBC	5060	Trusted	
SM to Acme s1p0	MA_Session Manager	TCP	5060	Acme Packet s1p0	5060	Trusted	
SM to Acme s1p1	HG Session Manager	TCP	5060	Acme Packet s1p1	5060	Trusted	
SM to ASBCE	MA_Session Manager	TCP	5060	ASBCE	5060	Trusted	
SM to CM trunk 1	MA_Session Manager	TCP	5060	C.M. Trunk 1	5060	Trusted	
S.M. to CM Trunk10	MA_Session Manager	TCP	5080	C.M.Trunk 10	5080	Trusted	
SM to CM Trunk 2	MA_Session Manager	TCP	5070	C.M. Trunk 2 AT&T PR	5070	Trusted	

Select : All, None

## 6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for the Avaya CS1000 and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the

left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

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

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

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

The following screen show the Routing Policy for the Avaya CS1000.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing'. The main content area is titled 'Routing Policy Details' and shows the 'General' tab. The 'Name' field is set to 'To CS1K75', 'Disabled' is unchecked, and 'Notes' is 'Inbound Calls to CS1K75'. Below this is the 'SIP Entity as Destination' section with a 'Select' button. A table at the bottom lists the selected SIP entity:

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

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

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is expanded to 'Routing'. The main content area is titled 'Routing Policy Details' and shows the 'General' tab. The 'Name' field is set to 'HG ASBCE', 'Disabled' is unchecked, and 'Notes' is 'Outbound calls via ASBCE'. Below this is the 'SIP Entity as Destination' section with a 'Select' button. A table at the bottom lists the selected SIP entity:

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

## 6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Avaya Aura® Session Manager. For the compliance test, dial patterns were needed to route calls from Avaya CS1000 to CenturyLink and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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

Examples of the dial patterns used for the compliance testing are shown below. The first example shows dial pattern “0” for calls to the Operator, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab**, uses **Routing Policy Name** of **HG ASBCE**.

**AVAYA** Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing × Home

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details Help ?  
Commit Cancel

General

\* Pattern: 0

\* Min: 1

\* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items Refresh Filter: Enable

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

Select : All, None

The next example shown below is for dial pattern “1” for the North American Numbering Plan area prefix, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab**, uses **Routing Policy Name** of **HG ASBCE**.

**AVAYA** Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing × Home

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details Help ?  
Commit Cancel

General

\* Pattern: 1

\* Min: 11

\* Max: 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To AT&T PR	0	<input type="checkbox"/>	MA_AA-SBC	
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K.)	HG-ACME	0	<input type="checkbox"/>	HG-ACME	
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K.)	HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE

Select : All, None

The next example shown below is for dial pattern “318360” to route inbound calls to DID numbers provided by CenturyLink (DID numbers assigned to extensions in the CS1000), have a

destination domain of **ALL**, **Originating Location Name** of **HG Lab**, uses **Routing Policy Name** of **To CS1K75**.

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

General

\* Pattern: 318360

\* Min: 6

\* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Inbound Calls From CenturyLink to CS1K

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K,)	To CS1K75	0	<input type="checkbox"/>	CS1K7.5	Inbound Calls to CS1K75

Select : All, None

The next example shown below is for dial pattern “**411**” for calls to Directory Assistance, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab**, uses **Routing Policy Name** of **HG ASBCE**.

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

General

\* Pattern: 411

\* Min: 3

\* Max: 3

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K,)	HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K,)	HG-ACME	0	<input type="checkbox"/>	HG-ACME	
<input type="checkbox"/>	SIL Lab		To AT&T PR	0	<input type="checkbox"/>	MA_AA-SBC	

Select : All, None



The next example shown below is for dial pattern “711” for calls for Telecommunications Relay Service, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab**, uses **Routing Policy Name** of **HG ASBCE**.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

General

\* Pattern: 711

\* Min: 3

\* Max: 3

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

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

Select : All, None

The next example shown below is for dial pattern “911” for emergency calls, have a destination domain of **ALL** (since it’s shared among other test activities in the lab), **Originating Location Name** of **HG Lab**, uses **Routing Policy Name** of **HG ASBCE**.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home /Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details

General

\* Pattern: 911

\* Min: 3

\* Max: 3

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	HG Lab	Simulated Enterprise Customer (CM, SM, CS1K,)	HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE
<input type="checkbox"/>	STL Lab		To AT&T PR	0	<input type="checkbox"/>	MA_AA-SBC	

Select : All, None

## 6.9. Add/View Avaya Aura® Session Manager

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

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

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

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

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

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



- ▼ Session Manager
  - Dashboard
  - Session Manager
  - Administration
  - Communication Profile Editor
  - ▶ Network Configuration
  - ▶ Device and Location Configuration
  - ▶ Application Configuration
  - ▶ System Status
  - ▶ System Tools

[Home](#) / [Elements](#) / [Session Manager](#) / [Session Manager Administration- Session Manager Administration](#)[Help ?](#)

## View Session Manager

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

### General ▼

**SIP Entity Name** **Description** **Management Access Point Host Name/IP** **Direct Routing to Endpoints** 

### Security Module ▼

**SIP Entity IP Address** **Network Mask** **Default Gateway** **Call Control PHB** **QOS Priority** **Speed & Duplex** **VLAN ID**

## 7. Configure the Avaya Session Border Controller for Enterprise.

This section describes the required configuration of the Avaya SBCE to connect to CenturyLink BroadWorks SIP Trunk service. This configuration is done in two stages. The first part or initial configuration is done via the Provisioning Script, which requires a serial connection between a terminal device and the Console port of the Avaya SBCE.

Once the Avaya SBCE is provisioned and ready to be used on the IP network, the remainder of the configuration is accomplished using the Avaya SBCE web interface.

It is assumed in these Application Notes that the Avaya SBCE contains no previous configuration, and it is being provisioned for the first time.

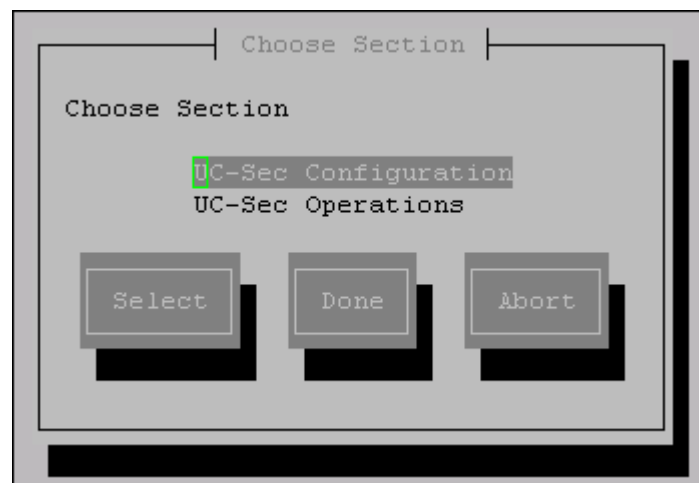
### 7.1. Provisioning Script

Use the following procedure to establish the initial serial connection to the Avaya SBCE:

- Connect a DB9 serial communications cable from a PC or terminal device to the Console port in the back of the Avaya SBCE.
- Configure the communications parameters of the terminal program in the PC, like HyperTerminal or Putty, to the following settings: **Baud rate: 19200, Data Bits: 8, Stop Bits: 1, Parity: None**
- Apply power to the chassis.

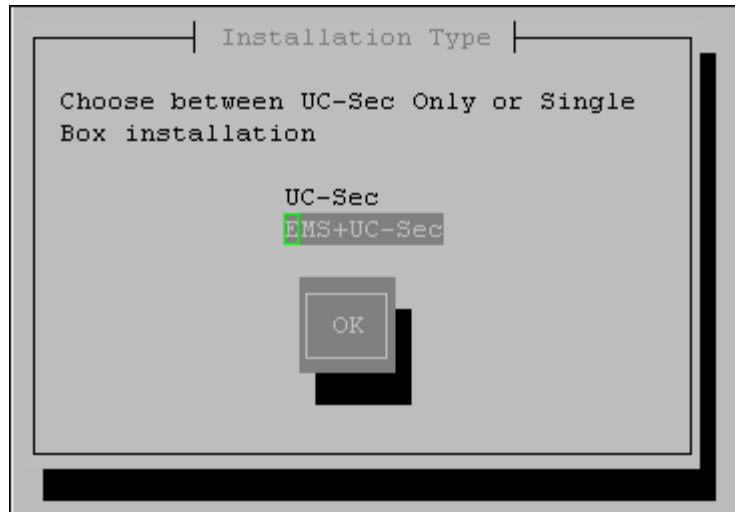
Once power has been applied to the Avaya SBCE, a series of scripts run automatically preparing the chassis to be configured. The provisioning process is ready to be completed when the prompt **Press ENTER to continue...** is displayed. Press the **ENTER** key.

The Top Level Provisioning Screen is displayed. Use the arrows to select **UC-Sec Configuration** and press **ENTER**.

