



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

---

# **Application Notes for Configuring Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 to support OneStream Global SIP Trunking Services - Issue 1.0**

## **Abstract**

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.3 to support OneStream Global SIP Trunking Services.

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.

OneStream Global SIP Trunking services provides PSTN access via SIP trunks between the enterprise and OneStream as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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) .....	20
5.3.	Administer Voice Codec .....	22
5.3.1.	Enable Voice Codec, Node IP Telephony .....	22
5.3.2.	Synchronize the New Configuration.....	27
5.3.3.	Enable Voice Codec on Media Gateways.....	30
5.4.	Administer Zones and Bandwidth.....	32
5.4.1.	Create a zone for IP phones (zone 5).....	32
5.4.2.	Create a zone for virtual SIP trunks (zone 4).....	34
5.5.	Administer SIP Trunk Gateway .....	35
5.5.1.	Administer the SIP Trunk Gateway to Session Manager .....	38
5.5.2.	Administer Virtual D-Channel.....	40
5.5.3.	Administer Virtual Superloop.....	44
5.5.4.	Administer Virtual SIP Routes .....	45
5.5.5.	Administer Virtual Trunks.....	49
5.5.6.	Administer Calling Line Identification Entries.....	52
5.6.	Administer Dialing Plans .....	56
5.6.1.	Define ESN Access Codes and Parameters (ESN) .....	56
5.6.2.	Associate NPA and SPN call to ESN Access Code 1 .....	57
5.6.3.	Digit Manipulation Block Index (DMI).....	58
5.6.4.	Route List Block (RLB).....	60
5.6.5.	Inbound Digit Translation.....	61
5.6.6.	Outbound Call - Special Number Configuration .....	64
5.6.7.	Outbound Call - Numbering Plan Area Code (NPA) .....	66
5.7.	Administer Phone.....	66
5.7.1.	Phone creation.....	66
5.7.2.	Enable Privacy for the Phone.....	68
5.7.3.	Enable Call Forward for the Phone.....	69
5.7.4.	Enable Call Waiting for the Phone .....	74

6.	Configure Avaya Aura® Session Manager .....	75
6.1.	System Manager Login and Navigation .....	76
6.2.	Specify SIP Domain .....	77
6.3.	Add Location .....	78
6.4.	Add Adaptation Module .....	81
6.5.	Add SIP Entities .....	83
6.6.	Add Entity Links .....	87
6.7.	Add Routing Policies .....	89
6.8.	Add Dial Patterns .....	90
6.9.	Add/View Session Manager .....	92
7.	Configure Avaya Session Border Controller for Enterprise (Avaya SBCE) .....	94
7.1.	Log in Avaya SBCE .....	94
7.2.	Global Profiles .....	97
7.2.1.	Server Interworking - Avaya-SM .....	97
7.2.2.	Server Interworking - SP-General .....	100
7.2.3.	Server Configuration .....	102
7.2.4.	Routing Profiles .....	107
7.2.5.	Topology Hiding .....	110
7.2.6.	Signaling Manipulation .....	113
7.3.	Domain Policies .....	116
7.3.1.	Create Application Rules .....	116
7.3.2.	Media Rules .....	117
7.3.3.	Signaling Rules .....	118
7.3.4.	End Point Policy Groups .....	125
7.4.	Device Specific Settings .....	127
7.4.1.	Network Management .....	127
7.4.2.	Media Interface .....	129
7.4.3.	Signaling Interface .....	131
7.4.4.	End Point Flows .....	133
8.	OneStream SIP Trunk Service Configuration .....	137
9.	Verification Steps .....	137
9.1.	General .....	137
9.2.	Protocol Traces .....	139
10.	Conclusion .....	140
11.	References .....	141
12.	Appendix A: SigMa Script .....	143

# 1. Introduction

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.3 to support OneStream Global SIP Trunking Services.

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

In the sample configuration, the Avaya enterprise 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. 6.3 (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 OneStream's network via SIP trunks. Various call types were made from the CS1000 to OneStream and vice versa to verify interoperability between the CS1000 and OneStream.

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 and the Avaya SBCE can interoperate with the OneStream's network. The following interoperability areas were covered:

- Incoming calls from the PSTN were routed to DID numbers assigned by OneStream. 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 OneStream'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 and G.729A, OneStream's 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.
- T.38 fax.
- G.711Mu fax pass-through.
- Long duration calls (one hour).
- Early Media transmission.
- Mobility: Mobil X and Personal Call Assistance (PCA).

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.  
Operator calls (e.g., 0) and operator assisted calls (e.g., 0+10) are not supported in OneStream's VoIP environment.

## 2.2. Test Results

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

- **No ring back tone on PSTN stations after Blind Transfers to internal CS1000 stations:** Ring back tone is not heard (only silence) on PSTN stations after calls from the PSTN to the CS1000 are Blind Transferred from one CS1000 station to another CS1000 station (internal CS1000 transfer) and while the CS1000 station the call was transferred to is ringing (Scenario: PSTN\_Station\_1 → CS1000\_Station\_1 → Blind Transfer → CS1000\_Station\_2). This issue is under investigation by Avaya.
- **No ring back tone on PSTN stations after Blind Transfers to the PSTN:** Ring back tone is not heard (only silence) on PSTN stations after calls from the PSTN to CS1000 SIP stations are Blind Transferred back out to another PSTN station (external CS1000 transfer) and while the PSTN station the call was transferred to is ringing (Scenario: PSTN\_Station\_1 → CS1000\_SIP\_Station\_1 → Blind Transfer → PSTN\_Station\_2). This issue is only seen on CS1000 SIP endpoints, this behavior is not seen on UniStim endpoints. This issue was solved by the addition of a Signaling Rule to the Avaya SBCE (Refer to **Section: 7.3.3**)

- **Caller-ID on re-directed calls to the PSTN:** Caller ID works properly between the CS1000 and OneStream 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 **Anonymous** and the access code of the trunk route (ACOD). 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. These particular headers and MIME have no real use in the service provider network.

## 2.3. Support

For support on OneStream systems, call Toll Free at 1-800-869-0315 or visit the corporate Web page at: <http://www.onestreamnetworks.com/Default.aspx?RD=3340>

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 OneStream Global SIP Trunking Services 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).
- Avaya 2050 IP Softphone.
- Avaya M3904 Digital Deskphones.
- Analog Deskphones.
- Fax machines.
- Desktop with administration interfaces.

