



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

---

# **Application Notes for Configuring SaskTel SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2.1 - Issue 1.0**

## **Abstract**

These Application Notes describe the procedures necessary for configuring SaskTel SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2.1.

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

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results .....	5
2.3.	Support .....	6
3.	Reference Configuration .....	7
4.	Equipment and Software Validated .....	9
5.	Configure Avaya Communication Server 1000E .....	12
5.1.	Login to the CS1000 System.....	12
5.1.1.	Login to Unified Communications Management (UCM) and Element Manager ..	12
5.1.2.	Login to the Call Server Command Line Interface (CLI).....	15
5.2.	Administer an IP Telephony Node.....	16
5.2.1.	Obtain Node IP address .....	16
5.2.2.	Administer Terminal Proxy Server .....	18
5.2.3.	Administer Quality of Service (QoS) .....	19
5.3.	Administer Voice Codec .....	20
5.3.1.	Enable Voice Codec, Node IP Telephony. ....	20
5.3.2.	Synchronize the New Configuration.....	23
5.3.3.	Enable Voice Codec on Media Gateways.....	25
5.4.	Administer Zones and Bandwidth.....	27
5.4.1.	Create a zone for IP phones (zone 5).....	27
5.4.2.	Create a zone for virtual SIP trunks (zone 4).....	28
5.5.	Administer SIP Trunk Gateway .....	29
5.5.1.	Administer the SIP Trunk Gateway to Session Manager .....	31
5.5.2.	Administer Virtual D-Channel.....	33
5.5.3.	Administer Virtual Superloop.....	37
5.5.4.	Administer Virtual SIP Routes .....	38
5.5.5.	Administer Virtual Trunks.....	41
5.5.6.	Administer Calling Line Identification Entries.....	44
5.6.	Administer Dialing Plans .....	47
5.6.1.	Define ESN Access Codes and Parameters (ESN) .....	47
5.6.2.	Associate NPA and SPN call to ESN Access Code 1 .....	48
5.6.3.	Digit Manipulation Block Index (DMI).....	49
5.6.4.	Route List Block (RLB).....	51
5.6.5.	Inbound Digit Translation.....	52
5.6.6.	Outbound Call - Special Number Configuration. ....	55
5.6.7.	Outbound Call - Numbering Plan Area Code (NPA) .....	56
5.7.	Administer Phone.....	56
5.7.1.	Phone creation.....	56
5.7.2.	Enable Privacy for Phone.....	58
5.7.3.	Enable Call Forward for the Phone.....	59
5.7.4.	Enable Call Waiting for the Phone .....	64

6.	Configure Avaya Aura® Session Manager .....	65
6.1.	System Manager Login and Navigation .....	66
6.2.	Specify SIP Domain .....	67
6.3.	Add Location .....	68
6.4.	Add Adaptation Module .....	71
6.5.	Add SIP Entities .....	73
6.6.	Add Entity Links .....	77
6.7.	Add Routing Policies .....	79
6.8.	Add Dial Patterns .....	80
6.9.	Add/View Session Manager .....	82
7.	Configure Avaya Session Border Controller for Enterprise (Avaya SBCE) .....	84
7.1.	Log in Avaya SBCE .....	84
7.2.	Global Profiles .....	87
7.2.1.	Server Interworking - Avaya-SM .....	87
7.2.2.	Server Interworking - SP-General .....	89
7.2.3.	Routing Profiles .....	90
7.2.4.	Server Configuration .....	93
7.2.5.	Topology Hiding .....	99
7.2.6.	Signaling Manipulation .....	101
7.3.	Domain Policies .....	103
7.3.1.	Create Application Rules .....	103
7.3.2.	Media Rules .....	105
7.3.3.	Signaling Rules .....	105
7.3.4.	End Point Policy Groups .....	111
7.4.	Device Specific Settings .....	114
7.4.1.	Network Management .....	114
7.4.2.	Media Interface .....	116
7.4.3.	Signaling Interface .....	118
7.4.4.	End Point Flows .....	120
8.	SaskTel SIP Trunk Service Configuration .....	125
9.	Verification Steps .....	125
9.1.	General .....	125
9.2.	Verify Call Establishment on the CS1000 Call Server .....	126
9.3.	Protocol Traces .....	128
10.	Conclusion .....	130
11.	References .....	131
12.	Appendix A: SigMa Script .....	133

# 1. Introduction

These Application Notes provide the procedures necessary for configuring SaskTel SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2.1.

During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure interoperability between SaskTel and the Avaya Communication Server 1000E.

In the sample configuration, the Avaya solution consists of a Communication Server 1000E Rel. 7.6 (hereafter referred to as CS1000), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.2.1 (hereafter referred to as the Avaya SBCE), and various Avaya endpoints. This documented solution does not extend to configurations without the Avaya SBCE or Session Manager.

## 2. General Test Approach and Test Results

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

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

### 2.1. Interoperability Compliance Testing

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

- Incoming calls from the PSTN were routed to DID numbers assigned by SaskTel. Incoming PSTN calls were terminated to the following Avaya Endpoints: Avaya 1100 Series IP Telephones (SIP), Avaya 1100 Series IP Telephones (UniStim), Avaya M3904 Digital Telephones, Avaya 2050 IP Softphone, Analog Telephones and Fax machines.
- Outgoing calls to the PSTN were routed via SaskTel's network.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect during normal active call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voice mail off).
- Proper response to busy endpoints.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU, G.711A and G.729A, the SaskTel preferred codec order.
- No matching codecs.

- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- Call Pilot Voice Mail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with Interactive Voice Response systems (IVR).
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call transfers.
- Call Park.
- Station Conference.
- G.711Mu fax pass-through.
- Long duration calls (one hour).
- Early Media transmission.
- Mobility: Mobil X and Personal Call Assistance (PCA).

## 2.2. Test Results

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

- **No Ring-Back tone after Blind Transfers to the PSTN:** No ring back tone is heard (only silence) on PSTN phones after execution of Blind Transfers to the PSTN from CS1000 phones (PSTN\_1 → CS1000\_IP\_Phone → Blind Transfer → PSTN\_2). The default operation of the CS1000 is as follows: If the Service Provider **does not** support SIP UPDATE, the CS1000 will prevent execution of Blind Transfers from one PSTN endpoint to another PSTN endpoint by disabling the **Trans** key on the CS1000 phone. As a work around **Plug-in 501** can be enabled to allow Blind Transfer when SIP UPDATE is not supported, but with a known limitation that there will be **NO** ring-back tone provided after execution of the Blind Transfer. The compliance testing was done with **Plug-in 501** enabled to allow Blind Transfers to be performed to PSTN endpoints.
- **Caller-ID on re-directed calls to the PSTN:** Caller ID works properly between the CS1000 and SaskTel when there is no call re-direction involved. However, when calls are re-directed to the PSTN at the CS1000 extension, the Caller ID will not properly reflect the true originator of the call. In normal conditions if a call is re-directed at the CS1000 to a PSTN extension, the Caller ID displayed at the PSTN extension will be of the extension doing the re-direction (i.e., transferee) and not the Caller ID of the extension that originated the call. This is a known issue.
- **Outbound call CS1000 hold/retrieve and Transfer scenarios:** If a CS1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed; instead the access code of the trunk route (ACOD) is displayed. Also, the trunk route (ACOD), instead of the Caller ID of the extension that originated the call, is displayed during some call transfer scenarios. These are known CS1000 issues.

- **PSTN to CS1000 calls with Privacy enabled:** Calls from the PSTN to the CS1000 with Privacy enabled (Calling Party Name/Number Block) will display the access code of the trunk route (ACOD) instead of **Anonymous**. This is a known CS1000 issue.
- **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** if they were present in the INVITE. Also the multipart MIME SDP, which included the **x-nt-mcdn-frag-hex**, **x-nt-esn5-frag-hex**, and **x-nt-epid-frag**, were stripped out. These particular headers and MIME have no real use in the service provider network.

Items not supported or not tested included the following:

- Inbound toll-free calls and 911 emergency calls are supported but were not tested as part of the compliance test.
- T.38 fax is not supported by SaskTel; therefore T.38 fax was not tested. G.711 fax pass-through was tested successfully.

## 2.3. Support

For support on SaskTel systems, call Toll Free at 1-888-773-2122 or visit the corporate Web page at: <https://www.sasktel.com/support>

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

### 3. Reference Configuration

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

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

- Avaya Communication Server 1000E (CS1000E).
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® Session Manager.
- Avaya HP® Proliant DL360 G7 server running Avaya Aura® System Manager.
- DELL R210 V2 Server running Avaya Session Border Controller for Enterprise.
- Avaya 1100-Series IP Deskphones (UniStim).
- Avaya 1100-Series Deskphones (SIP).
- 2050 Avaya IP Softphone.
- Avaya M3904 Digital Deskphones.
- Analog Deskphones.
- Fax machines.
- Desk top with administration interfaces.

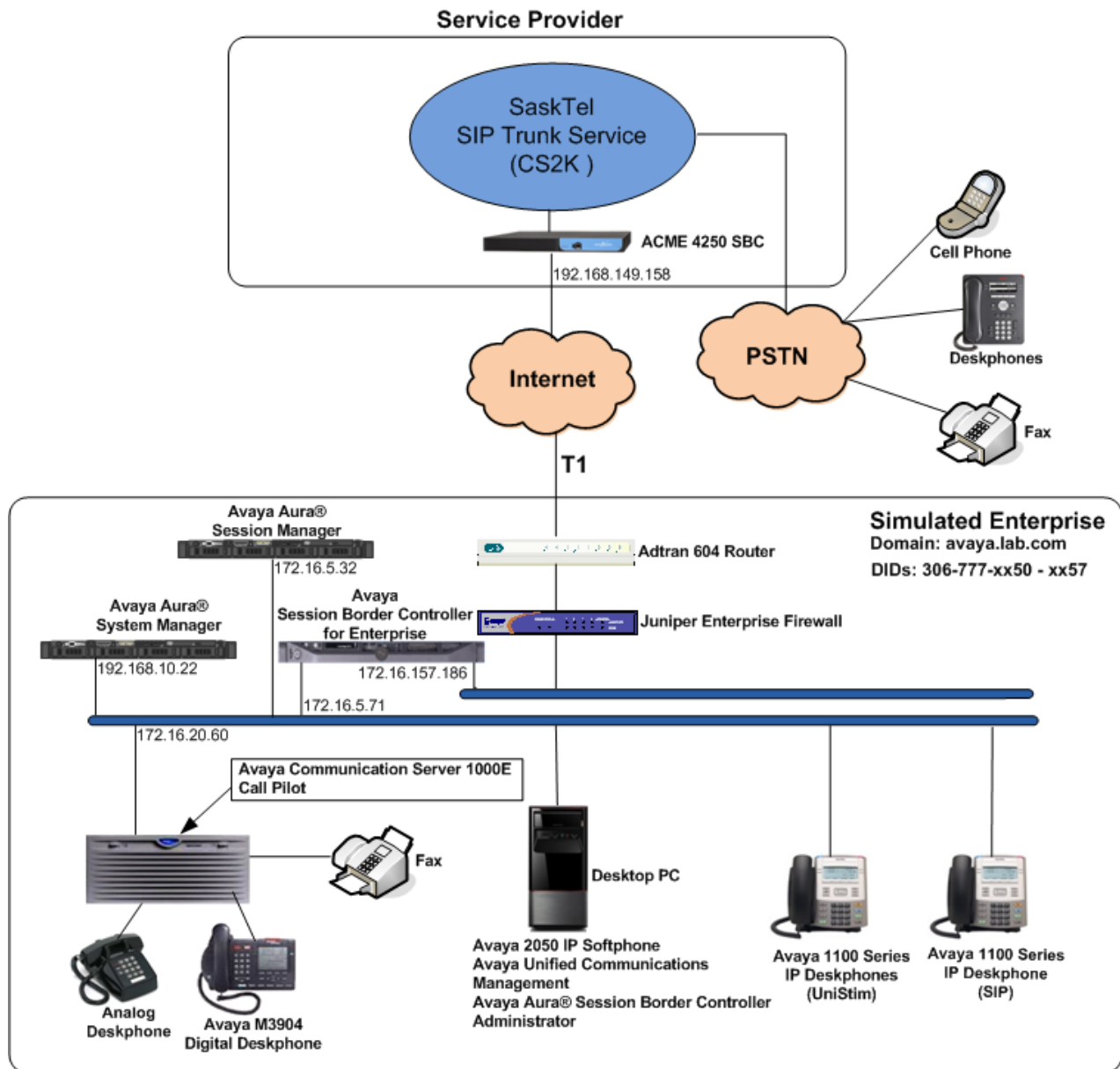
Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect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

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

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

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

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



**Figure 1: SaskTel SIP Trunk service with Avaya CS1000E**



## 4. Equipment and Software Validated

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

<b>Avaya:</b>	
<b>Equipment</b>	<b>Release/Version</b>
Avaya Communication Server 1000E running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	RELEASE 7 ISSUE 65 P +  <b>Call Server:</b> DepList 1: core Issue: 01 (created: 2013-12-17 04:32:53 (est))  <b>Signaling Server:</b> 7.65.16.00 <b>(Service Pack 4)</b> (See Service Updates & Patches below)
Avaya Call Pilot 202i	Call Pilot Manager Version: 05.00.41.156
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.5 (Service Pack 5) (6.3.5.0.635005)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.5 (Feature Pack 3) Build No. 6.3.0.8.5682-6.3.8.2826 Software Update Rev. No. 6.3.5.5.2017
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.1.Q07
Avaya Deskphones	1110: 0623C8T (UniStim) 1120: 0624C8T (UniStim) 1150: 0627C8T (UniStim) 1165: 0626C8T (UniStim) 1120: 04.04.10.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.02.0062
Lucent Analog Phone	N/A
Fax Machines	N/A
<b>SaskTel:</b>	
<b>Equipment</b>	<b>Release/Version</b>
CS2K	CVM16
ACME Session Border Controller (4250)	SC6.2.0 MR-5 GA (Build 777)

**Signaling Server Service Updates (SU) and Patches:****(CS1000 Linux Service Updates (SU) included in Release 7.6 Service Pack 4):**

cs1000-dmWeb-7.65.16.22-1.i386.000  
tzdata-2013c-2.el5.i386.001  
cs1000-linuxbase-7.65.16.22-02.i386.000  
cs1000-cs1000WebService\_6-0-7.65.16.21-00.i386.000  
cs1000-Jboss-Quantum-7.65.16.22-3.i386.000  
cs1000-pd-7.65.16.21-00.i386.000  
cs1000-shared-carrrdtct-7.65.16.21-01.i386.000  
cs1000-shared-tpselect-7.65.16.21-01.i386.000  
cs1000-dbcom-7.65.16.21-00.i386.000  
cs1000-patchWeb-7.65.16.22-1.i386.000  
cs1000-shared-xmsg-7.65.16.21-00.i386.000  
cs1000-cs-7.65.P.100-02.i386.000  
cs1000-tps-7.65.16.21-11.i386.000  
cs1000-mscAnnc-7.65.16.21-02.i386.001  
cs1000-mscAttn-7.65.16.21-04.i386.001  
cs1000-mscConf-7.65.16.21-02.i386.001  
cs1000-mscMusc-7.65.16.21-02.i386.001  
cs1000-mscTone-7.65.16.21-03.i386.001  
cs1000-sps-7.65.16.21-8.i386.000  
cs1000-shared-omm-7.65.16.21-2.i386.000  
cs1000-baseWeb-7.65.16.22-1.i386.000  
cs1000-csmWeb-7.65.16.22-1.i386.000  
cs1000-gk-7.65.16.21-01.i386.000  
cs1000-csoneksvrMgr-7.65.16.22-1.i386.000  
cs1000-snmp-7.65.16.21-00.i686.000  
cs1000-emWebLocal\_6-0-7.65.16.22-1.i386.000  
cs1000-ftpkg-7.65.16.22-1.i386.000  
cs1000-ipsec-7.65.16.22-1.i386.000  
cs1000-vtrk-7.65.16.22-4.i386.000  
cs1000-cppmUtil-7.65.16.22-1.i686.000  
cs1000-oam-logging-7.65.16.22-3.i386.000  
cs1000-bcc-7.65.16.22-6.i386.000  
cs1000-emWeb\_6-0-7.65.16.22-5.i386.000

**Signaling Server Patches:**

p31484\_1

**MGC Loadware:**

DSP1AB07.LW  
DSP2AB07.LW  
DSP3AB07.LW  
DSP4AB07.LW  
DSP5AB07.LW  
Udtcab21.lw  
MGCCDC03.LW

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

**Enable Plug-In 501** as follows:

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

**ENABLED PLUGINS:**

PLUGIN	STATUS	PRS/CR_NUM	MPLR_NUM	DESCRIPTION
501	ENABLED	Q02138637	MPLR30070	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end