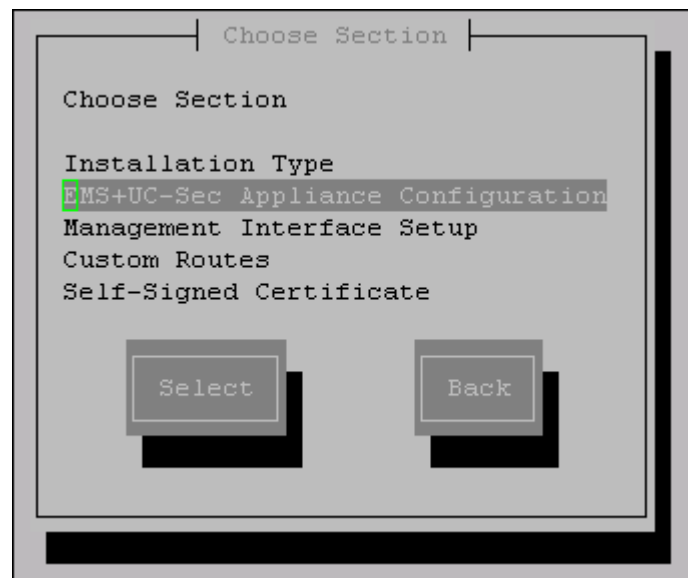


The Provisioning screen is displayed (not shown). **Select Installation Type.** Press **Select**.

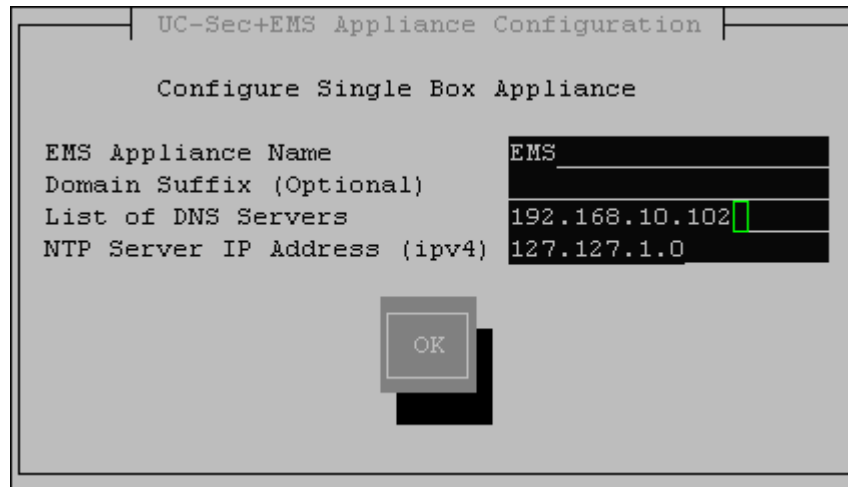
In our test scenario, both the SBC (UC-Sec) and the Element Management System (EMS) reside in the same server. Select **EMS+UC-Sec** for a single box installation. Click **OK**.



On the next screen, the EMS+UC-Sec Provisioning screen, select **EMS+UC- SEC Appliance Configuration**. Press **Select**.



Enter the required information into the appropriate fields. Click **OK**.



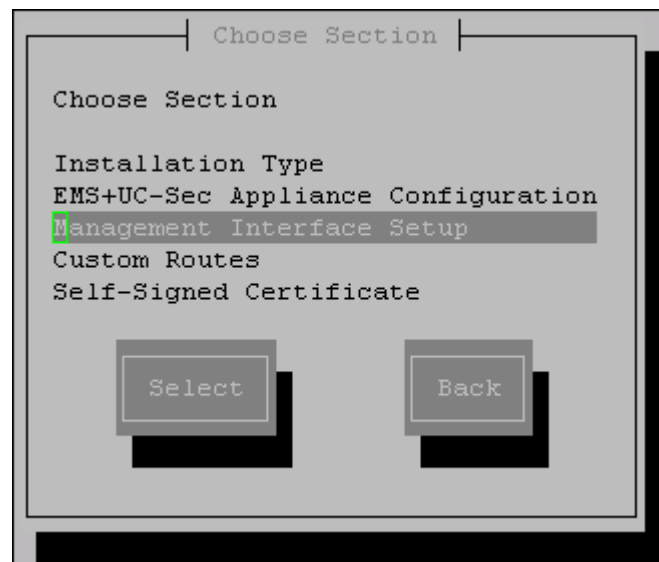
UC-Sec+EMS Appliance Configuration

Configure Single Box Appliance

EMS Appliance Name	EMS
Domain Suffix (Optional)	
List of DNS Servers	192.168.10.102
NTP Server IP Address (ipv4)	127.127.1.0

OK

In the same EMS+UC-Sec Provisioning screen previously shown (shown below), select **Management Interface Setup** and press **Select**.



Choose Section

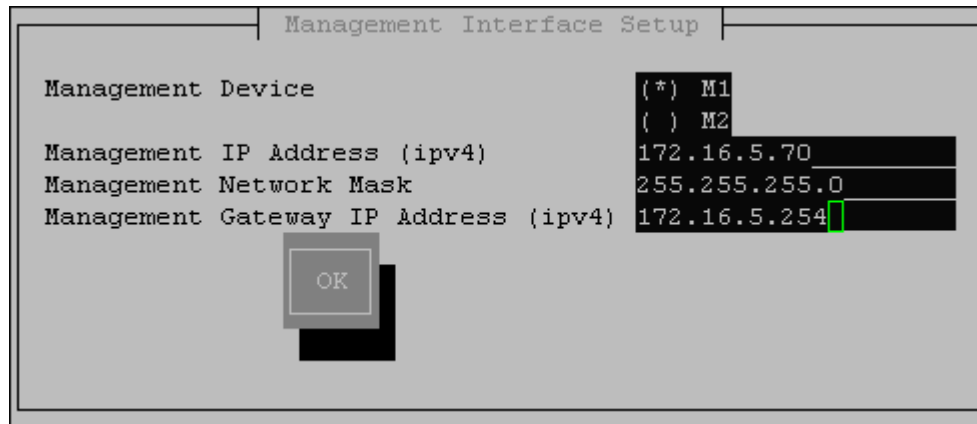
Choose Section

Installation Type

- EMS+UC-Sec Appliance Configuration
- Management Interface Setup**
- Custom Routes
- Self-Signed Certificate

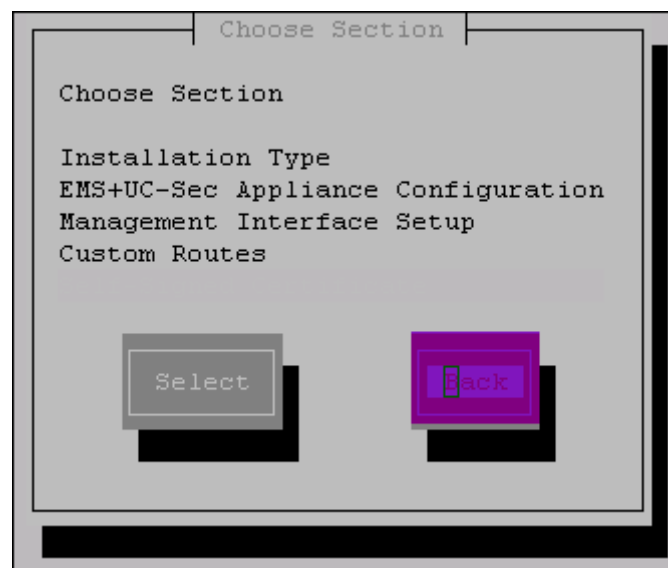
Select Back

Select the **M1 Management Device**, and enter the IP address, Netmask and Gateway to be used to manage the Avaya SBCE on the network. Click **OK**.



The screenshot shows a terminal window titled "Management Interface Setup". It contains four input fields: "Management Device" with a dropdown menu showing "(\*) M1" and "( ) M2"; "Management IP Address (ipv4)" with the value "172.16.5.70"; "Management Network Mask" with the value "255.255.255.0"; and "Management Gateway IP Address (ipv4)" with the value "172.16.5.254". A green cursor is visible at the end of the gateway address. Below the fields is an "OK" button.

Press **Back** at EMS+UC-Sec Provisioning screen. This will bring up the Top Level Provisioning screen. Select **Done**.



The screenshot shows a terminal window titled "Choose Section". It lists four options: "Installation Type", "EMS+UC-Sec Appliance Configuration", "Management Interface Setup", and "Custom Routes". At the bottom, there are two buttons: "Select" and "Back". The "Back" button is highlighted with a red box.

At this point the initial configuration is complete and the Avaya SBCE is ready to be administered via the browser through the Management Interface.

## 7.2. Install Device

Log on to the Avaya SBCE web interface by pointing a browser to the previously configured management interface address. For the Compliance Test, this was **https://172.16.5.70**. Click the **UC-Sec Control Center** box. Log in using the proper credentials (the GUI default password for the account "ucsec" is "ucsec"). Once in the UC-Sec Control Center home page, on the left hand side navigation panel select **System Management**. Select the **Installed** tab.

After the Avaya SBCE has been initially installed and connected to the network, it will show the status of **Registered**. In addition, the **Install Device** icon, (right arrow on the screen capture shown below), is displayed only for the devices which have not yet been configured.