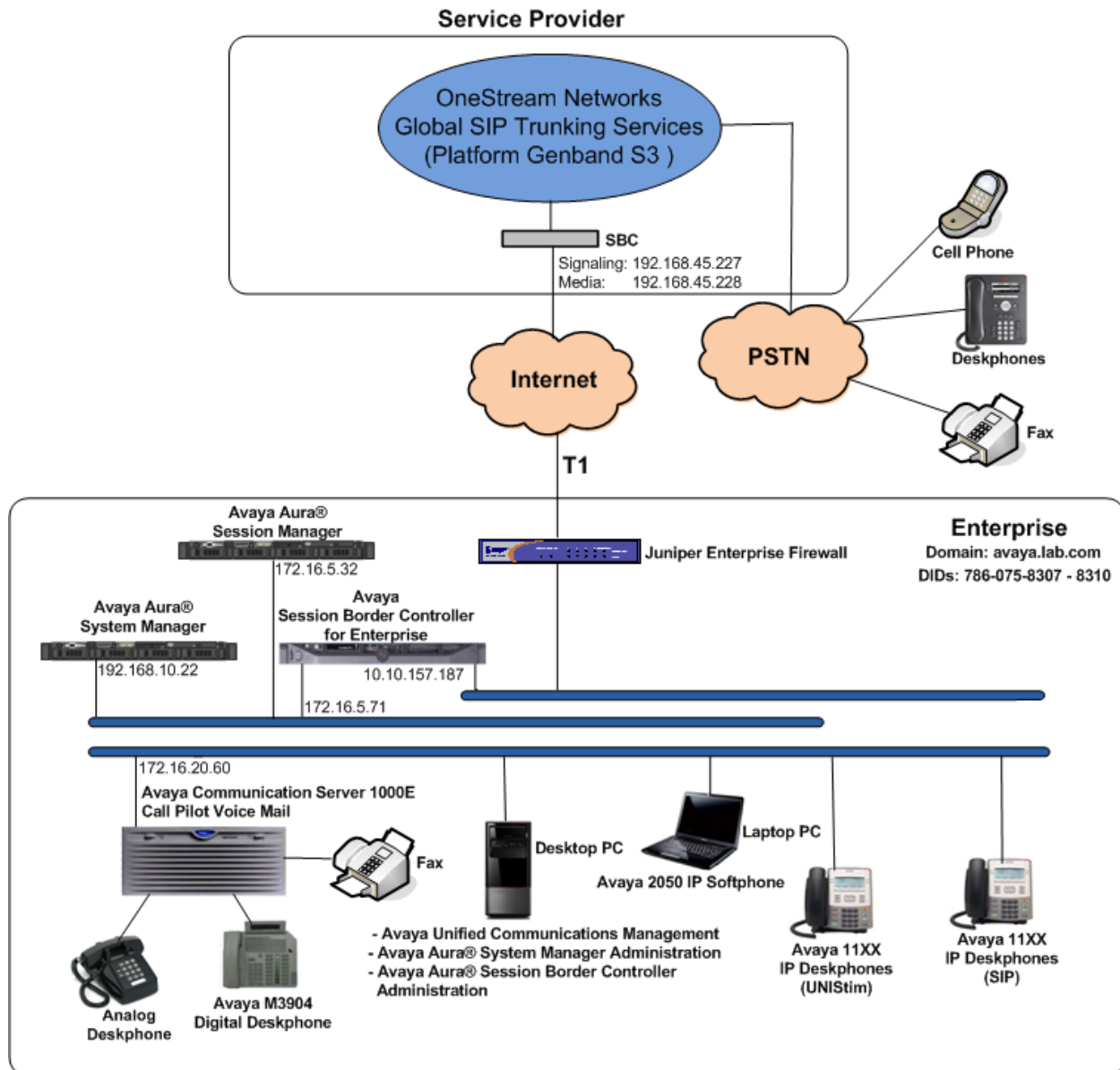
Located at the edge of the enterprise is the Avaya SBCE. It has a public side that connects to the public network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect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

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 OneStream 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 OneStream. At the simulated enterprise site a T1 connection was used for local access to the Internet.



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



## 4. Equipment and Software Validated

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

Avaya	
Equipment	Release/Version
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: 2014-09-04 06:05:08 (est))  <b>Signaling Server:</b> 7.65.16.00 (Service Pack 5)
Avaya Call Pilot 202i	Call Pilot Manager Version: 05.00.41.156
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.9 (Service Pack 9) (6.3.9.0.639011)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.9 (Service Pack 9) Build No. 6.3.0.8.5682-6.3.8.4414 Software Update Rev. No. 6.3.9.1.2482
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.3.000-19-4338
Avaya Deskphones	1110: 0623C8V (UniStim) 1120: 0624C8V (UniStim) 1150: 0627C8V (UniStim) 1165: 0626C8V (UniStim) 1120E: 04.04.18.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.02.0062
Lucent Analog Phone	N/A
Fax Machines	N/A
OneStream Networks	
Equipment	Release/Version
Genband S3	8.1.2
Genband SBC	8.1.2

**Signaling Server Service Updates (SU) and Patches:**

**(CS1000 Linux Service Updates (SU) and patches included in Release 7.6 Service Pack 5):**

cs1000-csmWeb-7.65.16.22-2.i386.000  
cs1000-linuxbase-7.65.16.23-1.i386.000  
tzdata-2013c-2.el5.i386.001  
cs1000-Jboss-Quantum-7.65.16.22-8.i386.000  
cs1000-patchWeb-7.65.16.22-4.i386.000  
cs1000-cs1000WebService\_6-0-7.65.16.21-00.i386.000  
cs1000-dmWeb-7.65.16.22-6.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-csoneksvrmgr-7.65.16.22-5.i386.000  
cs1000-dbcom-7.65.16.21-00.i386.000  
cs1000-baseWeb-7.65.16.22-4.i386.000  
cs1000-cs-7.65.P.100-02.i386.000  
cs1000-shared-omm-7.65.16.21-2.i386.000  
cs1000-bcc-7.65.16.22-14.i386.000  
cs1000-ftpkg-7.65.16.22-2.i386.000  
cs1000-snmp-7.65.16.21-00.i686.000  
cs1000-oam-logging-7.65.16.22-4.i386.000  
cs1000-csv-7.65.16.22-2.i386.000  
cs1000-tps-7.65.16.22-8.i386.000  
cs1000-mscTone-7.65.16.22-2.i386.000  
cs1000-mscMusc-7.65.16.22-4.i386.000  
cs1000-mscConf-7.65.16.22-2.i386.000  
cs1000-emWebLocal\_6-0-7.65.16.22-1.i386.000  
cs1000-ipsec-7.65.16.22-1.i386.000  
cs1000-cppmUtil-7.65.16.22-1.i686.000  
cs1000-mscAnnc-7.65.16.22-2.i386.000  
cs1000-mscAttn-7.65.16.22-2.i386.000  
cs1000-gk-7.65.16.22-1.i386.000  
cs1000-emWeb\_6-0-7.65.16.22-9.i386.000  
cs1000-sps-7.65.16.22-3.i386.000  
cs1000-shared-pbx-7.65.16.22-3.i386.000  
cs1000-shared-xmsg-7.65.16.22-1.i386.000  
cs1000-vtrk-7.65.16.22-50.i386.000