## 5. Configure Avaya Communication Server 1000E

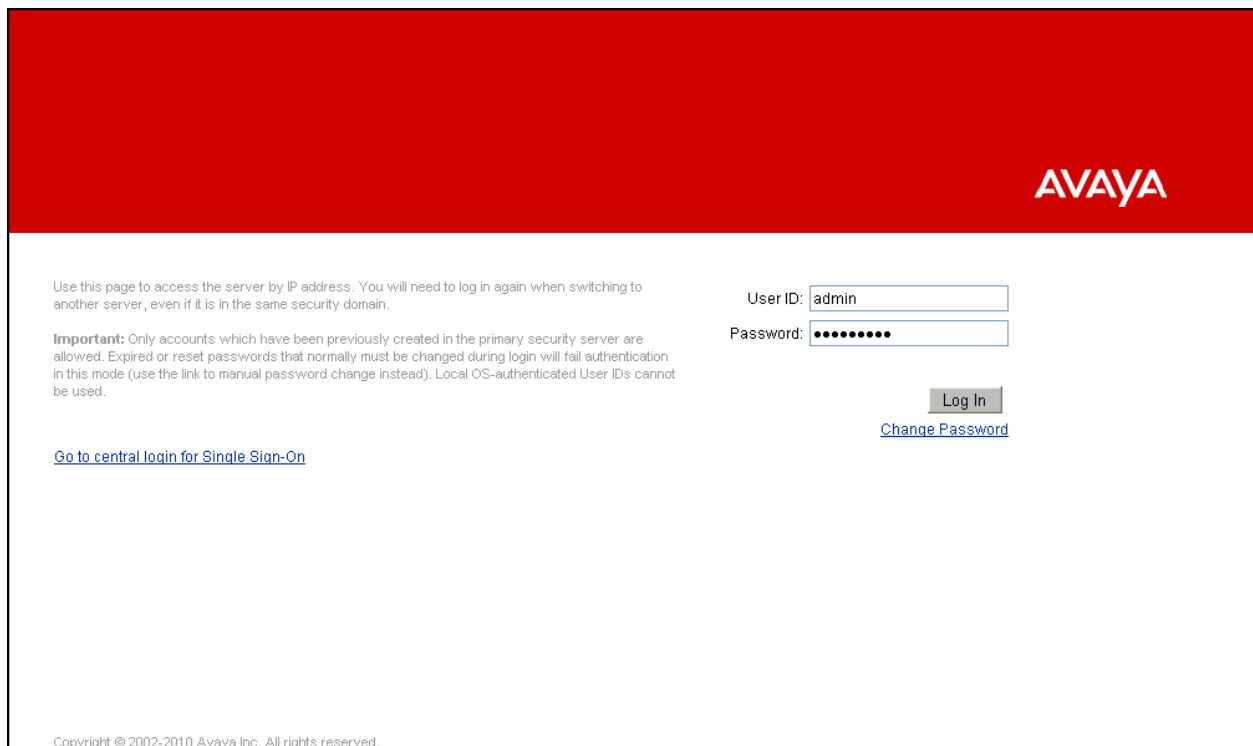
These Application Notes assume that the basic Avaya Communications Server 1000 configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11**.

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

### 5.1. Login to the CS1000 System

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

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

A screenshot of the Avaya login page. The page has a red header with the 'AVAYA' logo in white. Below the header, there is a login form. On the left, there is a paragraph of text: 'Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.' Below this is an 'Important' note: 'Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.' Below the important note is a link: 'Go to central login for Single Sign-On'. On the right side of the page, there are two input fields: 'User ID:' with the value 'admin' and 'Password:' with a masked password '••••••••'. Below these fields is a 'Log In' button and a 'Change Password' link. At the bottom left, there is a copyright notice: 'Copyright © 2002-2010 Avaya Inc. All rights reserved.'

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

**Avaya Unified Communications Management**

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

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

Host Name: 172.16.20.60    Software Version: 02.30.0086.00(6653)    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"/>	EM on cs1k	CS1000	7.6	172.16.21.61	New element.
<input type="checkbox"/>	cs1k.avaya.lab.com (primary)	Linux Base	7.6	172.16.20.61	Base OS element.
<input type="checkbox"/>	172.16.21.62	Media Gateway Controller	7.6	172.16.21.62	New element.

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

**AVAYA**

**CS1000 Element Manager**

Help | Logout

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

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

### System Overview

IP Address: 172.16.21.61  
Type: Avaya Communication Server 1000E CPMG128 Linux  
Version: 4421  
Release: 765 P +

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

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

```
login as: admin

                Avaya Inc. Linux Base  7.65
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@172.16.20.60's password:
Last login: Thu Feb 27 16:58:30 2014 from 172.16.5.250
[admin@cs1k ~]$ cslogin

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

TTY 15 SCH MTC BUG OSN    10:24
OVL111 IDLE    0
>logi
USERID? admin
PASS?
.
TTY #15 LOGGED IN ADMIN 1
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.
0:25  28/2/2014

>
```

## 5.2. Administer an IP Telephony Node

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

### 5.2.1. Obtain Node IP address

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

Select **System** → **IP Network** → **Nodes: Servers, Media Cards**. The following is the display of the **IP Telephony Nodes** page. Click on the **Node ID** of the 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.

[Add...](#) [Import...](#) [Export...](#) [Delete](#) [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	-	<a href="#">Synchronized</a>

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



The **Node Details** screen is displayed below with the IP address of the CS1000 node. The **Node IPv4 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 IPv4 Address** to communicate with other components for call processing.

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 (

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Software

Customers

Routes and Trunks

Dialing and Numbering Plans

Phones

Tools

Security

Managing: 172.16.21.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

Node ID: 1006 \* (0-9999)

Call server IP address: 172.16.21.61 \*

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 172.16.21.254 \*

Subnet mask: 255.255.255.0 \*

Telephony LAN (TLAN)

Node IPv4 address: 172.16.20.60 \*

Subnet mask: 255.255.255.0 \*

Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value.

Save Cancel

Associated Signaling Servers & Cards

Select to add

Add

Remove

Make Leader

Print | Refresh

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

Show: ☐ IPv6 address

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

HG; Reviewed:  
SPOC 7/22/2014

Solution & Interoperability Test Lab Application Notes  
©2014 Avaya Inc. All Rights Reserved.

17 of 134  
Sask\_CS1KSMSBCE

## 5.2.2. Administer Terminal Proxy Server

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

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

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

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: \*

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

\* Required Value. Save Cancel

**Associated Signaling Servers & Cards**

Select to add Add Remove Make Leader Print Refresh

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

Show: ☐ IPv6 address

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

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

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

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

Firmware | DTLS | Network Connect Server

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

Firmware

IP address: 0.0.0.0  
Full file path: download/firmware  
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. Save Cancel

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

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

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

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

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

Node ID: 1006 \* (0-9999)  
Call server IP address: 172.16.21.61 \*  
TLAN address type: ☒ IPv4 only  
☐ IPv4 and IPv6

Embedded LAN (ELAN)  
Gateway IP address: 172.16.21.254 \*  
Subnet mask: 255.255.255.0 \*  
Telephone LAN (TLAN)  
Node IPv4 address: 172.16.20.60 \*  
Subnet mask: 255.255.255.0 \*  
Node IPv6 address: \*

**IP Telephony Node Properties**

- Voice Gateway (V/GW) and Codecs
- Quality of Service (QoS)**
- LAN
- SNTP
- Numbering Zones
- MCN 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 (SIP/H323), PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

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

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

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

**Diffserv Codepoint (DSCP)**

Enable Avaya automatic QoS: ☒

Control packets: 40 (0-63)  
Voice packets: 46 (0-63)  
VLAN tagging: ☒ 802.1Q support  
802.1Q bits value (802.1P): 6 (0-7)

\* Required Value. Save Cancel

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

## 5.3. Administer Voice Codec

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

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

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

**AVAYA CS1000 Element Manager** Help | Logout

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

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

Node ID: 1006 \* (0-9999)  
Call server IP address: 172.16.21.61 \* TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

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

**Telephony LAN (TLAN)**  
Node IPv4 address: 172.16.20.60 \*  
Subnet mask: 255.255.255.0 \*  
Node IPv6 address:

**IP Telephony Node Properties**

- ☒ **Voice Gateway (VGW) and Codecs**
- ☐ Quality of Service (QoS)
- ☐ LAN
- ☐ SIP
- ☐ 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 (SIPH323), PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv4 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.

The **Voice Gateway (VGW) and Codec** screen is displayed below. SaskTel supports codecs **G.711MU**, **G.711A** and **G.729A** (SaskTel preferred codec order) with **Voice Activity Detection (VAD)** disabled.

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

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

For Fax over IP, SaskTel supports **G.711Mu pass-through** (T.38 is not supported). (Refer to **Section 2.2**).

The following screenshot shows the General settings. **Modem/Fax pass-through** is selected for Node 1006; this enables the G.711 codec to be used for fax calls between the CS1000 and SaskTel. The **V.21 Fax tone detection** should be unchecked to disable T.38 fax capability on the SIP Trunk. Click the **Save** button.

The screenshot displays the 'CS1000 Element Manager' web interface. On the left is a navigation tree with categories like 'UCM Network Services', 'System', 'IP Network', and 'Nodes'. The 'Nodes' category is expanded, and 'Nodes: Servers, Media Cards' is selected. The main content area shows the configuration for 'Node ID: 1006 - Voice Gateway (VGW) and Codecs'. The 'General' tab is active, showing various settings. Under 'Signaling options', the 'Modem/Fax pass-through' checkbox is checked and highlighted with a red box. Other settings include 'Echo cancellation' (checked), 'Voice activity detection threshold' (-17), 'Idle noise level' (-65), and 'Voice Codescs' (G711: Enabled (required)). At the bottom, there are 'Save' and 'Cancel' buttons.

### 5.3.2. Synchronize the New Configuration

Continue from **Section 5.3.1**. Clicking on the Save button above will return to the **Node Details** page shown below, click on the **Save** button shown below.

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

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

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:

**IP Telephony Node Properties**

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

**Applications (click to edit configuration)**

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

\* Required Value. Save Cancel

**Associated Signaling Servers & Cards**

Select to add    Print | Refresh

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

Show: ☐ IPv6 address

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

The **Node Saved** screen is displayed. Click on **Transfer Now**.

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

**Node Saved**

Node ID: 1006 has been saved on the call server.

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

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

Show Nodes You may initiate a transfer manually at a later time.

The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server check box (**cs1k**), and click on the **Start Sync** button.

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

### Synchronize Configuration Files (Node ID <1006>)

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

[Start Sync](#) [Cancel](#) [Restart Applications](#) [Print](#) [Refresh](#)

Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence, Publisher, IP Media Services	Sync required

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

When the synchronization completes, check the Signaling Server (**cs1k**) check box again and click on the **Restart Applications** button.

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

### Synchronize Configuration Files (Node ID <1006>)

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

[Start Sync](#) [Cancel](#) [Restart Applications](#) [Print](#) [Refresh](#)

Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence, Publisher, IP Media Services	Synchronized

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



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

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

The screenshot displays the Avaya CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards, Maintenance and Reports, Media Gateways (highlighted), Zones, Host and Route Tables, Network Address Translation, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Software, Customers, Routes and Trunks, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area is titled 'CS1000 Element Manager' and shows configuration for two codecs. The first section is for 'Codec G711', with fields for 'Voice payload size' (20 ms/frame), 'Voice playout (jitter buffer) nominal delay' (40), and 'Voice playout (jitter buffer) maximum delay' (80). A red warning message states 'Modifications may cause changes to dependent settings'. The 'VAD' checkbox is unchecked. The second section is for 'Codec G729A', with similar fields for payload size (20 ms/frame), nominal delay (40), and maximum delay (80). A red warning message also states 'Modifications may cause changes to dependent settings'. The 'VAD' checkbox is checked. Below these sections are other codec options: 'Codec G723.1' (unchecked), 'Codec T38 FAX' (checked), '+ QoS', '+ Media Based CLID', and '- Call Server LAN'.

For Fax over IP, SaskTel supports **G.711Mu pass-through** (T.38 is not supported). (Refer to **Section 2.2**).

Under **VGW and IP phone codec profile**, ensure that **Enable V.21 FAX tone detection** is unchecked to disable T.38 fax capability on the SIP Trunk, and ensure that **Enable modem/fax pass through mode** is checked. Click on the **Save** button.

AVAYA CS1000 Element Manager Help | Logout

Telephony LAN (T-LAN) subnet mask 255.255.255.0

Hostname DB1

**- VGW and IP phone codec profile**

- Enable echo canceller ☒
- Echo canceller tail delay 128 (milliseconds)
- Enable dynamic attenuation ☒
- Voice activity detection threshold 1 (0 - 4 dBm)
- Idle noise level 0 (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 2
- FAX maximum rate 14400 (bps)
- FAX playout nominal delay 100 (0 - 300 milliseconds)
- FAX no activity timeout 20 (10 - 32000 milliseconds)
- FAX packet size 30

+ Codec	G711	Select	<input checked="" type="checkbox"/>
+ Codec	G729A	Select	<input checked="" type="checkbox"/>
+ Codec	G723.1	Select	<input type="checkbox"/>
+ Codec	T38 FAX	Select	<input checked="" type="checkbox"/>

+ QoS

+ Media Based CLID

+ Call Server LAN

Save Cancel VGW Channels

## 5.4. Administer Zones and Bandwidth

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

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

The screenshot displays the Avaya CS1000 Element Manager web interface. The top header shows the Avaya logo and the title 'CS1000 Element Manager'. A navigation sidebar on the left lists various system components, with 'Zones' selected and highlighted. The main content area, titled 'Zones', provides a description of their purpose and lists two sub-sections: 'Bandwidth Zones' (which is highlighted with a red rectangular box) and 'Numbering Zones'.

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

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

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

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

Follow **Section 5.4.2** to create a zone for the Virtual SIP Trunks. The difference is in the **Zone Intent (ZBRN)** field; for **ZBRN** select **VTRK** for virtual trunk, and then select **Best Quality (BQ)** for both **INTRA\_STGY** and **INTER\_STGY**, as shown below. Click on the **Save** button. For SaskTel, **Zone 4** was created for the Virtual SIP Trunks.

## 5.5. Administer SIP Trunk Gateway

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

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

The screenshot shows the CS1000 Element Manager interface. The left navigation pane has 'Customers' highlighted. The main area displays a table of customers. The table has columns for 'Customer Number', 'Total Routes', and 'Total Trunks'. There is one row with 'Customer Number' 00, 'Total Routes' 3, and 'Total Trunks' 17. The '00' is highlighted with a red box. Above the table are 'Add...' and 'Delete' buttons. A 'Refresh' button is in the top right of the table area. The top of the page shows the Avaya logo, 'CS1000 Element Manager', and user information: 'Managing: 172.16.21.61 Username: admin Customers'.

Customer Number	Total Routes	Total Trunks
10 00	3	17

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

The screenshot shows the CS1000 Element Manager 'Customer Details' page. The left navigation pane has 'Customers' highlighted. The main area lists various configuration options for customer 00. The 'Feature Packages' option is highlighted with a red box. The top of the page shows the Avaya logo, 'CS1000 Element Manager', and user information: 'Managing: 172.16.21.61 Username: admin Customers > Customer 00 > Customer Details'.

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

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

**AVAYA CS1000 Element Manager** Help | Logout

– UCM Network Services  
– Home  
+ Links  
+ System  
**+ Customers**  
+ Routes and Trunks  
– Dialing and Numbering Plans  
– Electronic Switched Network  
– Flexible Code Restriction  
– Incoming Digit Translation  
+ Phones  
+ Tools  
+ Security

– Integrated Services Digital Network  
+ Dial Access Prefix on CLID table entry option

Package: 145

Integrated Services Digital Network: ☒

– Virtual private network identifier:  (1 - 16383)

– Private network identifier:  (1 - 16383)

– Node DN:

Multi-location business group:  (0 - 65535)

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

Prefix 1:

Prefix 2:

Home number plan area code:  (200 - 999)

Prefix for central office:  (100 - 9999)

Local steering code:

Calling number type:

Redirection count for ISDN calls:

CLID information for incoming/outgoing calls:

Public service telephone networks: ☐

+ Network Attendant Service Package: 159  
+ Flexible Numbering Plan Package: 160  
+ Trunk Failure Monitor Package: 182  
+ Radio Paging Package: 187  
+ Commonwealth of Independent States -Trunk Package: 221  
+ Called Party Control on Internal Calls Package: 310  
+ M3900 Product Enhancement Package: 386  
+ IP Media Services Package: 422

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

Select **System** → **IP Network** → **Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen displayed, select the **Node ID** of the CS1000 system. 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 Session Manager (these are shown in **Section 6.6**).

- **Vtrk gateway application:** SIP Gateway (SIPGw).
- **SIP domain name:** avaya.lab.com
- **Local SIP port:** 5085.
- **Gateway endpoint name:** CS1KGateway.
- **Application node ID:** 1006.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar shows a navigation tree with 'Nodes: Servers, Media Cards' selected. The main content area is titled 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details'. The 'General' tab is active, showing the 'Vtrk gateway application' set to 'SIP Gateway (SIPGw)' and 'Enable gateway service on this node' checked. Other fields include 'SIP domain name' (avaya.lab.com), 'Local SIP port' (5085), 'Gateway endpoint name' (CS1KGateway), and 'Application node ID' (1006). A 'Virtual Trunk Network Health Monitor' section is also visible on the right.