The screenshot shows the UC-Sec Control Center web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar lists various system management options, with 'System Management' currently selected. The main content area displays a table of installed devices. The table has columns for Device Name, Serial Number, Version, and Status. A single device is listed with the name 'SS\_172\_16\_5\_70', serial number 'IPCS31020132', and version '4.0.5.Q02'. Its status is 'Registered'. To the right of the status text are several icons: a power button, a refresh icon, a red stop icon, a blue right-pointing arrow (labeled 'Install Device'), and a red X icon. A red arrow points to the 'Install Device' icon.

Device Name	Serial Number	Version	Status
SS_172_16_5_70	IPCS31020132	4.0.5.Q02	Registered

Click the **Install Device** icon (right arrow on the screen capture shown above).



On the Installation Wizard that follows, fill in the required information for the **Appliance Name**, DNS servers and the Private (A1) and Public (B1) interfaces of the Avaya SBCE as shown. Click **Finish** when done.

For the Public (B1) interface, enter the public IP address (outside address), **Netmask** and **Gateway**.

**Installation Wizard**

**SIP Proxy**

**Device Settings**

Appliance Name:

High Availability (HA): ☐

Secure Channel Type: ☒ None ☐ DMZ ☐ Core

**DNS Configuration**

Primary:  Ex: 202.201.192.1

Secondary:  Optional, Ex: 202.201.192.1

**Network Settings**

At least one address is required. Netmask and subnet must be common across the same interface.

	IP	Public IP	Netmask	Gateway	Interface	DNS Client
Address #1	<input type="text" value="172.16.5.71"/>	<input type="text" value="172.16.5.71"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="172.16.5.254"/>	<input type="text" value="A1"/>	<input checked="" type="radio"/>
Address #2	<input type="text" value="111.111.111.187"/>	<input type="text" value="111.111.111.187"/>	<input type="text" value="255.255.255.192"/>	<input type="text" value="111.111.111.129"/>	<input type="text" value="B1"/>	<input type="radio"/>
Address #3	<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text" value="A1"/>	<input type="radio"/>
Address #4	<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text" value="A1"/>	<input type="radio"/>
Address #5	<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="text"/>	<input type="text" value="A1"/>	<input type="radio"/>

**Finish**

The last screen in the Wizard is a basic reminder of topics that need to be visited in order to complete the configuration. It can be closed at this point.

**Installation Wizard**

Installation is now complete, please configure the following items in order to get your UC-Sec up and running. Clicking on any of the links below will take you to the corresponding configuration page for that item.

- [Server Configuration](#)
- [Media Interface](#)
- [Signaling Interface](#)
- [SIP Cluster](#)
- [End Point Flows](#)

## 7.3. Global Profiles

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

### 7.3.1. Server Interworking

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

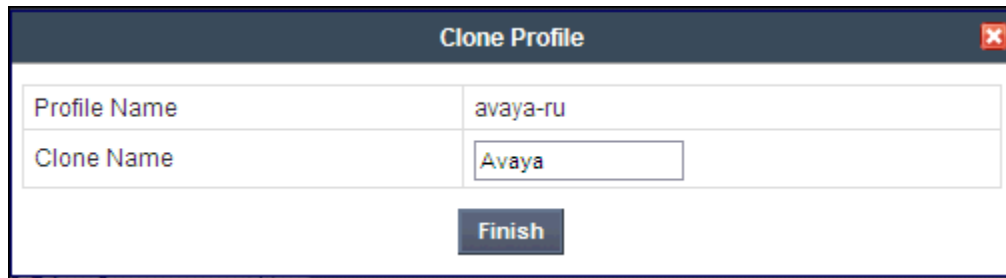
Several profiles have been already pre-defined and they populate the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since modifying a default profile is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

On the left navigation pane, select **Global Profiles → Server Interworking**. From the **Interworking Profiles** list, select **avaya-ru**. Click **Clone Profile**.

The screenshot displays the UC-Sec Control Center web interface. The left navigation pane shows the hierarchy: UC-Sec Control Center > Global Profiles > Server Interworking. The main content area is titled 'Global Profiles > Server Interworking: avaya-ru'. It features a list of 'Interworking Profiles' including cs2100, avaya-ru (selected), OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, and Avaya. A 'Clone Profile' button is visible. Below the list, a warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' The 'Advanced' tab is selected, showing a table of 'Advanced Settings'.

Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
SLIC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No

Enter the new profile name in the **Clone Name** field. Click **Finish**.



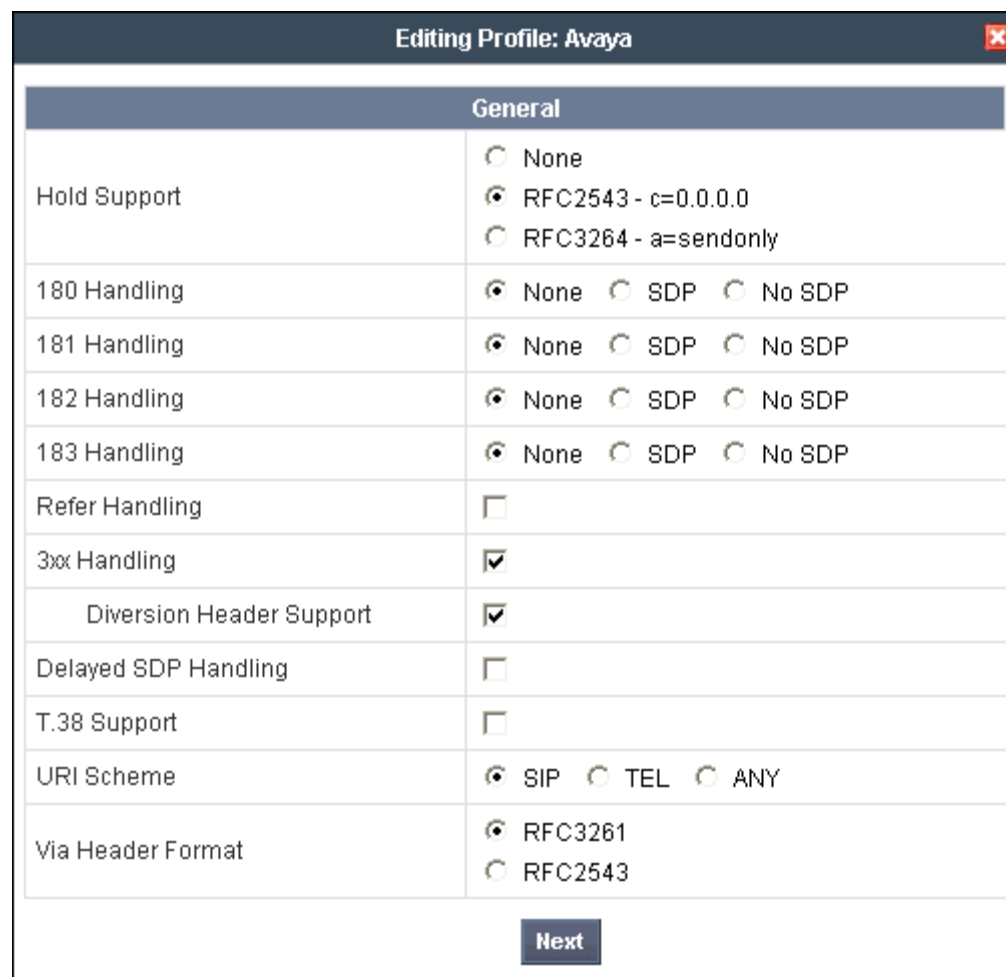
The 'Clone Profile' dialog box has a title bar with a close button. It contains two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Avaya'. Below these fields is a 'Finish' button.

Profile Name	avaya-ru
Clone Name	Avaya

Finish

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

- Verify that for **Hold Support**, **RFC2543** is selected.
- Verify that **3xx Handling** and **Diversion Header Support** are selected.
- Leave other fields with their default values.
- Click **Next**.



The 'Editing Profile: Avaya' dialog box has a title bar with a close button. It contains a 'General' tab with various settings. The settings are as follows:

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

Next

Click **Finish** on the **Privacy and DTMF** tab.

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

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

**Back** **Finish**

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 11:25:19 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Server Interworking: Avaya

**Interworking Profiles**

- cs2100
- avaya-ru
- OCS-Edge-Server
- cisco-ccm
- cups
- Sipera-Halo
- OCS-FrontEnd-Server
- Avaya**

**General** Timers URI Manipulation Header Manipulation Advanced

Click here to add a description.