#####

Patches:

p31484\_1  
p33054\_2  
p33125\_1  
p33274\_1  
p33275\_1

#####

**MGC Loadware:**

DSP1AB07.LW

DSP2AB07.LW

DSP3AB07.LW

DSP4AB07.LW

DSP5AB07.LW

udtcab25.lw

MGCCDC04.LW

## 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**.

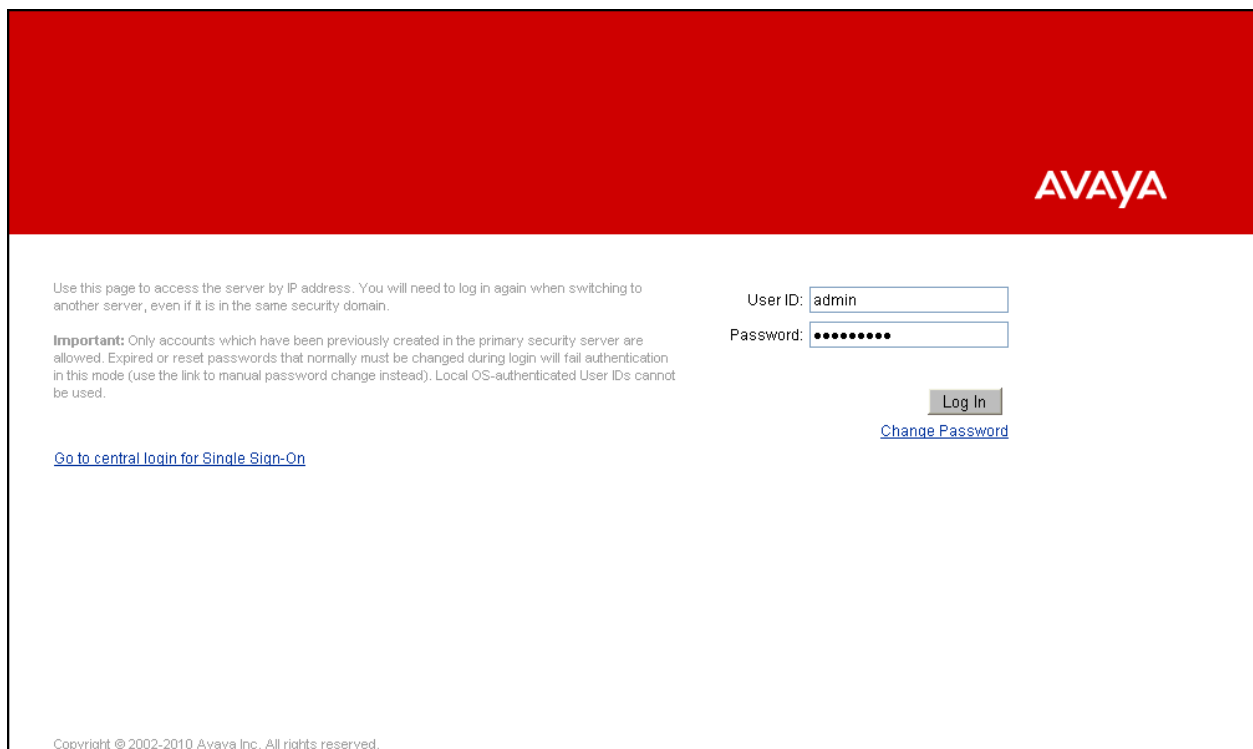
The procedures shown below describe the configuration details of the CS1000 with SIP trunks to the OneStream network.

**Note:** Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

### 5.1. Login to the CS1000 System

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

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



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

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

Go to central login for Single Sign-On

User ID:

Password:

[Change Password](#)

Copyright © 2002-2010 Avaya Inc. All rights reserved.

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

AVAYA

Avaya Unified Communications Management

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: 02.30.0092.00(6691)

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 ca

Search

Reset

Add...

Edit...

Delete

	<input type="checkbox"/> Element Name	Element Type ▲	Release
1	<input type="checkbox"/> <b>EM on cs1k</b>	CS1000	7.6
2	<input type="checkbox"/> <a href="#">cs1k.avaya.lab.com (primary)</a>	Linux Base	7.6
3	<input type="checkbox"/> 172.16.21.62	Media Gateway Controller	7.6

HG; Reviewed:  
SPOC 3/2/2015

Solution & Interoperability Test Lab Application Notes  
©2015 Avaya Inc. All Rights Reserved.

13 of 144  
OneStCS1KSMSBCE

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

AVAYA

CS1000 Element Manager

- UCM Network Services

- Home

- Links

- Virtual Terminals

- System

+ Alarms

- Maintenance

+ Core Equipment

- Peripheral Equipment

+ IP Network

+ Interfaces

- Engineered Values

+ Emergency Services

+ Software

- Customers

- Routes and Trunks

- Routes and Trunks

- D-Channels

- Digital Trunk Interface

- Dialing and Numbering Plans

- Electronic Switched Network

- Flexible Code Restriction

- Incoming Digit Translation

- Phones

- Templates

- Reports

- Views

- Lists

- Properties

- Migration

- Tools

+ Backup and Restore

- Date and Time

+ Logs and reports

- Security

+ Passwords

+ Policies

+ Login Options

Managing: 172.16.21.61 Username: admin  
System Overview

System Overview

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

HG; Reviewed:  
SPOC 3/2/2015

Solution & Interoperability Test Lab Application Notes  
©2015 Avaya Inc. All Rights Reserved.

14 of 144  
OneStCS1KSMSBCE

### 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 OneStream.

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**

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	-	Synchronized

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**

---

- UCM Network Services  
 - Home  
 + Links  
 - System  
   + Alarms  
   - Maintenance  
   + Core Equipment  
   - Peripheral Equipment  
   - IP Network  
     - **Nodes, Servers, Media Cards**  
       - Maintenance and Reports  
       - Media Gateways  
       - Zones  
       - Host and Route Tables  
       - Network Address Translation (NAT)  
       - QoS Thresholds  
       - Personal Directories  
       - Unicode Name Directory  
   + Interfaces  
   - Engineered Values  
   + Emergency Services  
   + Software  
 - Customers  
 + Routes and Trunks  
 + Dialing and Numbering Plans  
 + Phones  
 + Tools  
 + 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:  \* (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 (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT)
- Causes

**Applications (click to edit configuration)**

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

\* Required Value.