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the values highlighted in red boxes for the Primary TLAN, and Secondary TLAN if one exists, and retain the default values for the remaining fields as shown below. For the compliance testing only the Primary TLAN was configured. Values shown correspond to the IP address, Port, and Transport protocol of the Session Manager SIP Entity (created in **Section 6.5**).

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes, Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Software, Customers, Routes and Trunks, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, and Tools. The main content area is titled 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details'. It has tabs for General, SIP Gateway Settings, and SIP Gateway Services. The 'SIP Gateway Settings' tab is active, showing the 'Proxy or Redirect Server' section. This section has a sub-section 'Proxy Server Route 1:' which contains a red-bordered box. Inside this box are the following fields: 'Primary TLAN IP address:' with the value '172.16.5.32', 'Port:' with the value '5085', and 'Transport protocol:' with a dropdown menu set to 'UDP'. Below this box, there are checkboxes for 'Support registration' and 'Primary CDS proxy'. Further down, there are fields for 'Secondary TLAN IP address:' with the value '0.0.0.0', 'Port:' with the value '5060', and 'Transport protocol:' with a dropdown menu set to 'UDP'. At the bottom of the form, there are 'Save' and 'Cancel' buttons. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

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

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

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

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

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

**Note:** The SIP URI Map entries shown above were used during the compliance testing; it is possible that in a customer environment other values are used.



Click on the **Save** button and synchronize the new configuration as shown under **Section 5.3.2**.

AVAYA CS1000 Element Manager

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

National:

Subscriber:

Special number:

Unknown:

Private domain names

UDP:

CDP:

Special number:

Vacant number:

Unknown:

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

## 5.5.2. Administer Virtual D-Channel

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

AVAYA CS1000 Element Manager

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)  
ISDL Diagnostics (LD 96)  
TMDI Diagnostics (LD 96)  
D-Channel Expansion Diagnostics (LD 48)

Configuration

Choose a D-Channel Number:  and type:

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

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

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

AVAYA CS1000 Element Manager Help | Logout

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

### D-Channels 0 Property Configuration

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 #102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<a href="#">more PRI</a>
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

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

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

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

Retain the default values for the remaining fields.

**AVAYA CS1000 Element Manager** Help | Logout

Release ID of the switch at the far end: 2.2

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)**

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

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

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

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

- Remote Capabilities: Edit

**+ - Change protocol timer value (TMR)**

**- 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 Timer:

- Multilocation Business Group Allowed: ☐

**- Network Attendant Service Allowed: ☒**

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

**+ Feature Packages**

Submit Refresh Delete Cancel

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

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

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

**- Basic options (BSCOPT)**

PRI loop number for Backup D-channel:   
 User: Integrated Services Signaling Link Dedicated (ISLD) \*  
 Interface type for D-channel: Meridian Meridian1 (SL1)  
 Country: ETS 300 102 basic protocol (ETSI)  
 D-Channel PRI loop number:   
 Primary Rate Interface:  [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  
 Primary D-channel for a backup DCH:  Range: 0 - 254  
 - PINX customer number:   
 - Progress signal:   
 - Calling Line Identification:   
 - Output request Buffers: 32  
 - D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)  
 - Channel Negotiation option: No alternative acceptable, exclusive. (1)  
 - Remote Capabilities: [Edit](#)  
 - B channel Service messaging: ☐

+ - Change protocol timer value (TIMR)  
 + Advanced options (ADVOPT)  
 + Feature Packages

[Submit](#) [Refresh](#) [Delete](#) [Cancel](#)

The **Remote Capabilities Configuration** page will appear. Check **ND2** and **MWI** (if mailboxes are present on the CS1000 Call Pilot) checkboxes as shown below.

Click on **Return – Remote Capabilities** button.

Click on the **Submit** button shown at the bottom of the previous screen.

**AVAYA CS1000 Element Manager** Help | Logout

- UCM Network Services
  - Home
  - + Links
  - 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
  - + Tools
  - + Security

☐ Diversion info. is sent using object identifier (DV10)  
☐ Rerouting requests processed using integer value (DV2)  
☐ Rerouting requests processed using object identifier (DV20)  
☐ Diversion info. sent. rerouting requests processed (DV3)  
☐ EuroISDN - div. info sent. rerouting req. processed (DV30)  
☐ Call transfer notification and invocation to EuroISDN (ECTO)  
☐ Malicious call identification (MCID)  
☐ MCDN QSIG conversion (MQC)  
☐ Remote D-channel is on a MSDL card (MSL)  
☒ Message waiting interworking with DMS-100 (MWI)  
☐ Network access data (NAC)  
☐ Network call trace supported (NCT)  
☐ Network name display method 1 (ND1)  
☒ Network name display method 2 (ND2)  
☐ Network name display method 3 (ND3)  
☐ Name display - integer ID coding (NDI)  
☐ Name display - object ID coding (NDO)  
☐ Path replacement uses integer values (PRI)  
☐ Path replacement uses object identifier (PRO)  
☐ Release Link Trunks over IP (RLTI)  
☐ Remote virtual queuing (RVQ)  
☐ Trunk anti-tromboning operation (TAT)  
☐ User to user service 1 (UUS1)  
☐ NI-2 name display option. (NDS)  
☐ Message waiting indication using integer values (QMWI)  
☐ Message waiting indication using object identifier (QMWI)  
☐ User to user signalling (UUI)

Return - Remote Capabilities Cancel

### 5.5.3. Administer Virtual Superloop

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

**AVAYA CS1000 Element Manager** Help | Logout

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

**Superloops**

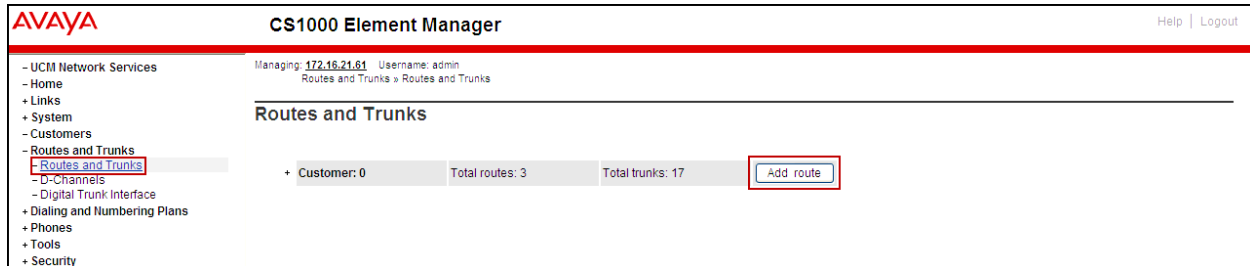
Add... Delete Refresh

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

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

### 5.5.4. Administer Virtual SIP Routes

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



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

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

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 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): RDB

Customer number (CUST): 00

Route number (ROUT): 0

Designator field for trunk (DES): SERVICE PROVIDE

Trunk type (TKTP): TIE

Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)

Access code for the trunk route (ACOD): 7916

Trunk type M911P (M911P): ☐

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

- Zone for codec selection and bandwidth management (ZONE): 00004 (0 - 8000)

- Node ID of signalling server of this route (NODE): 1006 (0 - 9999)

- Protocol ID for the route (PCID): SIP (SIP)

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

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

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE): Route uses ISDN Signalling Link (ISLD)

- D channel number (DCH): 0 (0 - 254)

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

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

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- **Insert ESN access code (INAC):** Check box.

Click on **Basic Route Options**,

- Check **North American toll scheme (NATL)**.
- Check **Incoming DID digit conversion on this route (IDC)** and input **DCNO 0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown in screenshot below. The IDC is discussed in **Section Error!** Reference source not found..
- Click on the **Submit** button shown at the bottom of the screen.



### 5.5.5. Administer Virtual Trunks

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

AVAYA CS1000 Element Manager Help | Logout

Managing: 172.16.21.81 Username: admin  
Routes and Trunks > Routes and Trunks

#### Routes and Trunks

- Customer: 0 Total routes: 3 Total trunks: 17 [Add route](#)

+ Route: 0	Type: TIE	Description: SERVICE PROVIDER	<a href="#">Edit</a>	<a href="#">Add trunk</a>
+ Route: 1	Type: IMUS	Description: MUSIC	<a href="#">Edit</a>	<a href="#">Add trunk</a>
+ Route: 96	Type: TIE	Description: SIP_ROUTE	<a href="#">Edit</a>	<a href="#">Add trunk</a>

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

Note: The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 11 trunks were created.

- **Trunk data block (TYPE): IP Trunk (IPTI).**
- **Terminal Number (TN):** Available terminal number (use virtual superloop created in Section 5.5.3).
- **Designator field for trunk (DES):** A descriptive text.
- **Extended Trunk (XTRK): Virtual trunk (VTRK).**
- **Member number (RTMB):** Starting member.
- **Start arrangement Incoming (STRI): Immediate (IMM).**
- **Start arrangement Outgoing (STRO): Immediate (IMM).**
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level.
- **Channel ID for this trunk (CHID):** An available starting channel ID.

AVAYA CS1000 Element Manager Help | Logout

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

Customer 0, Route 0, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:  \*

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

+ Advanced Trunk Configurations

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

AVAYA

CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
- System
- Customers
- Routes and Trunks
- B-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Phones
- Tools
- Security

Class of Service Configuration

- Class of Service

Input Description	Input Value
- ACD Priority:	ACD Priority not required (APN)
- Analog Semi-Permanent Connections:	Analog Semi-Permanent Connections Denied (SPCD)
- ARF Supervised COT:	
- Barring:	
- Battery Supervised COT:	
- Busy Tone Supervised COT:	
- Calling party:	Calling party Denied (CND)
- Central Office Ringback:	
- Centrex Switchhook Flash:	Centrex Switchhook Flash Denied (THFD)
- Dial Pulse:	Dial Pulse (DIP)
- DTR PAD value:	
- Echo Canceling:	Echo Canceling Denied (ECD)
- Hong Kong DTI:	
- Loop Break Supervised COT:	
- Make-break ratio for dial pulse:	10 pulses per second (P10)
- Manual Incoming:	Manual Incoming Denied (MID)
- Media Security:	Media Security Never (MSNV)
- Network Hook Flash Over M911P:	
- Polarity:	
- Priority:	Low Priority (LPR)
- Restriction level:	Unrestricted (UNR)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- Short or long line:	
- Transmission Class of Service:	Non-Transmission Compensated (NTC)
- Warning Tone:	Warning Tone Allowed (WTA)

## 5.5.6. Administer Calling Line Identification Entries

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

**AVAYA CS1000 Element Manager** Help | Logout

**General Properties**

Flexible trunk to trunk connection option: **Connections restricted**

Flexible orbiting prevention timer: **5**

Country code: **1** (0 - 9999)

Code for processing the called number

National access code: **1**

International access code: **011**

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

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan: **Private dialing plan**

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

Extended Local Calls: ☐

Extended Local Calls for IMS Line user: ☐

Extended Local Calls Route list index: **1** (0 - 1999)

**Calling Line Identification**

Information for incoming/outgoing calls: **No manipulation is done**

Size: **256** (0 - 4000)

Country code: **1** (0 - 9999)

Code displayed as part of calling number

**Calling Line Identification Entries**

Save Cancel

Click on **Add** as shown below.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: **172.16.21.61** Username: admin  
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries

**Calling Line Identification Entries**

Search for CLID

Start range: **1**

End range: **2**

End range should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add... Delete Refresh

	Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1	0	306	777	50		NO	
2	1	306	777	51		NO	
3	2	306	777	52		NO	
4	3	306	777	53		NO	
5	4	306	777	54		NO	
6	5	306	777	55		NO	
7	6	306	777	56		NO	
8	7	306	777	57		NO	

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 **306**.
- **Local Code:** input the seven digit number of the DID assigned by Service Provider, in this case it is **777xx50** (Note that 2 digits have been masked with “x” for security reasons).
- **Use DN as DID:** Select **NO**.
- **Calling Party Name Display:** Uncheck for **Roman characters**.

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

**AVAYA CS1000 Element Manager** Help | Logout

Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » New Calling Line Identification

### New Calling Line Identification

**General Properties**

Entry Id:  (0 - 255)

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

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

Local Steering Code:  (1-7 digits)

Use DN as DID:

**Emergency Services Access**

Emergency Local Code:  (1-12 digits)  
Code for home local number during Emergency calls

Emergency Options: ☐ Home national number for emergency services access calls  
☒ Append the originating directory number for emergency services access calls

**Calling Party Name Display**

Roman characters: ☐

CPND Name:   
first name, last name

Expected Length:

Display Format:

The following screen shows the **Calling Line Identification Entries** used for the compliance testing.

**AVAYA**
CS1000 Element Manager
Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
+ Dialing and Numbering Plans
+ Phones
+ Tools
+ Security

Managing: 172.16.21.81 Username: admin  
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries

### Calling Line Identification Entries

Search for CLID

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

Calling Line Identification Entries

<input type="checkbox"/>	Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
<input type="checkbox"/>	1 0	306	777	50		NO	
<input type="checkbox"/>	2 1	306	777	51		NO	
<input type="checkbox"/>	3 2	306	777	52		NO	
<input type="checkbox"/>	4 3	306	777	53		NO	
<input type="checkbox"/>	5 4	306	777	54		NO	
<input type="checkbox"/>	6 5	306	777	55		NO	
<input type="checkbox"/>	7 Z	306	777	56		NO	
<input type="checkbox"/>	8 8	306	777	57		NO	

## Enable External Trunk to Trunk Transfer:

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

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

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

```
....
TRNX yes
EXTT yes
....
```

## 5.6. Administer Dialing Plans

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

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

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

The screenshot displays the Avaya CS1000 Element Manager web interface. The top header shows the Avaya logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". The left navigation pane lists various configuration categories, with "Dialing and Numbering Plans" and its sub-item "Electronic Switched Network" highlighted. The main content area is titled "Electronic Switched Network (ESN)" and shows a tree structure of configuration options. Under "Customer 00", the "Network Control & Services" section is expanded, and "ESN Access Codes and Parameters (ESN)" is selected and highlighted with a red box. Other visible sections include "Coordinated Dialing Plan (CDP)" and "Numbering Plan (NET)".

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

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

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

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

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

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



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

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

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

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

The screenshot displays the Avaya CS1000 Element Manager web interface. The top header shows the Avaya logo and 'CS1000 Element Manager'. Below the header, a navigation pane on the left lists various system components, with 'Dialing and Numbering Plans' expanded to show 'Electronic Switched Network'. The main content area is titled 'Electronic Switched Network (ESN)' and shows a tree view for 'Customer 00'. Under 'Network Control & Services', the 'Digit Manipulation Block (DGT)' is highlighted with a red box. Other visible options include 'Network Control Parameters (NCTL)', 'ESN Access Codes and Parameters (ESN)', 'Home Area Code (HNPA)', 'Flexible CLID Manipulation Block (CLMDB)', 'Free Calling Area Screening (FCAS)', 'Free Special Number Screening (FSNS)', 'Route List Block (RLB)', 'Incoming Trunk Group Exclusion (ITGE)', and 'Network Attendant Services (NAS)'. At the bottom, there are links for 'Coordinated Dialing Plan (CDP)' and 'Numbering Plan (NET)'.

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

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

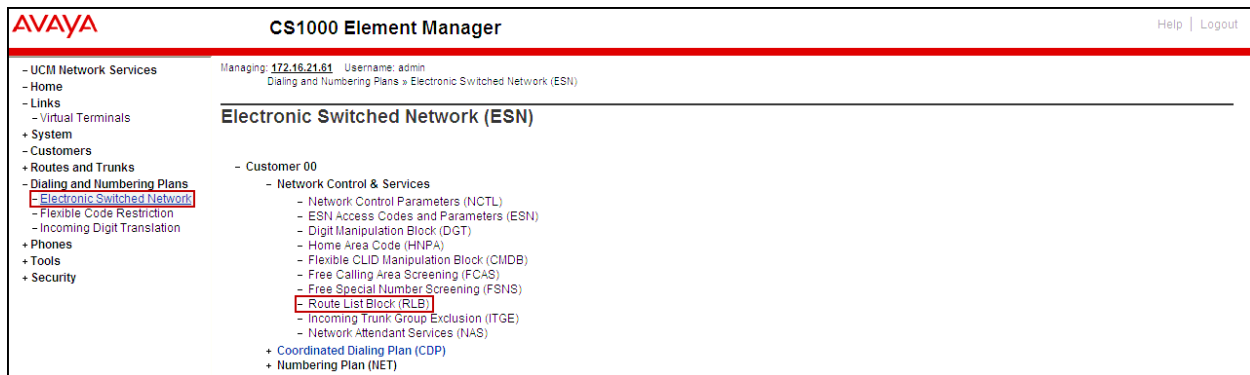
The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Electronic Switched Network (highlighted), Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area is titled "Digit Manipulation Block List". It displays a table with two entries: "Digit Manipulation Block Index -- 1" and "Digit Manipulation Block Index -- 2", each with an "Edit" link. Above the table, there is a dropdown menu labeled "Please choose the" with "Digit Manipulation Block Index 3" selected, and a "to Add" button. The top of the page shows the AVAYA logo, "CS1000 Element Manager", and "Help | Logout" links. The bottom status bar indicates "Managing: 172.16.21.61 Username: admin" and the breadcrumb "Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List".