3xx Handling	Yes
Diversion Header Support	Yes
Delayed SDP Handling	No
T.38 Support	No
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

**Edit**

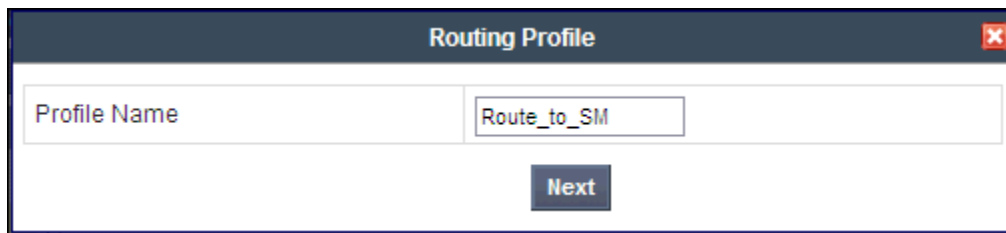
### 7.3.2. Routing Profiles

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

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

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

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

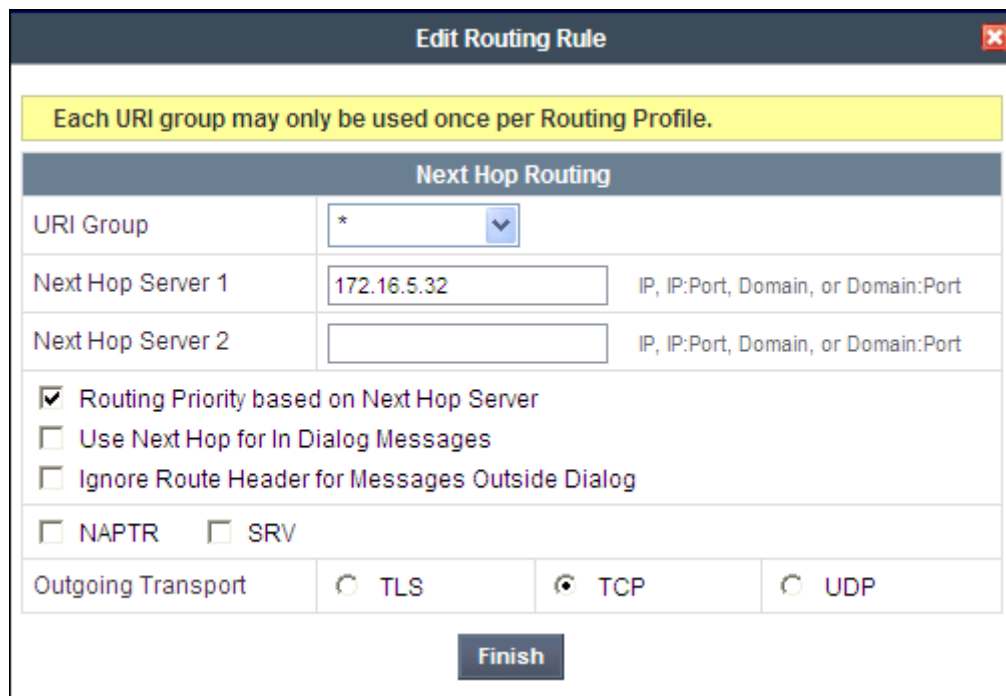


The screenshot shows a 'Routing Profile' configuration window. It has a title bar with a close button. Inside, there is a 'Profile Name' label followed by a text input field containing 'Route\_to\_SM'. Below the input field is a 'Next' button.

On the next screen, complete the following:

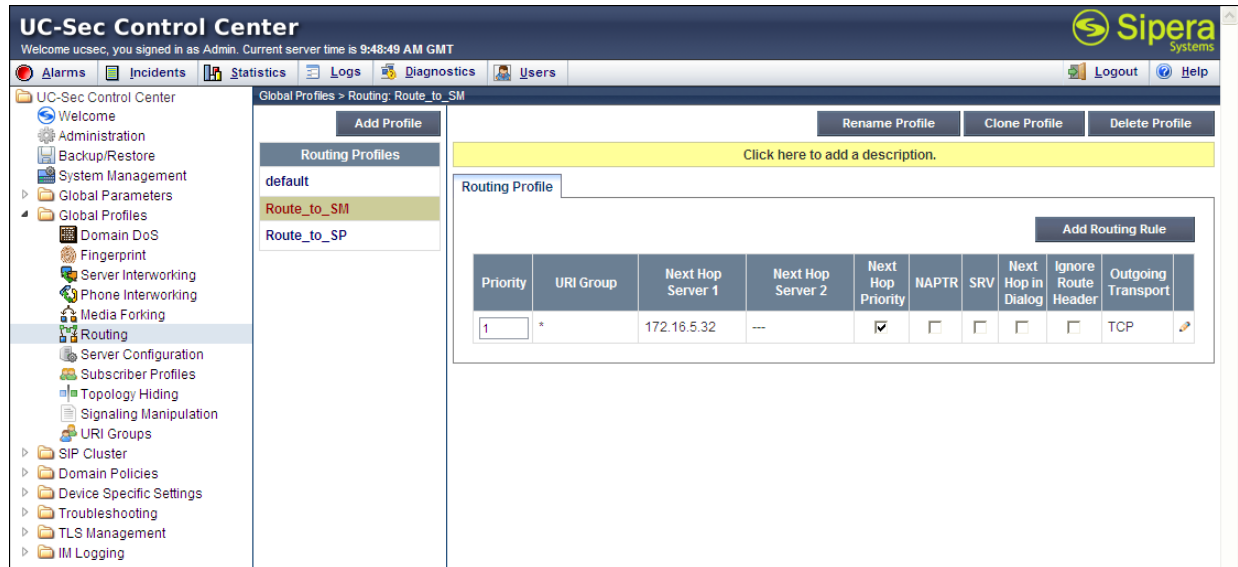
- **Next Hop Server 1: 172.16.5.32** (Session Manager IP address)
- Check **Routing Priority Based on Next Hop Server**
- **Outgoing Transport: TCP**

Click **Finish**.



The screenshot shows an 'Edit Routing Rule' configuration window. It has a title bar with a close button. Below the title bar is a yellow warning banner that reads 'Each URI group may only be used once per Routing Profile.' Below this is a section titled 'Next Hop Routing'. It contains a table with three rows: 'URI Group' with a dropdown menu showing '\*', 'Next Hop Server 1' with a text input field containing '172.16.5.32' and a label 'IP, IP:Port, Domain, or Domain:Port', and 'Next Hop Server 2' with an empty text input field and the same label. Below the table are three checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (unchecked), and 'Ignore Route Header for Messages Outside Dialog' (unchecked). Below these are two more checkboxes: 'NAPTR' (unchecked) and 'SRV' (unchecked). At the bottom is a row for 'Outgoing Transport' with three radio buttons: 'TLS' (unchecked), 'TCP' (checked), and 'UDP' (unchecked). A 'Finish' button is located at the bottom center.

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



Similarly, for the outbound route:

- Select **Add Profile**.
- Enter Profile Name: **Route\_to\_SP**
- Click **Next**.
- **Next Hop Server 1: 222.222.222.247:6003** (service provider SIP Proxy IP:Port).
- Check **Routing Priority Based on Next Hop Server**
- **Outgoing Transport: UDP**
- Click **Finish**

**Edit Routing Rule**
✕

Each URI group may only be used once per Routing Profile.

**Next Hop Routing**

URI Group	* <span style="float: right;">▼</span>		
Next Hop Server 1	222.222.222.247:6003	IP, IP:Port, Domain, or Domain:Port	
Next Hop Server 2		IP, IP:Port, Domain, or Domain:Port	

☒ Routing Priority based on Next Hop Server  
☐ Use Next Hop for In Dialog Messages  
☐ Ignore Route Header for Messages Outside Dialog  
  
☐ NAPTR    ☐ SRV

Outgoing Transport

☐ TLS
 ☐ TCP
 ☒ UDP

Finish

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

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 9:52:10 AM GMT

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

- UC-Sec Control Center
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
  - Domain DoS
  - Fingerprint
  - Server Interworking
  - Phone Interworking
  - Media Forking
  - Routing
  - Server Configuration
  - Subscriber Profiles
  - Topology Hiding
  - Signaling Manipulation
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Global Profiles > Routing: Route\_to\_SP

Add Profile
Rename Profile
Clone Profile
Delete Profile

Click here to add a description.

Routing Profile

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	222.222.222.247:6003	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

### 7.3.3. Server Configuration

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

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

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

- Select **Server Type: Call Server**
- **IP Address: 172.16.5.32 (IP Address of Session Manager Security Module)**
- **Supported Transports: Check TCP**
- **TCP Port: 5060**
- Click **Next**

Add Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma separated list	172.16.5.32
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
<div>Back Next</div>	

- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.