**Associated Signaling Servers & Cards**

<input type="checkbox"/> 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.

## 5.2.2. Administer Terminal Proxy Server

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

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

– UCM Network Services

– Home

+ Links

– System

+ Alarms

– Maintenance

+ Core Equipment

– Peripheral Equipment

– IP Network

– Nodes, Servers, Media Cards

– Maintenance and Reports

– Media Gateways

– Zones

– Host and Route Tables

– Network Address Translation (NAT)

– QoS Thresholds

– Personal Directories

– Unicode Name Directory

+ Interfaces

– Engineered Values

– Emergency Services

+ Software

– Customers

+ Routes and Trunks

+ Dialing and Numbering Plans

+ Phones

+ Tools

+ 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 \*

**IP Telephony Node Properties**

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

**Telephony LAN (TLAN)**

Node IPv4 address: 172.16.20.60 \*

Subnet mask: 255.255.255.0 \*

Node IPv6 address:

**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**.

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

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

**Save** **Cancel**

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

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

AVAYA

CS1000 Element Manager

UCM Network Services

Home

Links

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes, Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation (NAT)

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Software

Customers

Routes and Trunks

Dialing and Numbering Plans

Phones

Tools

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

Applications (click to edit configuration)

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

\* Required Value. 

Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader

Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway (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.

**AVAYA**

**CS1000 Element Manager**

- UCM Network Services

- Home

+ Links

- System

+ Alarms

- Maintenance

+ Core Equipment

- Peripheral Equipment

- IP Network

- Nodes, Servers, Media Cards

- Maintenance and Reports

- Media Gateways

- Zones

- Host and Route Tables

- Network Address Translation (NAT)

- QoS Thresholds

- Personal Directories

- Unicode Name Directory

+ Interfaces

- Engineered Values

+ Emergency Services

+ Software

- Customers

+ Routes and Trunks

+ Dialing and Numbering Plans

+ Phones

+ Tools

+ Security

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:  (0-63)

Voice packets:  (0-63)

VLAN tagging: ☐ 802.1Q support

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

\* Required Value.

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**

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
- 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 **Voice Gateway (VGW) and Codecs** screen is displayed as shown below. OneStream supports codecs **G.711MU** and **G.729A** (OneStream's 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.

**AVAYA CS1000 Element Manager**

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

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

**General | Voice Codescs | Fax**

**Voice Codescs**

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

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

\* Required Value.

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

Save Cancel

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

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

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

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

General | **Voice Codescs** | Fax

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

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

**Fax**  
Codec name: T.38 FAX  
Maximum rate: 14400 (bps)

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



For Fax over IP, **T.38** was used as default and **G.711MU fax pass-through** as fallback. During the testing, **T.38** fax transport and **G.711MU fax pass-through** were tested successfully.

For CS1000 FAX over IP Support recommendation refer to **Section 5.7.1** for analog station provisioning and the Avaya Product Support Notice (PSN) referred to in **Section 11** [7], including the “**Analog Station provisioning for T.38** section” and “**Minimum Vintage Loadware Recommendation**” for MGC.

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

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar shows 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, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Software, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Node ID: 1006 - Voice Gateway (VGW) and Codecs'. It has tabs for General, Voice Codecs, and Fax. The General tab is active, showing settings for Echo cancellation (checked, Use canceller, with tail delay: 128), Dynamic attenuation (checked), Voice activity detection threshold (-17), Idle noise level (-65), Signaling options (checked, DTMF tone detection, unchecked, Low latency mode, checked, Remove DTMF delay (squelch DTMF from TDM to IP), checked, Modem/Fax pass-through, checked, V.21 Fax tone detection, unchecked, R factor calculation). The Voice Codecs section shows Codec G711: Enabled (required), Voice payload size: 20 (milliseconds per frame), and Voice playout (jitter buffer) delay: 40 (milliseconds). A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are Save and Cancel buttons.

T.38 with payload size **30ms** was chosen for fax. Clicking on the **Save** button.

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

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

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

General | Voice Codescs | Fax

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

**Fax**

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

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

### 5.3.2. Synchronize the New Configuration

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

**AVAYA**

**CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

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 \*

**IP Telephony Node Properties**

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

**Telephony LAN (TLAN)**

Node IPv4 address: 172.16.20.60 \*

Subnet mask: 255.255.255.0 \*

Node IPv6 address:

**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 ▼AddRemoveMake LeaderPrint | Refresh

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

Show: ☐ IPv6 address

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

HG; Reviewed:  
SPOC 3/2/2015

Solution & Interoperability Test Lab Application Notes  
©2015 Avaya Inc. All Rights Reserved.

27 of 144  
OneStCS1KSMSBCE

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

**AVAYA CS1000 Element Manager**

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.

**AVAYA CS1000 Element Manager**

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](#)

<input checked="" type="checkbox"/>	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, wait a couple of minutes for the Application restart to complete.

## CS1000 Element Manager

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.

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

<input checked="" type="checkbox"/>	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.

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

### 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).

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

**UCM Network Services**

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

**Remove DTMF delay (squellch 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** ☒

**Codec name G711**

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

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

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

**VAD** ☐

**- Codec G729A** **Select** ☒

**Codec name G729A**

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

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

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

**VAD** ☐

For Fax over IP, **T.38** was used as default and **G.711MU fax pass-through** as fallback. During the testing, **T.38** fax transport and **G.711MU fax pass-through** were tested successfully.

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

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, Home, Links, System, IP Network, 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, and Security. The 'Media Gateways' option is highlighted. The main configuration area is titled 'CS1000 Element Manager' and contains several sections: '+ Media Gateway (MGS)', '+ DSP Daughterboard', and '- VGW and IP phone codec profile'. The '- VGW and IP phone codec profile' section is expanded, showing various settings. Key settings include: 'Enable echo canceller' (checked), 'Echo canceller tail delay' (128 milliseconds), 'Enable dynamic attenuation' (checked), 'Voice activity detection threshold' (1, 0-4 DBM), 'Idle noise level' (0, 0-1 DBM), 'R factor calculation' (unchecked), 'DTMF tone detection' (checked), 'Enable low latency mode' (unchecked), 'Remove DTMF delay (squell DTMF from TDM to IP)' (checked), 'Enable modem/fax pass through mode' (checked), 'Enable V.21 FAX tone detection' (checked), '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), and 'FAX packet size' (30). Below these are codec settings: '+ Codec G711' (Select checked), '+ Codec G729A' (Select checked), '+ Codec G723.1' (Select unchecked), and '- Codec T38 FAX' (Select checked). The 'Codec name' is set to 'T38 FAX'. At the bottom of the configuration area are buttons for 'Save', 'Cancel', and 'VGW Channels'. A footer note states '\* Mandatory fields of current configuration'. The bottom of the page shows a copyright notice: 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