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**, then click **Submit** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface for configuring a "Digit Manipulation Block". The left sidebar is the same as the previous screenshot, with "Electronic Switched Network" highlighted. The main content area is titled "Digit Manipulation Block". It contains the following fields: "Digit Manipulation Index numbers:" with a value of "1"; "Number of leading digits to be deleted:" with a value of "0" and a range "(0 - 19)"; "Insert:" with an empty text field; "IP Special Number:" with a checkbox; and "Call Type to be used by the manipulated digits:" with a dropdown menu set to "NPA (NPA)". At the bottom right, there are four buttons: "Submit", "Refresh", "Delete", and "Cancel". The top of the page shows the AVAYA logo, "CS1000 Element Manager", and "Help | Logout" links. The bottom status bar indicates "Managing: 172.16.21.61 Username: admin" and the breadcrumb "Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block".

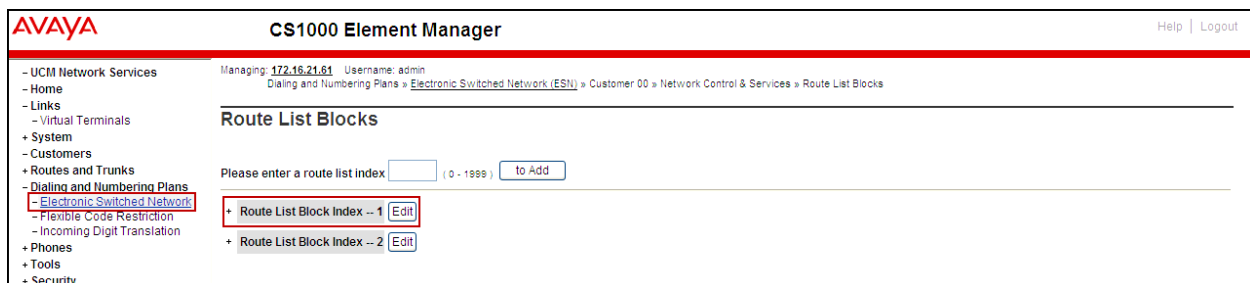
#### 5.6.4. Route List Block (RLB)

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



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

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



Enter the following values for the specified fields, and retain the default values for the remaining fields as shown below. Scroll down to the bottom of the screen, and click on the **Submit** button.

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

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks » Route List Block » Data Entry of a Route List Block

### Data Entry of a Route List Block

Route List Block Index: 1

**General Properties**

Entry Number for the Route List: 0

**Indexes**

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

**Digit Manipulation Index: 1**

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

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: ☐

Incoming CLID Table: 0 (0 - 255)

**Options**

Local Termination entry: ☐

**Route Number: 0**

Skip Conventional Signaling: ☐

Display Originator's Information: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

## 5.6.5. Inbound Digit Translation

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

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

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Incoming Digit Translation

### Incoming Digit Translation

- Customer: 00 **Edit IDC**

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

The screenshot displays the Avaya CS1000 Element Manager interface. The top header includes the Avaya logo and the title 'CS1000 Element Manager'. Below the header, the left sidebar contains a navigation menu with the following items: 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 (highlighted with a red box), Phones, Tools, and Security. The main content area is titled 'Customer 00 Incoming Digit Conversion Property'. It displays a table with 10 rows, each representing a digit conversion tree number from 0 to 9. Each row has a 'New DCNO' button. The first row (0) is highlighted with a red box, and its 'Edit DCNO' button is also highlighted. At the bottom of the table, there are 'Refresh' and 'Cancel' buttons. The top right corner of the interface shows 'Help | Logout'.

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

Detailed configuration of the **DCNO** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 system extension number. This **DCN0** has been assigned to route 0 as shown in **Section 5.5.4**

In the following configuration, the incoming call from the PSTN with the prefix 306777xx50 will be translated to the CS1000 extension number 8002 (note that 2 digits have been masked with “x” for security reasons).

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration » Add Incoming Digits

### Add Incoming Digits

Incoming Digits: 306777xx50  
Converted digits: 8002 (0 - 9999999)

Force storage or removal of data: ☐ In case of conflict between the new and existing Incoming Digits, force storage or removal may result in loss of portions of the tree.

CPND language: ☒ Roman characters  
CPND Name:   
first name, last name  
Expected length:   
Display format: First name, Last name  
☐ Katakana characters  
CPND Name:   
first name, last name  
Expected length:   
Display format: First name, Last name

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

The following screen shows the Incoming Digit Translations used during the compliance testing (note that 2 digits have been masked for security reasons)

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration

### Digit Conversion Tree 0 Configuration

Regular IDC tree  
Send calling party DID disabled

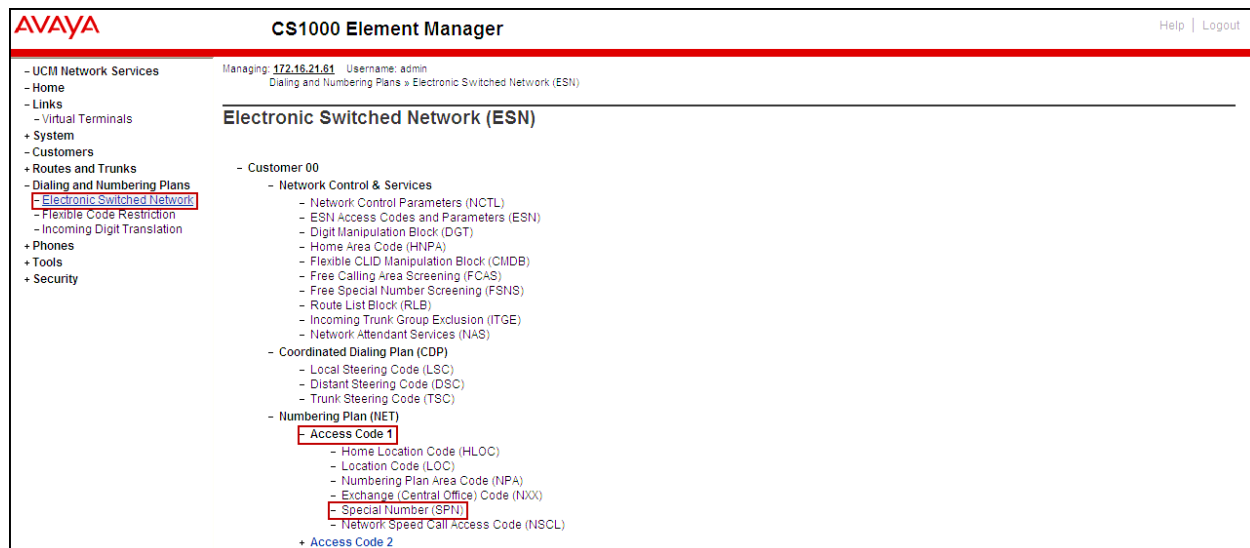
	Incoming Digits	Converted Digits	CPND Name	CPND language
1	306777xx50	8002	.	Roman characters
2	306777xx51	8007	.	Roman characters
3	306777xx52	8020	.	Roman characters
4	306777xx53	8011	.	Roman characters
5	306777xx54	8017	.	Roman characters
6	306777xx55	8004	.	Roman characters
7	306777xx56	8056	.	Roman characters
8	306777xx57	8050	.	Roman characters

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

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

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

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Under **Access Code 1**, select **Special Number (SPN)** as shown below.



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

#### Special Number: 0

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

#### Special Number: 011

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

#### Special Number: 1

- **Flexible length:** 11.
- **CallType:** NATL.

- **Route list index:** 1, created in **Section 5.6.4.**

#### **Special Number: 411**

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

#### **Special Number: 911**

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

Add any other special numbers as required.

**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

**Special Number -- 0** [Edit]

Flexible length: 0  
International dialing plan: NO  
Type of call that is defined by the special number: NONE  
Route list index: 1

**Special Number -- 011** [Edit]

Flexible length: 15  
Inhibit time-out handler: NO  
Type of call that is defined by the special number: NONE  
Route list index: 1

**Special Number -- 1** [Edit]

Flexible length: 11  
Inhibit time-out handler: NO  
Type of call that is defined by the special number: NATL  
Route list index: 1

+ Special Number -- 326 [Edit]

**Special Number -- 411** [Edit]

Flexible length: 3  
Inhibit time-out handler: NO  
Type of call that is defined by the special number: NONE  
Route list index: 1

+ Special Number -- 5 [Edit]

+ Special Number -- 611 [Edit]

+ Special Number -- 7 [Edit]

+ Special Number -- 8 [Edit]

**Special Number -- 911** [Edit]

Flexible length: 3  
Inhibit time-out handler: NO  
Type of call that is defined by the special number: NONE  
Route list index: 1

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

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

## **5.7. Administer Phone**

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

### **5.7.1. Phone creation**

Refer to **Section 5.5.3** to create a virtual superloop - **8** used for IP phone.

Refer to **Section 5.4.1** to create a bandwidth zone - **5** for IP phone.



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

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

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

**Note:** For CS1000 FAX over IP Support recommendation, refer to the Avaya Product Support Notice (PSN) referred to in **Section 11** [7], including the “**Analog Station Provisioning for V.34 Fax and Modem**” and “**Minimum Vintage Loadware Recommendation**” for MGC.

**The analog station used for fax should be provisioned as follows:**

**Analog Station Provisioning for V.34 Fax and Modem** (this setting is required for G.711 fax pass-through):

TYPE 500 .....Analog Station Type  
DN 3500.....Extension Number  
CLS DTN .....Digitone (DTMF)  
CLS FAXD .....Fax Class of Service  
CLS MPTA.....Will use the G.711 codec with optimizations when V.34 modem tones are detected.

### 5.7.2. Enable Privacy for Phone

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

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

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

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

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

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

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

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

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

### 5.7.3. Enable Call Forward for the Phone

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

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

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header shows the AVAYA logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". Below the header, a navigation pane on the left lists various system components, with "Customers" highlighted. The main content area is titled "Customers" and includes a table with columns for "Customer Number", "Total Routes", and "Total Trunks". A single row is visible, showing "00" for the customer number, "3" for total routes, and "17" for total trunks. The "00" in the customer number column is highlighted with a red box.

Customer Number	Total Routes	Total Trunks
00	3	17

Select **Call Redirection** as shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header bar includes the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. Below the header, a navigation sidebar on the left lists various system components: UCM Network Services, Home, Links, Virtual Terminals, System, Customers (highlighted with a red box), Routes and Trunks, Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area, titled 'Customer Details', shows a list of configuration options for a specific customer. The 'Call Redirection' option is highlighted with a red box. Other visible options include Basic Configuration, Application Module Link, Attendant, Call Detail Recording, Call Party Name Display, 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, and Timers.

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

Set the following fields:

- **Total redirection count limit: 0** (unlimited).
- **Call Forward: Check Originating.**
- **Number of normal ring cycles of CFNA: 4.**
- Click on **Save**.

**AVAYA** CS1000 Element Manager Help | Logout

Days for day option 3:

Redirection Holidays

Do not disturb hunting: ☐

Total redirection count limit:

Options:

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

Call forward: ☒ Originating ☐ Forwarding

Number of normal ringing cycles for CFNA

Option 0:

Option 1:

Option 2:

Number of distinctive ringing cycles for CFNA

Option 0:

Option 1:

Option 2:

Calls routed to message center

No answer DID calls: ☐

No answer non-DID calls: ☐

DID calls to busy telephones: ☐

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

```
REQ: prt
TYPE: 2050pc
TN 8003
CLS UNR FBA WTA LPR MTD FNA HTA 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 CCBF 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 ELCD
```

```
.....
19 CFW 12 919195551212
```

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

```
REQ: prt
TYPE: 2050pc
TN 8003
.....
CLS UNR FBA WTA LPR MTD 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 CCBF 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 ELCD
```

```
CPND LANG ENG
RCO 0
EFD 8004
HUNT 919195551212
.....
```