**Add Server Configuration Profile - Advanced**
✕

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya <span style="float: right;">▼</span>
Signaling Manipulation Script	None <span style="float: right;">▼</span>
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Back
Finish

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

**UC-Sec Control Center**

Welcome ucsec, you signed in as Admin. Current server time is 1:26:52 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users

Global Profiles > Server Configuration: Session Manager

UC-Sec Control Center  
 Administration  
 Backup/Restore  
 System Management  
 Global Parameters  
 Global Profiles  
   Domain DoS  
   Fingerprint  
   Server Interworking  
   Phone Interworking  
   Media Forking  
   Routing  
   **Server Configuration**  
     Subscriber Profiles  
     Topology Hiding  
     Signaling Manipulation  
     URI Groups  
 SIP Cluster  
 Domain Policies  
 Device Specific Settings  
 Troubleshooting  
 TLS Management  
 IM Logging

Add Profile
Rename Profile
Clone Profile
Delete Profile

Profile  
**Session Manager**  
 Service Provider

General
Authentication
Heartbeat
Advanced

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

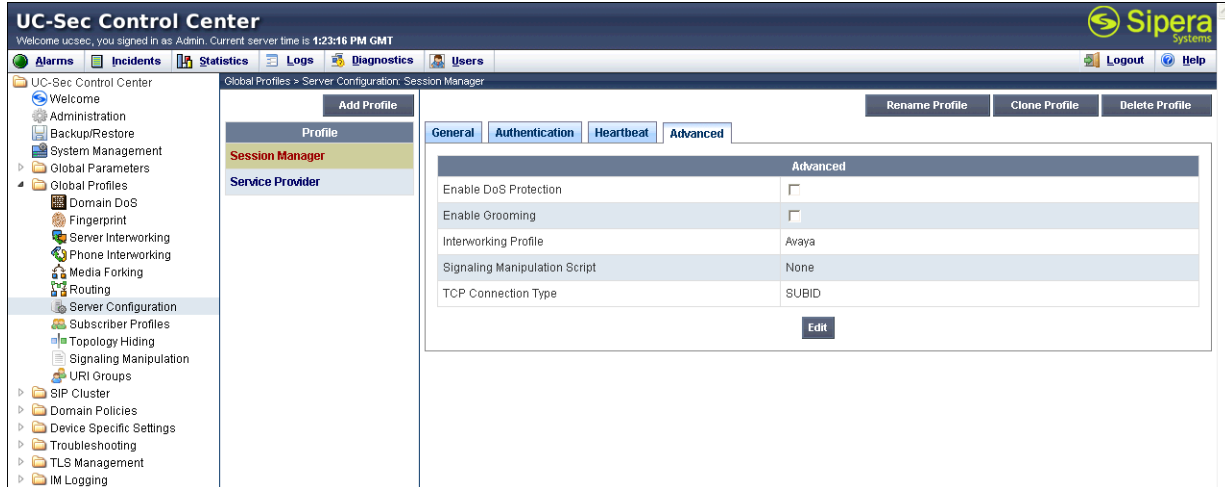
Edit

HG; Reviewed:  
SPOC 6/21/2012

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

81 of 110  
CTLCS1KSMSBCE

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



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

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

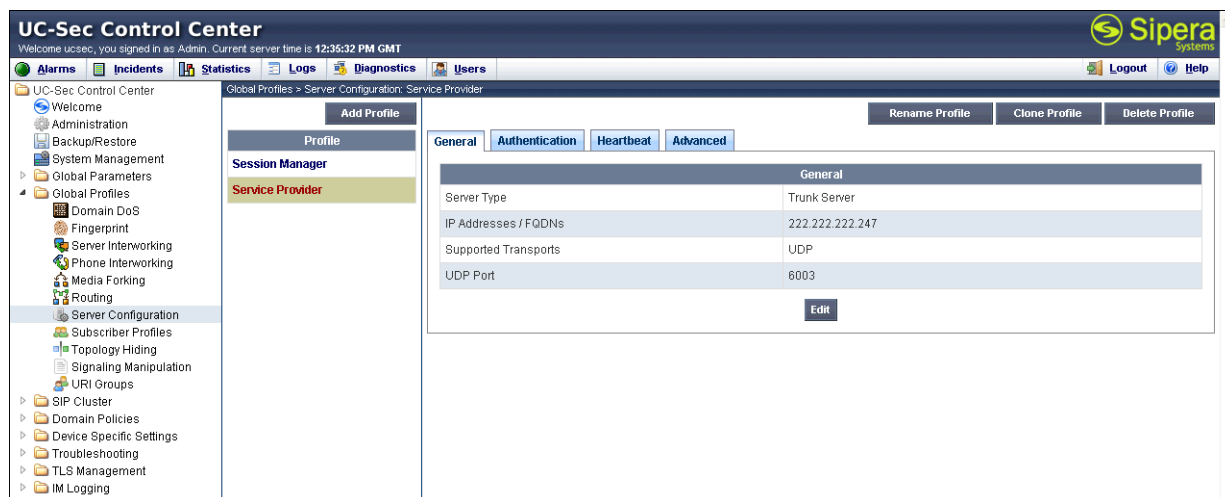
- Select **Server Type: Trunk Server**
- **IP Address: 222.222.222.247** (service provider's SIP Proxy IP address)
- **Supported Transports: Check UDP.**
- **UDP Port: 6003**
- Click **Next**

Edit Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma separated list	222.222.222.247
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	6003
TLS Port	
<div>Finish</div>	

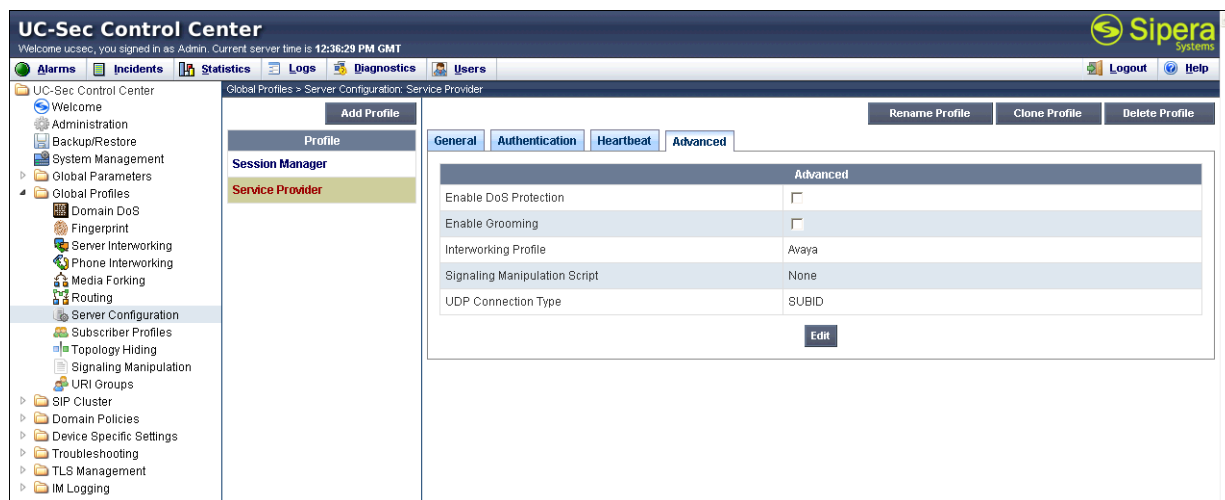
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya** from the **Interworking Profile** drop down menu. Leave other fields with their default values for now, a **Signaling Manipulation Script** will be assigned later.
-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

Add Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<div>Back</div> <div>Finish</div>	

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



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



### 7.3.4. Topology Hiding

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

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

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

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

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: Session\_Manager**.
- Leave all **Replace Action** as **Auto**.
- Click **Finish**.

The following screen capture shows the newly added **Session\_Manager** Profile.

The screenshot shows the UC-Sec Control Center interface. On the left, the 'Global Profiles' menu is expanded, showing 'Topology Hiding' selected. The main panel displays the 'Session\_Manager' profile configuration. The 'Topology Hiding' tab is active, showing a table with headers: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following data:

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

An 'Edit' button is located below the table. The interface also includes a sidebar with various system management options and a top navigation bar with tabs for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users.

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

- Click on **default** profile and select **Clone Profile**.
- Enter the **Profile Name: Service\_Provider**.
- For the **From** header, chose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider under **Overwrite Value**.
- For the **To** header, chose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider under **Overwrite Value**.
- For the **Request-Line** header, chose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider under **Overwrite Value**.
- Click **Finish**.

**Edit Topology Hiding Profile**
✕

Header	Criteria	Replace Action	Overwrite Value	
From	IP/Domain	Overwrite	bsoft.nc.labnet	✕
SDP	IP/Domain	Auto		✕
Via	IP/Domain	Auto		✕
To	IP/Domain	Overwrite	bsoft.nc.labnet	✕
Request-Line	IP/Domain	Overwrite	bsoft.nc.labnet	✕
Record-Route	IP/Domain	Auto		✕

Finish

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

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 12:49:23 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users
Logout Help

- UC-Sec Control Center
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
  - Domain DoS
  - Fingerprint
  - Server Interworking
  - Phone Interworking
  - Media Forking
  - Routing
  - Server Configuration
  - Subscriber Profiles
  - Topology Hiding
  - Signaling Manipulation
  - URI Groups
- SIP Cluster
- Domain Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Global Profiles > Topology Hiding > Service\_Provider

Add Profile
Rename Profile
Clone Profile
Delete Profile

Topology Hiding Profiles

default

cisco\_th\_profile

Session\_Manager

Service\_Provider

Click here to add a description.

Topology Hiding

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

Edit

### 7.3.5. 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 above.

For more information on the structure of the SigMa Scripting Language and details on its use, see [13].