## 5.4. Administer Zones and Bandwidth

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

### 5.4.1. Create a zone for IP phones (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 left-hand navigation pane shows a tree structure with the following items: - UCM Network Services, - Home, + Links, - System (expanded), + Alarms, - Maintenance, + Core Equipment, - Peripheral Equipment, - IP Network (highlighted with a red box), - Nodes: Servers, Media Cards, - Maintenance and Reports, - Media Gateways, - Zones (highlighted with a red box), - Host and Route Tables, - Network Address Translation (NAT), - QoS Thresholds, - Personal Directories, - Unicode Name Directory, + Interfaces, - Engineered Values, + Emergency Services, + Software, - Customers, + Routes and Trunks, + Dialing and Numbering Plans, + Phones, + Tools, and + Security. The main content area at the top shows 'Managing: 172.16.21.61 Username: admin' and 'System » IP Network » Zones'. Below this, the 'Zones' section is titled, followed by the text 'Zones are used to group related information for either bandwidth or dial plan numbering purposes.' The 'Bandwidth Zones' link is highlighted with a red box, with a description: 'Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.' The 'Numbering Zones' link is also visible, with a description: 'Numbering zones are used to route calls through a centralized call server.'



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

**AVAYA**

**CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 5 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

**Zone Basic Property and Bandwidth Management**

Input Description	Input Value
Zone Number (ZONE):	5 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ) ▼
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	MO (MO) ▼
Description (ZDES):	IPPHONES_G711
Location Name (ZNAME):	
Reserved BW Block Size (RESERVED_BW_SIZE):	0 (200 - 9999999)

Submit Refresh Cancel

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

Follow **Section 5.4.1** to create a zone for the Virtual SIP Trunks. The difference is in the **Zone Intent (ZBRN)** field; for **ZBRN** select **VTRK** for virtual trunk, and then select **Best Quality (BQ)** for both **INTRA\_STGY** and **INTER\_STGY**, as shown below. Click on the **Submit** button. For OneStream, **Zone 4** was created for the Virtual SIP Trunks.

AVAYA CS1000 Element Manager

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

### Zone Basic Property and Bandwidth Management

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

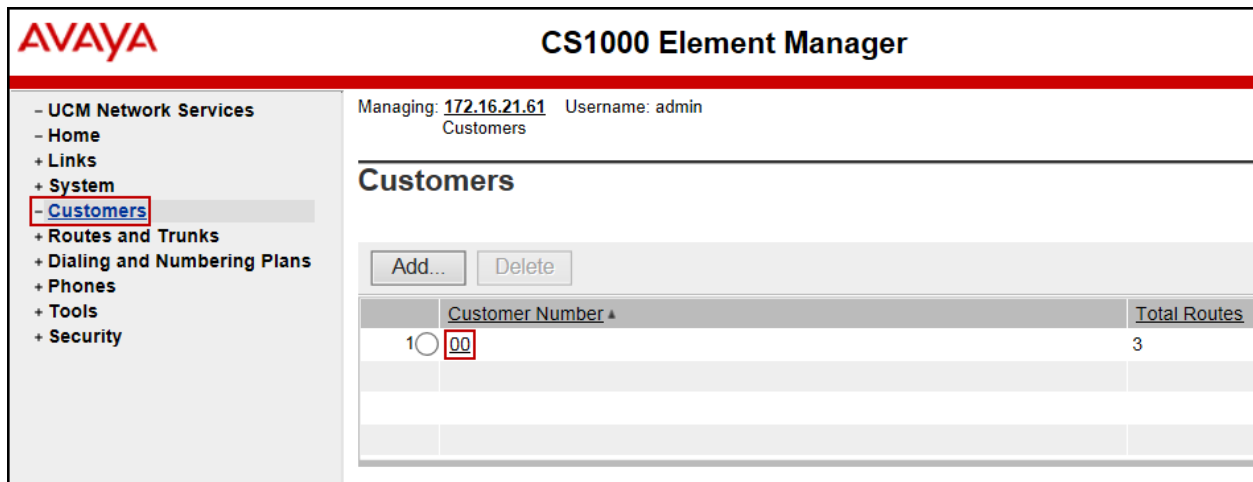
Submit Refresh Cancel

**Note:** OneStream only supports codec G.711MU and G.729A, non-supported codec's sent by the CS1000 (i.e., G.711A) will be ignored by OneStream.

## 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 displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation menu with options: UCM Network Services, Home, Links, System, Customers (highlighted with a red box), Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Customers' and shows a table with columns 'Customer Number' and 'Total Routes'. A single entry is visible with '00' in the 'Customer Number' column and '3' in the 'Total Routes' column. The '00' is also highlighted with a red box. Above the table are 'Add...' and 'Delete' buttons. At the top of the main area, it says 'Managing: 172.16.21.61 Username: admin Customers'.

Customer Number	Total Routes
00	3

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

The screenshot displays the Avaya CS1000 Element Manager web interface. On the left is a navigation menu with the following items: UCM Network Services, Home, Links, System, Customers (highlighted with a red box), Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Customer Details' and contains a list of configuration options: Basic Configuration, Application Module Link, Attendant, Call Detail Recording, Call Party Name Display, Call Redirection, Centralized Attendant Service, Controlled Class of Service, Features, Feature Packages (highlighted with a red box), Flexible Feature Codes, Intercept Treatments, ISDN and ESN Networking, Listed Directory Numbers, Media Services Properties, Mobile Service Directory Numbers, Multi-Party Operations, Night Service, Recorded Overflow Announcement, SIP Line Service, and Timers. At the top right of the interface, it shows 'Managing: 172.16.21.61' and 'Username: admin', with a breadcrumb trail: 'Customers » Customer 00 » Customer Details'.

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

**AVAYA**

**CS1000 Element Manager**

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

- + Enhanced Night Service
- **Integrated Services Digital Network**
- + Dial Access Prefix on CLID table entry option

Package: 133

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: ☐

### 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 (not shown). 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.**

**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

Vtrk gateway application: ☒ Enable gateway service on this node

**General**

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: avaya.lab.com

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

Gateway endpoint name: CS1KGateway

Gateway password: \* (0-9999)

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

Enable failsafe NRS: ☐

Note: FailSafe NRS will be enabled only on those servers in the node where NRS application is not deployed.

**Virtual Trunk Network Health Monitor**

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

Monitor IP: Add

Monitor addresses: Remove

\* Required Value.

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

Save Cancel

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**).

**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

Proxy Or Redirect Server:

Proxy Server Route 1:

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

Port: 5085 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration  
☐ Primary CDS proxy

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

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration

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

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:** blank.
- **Unknown:** blank.