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

```
REQ: prt
TYPE: 2050pc
TN 8003
....
FDN 919195551234
....
CLS UNR FBA WTA LPR MTD FNA HTA TOD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDA CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID DNAA BUZZ
UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRD
USMD USRD ULAD 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.

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

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



## 6. Configure Avaya Aura® Session Manager

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

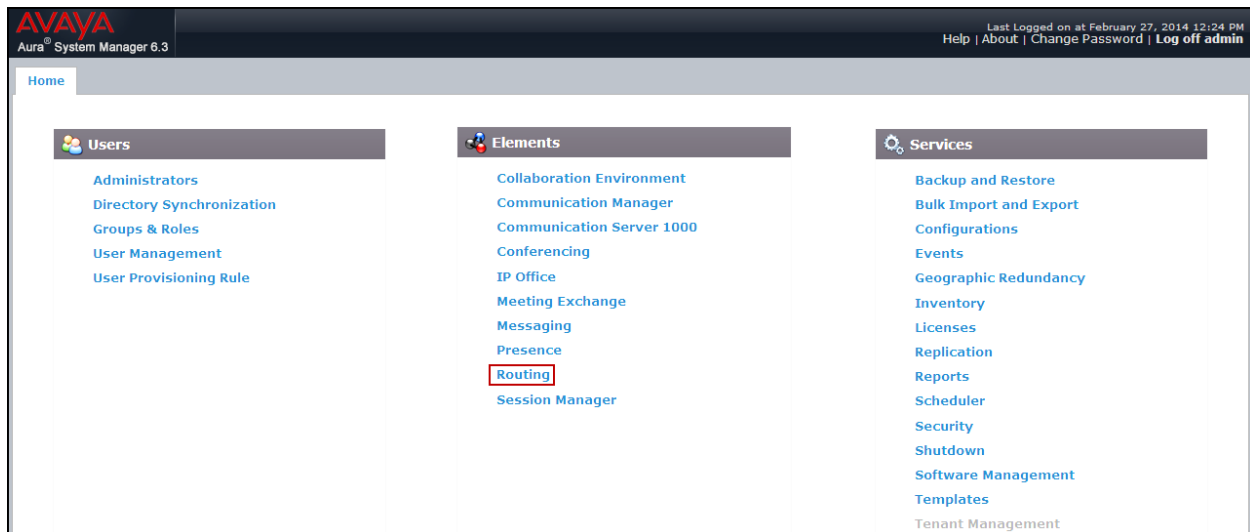
- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to the CS1000, the Avaya SBCE, and Session Manager itself.
- Entity Links, which define the SIP trunk parameters used by Session Manager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

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

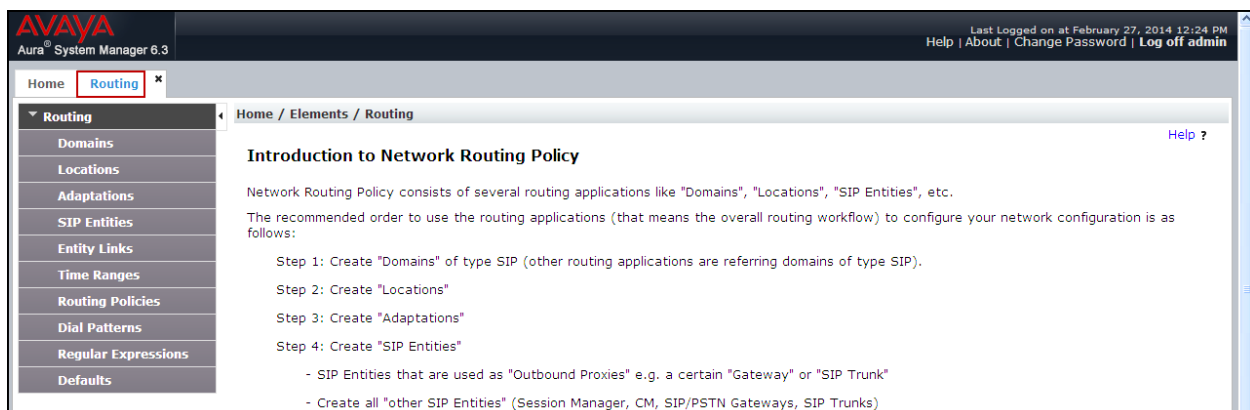
<b>Note:</b> Some of the default information in the screenshots that follow may have been cut out (not included) for brevity
--

## 6.1. System Manager Login and Navigation

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



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



## 6.2. Specify SIP Domain

Create a SIP domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test the enterprise domain **avaya.lab.com** was used.

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** to save.

The screen below shows the entry for the enterprise domain **avaya.lab.com**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header shows the Avaya logo and 'Aura System Manager 6.3'. The left navigation pane has 'Routing' and 'Domains' highlighted. The main content area is titled 'Domain Management' and shows a table with one item. The table has columns for Name, Type, and Notes. The Name column contains 'avaya.lab.com', the Type column contains 'sip', and the Notes column contains 'Lab-HG Domain'. There are 'Commit' and 'Cancel' buttons at the bottom of the table.

Name	Type	Notes
avaya.lab.com	sip	Lab-HG Domain

## 6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the 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).
- Click **Commit** to save.

The screen below shows the **HG Session Manager** location. This location will be assigned later to the SIP Entity corresponding to Session Manager.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains a 'Location Details' form. The 'General' section is active, showing the 'Name' field set to 'HG Session Manager' and the 'Notes' field empty. Below this, the 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section includes fields for 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', and 'Multimedia Bandwidth', with a checked box for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section shows 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)' both set to '1000 Kbit/Sec', and 'Minimum Multimedia Bandwidth' set to '64 Kbit/Sec'. The 'Alarm Threshold' section shows 'Overall Alarm Threshold' and 'Multimedia Alarm Threshold' both set to '80 %', with 'Latency before Overall Alarm Trigger' and 'Latency before Multimedia Alarm Trigger' both set to '5 Minutes'. The 'Location Pattern' section at the bottom has an 'Add' button and a table with one row: 'IP Address Pattern'. The interface includes a top header with the Avaya logo and 'Last Logged on at February 27, 2014 12:24 PM', and a bottom footer with 'Commit' and 'Cancel' buttons.

The following screen shows the **CS1k Node** location. This location will be assigned later to the SIP Entity corresponding to the CS1000.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and a user status bar indicating 'Last Logged on at February 27, 2014 12:24 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows a tree view with 'Routing' expanded and 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains a 'Location Details' form for 'CS1k Node'. The form includes a 'General' section with fields for 'Name' (CS1k Node) and 'Notes' (CS1K7.6). Below this is the 'Dial Plan Transparency in Survivable Mode' section with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (Kbit/sec), 'Total Bandwidth', 'Multimedia Bandwidth', and a checked 'Audio Calls Can Take Multimedia Bandwidth' checkbox. The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'. The 'Alarm Threshold' section includes 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', and latency settings for both. The 'Location Pattern' section at the bottom has 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' button. 'Commit' and 'Cancel' buttons are present at the top right and bottom right of the form.

AVAYA  
Aura System Manager 6.3

Last Logged on at February 27, 2014 12:24 PM  
Help | About | Change Password | Log off admin

Home Routing x

Home / Elements / Routing / Locations

Location Details

Commit Cancel

Help ?

General

\* Name: CS1k Node

Notes: CS1K7.6

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

\* Minimum Multimedia Bandwidth: 64 Kbit/Sec

\* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

\* Latency before Overall Alarm Trigger: 5 Minutes

\* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

Filter: Enable

IP Address Pattern

Notes

Commit Cancel

The following screen shows the **HG ASBCE** location. This location will be assigned later to the SIP Entity corresponding to the Avaya SBCE.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and a user status bar indicating 'Last Logged on at February 27, 2014 12:24 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows a tree view with 'Routing' expanded and 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains several sections: 'Location Details' with 'Name' (HG ASBCE) and 'Notes' (HG Avaya SBCE) fields; 'General' with an 'Enabled' checkbox; 'Dial Plan Transparency in Survivable Mode' with fields for 'Listed Directory Number' and 'Associated CM SIP Entity'; 'Overall Managed Bandwidth' with fields for 'Managed Bandwidth Units', 'Total Bandwidth', and 'Multimedia Bandwidth'; 'Per-Call Bandwidth Parameters' with fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'; 'Alarm Threshold' with fields for 'Overall Alarm Threshold', 'Multimedia Alarm Threshold', and latency triggers; and 'Location Pattern' with an 'Add' button and a table showing 0 items. The interface includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

AVAYA  
Aura System Manager 6.3

Last Logged on at February 27, 2014 12:24 PM  
Help | About | Change Password | Log off admin

Home Routing x

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

\* Name: HG ASBCE

Notes: HG Avaya SBCE

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

\* Minimum Multimedia Bandwidth: 64 Kbit/Sec

\* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

\* Latency before Overall Alarm Trigger: 5 Minutes

\* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

Filter: Enable

IP Address Pattern

Notes

Commit Cancel

## 6.4. Add Adaptation Module

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

The adaptation named **CS1K76** shown on the screen below was created. It will later be assigned to the SIP Entity corresponding to the CS1000.

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **CS1000Adapter** from the drop-down menu (or type the adapter name if not previously defined).
- Click **Commit** to save.

The following screen shows the **CS1K76** adaptation. This adaptation will be assigned later to the SIP Entity corresponding to the CS1000.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The 'Routing' tab is selected in the top navigation bar, and the 'Adaptations' sub-tab is active. The 'General' section of the 'Adaptation Details' form is shown, with 'Adaptation Name' set to 'CS1K76' and 'Module Name' set to 'CS1000Adapter'. Below this, there are fields for 'Module Parameter Type', 'Egress URI Parameters', and 'Notes'. The interface also features two sections for 'Digit Conversion', one for incoming calls and one for outgoing calls, each with an 'Add' button and a table for defining conversion rules. The sidebar on the left contains links to various system components, and the top right corner shows the user's login status and options to help, about, change password, or log off.

A second adaptation named **HG SBCE** shown below was created. This adaptation will later be assigned to the SIP Entity corresponding to the Avaya SBCE.

The adaptation uses the **DigitConversionAdapter**. **MIME** set to **no** will remove MIME types inserted by the CS1000 which are not used for call processing and should not be sent to SaskTel.

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DigitConversionAdapter**.
- **Module parameter Type:** Click **Add**
  - **Name:** Enter **MIME**.
  - **Value:** Enter **no**.
- Click **Commit** to save.

The following screen shows the **HG SBCE** adaptation. This adaptation will be assigned later to the SIP Entity corresponding to the Avaya SBCE.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'Adaptation Details' and includes a 'General' tab. A red box highlights the 'Adaptation Name' field (containing 'HG SBCE'), the 'Module Name' dropdown (set to 'DigitConversionAdapter'), and the 'Module Parameter Type' dropdown (set to 'Name-Value Parameter'). Below these, there is an 'Add' button and a table with two rows: 'Name' (containing 'MIME') and 'Value' (containing 'no'). The 'Egress URI Parameters' and 'Notes' fields are also visible. At the bottom, there are sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM', each with an 'Add' button and a table with columns: 'Matching Pattern', 'Min', 'Max', 'Phone Context', 'Delete Digits', 'Insert Digits', 'Address to modify', 'Adaptation Data', and 'Notes'. The interface includes 'Commit' and 'Cancel' buttons at the top right and bottom right.



## 6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it, which includes the CS1000 and 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).

Add the SIP entity for Session Manager, as follows:

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, in this case the IP address of the Session Manager Security Module Interface.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for the 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 in **Section 6.4**.
- **Location:** Select one of the locations defined in **Section 6.3**.
- **Time Zone:** Select the time zone which the entity belongs to.

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

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

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 CS1000.
- Click **Commit** to save.

The following screen shows the addition of the **HG Session Manager** SIP Entity. This SIP Entity will be assigned later to the Entity Link corresponding to the CS1000 and the Avaya SBCE.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields:

- Name:** HG Session Manager
- FQDN or IP Address:** 172.16.5.32
- Type:** Session Manager
- Notes:** HG Session Manager
- Location:** HG Session Manager
- Outbound Proxy:** (empty)
- Time Zone:** America/New\_York
- Credential name:** (empty)

Below the form, there is a 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. Under the 'Port' section, there are input fields for 'TCP Failover port' and 'TLS Failover port', and 'Add' and 'Remove' buttons. A table lists 9 items with columns for 'Port', 'Protocol', 'Default Domain', and 'Notes':

Port	Protocol	Default Domain	Notes
5060	TCP	avaya.lab.com	
5085	UDP	avaya.lab.com	

Below the table, there is a 'SIP Responses to an OPTIONS Request' section with 'Add' and 'Remove' buttons. A table lists 0 items with columns for 'Response Code & Reason Phrase', 'Mark Entity Up/Down', and 'Notes':

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

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

A separate SIP entity for the CS1000, other than the one created for Session Manager during installation, is required in order to route calls to the CS1000.

For the compliance testing, the following values were used:

- **Name:** Enter a descriptive name.
- The **FQDN or IP Address** field is set to the TLAN IP address of the CS1000 Signaling Gateway (Node IP address), refer to **Section 5.2.1**.
- For Adaptation select the **CS1K76** adaptation defined in **Section 6.4**.
- For Location select the **CS1k Node** location defined in **Section 6.3**.

The following screen shows the addition of the **CS1K76** SIP entity. This SIP Entity will be assigned later to the Entity Link corresponding to the CS1000.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 6.3", and a user status bar indicating "Last Logged on at February 27, 2014 12:24 PM" with links for "Help", "About", "Change Password", and "Log off admin". The left sidebar contains a menu with "Routing" selected, and sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted with a red box), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the "SIP Entity Details" form for "CS1K76". The form is titled "SIP Entity Details" and has "Commit" and "Cancel" buttons. The "General" tab is active. The form fields are: \* Name: CS1K7.6; \* FQDN or IP Address: 172.16.20.60; Type: Other (dropdown); Notes: CS1000 Rel. 7.6; Adaptation: CS1K76 (dropdown); Location: CS1k Node (dropdown); Time Zone: America/New\_York (dropdown); \* SIP Timer B/F (in seconds): 4; Credential name: (empty field); Call Detail Recording: none (dropdown); CommProfile Type Preference: (empty dropdown); Loop Detection Mode: Off (dropdown); and SIP Link Monitoring: Use Session Manager Configuration (dropdown). A red box highlights the fields from Name to Time Zone.

A separate SIP entity for the Avaya SBCE, other than the one created for Session Manager during installation, is required in order to route calls to the service provider.

For the compliance test the following values were used:

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

The following screen shows the addition of the **HG ASBCE** SIP entity. This SIP Entity will be assigned later to the Entity Link corresponding to the Avaya SBCE.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar shows the navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. A red box highlights the following fields: Name (HG ASBCE), FQDN or IP Address (172.16.5.71), Type (Other), Notes (HG ASBCE), Adaptation (HG SBCE), Location (HG ASBCE), and Time Zone (America/New\_York). Below this, other fields include SIP Timer B/F (4), Credential name, Call Detail Recording (none), CommProfile Type Preference, Loop Detection Mode (Off), and SIP Link Monitoring (Use Session Manager Configuration). The top right corner shows the user is logged in as 'admin' on February 27, 2014.

## 6.6. Add Entity Links

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

The following screens illustrate the Entity Links to the CS1000.

AVAYA  
Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
*HG Session Manager	*HG Session Manager	UDP	*5085	*CS1K7.6	<input type="checkbox"/>	*5085	trusted	<input type="checkbox"/>	

Commit Cancel

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

AVAYA Aura System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item

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

Select : All, None

Commit Cancel

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

AVAYA Aura System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete Duplicate More Actions

21 Items

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
HG Session Manager AAC 5060 TCP	HG Session Manager	TCP	5060	AAC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	AAC Entity Link
HG Session Manager Acme Packet sip1 5060 TCP	HG Session Manager	TCP	5060	Acme Packet sip1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager CS1K7.6 5085 UDP	HG Session Manager	UDP	5085	CS1K7.6	<input type="checkbox"/>	5085	trusted	<input type="checkbox"/>	
HG Session Manager EdgeMarc SRC 5060 UDP	HG Session Manager	UDP	5060	EdgeMarc SRC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager HG AA-SBC 5060 TCP	HG Session Manager	TCP	5060	HG AA-SBC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager HG ASBCE 5060 TCP	HG Session Manager	TCP	5060	HG ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

## 6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added for this compliance test: one for the CS1000 and one for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. 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 shows the Routing Policy for the CS1000.

AVAYA  
Aura® System Manager 6.3

Last Logged on at February 27, 2014 12:24 PM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

\* Name: To CS1K76

Disabled: ☐

\* Retries: 0

Notes: Inbound Calls to CS1K76

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K7.6	172.16.20.60	Other	CS1000 Rel. 7.6

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left navigation pane shows 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. A red box highlights the configuration fields: 'Name' (To HG ASBCE), 'Disabled' (checkbox), 'Retries' (0), and 'Notes' (Outbound calls via ASBCE). Below this, the 'SIP Entity as Destination' section has a 'Select' button. At the bottom, a table lists the configuration details.

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

## 6.8. Add Dial Patterns

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

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain configured in **Section 6.2** used in the matching criteria.
- **Notes:** Add a brief description (optional).
- In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.
- Default values can be used for the remaining fields.
- Click **Commit** to save.



The example below shows that for calls beginning with dial pattern **1** (the North American Numbering Plan area prefix), with a length between **1** and **11** digits, with a SIP Domain of **-ALL-** and an Originating Location Name of **CS1k Node**, the Routing Policy **To HG ASBCE** will be used. Note that **-ALL-** was used for the SIP Domain since dial pattern “**1**” is being shared with other domain names being used by other test activities in the lab. The specific domain name could have been used instead (i.e., avaya.lab.com)