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click on **Add Script** to open the SigMa Editor screen. On the **Title**, enter **Remove\_Unwanted\_Headers**. Enter the script as shown on the screen below:

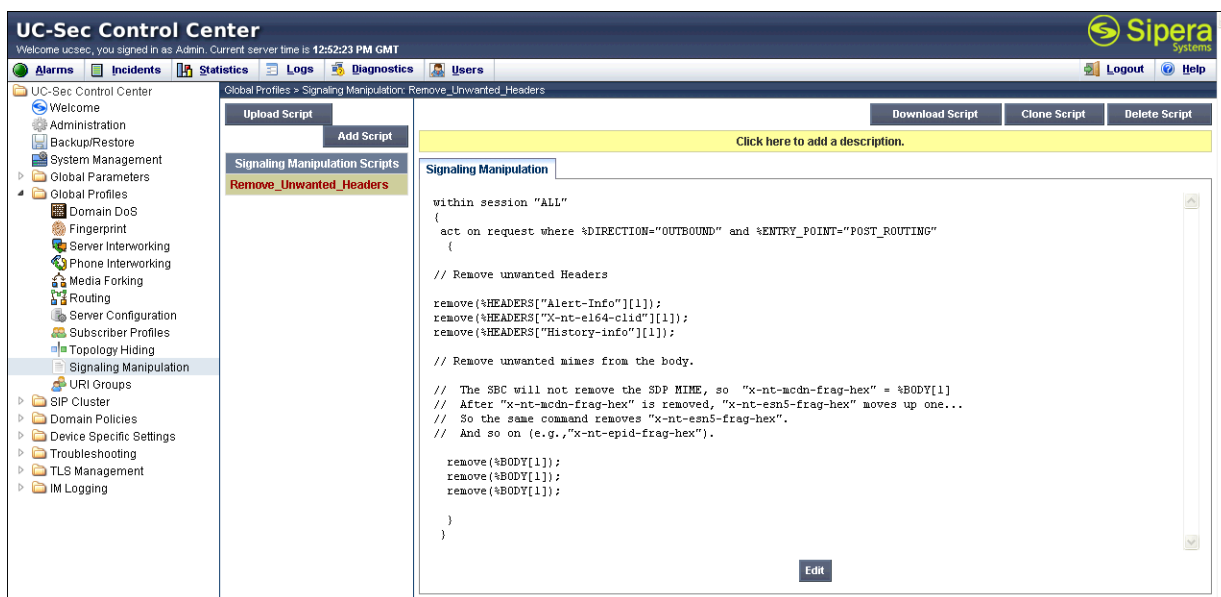
The screenshot shows the Sigma Editor window with a script titled "Remove\_Unwanted\_Headers". The script is as follows:

```

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

```

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



After the Signaling Manipulation Script is created, it should be applied to the **Service Provider** Server Profile previously created in **Section 7.3.3**.

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



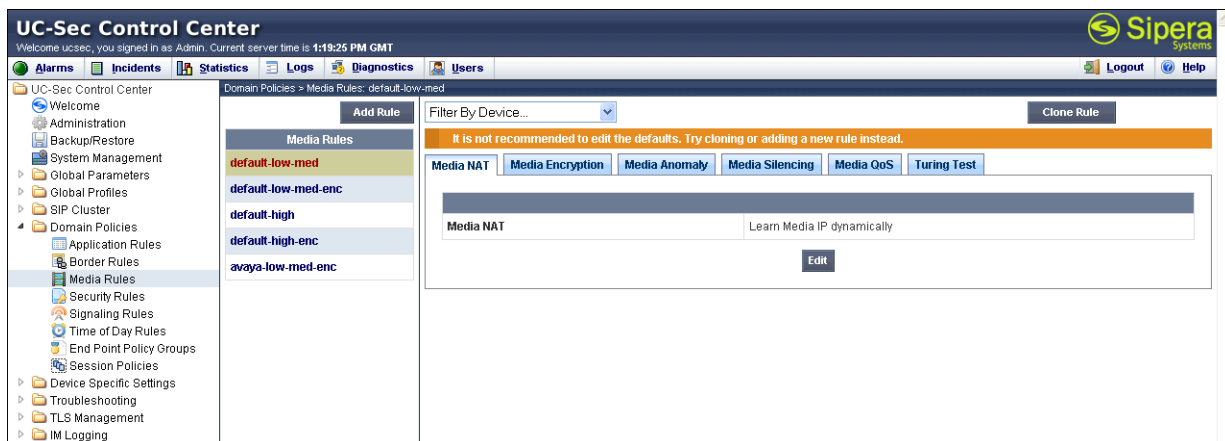


## 7.4. Domain Policies

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

### 7.4.1. Media Rules

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



### 7.4.2. Signaling Rules

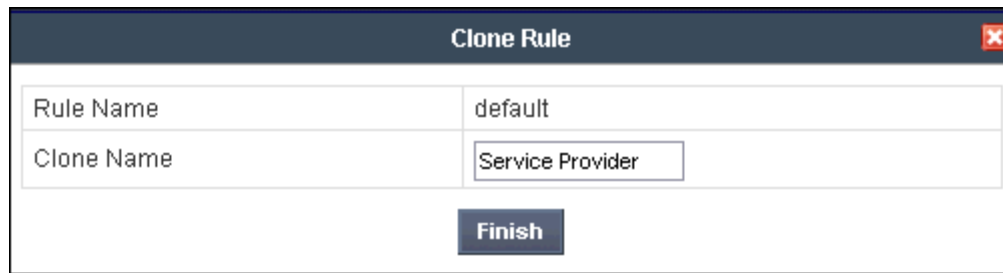
Signaling Rules define the actions to be taken (*Allow, Block, Block with Response, etc.*) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

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

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

- Click on the **default** Signaling Rule.
- Click on **Clone Rule**.

Enter a name: **Service\_Provider**. Click **Finish**.

A screenshot of a 'Clone Rule' dialog box. The dialog has a dark blue header bar with the title 'Clone Rule' and a red close button. Below the header, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'Service Provider'. At the bottom center, there is a dark blue button labeled 'Finish'.

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

To add the Alert-Info header:

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

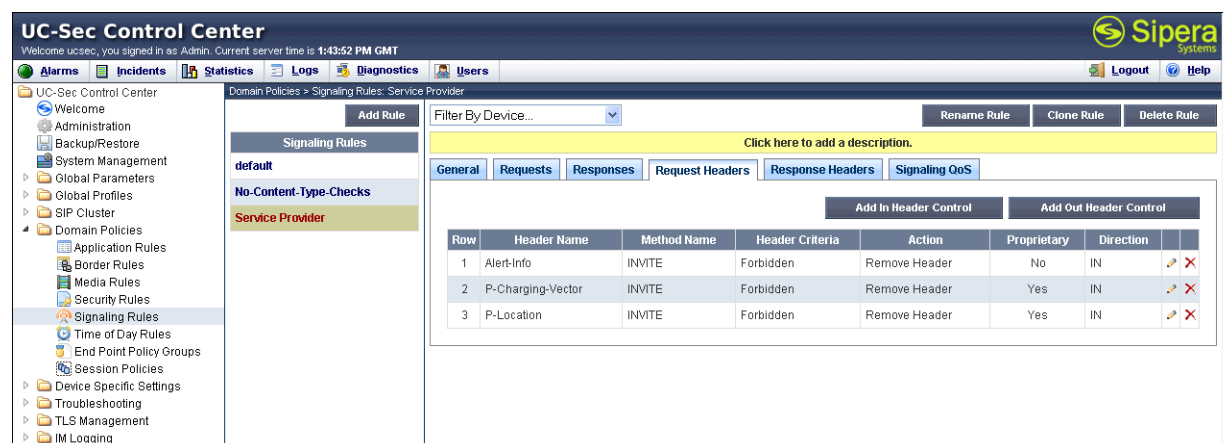
To add the P-Location header:

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

To add the P-Charging-Vector header:

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

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



Select the **Response Headers** tab.

To add the Alert-Info header:

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

To add the P-Location header:

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

To add the P-Charging-Vector header:

- Select **Add in Header Control**.
- Check the **Proprietary Request Header** box
- **Header Name: P-Charging-Vector**
- **Response Code: 200**

- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

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

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

### 7.4.3. 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: default**
- **Border Rule: default**
- **Media Rule: default-low-med**
- **Security Rule: default-low**
- **Signaling Rule: Service Provider**
- **Time of Day: default**
- Click **Finish**.

Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Service Provider
Time of Day Rule	default

Finish

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 1:52:34 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Domain Policies > End Point Policy Groups: Enterprise

Filter By Device...

Click here to add a description.

Hover over a row to see its description.

Policy Group

View Summary Add Policy Set

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

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

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

Edit Policy Set
✕

<b>Application Rule</b>	default ▼
<b>Border Rule</b>	default ▼
<b>Media Rule</b>	default-low-med ▼
<b>Security Rule</b>	default-low ▼
<b>Signaling Rule</b>	default ▼
<b>Time of Day Rule</b>	default ▼

Finish

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

UC-Sec Control Center
Sipera Systems

Welcome ucsec, you signed in as Admin. Current server time is 1:55:42 PM GMT
Logout Help

- UC-Sec Control Center
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Application Rules
- Border Rules
- Media Rules
- Security Rules
- Signaling Rules
- Time of Day Rules
- End Point Policy Groups
- Session Policies
- Device Specific Settings
- Troubleshooting
- TLS Management
- IM Logging

Domain Policies > End Point Policy Groups: Service Provider
Filter By Device...

Add Group
Rename Group
Delete Group

**Policy Groups**

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- Enterprise
- Service Provider

Click here to add a description.

Click here to add a row description.