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

- **UDP:** blank.
- **CDP:** blank.
- **Special Number:** blank.
- **Vacant number:** blank.
- **Unknown:** blank.

**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 Private domain names

National:  UDP:

Subscriber:  CDP:

Special number:  Special number:

Unknown:  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)

Timeout for ringing indication:  (5 - 60 seconds)

\* 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)  
MSDL Diagnostics (LD 96)  
TMDI Diagnostics (LD 96)  
D-Channel Expansion Diagnostics (LD 48)

**Configuration**

Choose a D-Channel Number:  and type:  to Add

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

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:	<input type="button" value="more PRI"/>
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

+ Basic options (BSOFT)  
+ 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**

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

Pattern Service and Number Plan ID: [2521]  
D channel Card Type: [DCIP]  
Designator: [VoIP]  
Recovery to Primary: ☐  
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  
- 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: ☒  
--Overlap Timer: [ ]  
- Multilocation Business Group Allowed: ☐  
- Network Attendant Service Allowed: ☒  
+ Basic options (BSCOPT)  
- Advanced options (ADVOPT)  
+ H323 Overlap Signaling Settings (H323)  
+ 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

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

- Basic Configuration

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

- Basic options (BSCOPT)

+ - Change protocol timer value (TMR)

+ Advanced options (ADVOPT)

- Layer 3 call control message count per 5 second

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 (not shown).

Click on the **Submit** button at the bottom of the previous screen (not shown).

**AVAYA CS1000 Element Manager**

– UCM Network Services  
– Home  
– Links  
– Virtual Terminals  
+ System  
– Customers  
– Routes and Trunks  
– Routes and Trunks  
– D-Channels  
– Digital Trunk Interface  
+ Dialing and Numbering Plans  
+ Phones  
+ Tools  
+ Security

Call transfer integer (CTI) ☐  
Call transfer object (CTO) ☐  
Diversion info. is sent using integer value (DV1I) ☐  
Diversion info. is sent using object identifier (DV1O) ☐  
Rerouting requests processed using integer value (DV2I) ☐  
Rerouting requests processed using object identifier (DV2O) ☐  
Diversion info. sent. rerouting requests processed (DV3I) ☐  
EuroISDN - div. info sent. rerouting req. processed (DV3O) ☐  
Call transfer notification and invocation to EuroISDN (ECTO) ☐  
Malicious call identification (MCID) ☐  
MCDN QSIG conversion (MQC) ☐  
Remote D-channel is on a MSDL card (MSL) ☐  
**Message waiting interworking with DMS-100 (MWI) ☒**  
Network access data (NAC) ☐  
Network call trace supported (NCT) ☐  
Network name display method 1 (ND1) ☐  
**Network name display method 2 (ND2) ☒**  
Network name display method 3 (ND3) ☐  
Name display - integer ID coding (NDI) ☐  
Name display - object ID coding (NDO) ☐

### 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**

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

**Superloops**

Add... Delete

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

– UCM Network Services  
– Home  
– Links  
– Virtual Terminals  
– System  
+ Alarms  
– Maintenance  
+ Core Equipment  
– Loops  
– **Superloops**  
– MSDL/MISP Cards  
– Conference/TDS/Multifrequency  
– 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 screenshot displays the Avaya CS1000 Element Manager interface. The top header shows the Avaya logo and the title 'CS1000 Element Manager'. Below the header, a status bar indicates 'Managing: 172.16.21.61 Username: admin' and 'Routes and Trunks » Routes and Trunks'. The left sidebar contains a navigation menu with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks (highlighted), D-Channels, Digital Trunk Interface, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Routes and Trunks' and displays a summary for 'Customer: 0' with 'Total routes: 3' and 'Total trunks: 17'. An 'Add route' button is visible in the top right corner of the main content area.

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.

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

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

## Customer 0, Route 0 Property Configuration

### - Basic Configuration

Route data block (RDB) (TYPE) :	<input type="text" value="RDB"/>
Customer number (CUST) :	<input type="text" value="00"/>
Route number (ROUT) :	<input type="text" value="0"/>
Designator field for trunk (DES) :	<input type="text" value="SERVICE PROVIDE"/>
Trunk type (TKTP) :	<input type="text" value="TIE"/>
Incoming and outgoing trunk (ICOG) :	<input type="text" value="Incoming and Outgoing (IAO)"/>
Access code for the trunk route (ACOD) :	<input type="text" value="7916"/> *
Trunk type M911P (M911P) :	<input type="checkbox"/>
The route is for a virtual trunk route (VTRK) :	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE) :	<input type="text" value="00004"/> (0 - 8000)
- Node ID of signalling server of this route (NODE) :	<input type="text" value="1006"/> (0 - 9999)
- Protocol ID for the route (PCID) :	<input type="text" value="SIP (SIP)"/>
- Print correlation ID in CDR for the route (CRID) :	<input type="checkbox"/>
- Enable Shared Bandwidth Management for the route (SBWM) :	<input type="checkbox"/>
Integrated services digital network option (ISDN) :	<input checked="" type="checkbox"/>
- Mode of operation (MODE) :	<input type="text" value="Route uses ISDN Signaling Link (ISLD)"/>
- D channel number (DCH) :	<input type="text" value="0"/> (0 - 254)
- Interface type for route (IFC) :	<input type="text" value="Meridian M1 (SL1)"/>
- Private network identifier (PNI) :	<input type="text" value="00001"/> (0 - 32700)
- Network calling name allowed (NCNA) :	<input checked="" type="checkbox"/>
- Network call redirection (NCRD) :	<input checked="" type="checkbox"/>
- Trunk route optimization (TRO) :	<input type="checkbox"/>
- Recognition of DT12 ABCD FALT signal for ISL (FALT) :	<input type="checkbox"/>

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

AVAYA

CS1000 Element Manager

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

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

☐

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

☐

Integrated services digital network option (ISDN) :

☒

- Mode of operation (MODE) :

Route uses ISDN Signaling Link (ISLD) ▼

- D channel number (DCH) :

0 (0 - 254)

- Interface type for route (IFC) :

Meridian M1 (SL1) ▼

- Private network identifier (PNI) :

00001 (0 - 32700)

- Network calling name allowed (NCNA) :

☒

- Network call redirection (NCRD) :

☒

- Trunk route optimization (TRO) :

☐

- Recognition of DT12 ABCD FALT signal for ISL (FALT) :

☐

- Channel type (CHTY) :

B-channel (BCH) ▼

- Call type for outgoing direct dialed TIE route (CTYP) :

Unknown Call type (UKWN) ▼

- Insert ESN access code (INAC) :

☒

- Integrated service access route (ISAR) :

☐

- Display of access prefix on CLID (DAPC) :

☐

- Mobile extension route (MBXR) :

☐

- Mobile extension outgoing type (MBXOT) :

National number (NPA) ▼

- Mobile extension timer (MBXT) :

0 (0 - 8000 milliseconds)

Calling number dialing plan (CNDP) :

Unknown (UKWN) ▼

+ Basic Route Options

+ Network Options

+ General Options

+ Advanced Configurations

Submit

Refresh

Delete

Cancel



Click on **Basic Route Options**,

- Check **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.