**AVAYA**  
Aura System Manager 6.3

Last Logged on at March 3, 2014 9:34 AM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

\* Pattern: 1

\* Min: 1

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

6 Items

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
CS1k Node	CS1K7.6	To HG ASBCE	0	<input type="checkbox"/>	HG ASBCE	Outbound calls via ASBCE

Select: All, None

Denied Originating Locations

Add Remove

0 Items

Originating Location	Notes
----------------------	-------

Commit Cancel

The next example shown below is for dial pattern **306** to route inbound calls to DID numbers provided by SaskTel (DID numbers assigned to extensions in the CS1000). For calls that begin with 306, are between **3** and **10** digits in length, have a SIP Domain of **avaya.lab.com** and an Originating Location Name of **HG ASBCE**, Routing Policy **To CS1K76** will be used.

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at March 3, 2014 9:34 AM  
Help | About | Change Password | Log off admin

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

\* Pattern: 306  
\* Min: 3  
\* Max: 10

Emergency Call: ☐  
Emergency Priority: 1  
Emergency Type:   
SIP Domain: avaya.lab.com  
Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> HG ASBCE	HG Avaya SBCE	To CS1K76	0	<input type="checkbox"/>	CS1K7.6	Inbound Calls to CS1K76

Select : All, None

Denied Originating Locations

Add Remove

0 Items

Originating Location	Notes
----------------------	-------

Commit Cancel

The same procedure should be followed to add other required dial patterns, such as: **011** for International calls, **411** for Directory Assistance calls, **911** for Emergency calls, **0** for Operator calls, etc.

## 6.9. Add/View Session Manager

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

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

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

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter the IP address of the Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of the Session Manager signaling interface.
- **Default Gateway:** Enter the IP address of the default gateway for the Session Manager signaling interface.
- Use default values for the remaining fields.
- Click **Save** (not shown) to add Session Manager.

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

AVAYA  
Aura® System Manager 6.3

Last Logged on at March 3, 2014 9:34 AM  
Help | About | Change Password | Log off admin

Home Session Manager

Session Manager Administration

View Session Manager

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

General

SIP Entity Name HG Session Manager  
Description Lab-HG SM  
Management Access Point Host Name/IP 172.16.5.31

Direct Routing to Endpoints Enable  
VMware Virtual Machine ☐

Security Module

SIP Entity IP Address 172.16.5.32  
Network Mask 255.255.255.0  
Default Gateway 172.16.5.254

Call Control PHB 46  
QOS Priority 5  
Speed & Duplex Auto  
VLAN ID

\*SIP Firewall Configuration Rule Set for HG Session Manager

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

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

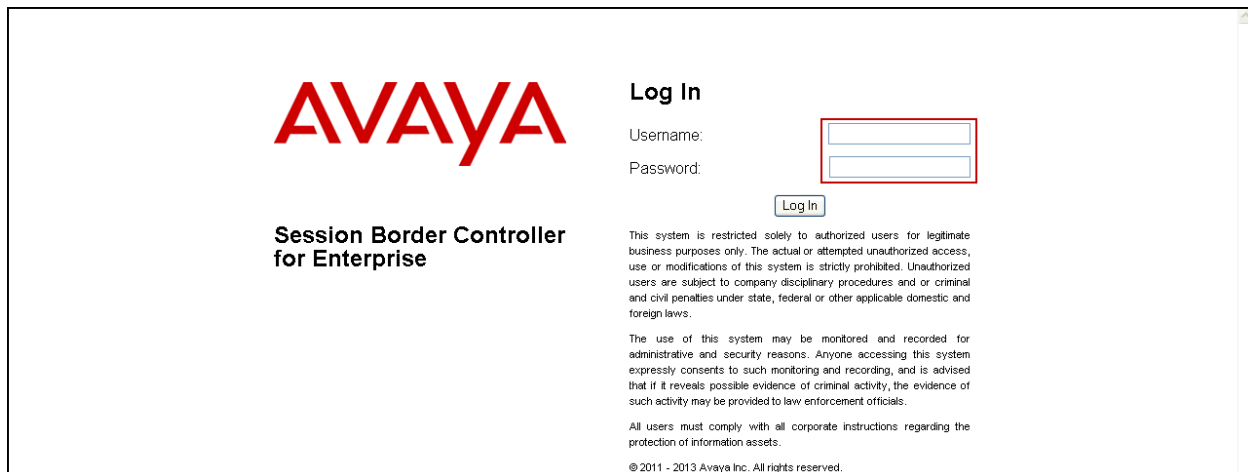
It is assumed that the Avaya SBCE was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBCE web interface.

**Note:** In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it.

### 7.1. Log in Avaya SBCE

Use a Web browser to access the Avaya SBCE Web interface. Enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the Avaya SBCE management IP address.

Enter the appropriate credentials and click **Log In**.



**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Username:

Password:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The **Dashboard** main page will appear as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The left sidebar contains a menu with 'Dashboard' highlighted. The main content area is divided into several sections: 'Information' (System Time: 07:00:14 AM GMT, Version: 6.2.1.Q07, Build Date: Mon Dec 9 17:33:02 CST 2013), 'Installed Devices' (listing EMS and Sipera), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (listing five incidents for Sipera), and 'Notes' (No notes found). The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out.

To view the system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **Sipera** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.

The screenshot shows the 'System Management' page. The left sidebar contains a menu with 'System Management' highlighted. The main content area is divided into several sections: 'Devices' (highlighted), 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' section contains a table with the following data:

Device Name (Serial Number)	Management IP	Version	Status	Reboot	Shutdown	Restart Application	View	Edit	Delete
Sipera (PCS31030132)	172.16.5.70	6.2.1.Q07	Commissioned						

The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out.

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed as shown below.

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

**System Information: Sipera** X

**General Configuration**

Appliance Name	Sipera
Box Type	SIP
Deployment Mode	Proxy

**Device Configuration**

HA Mode	No
Two Bypass Mode	No

**Network Configuration**

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
172.16.157.186	172.16.157.186	255.255.255.192	172.16.157.129	B1
[blurred]	[blurred]	[blurred]	[blurred]	[blurred]
[blurred]	[blurred]	[blurred]	[blurred]	[blurred]
[blurred]	[blurred]	[blurred]	[blurred]	[blurred]

**DNS Configuration**

Primary DNS	172.16.5.102
Secondary DNS	
DNS Location	DMZ
DNS Client IP	172.16.5.71

**Management IP(s)**

IP

On the previous screen, note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces of the Avaya SBCE, respectively. The **A1** and **B1** interfaces and IP addresses shown are the ones relevant to the configuration of the SIP trunk to SaskTel. Other IP addresses assigned to these interfaces are used to support other functionalities not discussed in this document, these IP addresses have been blurred out. The management IP has also been blurred out for security reasons.

**IMPORTANT! – During the Avaya SBCE installation, the Management interface (labeled “M1”) of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to have this resolved.**

## 7.2. Global Profiles

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

### 7.2.1. Server Interworking - Avaya-SM

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

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

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

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

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

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

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

- Uncheck **Include End Point IP for Context Lookup**.
- Leave other fields with their default values.
- Click **Finish**.

The following screen capture shows the **General** tab of the newly created **Avaya-SM** Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows a navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'Avaya-SM' which is selected. The 'General' tab is active, showing a table of configuration parameters.

Parameter	Value
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

The following screen capture shows the **Advanced** tab of the newly created **Avaya-SM** Profile.

The screenshot displays the 'Session Border Controller for Enterprise' web interface, showing the 'Advanced' tab of the 'Avaya-SM' profile. The 'Advanced' tab is selected, and a table of configuration parameters is visible.

Parameter	Value
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
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No



## 7.2.2. Server Interworking - SP-General

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

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

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

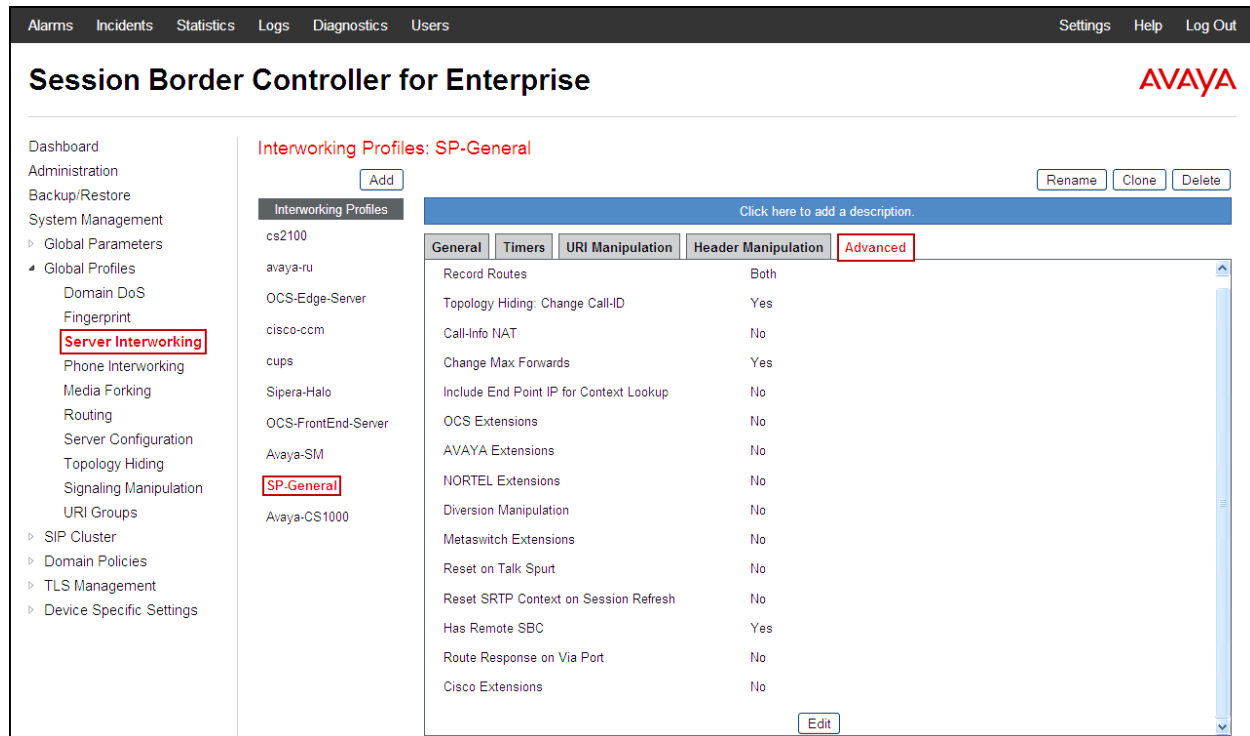
The following screen capture shows the **General** tab of the newly created **SP-General** profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a navigation pane lists various configuration areas, with 'Server Interworking' highlighted under 'Global Profiles'. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button. Below this, a list of profiles is shown, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), and 'Avaya-CS1000'. The 'SP-General' profile is selected, and its configuration is displayed in the 'General' tab. The configuration table lists various parameters and their values:

Parameter	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

The bottom of the configuration pane shows a 'Privacy' section.

The following screen capture shows the **Advanced** tab of the newly created **SP-General** profile.



### 7.2.3. Routing Profiles

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

Two Routing profiles were created, 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**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route\_to\_SM**.
- Click **Next**.

On the next screen, complete the following:

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

Edit Routing Rule
X

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

Next Hop Routing

URI Group
\*

Next Hop Server 1  
IP, IP:Port, Domain, or Domain:Port
172.16.5.32

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 shows the newly created **Route\_to\_SM** Profile.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise
AVAYA

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

Routing Profiles: Route\_to\_SM
Add
Rename Clone Delete

Routing Profiles
default
Route\_to\_SM
Route\_to\_SP
Route\_to\_CM
Route\_to\_CS1000

Click here to add a description.

Routing Profile
Add

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	*	172.16.5.32	...	View Edit

To SM from Rem W

Similarly, for the outbound route:

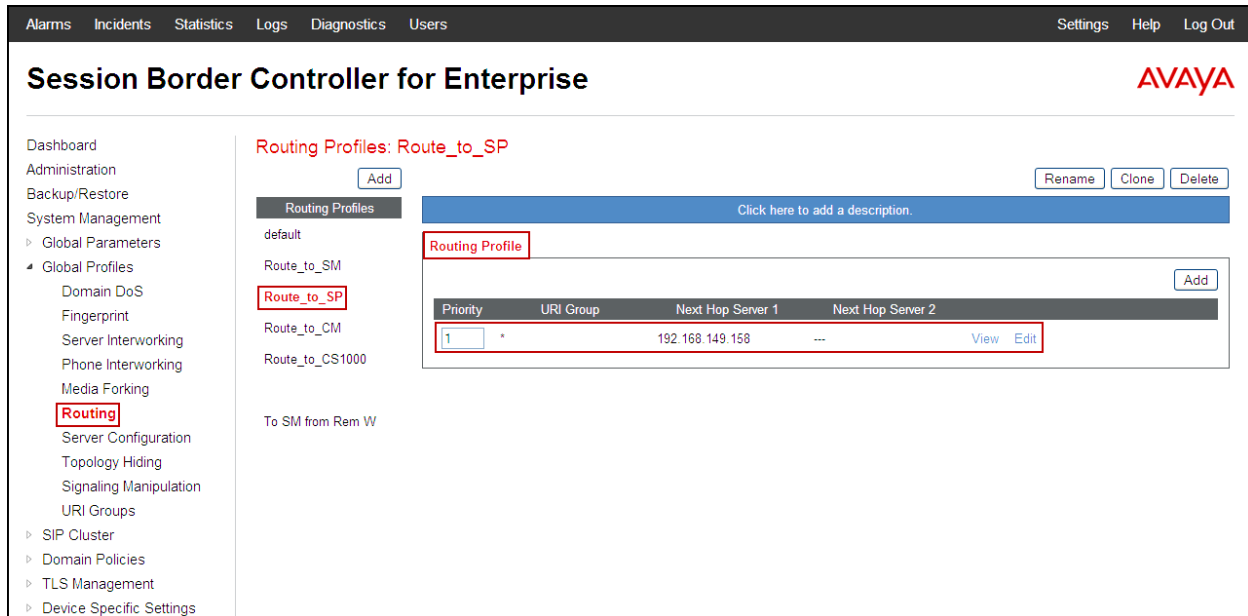
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route\_to\_SP**
- Click **Next**.
- **Next Hop Server 1: 192.168.149.158** (Service Provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport:** select **UDP**.
- Click **Finish**.

The screenshot shows the 'Edit Routing Rule' dialog box with the 'Next Hop Routing' tab selected. The dialog has a title bar with 'Edit Routing Rule' and a close button 'X'. Below the title bar is a blue banner with the text 'Each URI group may only be used once per Routing Profile.' The main content area is titled 'Next Hop Routing' and contains the following fields and options:

- URI Group:** A dropdown menu with a '\*' symbol and a downward arrow.
- Next Hop Server 1:** A text field containing '192.168.149.158'. Below the field is the label 'IP, IP:Port, Domain, or Domain:Port'.
- Next Hop Server 2:** An empty text field. Below the field is the label 'IP, IP:Port, Domain, or Domain:Port'.
- Routing Priority based on Next Hop Server:** A checkbox that is checked, indicated by a green checkmark.
- Use Next Hop for In Dialog Messages:** An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog:** An unchecked checkbox.
- NAPTR:** An unchecked checkbox.
- SRV:** An unchecked checkbox.
- Outgoing Transport:** A radio button group with three options: 'TLS', 'TCP', and 'UDP'. The 'UDP' option is selected, indicated by a green dot.

At the bottom of the dialog is a 'Finish' button.

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



## 7.2.4. Server Configuration

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

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

On the **Add Server Configuration Profile - General** window:

- **Server Type:** Select **Call Server**.
- **IP Address:** **172.16.5.32** (IP Address of Session Manager Security Module).
- **Supported Transports:** Check **TCP**.
- **TCP Port:** **5060** (This port must match the port number defined in **Section 6.6**).
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.

The following screen capture shows the **General** tab of the **Session Manager** profile.

**Add Server Configuration Profile - General** X

Server Type: Call Server

IP Addresses / Supported FQDNs  
Separate entries with commas: 172.16.5.32

Supported Transports:  
☒ TCP  
☐ UDP  
☐ TLS

TCP Port: 5060

UDP Port:

TLS Port:

Back Next

On the **Advanced** window

- Check **Enable Grooming**
- Select **Avaya-SM** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

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

**Edit Server Configuration Profile - Advanced** X

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya-SM ▼

TLS Client Profile None ▼

Signaling Manipulation Script None ▼

TCP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

TLS Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

The following screen capture shows the **General** tab of the newly created **Session Manager** profile.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The left sidebar contains a navigation menu with 'Server Configuration' highlighted. The main area is titled 'Server Configuration: Session Manager' and has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a table with the following configuration:

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

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

The following screen capture shows the **Advanced** tab of the newly created **Session Manager** profile

The screenshot shows the 'Session Manager' interface with the 'Advanced' tab selected. The configuration settings are as follows:

Property	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM
Signaling Manipulation Script	None
TCP Connection Type	SUBID

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



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

In the **Add Server Configuration Profile - General** window

- **Server Type:** select **Trunk Server**.
- **IP Address:** **192.168.149.158** (service provider's SIP Proxy IP address).
- **Supported Transports:** check **UDP**.
- **UDP Port:** enter **5060**.
- Click **Next**.
- Click **Next** in the **Authentication** window.
- Click **Next** in the **Heartbeat** window.

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

The screenshot displays the 'Add Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Trunk Server'. The 'IP Addresses / Supported FQDNs' field contains '192.168.149.158'. Under 'Supported Transports', the 'UDP' checkbox is checked, while 'TCP' and 'TLS' are unchecked. The 'UDP Port' field is set to '5060'. The 'TCP Port' and 'TLS Port' fields are empty. At the bottom, there are 'Back' and 'Next' buttons.

Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Separate entries with commas</small>	192.168.149.158
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
<input type="button" value="Back"/> <input type="button" value="Next"/>	

On the **Advanced** window:

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

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

**Edit Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

Signaling Manipulation Script None

UDP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

**Finish**

The following screen capture shows the **General** tab of the newly created **Service Provider** profile.

**Session Border Controller for Enterprise**

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

**Server Configuration: Service Provider**

Add Rename Clone Delete

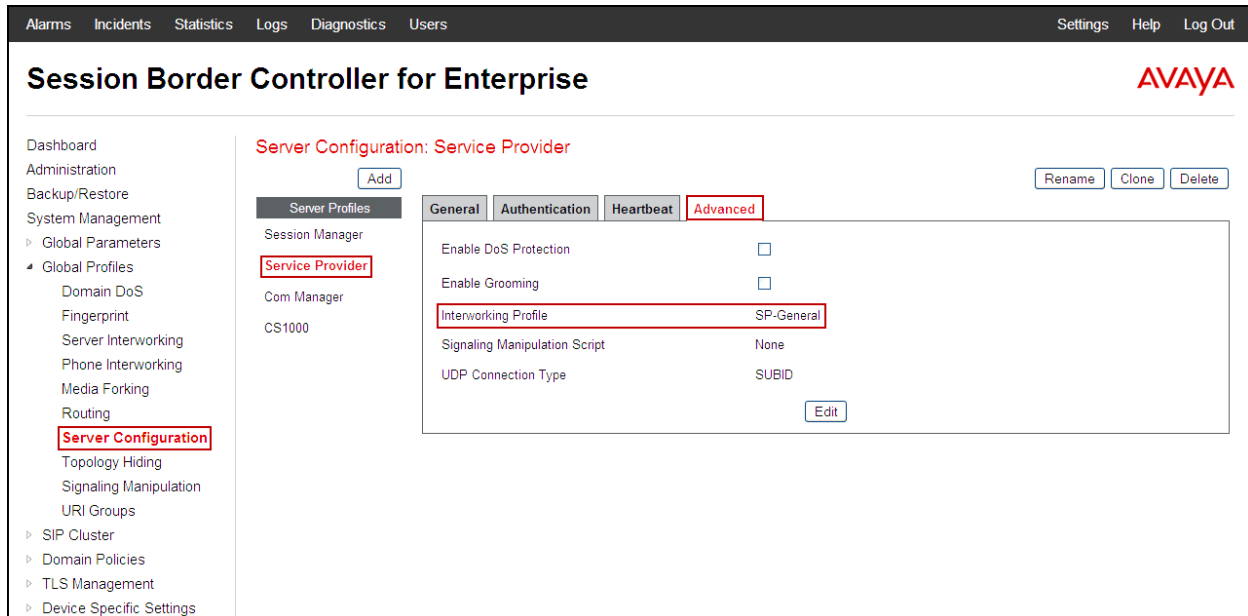
Server Profiles  
Session Manager  
**Service Provider**  
Com Manager  
CS1000

General Authentication Heartbeat Advanced

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.149.158
Supported Transports	UDP
UDP Port	5060

Edit

The following screen capture shows the **Advanced** tab of the newly created **Service Provider** profile.



### 7.2.5. Topology Hiding

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

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

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

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

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

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

AlarmsIncidentsStatisticsLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for EnterpriseAVAYA

DashboardAdministrationBackup/RestoreSystem ManagementGlobal ParametersGlobal ProfilesDomain DoSFingerprintServer InterworkingPhone InterworkingMedia ForkingRoutingServer ConfigurationTopology HidingSignaling ManipulationURI GroupsSIP ClusterDomain PoliciesTLS ManagementDevice Specific Settings

Topology Hiding Profiles: Session\_ManagerAddRenameCloneDelete

Topology Hiding ProfilesClick here to add a description.

defaultcisco\_th\_profileSession\_ManagerService\_ProviderCom ManagerCS1000

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

Edit

HG; Reviewed:  
SPOC 7/22/2014

Solution & Interoperability Test Lab Application Notes  
©2014 Avaya Inc. All Rights Reserved.

100 of 134  
Sask\_CS1KSMSBCE

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**.
- Click **Finish**.

The following screen capture shows the newly added **Service\_Provider** Profile. Note that for the Service Provider no values were overwritten (default).

**Session Border Controller for Enterprise** AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

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

**Topology Hiding Profiles: Service\_Provider**

Add Rename Clone Delete

Topology Hiding Profiles Click here to add a description.

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

Edit

## 7.2.6. Signaling Manipulation

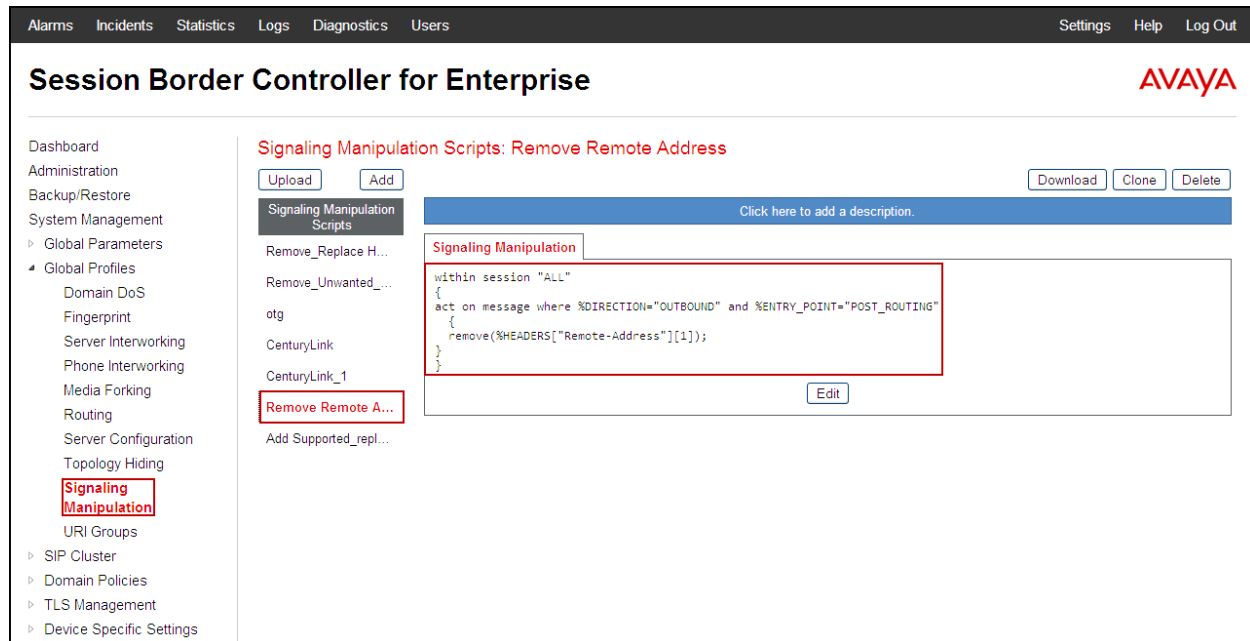
The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For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