Policy Group
View Summary
Add Policy Set

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

## 7.5. Device Specific Settings

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

### 7.5.1. Network Management

The network information should have been previously completed in **Section 7.2**. To verify the network configuration, from the **Device Specific Menu** on the left hand side, select **Network Management**. Select the **Network Configuration** tab.

HG; Reviewed:  
SPOC 6/21/2012

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

94 of 110  
CTLCS1KSMSBCE

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 1:59:29 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Device Specific Settings > Network Management: Sipera

UC-Sec Devices

Sipera

Network Configuration Interface Configuration

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

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.192 B2 Netmask

Add IP

Changes will not take effect until the interface is updated.

Save Changes Clear Changes

IP Address	Public IP	Gateway	Interface
172.16.5.71		172.16.5.254	A1
111.111.111.187		111.111.111.129	B1

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

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:01:09 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Device Specific Settings > Network Management: Sipera

UC-Sec Devices

Sipera

Network Configuration Interface Configuration

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

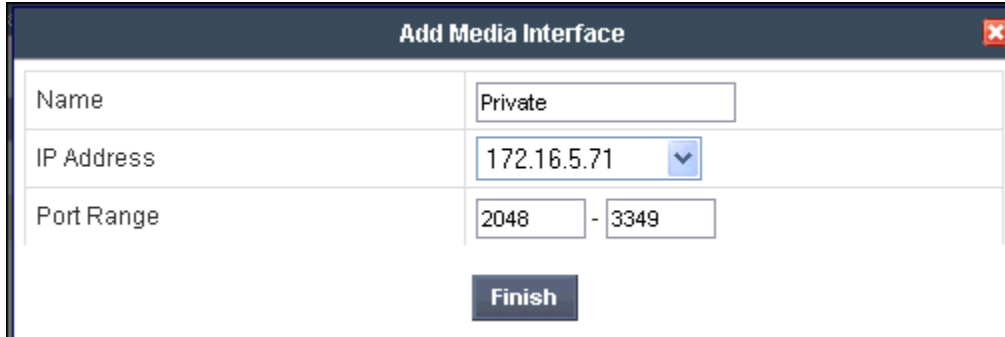
### 7.5.2. Media Interface

Media Interfaces were created to adjust the port range assigned to media streams leaving the interfaces of the Avaya SBCE. On the Private interface of the Avaya SBCE ports range 2048 to 3349 was used. On the Public interface port range 40150 to 40199 was used, matching the port range specified by the Service Provider.

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

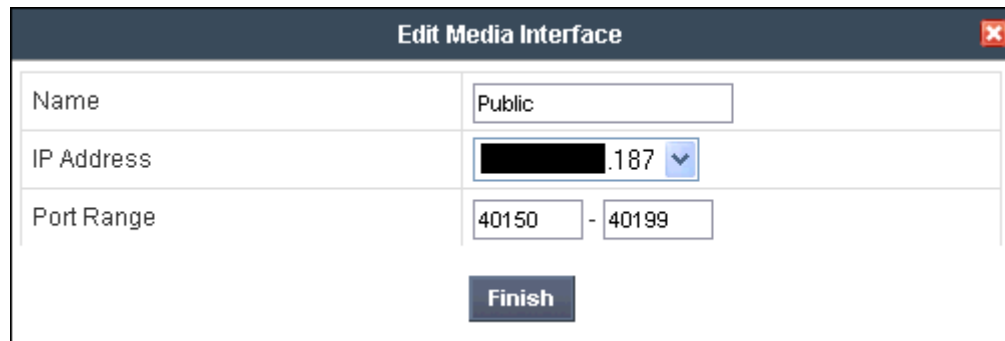
- Select **Add Media Interface**
- **Name: Private**

- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager)
- **Port Range: 2048-3349**
- Click **Finish**



Add Media Interface	
Name	Private
IP Address	172.16.5.71
Port Range	2048 - 3349
<div>Finish</div>	

- Select **Add Media Interface**
- **Name: Public**
- Select **IP Address: 111.111.111.187** (Outside IP Address of the Avaya SBCE, toward Service Provider)
- **Port Range: 40150-40199**
- Click **Finish.**
- 



Edit Media Interface	
Name	Public
IP Address	[REDACTED].187
Port Range	40150 - 40199
<div>Finish</div>	



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

The screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a tree view with categories like Administration, System Management, and Device Specific Settings. Under Device Specific Settings, 'Media Interface' is selected. The main content area is titled 'Media Interface' and includes a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table with two columns: 'Name' and 'Media IP', and a 'Port Range' column. The table lists two interfaces: 'Private' with IP 172.16.5.71 and port range 2048 - 3349, and 'Public' with IP 111.111.111.187 and port range 40150 - 40199. Each row has edit and delete icons. An 'Add Media Interface' button is located at the top right of the table.

Name	Media IP	Port Range
Private	172.16.5.71	2048 - 3349
Public	111.111.111.187	40150 - 40199

### 7.5.3. Signaling Interface

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

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

**Add Signaling Interface**
✖

**Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.**

Name	Private
IP Address	172.16.5.71 ▼
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	5060
TLS Port <small>Leave blank to disable</small>	
Cluster TLS <small>Only for use with Cisco SIP Clusters</small>	<input type="checkbox"/>
Enable Stun <small>Requires a UDP Port</small>	<input type="checkbox"/>

Finish

- Select **Add Signaling Interface**:
- **Name: Public**
- Select **IP Address: 111.111.111.187** (Outside IP Address of the Avaya SBCE, toward the Service Provider)
- **TCP Port: 5060**
- **UDP Port: 5060**
- Click **Finish**

**Edit Signaling Interface**
✕

**Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.**

Name	<input type="text" value="Public"/>
IP Address	<input type="text" value="111.111.111.187"/> <span style="float: right;">▼</span>
TCP Port <small>Leave blank to disable</small>	<input type="text" value="5060"/>
UDP Port <small>Leave blank to disable</small>	<input type="text" value="5060"/>
TLS Port <small>Leave blank to disable</small>	<input type="text"/>
Cluster TLS <small>Only for use with Cisco SIP Clusters</small>	<input type="checkbox"/>
Enable Stun <small>Requires a UDP Port</small>	<input type="checkbox"/>

Finish

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

**UC-Sec Control Center**
Sipera systems

Welcome ucsec, you signed in as Admin. Current server time is 2:17:46 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users

Logout Help

UC-Sec Control Center

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

SIP Cluster

Domain Policies

Device Specific Settings

Network Management

Media Interface

Signaling Interface

Signaling Forking

SNMP

End Point Flows

Session Flows

Two Factor

Relay Services

Troubleshooting

TLS Management

IM Logging

Device Specific Settings > Signaling Interface: Sipera

UC-Sec Devices

Sipera

Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private	172.16.5.71	5060	5060	---	None	✕
Public	111.111.111.187	5060	5060	---	None	✕

## 7.5.4. End Point Flows

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

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, 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\_SM** (Note that this is the reverse route of the flow).
- **Topology Hiding Profile: Service\_Provider**
- **File Transfer Profile: None**
- Click **Finish**

Criteria	
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_SM
Topology Hiding Profile	Service_Provider
File Transfer Profile	None

**Finish**

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

- **Name: Session\_Manager\_Flow**
- **Server Configuration: Session Manager**
- **URI Group: \***
- **Transport: \***

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

Edit Flow: Session\_Manager\_Flow

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

Finish

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

**UC-Sec Control Center**  
Welcome ucsec, you signed in as: Admin. Current server time is 2:25:11 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

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

Device Specific Settings > End Point Flows: Sipera

UC-Sec Devices  
Sipera

Subscriber Flows Server Flows

Add Flow

Click here to add a row description.

**Server Configuration: Service Provider**

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	SIP_Trunk_Flow	*	*	*	Private	Public	Public	Service Provider	Route_to_SM	Service_Provider	None			

**Server Configuration: Session Manager**

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Session_Manager_Flow	*	*	*	Public	Private	Private	Enterprise	Route_to_SP	Session_Manager	None			

## 8. CenturyLink BroadWorks SIP Trunk Service Configuration

To use CenturyLink BroadWorks 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/Pages/Support/> and requesting information via the online sales links or telephone numbers.

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, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Avaya CS1000, Avaya Aura® Session Manager, and the Avaya SBCE configuration discussed in the previous sections.

The configuration between CenturyLink and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to CenturyLink's network.

## 9. Verification Steps

The following steps may be used to verify the configuration.

### 9.1. General

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

### 9.2. 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 DN when the call is in progress or idle. The call scenario involved the CS1000 extension 8005 calling PSTN phone number 7863311234.