AVAYA CS1000 Element Manager

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  
- Basic Route Options

Attendant announcement (ATAN): No Attendant Announcement. (NO) [v]  
Billing number required (BILN): [ ]  
Call detail recording (CDR): [ ]  
North American toll scheme (NATL): [x]  
Controls or timers (CNTL): [ ]  
Conventional (Tie trunk only) (CNVT): [ ]  
Incoming DID digit conversion on this route (IDC): [x]  
- Day IDC tree number (DCNO): 0 (0 - 254)  
- Night IDC tree number (NDNO): 0 (0 - 254)  
- Display external dialed digits (DEXT): [ ]  
Multifrequency compelled or MFC signaling (MFC): No MFC. (NO) [v]  
Process notification networked calls (PNNC): [ ]

+ Network Options  
+ General Options  
+ Advanced Configurations

Submit Refresh Delete Cancel

### 5.5.5. Administer Virtual Trunks

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

AVAYA CS1000 Element Manager

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

**Routes and Trunks**

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

+ Route: 0	Type: TIE	Description: SERVICE PROVIDER	Edit	Add trunk
+ Route: 1	Type: IMUS	Description: MUSIC	Edit	Add trunk
+ Route: 96	Type: TIE	Description: SIPL_ROUTE	Edit	Add trunk

The **Customer 0, Route 0, Trunk 1 Property Configuration** screen is displayed as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

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**

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: IPTI

Terminal number: 048 0 00 00

Designator field for trunk: VIR\_TRK

Extended trunk: VTRK

Member number: 1 \*

Level 3 Signaling:

Card density: 8D

Start arrangement Incoming: Immediate (IMM)

Start arrangement Outgoing: Immediate (IMM)

Trunk group access restriction: 1

Channel ID for this trunk: 1

Class of Service: Edit

- 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 (not shown).

**AVAYA**

**CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
Routes and Trunks » [Routes and Trunks](#) » [Customer 0\\_Route 0\\_Trunk 1 Property Configuration](#) » Class of Service Configuration

**Class of Service Configuration**

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

- 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) ▼
- Reversed Ear Piece :	Reversed Ear Piece denied (XREP) ▼

## 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**

**ISDN and ESN Networking**

**General Properties**

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code:  (0 - 9999)

Code for processing the called number

National access code:

International access code:

Options: ☒ Transfer on ringing of supervised external trunks

☒ Connection of supervised external trunks

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

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

Extended Local Calls: ☐

Extended Local Calls for IMS Line user: ☐

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

**Calling Line Identification**

Information for incoming/outgoing calls:

Size:  (0 - 4000)

Country code:  (0 - 9999)

Code displayed as part of calling number

[Calling Line Identification Entries](#)

Click on **Add** as shown below.

**AVAYA CS1000 Element Manager**

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:

End range:

\*End range\* should not exceed the CLID size specified

**Calling Line Identification Entries**

	Entry Id *	National Code	Local Code	Home location code	Local steering code	Use DN as DID
1	<input type="checkbox"/> 0	786	0758307			NO
2	<input type="checkbox"/> 1	786	0758308			NO
3	<input type="checkbox"/> 2	786	0758309			NO
4	<input type="checkbox"/> 3	786	0758310			NO

Add entry **0** as shown below, click on the **Save** button (not shown) after adding each entry.

- **National Code:** Input the three digit area code prefix of the DID number assigned by the service provider, in this case **786**.
- **Local Code:** input the seven digit number of the DID assigned by Service Provider, in this case it is **0758307** (Note that digits have been masked 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 using **Entry Id 1, 2, 3, 4, etc.**

**AVAYA** CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
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

UCM Network Services

Home

Links

Virtual Terminals

System

Customers

Routes and Trunks

Dialing and Numbering Plans

Phones

Tools

Security

Managing: 172.16.21.61    Username: admin

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

Calling Line Identification Entries

Search for CLID

Start range :

End range :

End range should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add...Delete

	Entry Id *	National Code	Local Code	Home location code	Local steering code	Use DN as DID
1	<input type="checkbox"/> 0	786	0758307			NO
2	<input type="checkbox"/> 1	786	0758308			NO
3	<input type="checkbox"/> 2	786	0758309			NO
4	<input type="checkbox"/> 3	786	0758310			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 and the title "CS1000 Element Manager". Below the header, a navigation pane on the left lists various system components, with "Dialing and Numbering Plans" and its sub-item "Electronic Switched Network" highlighted with a red box. The main content area shows the "Electronic Switched Network (ESN)" configuration page. At the top of this page, it indicates the user is managing IP address 172.16.21.61 with the username 'admin', and the current path is "Dialing and Numbering Plans » Electronic Switched Network (ESN)". The main configuration area is titled "Electronic Switched Network (ESN)" and contains a tree structure. Under "Customer 00", there is a "Network Control & Services" section. Within this section, "ESN Access Codes and Parameters (ESN)" is highlighted with a red box. Other items in the tree include "Coordinated Dialing Plan (CDP)" and "Numbering Plan (NET)".

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

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN)

**Electronic Switched Network (ESN)**

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - **ESN Access Codes and Parameters (ESN)**
    - Digit Manipulation Block (DGT)
    - Home Area Code (HNPA)
    - Flexible CLID Manipulation Block (CMDB)
    - Free Calling Area Screening (FCAS)
    - Free Special Number Screening (FSNS)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)
  - + Coordinated Dialing Plan (CDP)
  - + 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.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » ESN Access Codes and Basic Parameters

**ESN Access Codes and Basic Parameters**

**General Properties**

NARS/BARS Access Code 1:

NARS Access Code 2:

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

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time:  (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

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

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

### 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.

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

Managing: **172.16.21.61** Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN)

### Electronic Switched Network (ESN)

- 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

- Customer 00

- Network Control & Services
  - Network Control Parameters (NCTL)
  - ESN Access Codes and Parameters (ESN)
  - **Digit Manipulation Block (DGT)**
  - Home Area Code (HNPA)
  - Flexible CLID Manipulation Block (CMDB)
  - Free Calling Area Screening (FCAS)
  - Free Special Number Screening (FSNS)
  - Route List Block (RLB)
  - Incoming Trunk Group Exclusion (ITGE)
  - Network Attendant Services (NAS)
- + Coordinated Dialing Plan (CDP)
- + 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.