The Signaling Manipulation Script shown below is needed to remove unwanted headers from being sent to the Service provider, in this case the **Remote Address** header. This is in addition to the Signaling Rules created to remove headers under **Section 7.3.3**.

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

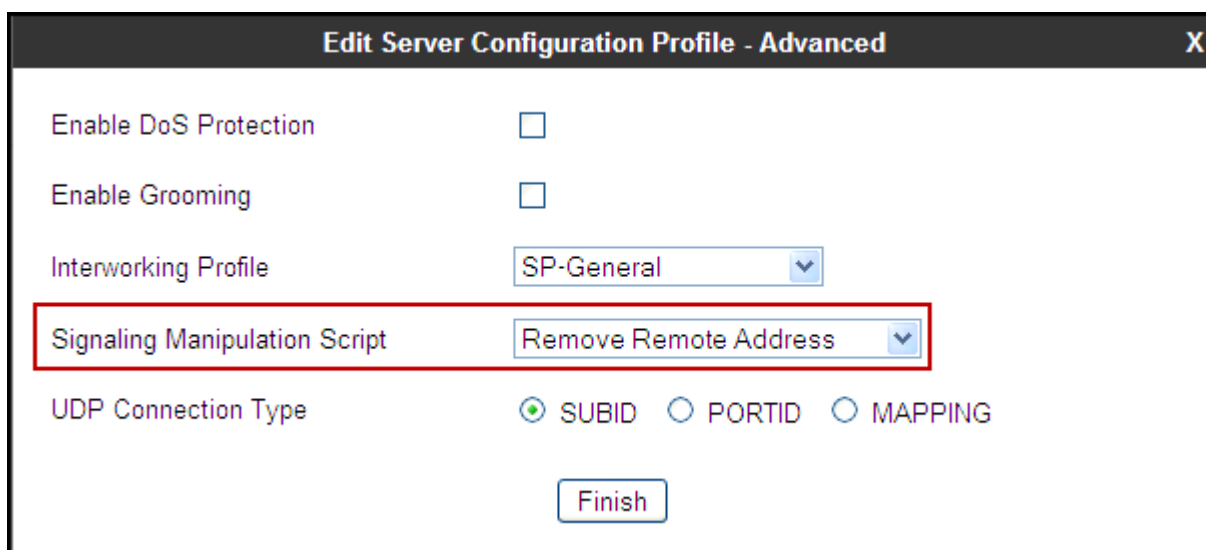
- On the **Title** enter a name, the name of **Remove Remote Address** was chosen in this example.
- Enter the script as shown on the screen below (**Note:** The script can be copied from **Appendix A**).
- Click **Save**.

The following screen shows the newly added Signaling Manipulation script.

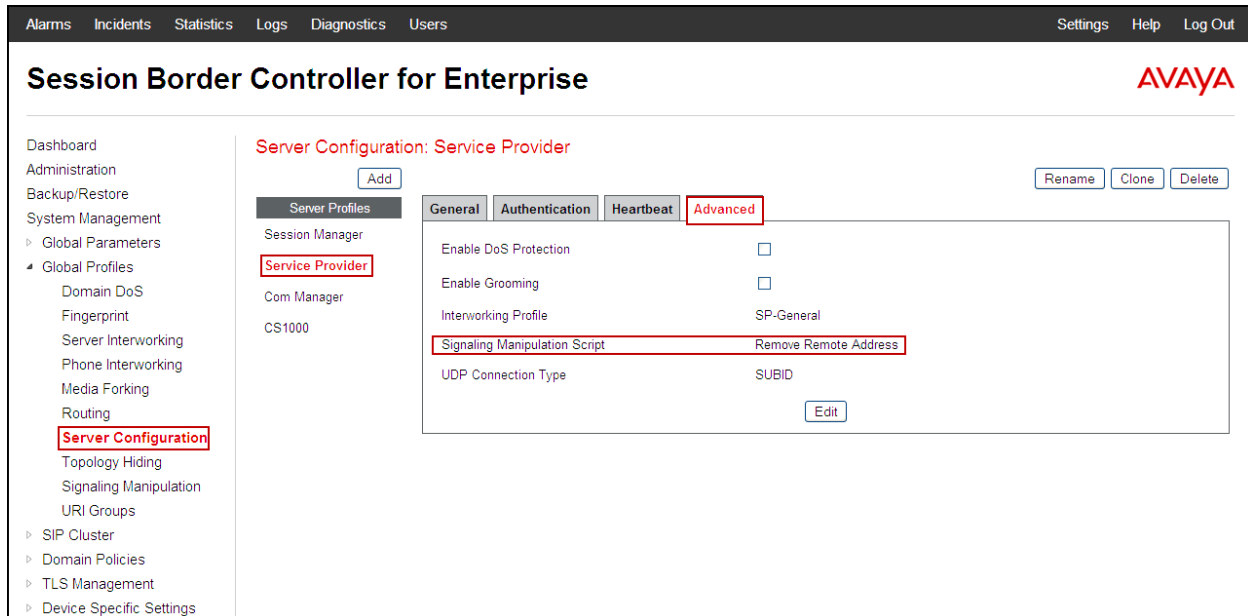


After the Signaling Manipulation Script is created, it should be applied to the **Service Provider Server Configuration Profile** previously created in **Section 7.2.4**.

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



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



## 7.3. Domain Policies

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

### 7.3.1. Create Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select **default** Rule.
- Select **Clone Rule** button.
- Name: enter the name of the profile, e.g., **1000 Sessions**.
- Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **1000** was used in the sample configuration.
- Click Finish.

Editing Rule: 1000 Sessions X

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

Miscellaneous

CDR Support ☒ None  
☐ CDR w/ RTP  
☐ CDR w/o RTP

RTCP Keep-Alive ☐

Finish

The following screen capture shows the newly created **1000 Sessions** application rule.

Alarms Incidents Statistics Logs Diagnostics Users
Settings Help Log Out

## Session Border Controller for Enterprise

AVAYA

Dashboard

Administration

Backup/Restore

System Management

▸ Global Parameters

▸ Global Profiles

▸ SIP Cluster

▸ Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Time of Day Rules

End Point Policy Groups

Session Policies

▸ TLS Management

▸ Device Specific Settings

Application Rules: 1000 Sessions

Add
Filter By Device...
Rename Clone Delete

Click here to add a description.

Application Rule

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

Miscellaneous

CDR Support None

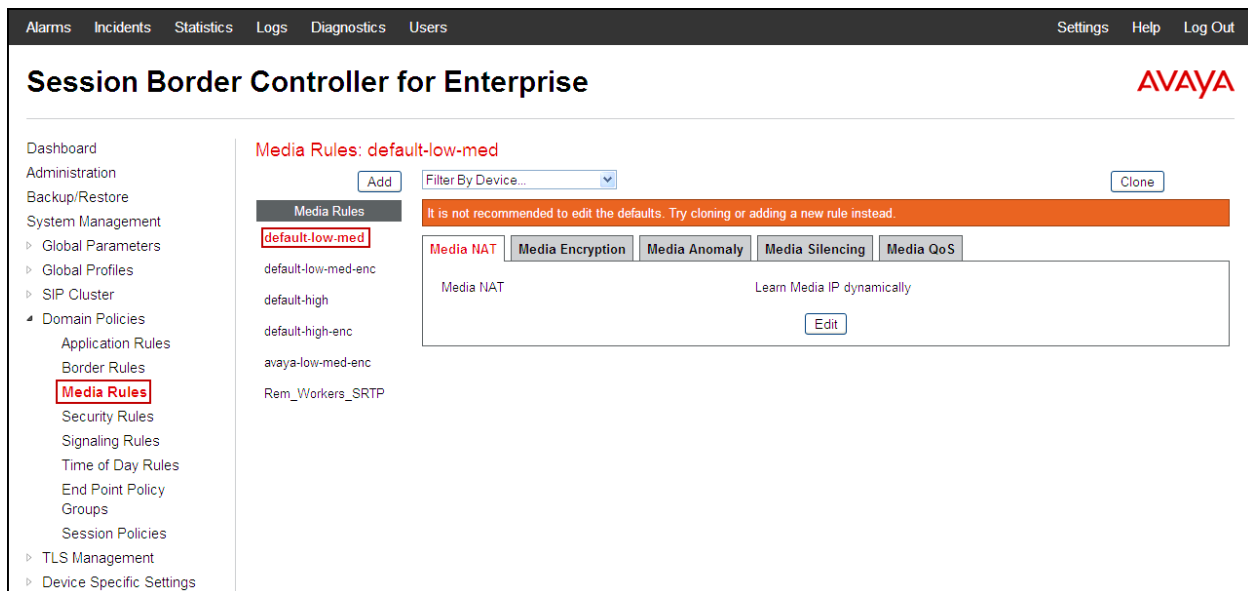
RTCP Keep-Alive No

Edit



### 7.3.2. Media Rules

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



### 7.3.3. Signaling Rules

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

Headers such as Alert-Info, P-Location, P-Charging-Vector and others are sent in SIP messages from Session Manager to the Avaya SBCE for egress 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 Rules was created, to later be applied in the direction of the Enterprise or the Service Provider. To create a rule to block these headers coming from Session Manager from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** in the **Signaling Rules** list.
- Click on **Clone** on top right of the screen.
- Enter a name: **SessMgr\_SigRule**. Click **Finish**.

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

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: AV-Global-Session-ID**

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

To add the **Alert-Info** header:

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

To add the **History-Info** header:

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

To add the **P-AV-Message-Id** header:

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

To add the **x-nt-e164-clid** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: x-nt-e164-clid**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

The following screen capture shows the **Request Headers** tab of the **SessMgr\_SigRule** signaling rule.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows a navigation menu with 'Signaling Rules' highlighted. The main content area shows the configuration for the 'SessMgr\_SigRule' signaling rule. The 'Request Headers' tab is selected, displaying a table of configured headers. The table has columns for Row, Header Name, Method Name, Header Criteria, Action, Proprietary, and Direction. Seven headers are listed, all with 'Remove Header' as the action and 'Forbidden' as the criteria. The headers are: AV-Global-Session-ID, Alert-Info, History-Info, P-AV-Message-Id, P-Charging-Vector, P-Location, and x-nt-e164-clid. The 'P-Location' and 'x-nt-e164-clid' headers are highlighted with a red border in the original image.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN
3	History-Info	ALL	Forbidden	Remove Header	No	IN
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN
5	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN
6	P-Location	ALL	Forbidden	Remove Header	Yes	IN
7	x-nt-e164-clid	ALL	Forbidden	Remove Header	Yes	IN

Select the **Response Headers** tab of the newly created Signaling rule.

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: AV-Global-Session-ID**
- **Response Code: 1XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **AV-Global-Session-ID** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: AV-Global-Session-ID**
- **Response Code: 200**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

To add the **Alert-Info** header:

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

To add the **P-AV-Message-Id** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-AV-Message-Id**
- **Response Code: 1XX**
- **Method Name: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**

- Click **Finish**

To add the **P-AV-Message-Id** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: P-AV-Message-Id**
- **Response Code: 200**
- **Method Name: ALL**
- **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: ALL**
- **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: 1XX**
- **Method Name: ALL**
- **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: ALL**
- **Header Criteria: Forbidden**
- **Presence Action: Remove Header**
- Click **Finish**

The following screen capture shows the **Response Headers** tab of the **SessMgr\_SigRule** signaling rule

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Signaling Rules' highlighted. The main content area shows the configuration for the 'SessMgr\_SigRule' signaling rule. The 'Response Headers' tab is selected, showing a table of configured headers. The table has columns for Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, Direction, and Edit/Delete links. The table lists 8 entries, all with 'Forbidden' criteria and 'Remove Header' action.

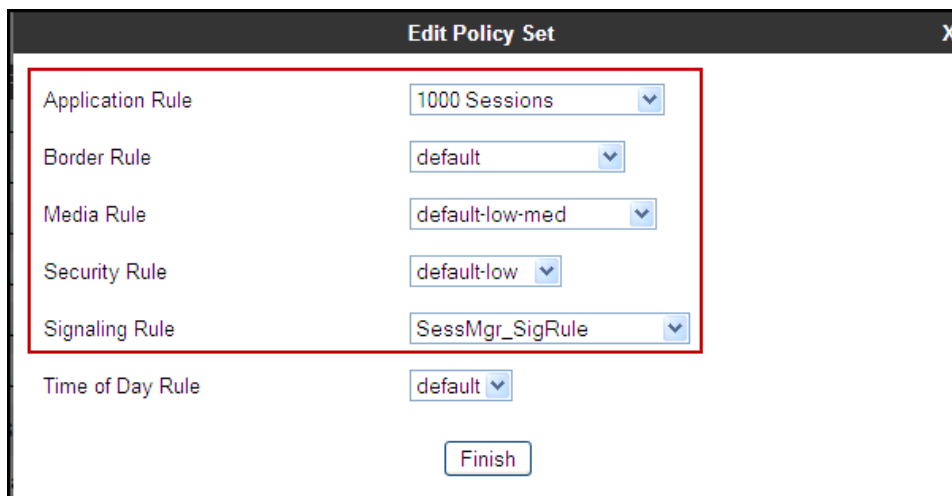
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
4	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

### 7.3.4. End Point Policy Groups

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

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

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



The screenshot shows a window titled "Edit Policy Set" with a close button (X) in the top right corner. Inside the window, there are six rows of configuration options, each with a label and a dropdown menu. A red rectangular box highlights the first five rows: Application Rule, Border Rule, Media Rule, Security Rule, and Signaling Rule. The values selected in these dropdowns are "1000 Sessions", "default", "default-low-med", "default-low", and "SessMgr\_SigRule" respectively. Below these, the "Time of Day Rule" is set to "default". At the bottom center of the window is a button labeled "Finish".

Rule Type	Selected Value
Application Rule	1000 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	SessMgr_SigRule
Time of Day Rule	default

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo.

On the left, a sidebar menu lists various configuration areas, with 'End Point Policy Groups' highlighted in red. The main content area is titled 'Policy Groups: Enterprise' and features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-subs...', 'avaya-def-high-server', and 'Enterprise' (highlighted in red). The 'Enterprise' group is selected, showing its configuration details on the right.

The configuration details for the 'Enterprise' group include a table with the following columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: Order 1, Application 1000 Sessions, Border default, Media default-low-med, Security default-low, Signaling SessMgr\_SigRule, and Time of Day default. The table also includes 'Edit' and 'Clone' buttons for each row.

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



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

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

**Edit Policy Set** [X]

Application Rule: 1000 Sessions

Border Rule: default

Media Rule: default-low-med

Security Rule: default-low

Signaling Rule: default

Time of Day Rule: default

**Finish**

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

**Session Border Controller for Enterprise** AVAYA

**Policy Groups: Service Provider**

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**

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

## 7.4. Device Specific Settings

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

### 7.4.1. Network Management

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Network Management" highlighted under "Device Specific Settings". The main content area is titled "Network Management: Sipera" and features two tabs: "Network Configuration" (selected) and "Interface Configuration". A red box highlights the "Network Configuration" tab. Below the tabs, a red box highlights a warning message: "Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management." Below this, there are input fields for "A1 Netmask" (255.255.255.0), "A2 Netmask", "B1 Netmask" (255.255.255.192), and "B2 Netmask". A red box highlights the "A1 Netmask" and "B1 Netmask" fields. Below these fields are "Add", "Save", and "Clear" buttons. A table below shows the network configuration for the device. The table has columns for IP Address, Public IP, Gateway, Interface, and a Delete button. The first two rows are highlighted with a red box.

IP Address	Public IP	Gateway	Interface	Delete
172.16.5.71		172.16.5.254	A1	Delete
172.16.157.186		172.16.157.129	B1	Delete
172.16.157.186		172.16.157.129	B1	Delete
172.16.157.186		172.16.157.129	B1	Delete
172.16.157.186		172.16.157.129	B1	Delete

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various configuration areas, with 'Network Management' highlighted. The main content area is titled 'Network Management: Sipera' and contains two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, showing a table with the following data:

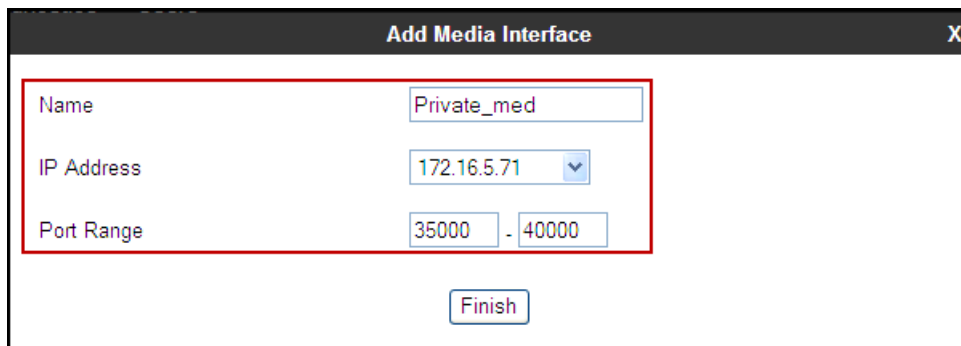
Name	Administrative Status	Toggle
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

### 7.4.2. Media Interface

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

From the **Device Specific Settings** menu on the left-hand side, select **Media Interface**. Below is the configuration of the inside, private Media Interface of the Avaya SBCE.

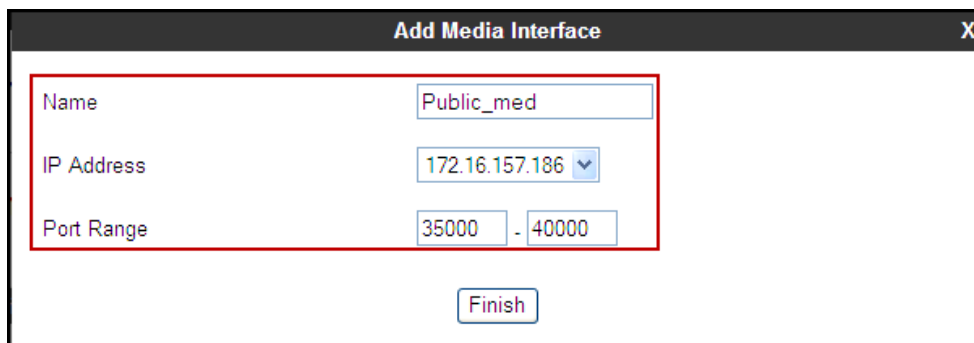
- Select **Add** in the **Media Interface** area (not shown).
- **Name: Private\_med.**
- **IP Address: 172.16.5.71** (Inside or Private IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000.**
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Private\_med", "IP Address" with a dropdown menu showing "172.16.5.71", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the dialog. A red rectangular box highlights the Name, IP Address, and Port Range fields.

Below is the configuration of the outside, public Media Interface of the Avaya SBCE.

- Select **Add** in the **Media Interface** area.
- **Name: Public\_med.**
- **IP Address: 172.16.157.186** (Outside or Public IP Address of the Avaya SBCE, toward the Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Public\_med", "IP Address" with a dropdown menu showing "172.16.157.186", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the dialog. A red rectangular box highlights the Name, IP Address, and Port Range fields.

The following screen capture shows the newly created media interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Media Interface' highlighted under 'Device Specific Settings'. The main content area is titled 'Media Interface: Sipera' and contains a sub-menu with 'Devices' and 'Media Interface'. A red-bordered box highlights the 'Media Interface' sub-menu item. Below this, a warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add' button is located to the right of the warning. A table lists the configured media interfaces:

Name	Media IP	Port Range	Edit	Delete
Private_med	172.16.5.71	35000 - 40000	<a href="#">Edit</a>	<a href="#">Delete</a>
Public_med	172.16.157.186	35000 - 40000	<a href="#">Edit</a>	<a href="#">Delete</a>
RW_Private_med	172.16.5.72	35000 - 40000	<a href="#">Edit</a>	<a href="#">Delete</a>
RW_Public_med	172.16.157.180	35000 - 40000	<a href="#">Edit</a>	<a href="#">Delete</a>

### 7.4.3. Signaling Interface

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

Below is the configuration of the inside, private Signaling Interface of the Avaya SBCE.

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

**Add Signaling Interface** X

Name: Private\_sig

IP Address: 172.16.5.71 ▼

TCP Port: 5060  
Leave blank to disable

UDP Port:   
Leave blank to disable

Enable Stun: ☐

TLS Port:   
Leave blank to disable

TLS Profile: AvayaSBCServer ▼

Enable Shared Control: ☐

Shared Control Port:

Finish

Below is the configuration of the outside, public signaling Interface of the Avaya SBCE.

- Select **Add** in the **Signaling Interface** area.
- **Name: Public\_sig.**
- **IP Address: 172.16.157.186** (Outside or Public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish.**

**Add Signaling Interface** X

Name

IP Address  ▼

TCP Port   
Leave blank to disable

UDP Port   
Leave blank to disable

Enable Stun ☐

TLS Port   
Leave blank to disable

TLS Profile  ▼

Enable Shared Control ☐

Shared Control Port

**Finish**

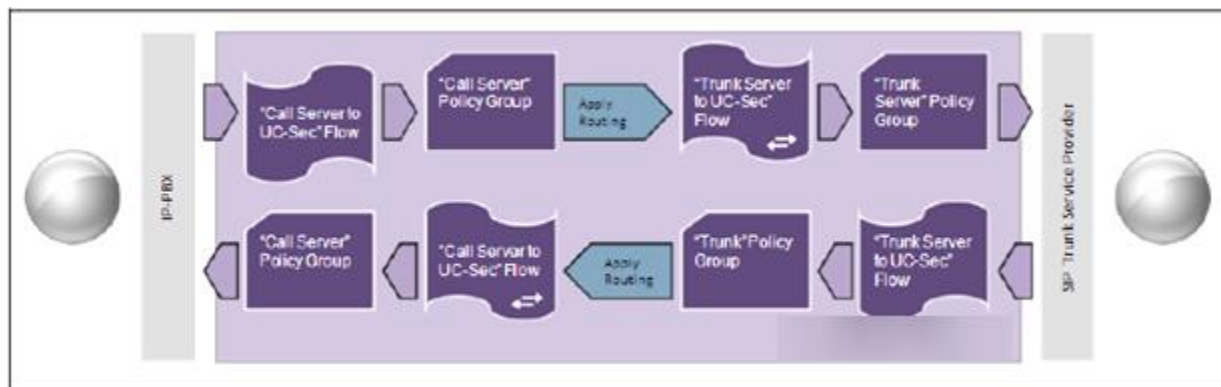
The following screen capture shows the newly created signaling interfaces.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Signaling Interface" highlighted under "Device Specific Settings". The main content area is titled "Signaling Interface: Sipera" and contains a table of configured signaling interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Private_sig	172.16.5.71	5060	---	---	None	Edit	Delete
Public_sig	172.16.157.186	---	5060	---	None	Edit	Delete

#### 7.4.4. End Point Flows

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





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

To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, and then the **Server Flows** tab. Click **Add Flow** (not shown).

- **Name:** SIP\_Trunk\_Flow.
- **Server Configuration:** Service Provider.
- **URI Group:** \*
- **Transport:** \*
- **Remote Subnet:** \*
- **Received Interface:** Private\_sig.
- **Signaling Interface:** Public\_sig.
- **Media Interface:** Public\_med.
- **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**.

Edit Flow: SIP\_Trunk\_Flow
X

Flow Name

Server Configuration

Service Provider ▼

URI Group

\* ▼

Transport

\* ▼

Remote Subnet

Received Interface

Private\_sig ▼

Signaling Interface

Public\_sig ▼

Media Interface

Public\_med ▼

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\_sig.**
- **Signaling Interface: Private\_sig.**
- **Media Interface: Private\_med.**
- **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** X

Flow Name	Session_Manager_Flow
Server Configuration	Session Manager ▼
URI Group	* ▼
Transport	* ▼
Remote Subnet	*
Received Interface	Public_sig ▼
Signaling Interface	Private_sig ▼
Media Interface	Private_med ▼
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 newly created **End Point Flows**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo.

On the left sidebar, the "Device Specific Settings" menu is expanded, and "End Point Flows" is highlighted. The main content area is titled "End Point Flows: Sipera" and features two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of configurations.

Below the "Server Flows" tab, there are two sections: "Server Configuration: Service Provider" and "Server Configuration: Session Manager". Each section contains a table of flows.

**Server Configuration: Service Provider**

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

**Server Configuration: Session Manager**

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

## 8. SaskTel SIP Trunk Service Configuration

To use SaskTel SIP Trunk service, a customer must request the service from SaskTel using the established sales processes. The process can be started by contacting SaskTel via the corporate web site at: <https://www.sasktel.com/support> or by calling the Toll Free number at 1-888-773-2122 and requesting information.

During the signup process, SaskTel will require that the customer provide the public IP address used to reach Avaya SBCE at the edge of the enterprise. SaskTel will provide the IP address of the SIP proxy/SBC, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya Communication Server 1000E, Avaya Aura® Session Manager, and the Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

## 9. Verification Steps

The following steps may be used to verify the configuration.

### 9.1. General

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

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

### Active Call Trace (LD 80).

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

- Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail)
- Login to the Overlay command prompt; issue the command **LD 80** and then **trac 0 8000** while the call is active.
- After the call is released, issue command **trac 0 8000** 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 8000 is in an active call:

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

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