- Log in to the Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Log in to the Overlay command prompt, issue the command **LD 80** and then **trac 0 8005**.
- After the call is released, issue command **trac 0 8005** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when extension 8005 is in an active call:

```
>ld 80
TRA000
.trac 0 8005

ACTIVE VTN 008 0 00 03

ORIG VTN 008 0 00 03 KEY 0 SCR MARP CUST 0 DN 8005 TYPE 2050PC
  SIGNALLING ENCRYPTION: INSEC
  FAR-END SIP SIGNALLING IP: 172.16.21.61
  FAR-END MEDIA ENDPOINT IP: 1.1.1.2 PORT: 5200
  FAR-END VendorID: Not available
TERM VTN 048 0 00 10 VTRK IPTI RMBR 0 11 OUTGOING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 172.16.5.71
  FAR-END MEDIA ENDPOINT IP: 172.16.5.71 PORT: 2050
  FAR-END VendorID: AVAYA-SM-6.1.5.0.615006
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 27 TERM 30 JUNCTOR ORIG0 TERM0
EES_DATA:
NONE
QUEU NONE
CALL ID 0 190

----- ISDN ISL CALL (TERM) -----
CALL REF # = 395
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 318360 NUM_PLAN:E164 TON:NATIONAL ESN:NPA
CALLED NO = 1786331 NUM_PLAN:E164 TON:NATIONAL ESN:NPA
```



Following is an example after the call on 8005 has been released.

```
trac 0 8005  
IDLE VTN 008 0 00 03   MARP
```

Following is an example after the call has been released, which shows that there are no trunks busy.

```
>ld 32  
NPR000  
.stat 0 0  
LOOP UNEQ  
.stat 48 0  
012 UNIT(S) IDLE  
000 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY
```

### 9.3. Protocol Traces

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

- RequestURI: verify the request number and SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- Diversion: verify the name 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, and DTMF event description
- Media Attribute: verify specific audio port, codec, ptime, and send/receive ability
- DTMF event and fax attributes.

Following is an example of a typical capture for a call made from the PSTN (7863311234) to a CS1000 extension 8005 (DID 3183601234).

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

The image shows a Wireshark packet capture of a SIP call. The top pane displays a list of packets, and the bottom pane shows the details of the selected packet (Frame 98).

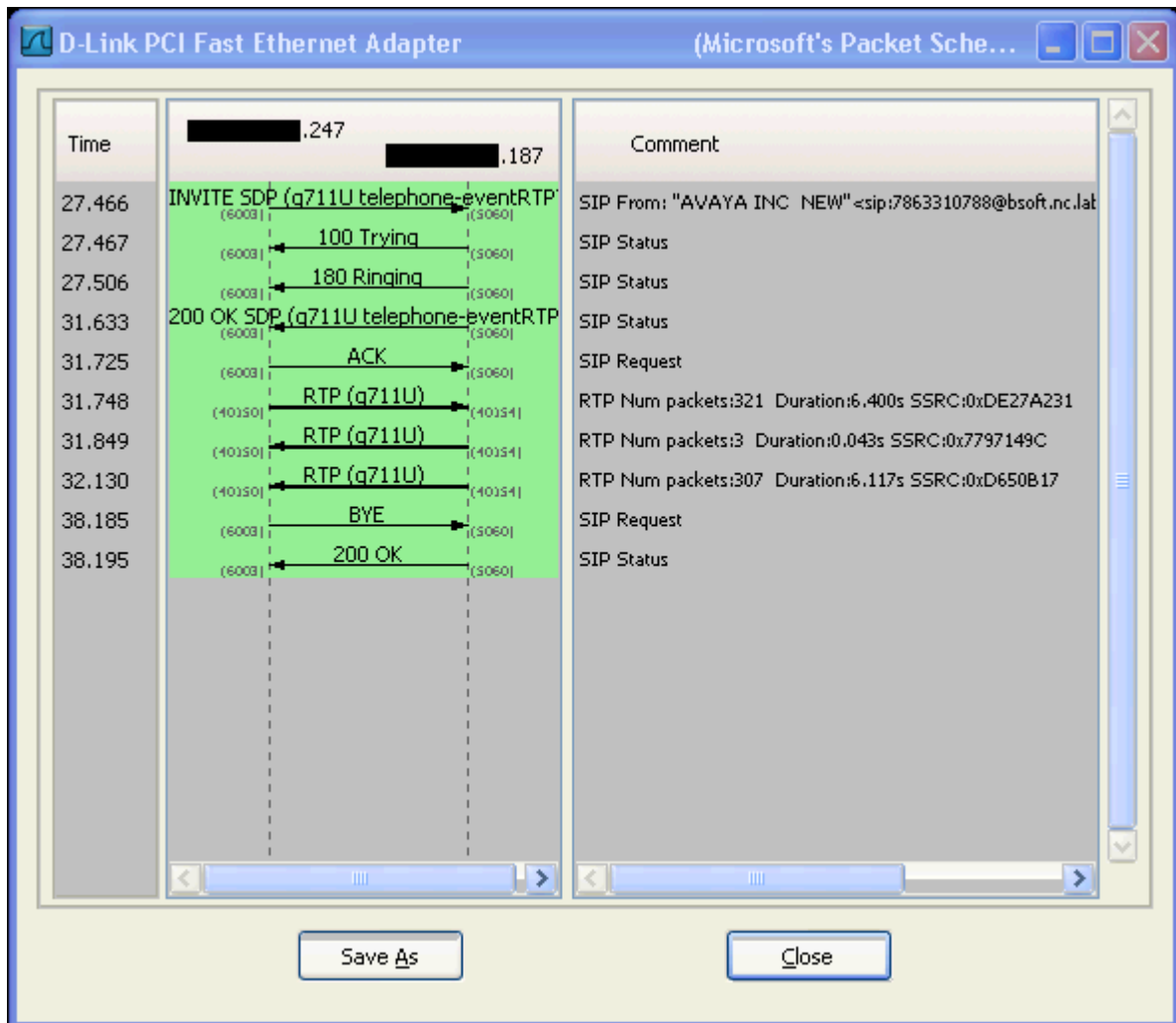
No.	Time	Source	Destination	Protocol	Length	Info
98	27.465793	.247	.187	SIP/SDP	985	Request: INVITE sip:318360.187:5060, with session description
99	27.467180	.187	.247	SIP	412	Status: 100 Trying
103	27.506418	.187	.247	SIP	1024	Status: 180 Ringing
119	31.633422	.187	.247	SIP/SDP	1334	Status: 200 OK, with session description
120	31.724990	.247	.187	SIP	659	Request: ACK sip:318360.187:5060;transport=udp;user=phone
767	38.184556	.247	.187	SIP	607	Request: BYE sip:318360.187:5060;transport=udp;user=phone
769	38.195446	.187	.247	SIP	694	Status: 200 OK

**Frame 98: 985 bytes on wire (7880 bits), 985 bytes captured (7880 bits)**

- Ethernet II, Src: Adtran\_30:cd:78 (00:a0:c8:30:cd:78), Dst: IntelCor\_cb:79:91 (00:1b:21:cb:79:91)
- Internet Protocol Version 4, Src: .247 ( ), Dst: .187 ( )
- User Datagram Protocol, Src Port: 6003 (6003), Dst Port: sip (5060)
- Session Initiation Protocol
  - Request-Line: INVITE sip:318360.187:5060 SIP/2.0
  - Message Header
    - Via: SIP/2.0/UDP .247:6003;branch=z9hG4bKp14ms430681ghicu02k1.1
    - From: "AVAYA INC NEW" <sip:786331@bsoft.nc.labnet;user=phone>;tag=Sdbuu3f01-894999433-1333053017453-
    - To: "318360 318360" <sip:318360@bsoft.nc.labnet>
    - Call-ID: Sdbuu3f01-6f37f0819b1bd55f8e76d0f916a4ec-a01q021
    - CSeq: 806577847 INVITE
    - Contact: <sip:786331.247:6003;transport=udp>
    - Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
    - Accept: application/media\_control+xml, application/sdp, multipart/mixed
    - Max-Forwards: 49
    - Content-Type: application/sdp
    - Content-Disposition: session;handling=optional
    - Content-Length: 244
  - Message Body

Frame (frame), 985 bytes      Packets: 817 Displayed: 7 Marked: 0 Dropped: 0      Profile: Default

Following is the SIP messaging flow of the same call listed above seen from Telephony → VoIP Calls of Wireshark.



## 10. Conclusion

These Application Notes describe the procedures necessary to configure SIP Trunk connectivity between Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1, Avaya Session Border Controller for Enterprise Release 4.0.5Q02 and CenturyLink BroadWorks SIP Trunk service as shown in **Figure 1**.

CenturyLink BroadWorks SIP Trunk service passed compliance testing.

## 11. References

Product documentation for Avaya products may be found at:

<http://support.avaya.com/css/appmanager/public/support>

- [1] Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.
- [2] IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010
- [3] Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011
- [4] Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011
- [5] Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010
- [6] Product Compatibility Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011
- [7] Installing and Configuring Avaya Aura® System Platform, Release 6.0.3, February 2011.
- [8] Administering Avaya Aura® System Platform, Release 6.0.3, February 2011.
- [9] Installing and Upgrading Avaya Aura® System Manager, Release 6.1, November 2010.
- [10] Installing and Configuring Avaya Aura® Session Manager, April 2011, Document Number 03-603473.
- [11] Administering Avaya Aura® Session Manager, November 2010, Document Number 03-603324.
- [12] Sipera Systems E-SBC 1U Installation Guide. Release 4.0.5. November 2011.
- [13] Sipera Systems E-SBC Administration Guide. Release 4.0.5. November 2011.
- [14] Sipera Systems E-SBC Release Notes. Release 4.0.5.Q02. November 2011.
- [15] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>.
- [16] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, <http://www.ietf.org/>

---

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

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

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