```
>ld 80
TRAO00
.trac 0 8000

ACTIVE VTN 008 0 00 00

ORIG VTN 008 0 00 00 KEY 0 SCR MARP CUST 0 DN 8000 TYPE 1165
SIGNALLING ENCRYPTION: INSEC
FAR-END SIP SIGNALLING IP: 172.16.21.61
FAR-END MEDIA ENDPOINT IP: 172.16.20.154 PORT: 5200
FAR-END SIP SIGNALLING IP: 172.16.21.61
FAR-END MEDIA ENDPOINT IP: 172.16.20.154 PORT: 5200
TERM VTN 048 0 00 10 VTRK IPTI RMBR 0 11 OUTGOING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 172.16.5.71
FAR-END MEDIA ENDPOINT IP: 172.16.5.71 PORT: 35010
FAR-END VendorID: AVAYA-SM-6.3.2.0.632023
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 91786331
MAIN_PM ESTD
TALKSLOT ORIG 10 TERM 15 JUNCTOR ORIGO TERMO
EES_DATA:
NONE
QUEUE NONE
CALL ID 0 489

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

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

```
.trac 0 8000

IDLE VTN 008 0 00 00 MARP
```

The following screen shows an example after the call was released, it shows that there are no trunks busy.

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

### 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, DTMF event description.
- **Media Attribute:** verify specific audio port, codec, ptime, send/ receive ability.
- **DTMF events and fax attributes.**



The following screen shows an example of a typical capture for a call made from an 1120 Deskphone (DID: 306777xx52) on the CS1000, to a PSTN number (786331xxxx).

```

17 4.698137 157.186 149.158 SIP/SDP 1297 Request: INVITE sip:1786331@149.158;user=phone |
19 4.807934 149.158 157.186 SIP 377 Status: 100 Trying |
28 9.186294 149.158 157.186 SIP/SDP 949 Status: 183 Session Progress |
29 9.199025 157.186 149.158 SIP 807 Request: PRACK sip:149.158:5060;transport=udp |
36 9.292319 149.158 157.186 SIP 619 Status: 200 OK |

Request-Line: INVITE sip:1786331@149.158;user=phone SIP/2.0
Message Header
  From: "Avaya 1120_21" <sip:306777xx52@157.186:5060;user=phone>;tag=85b7a50-3c1410ac-13dd-55013-253b-5cc4c664-253b
  To: <sip:1786331@149.158;user=phone>
  CSeq: 1 INVITE
  Call-ID: 947a467a8ec8270b71f3cb4c0302bd2c
  Contact: <sip:306777xx52@157.186:5060;transport=udp;user=phone;gsid=fda70520-99a2-11e3-82e6-78e3b51bf2d0>
  Record-Route: <sip:157.186:5060;ipcs-line=20779;r;transport=udp>
  Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE
  Supported: 100rel, x-nortel-sipvc, replaces
  User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.65.16 AVAYA-SM-6.3.5.0.635005
  Max-Forwards: 64
  Via: SIP/2.0/UDP 157.186:5060;branch=z9hG4bK-s1632-000797802196-1--s1632-
  Privacy: none
  P-Asserted-Identity: "Avaya 1120_21" <sip:306777xx52@64.197.157.186:5060;user=phone>
  Content-Type: application/sdp
  Content-Length: 284
Message Body
  Session Description Protocol
    Session Description Protocol version (v): 0
    Owner/Creator, Session Id (o): - 179 1 IN IP4 157.186
    Session Name (s): -
    Connection Information (c): IN IP4 157.186
    Time Description, active time (t): 0 0
    Media Description, name and address (m): audio 35048 RTP/AVP 0 18 101 111
    Connection Information (c): IN IP4 157.186
    Media Attribute (a): rtpmap:0 PCMU/8000
    Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute (a): rtpmap:101 telephone-event/8000
    Media Attribute (a): rtpmap:111 X-nt-inforeq/8000
    Media Attribute (a): fmtp:18 annexb=no
  
```

## 10. Conclusion

These Application Notes describe the procedures necessary for configuring SaskTel SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2.1 as shown in **Figure 1**.

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

## 11. References

This section references the documentation relevant to these Application Notes.

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

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

- [1] *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013.
- [2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013.
- [3] *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013.
- [4] *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.
- [5] *Dialing Plans Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.
- [6] *Product Compatibility Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013.
- [7] *Avaya Product Support Notice – PSN003460u – Configuring FAX over IP in CS 1000: An Overview.*
- [8] *Communication Server 1000 Release 7.6 & Service Pack 4 Release Notes*, Issue 2.0 February 2014.

Product documentation for Avaya Aura® Session Manager and Avaya Aura® System Manager, including the following, is available at:

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

- [9] *Avaya Aura® System Manager Overview and Specification*, Release 6.3, Issue 3, October 2013.
- [10] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013.
- [11] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013.

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

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

- [12] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014.
- [13] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2013.
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, July 2013.

Other resources:

- [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/>

## 12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE as shown in **Section 7.2.6**:

### **Title: Remove Remote Address**

```
within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
  remove(%HEADERS["Remote-Address"][1]);
}
}
```

**©2014 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).