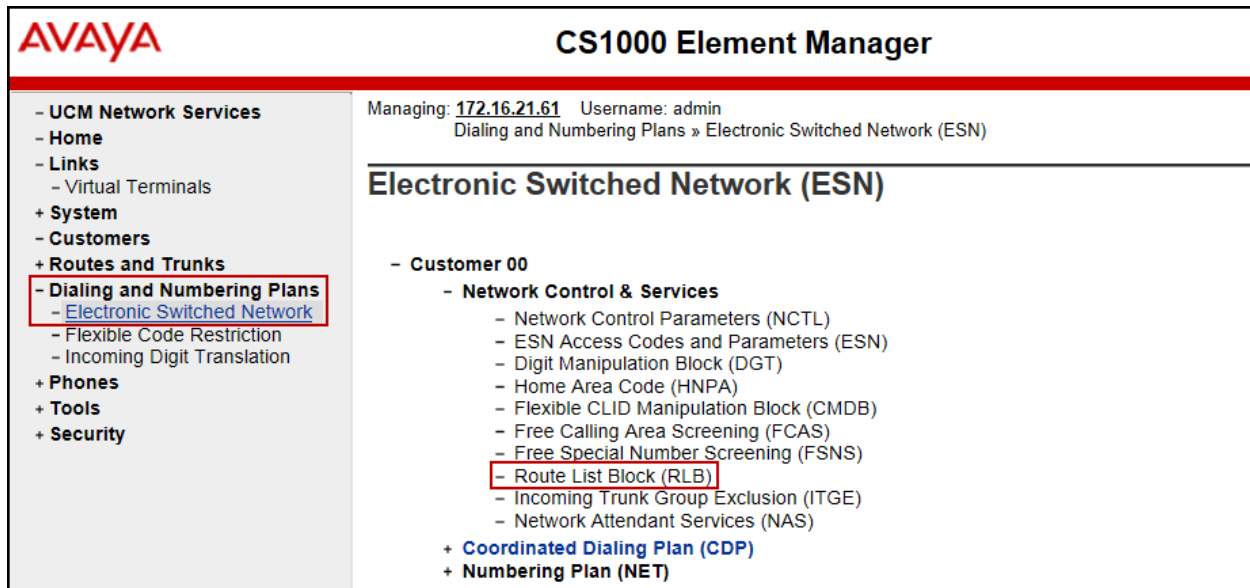
The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation menu with options like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'Dialing and Numbering Plans' section is expanded, showing 'Electronic Switched Network' as the selected option. The main content area is titled 'Digit Manipulation Block List'. It includes a breadcrumb trail: 'Managing: 172.16.21.61 Username: admin' followed by 'Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List'. Below the title, there is a form with a label 'Please choose the' followed by a dropdown menu currently showing 'Digit Manipulation Block Index 3' and a 'to Add' button. Below this, there are two entries: '+ Digit Manipulation Block Index -- 1' with an 'Edit' button, and '+ Digit Manipulation Block Index -- 2' with an 'Edit' button.

Enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits**, then click **Submit** (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface for configuring a 'Digit Manipulation Block'. The navigation menu on the left is the same as in the previous screenshot, with 'Electronic Switched Network' selected. The main content area is titled 'Digit Manipulation Block'. The breadcrumb trail is: 'Managing: 172.16.21.61 Username: admin' followed by 'Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block'. The configuration fields include: 'Digit Manipulation Index numbers:' with a text input containing '1'; 'Number of leading digits to be deleted:' with a text input containing '0' and a range '(0 - 19)' to its right; an 'Insert:' label with an empty text input field; an 'IP Special Number:' label with an unchecked checkbox; and 'Call Type to be used by the manipulated digits:' with a dropdown menu showing 'NPA (NPA)'.

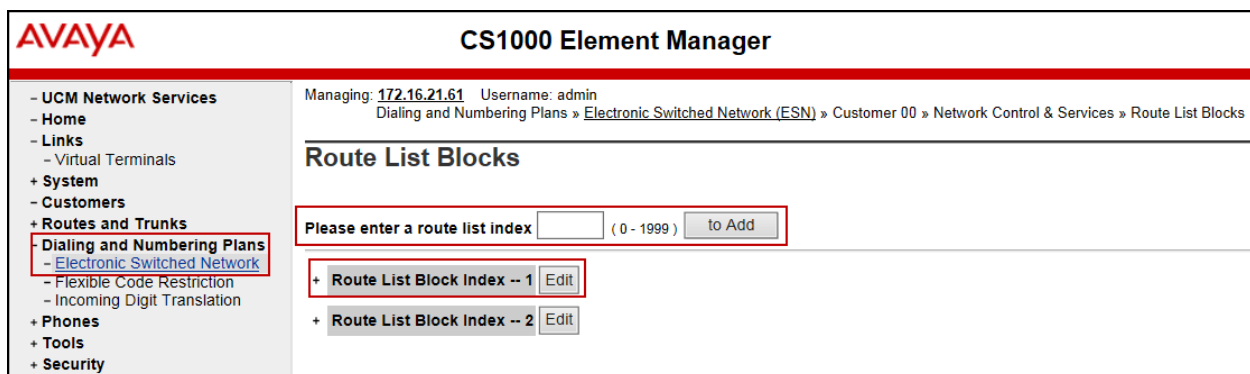
#### 5.6.4. Route List Block (RLB)

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** buttons (not shown).

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

**AVAYA CS1000 Element Manager**

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 - 256)

**Options**

Local Termination entry: ☐

**Route Number: 0**

Skip Conventional Signaling: ☐

Display Originator's Information: ☐

## 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.

**AVAYA**

**CS1000 Element Manager**

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

Managing: [172.16.21.61](#) Username: admin  
Dialing and Numbering Plans » [Incoming Digit Translation](#) » Customer 00

### Customer 00 Incoming Digit Conversion Property

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

RefreshCancel

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 7860758307 will be translated to the CS1000 extension number 8007 (note that digits have been masked for security reasons).

**AVAYA CS1000 Element Manager**

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: 7860758307 \*  
Converted digits: 8007 \* (0 - 99999999)

Force storage or removal of data: ☐

In case of conflict between the new and existing Incoming Digits, CPND language: ☒ Roman characters

CPND Name:   
first name, last name

Expected length:

Display format: First name, Last name

☐ Katakana characters

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 one of the digits have been blurred out for security reasons).

**AVAYA CS1000 Element Manager**

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

Add... Delete IDC Delete IDC tree

	Incoming Digits *	Converted Digits	CPND Name	CPND language
1	786 758307	8007	,	Roman characters
2	786 758308	8002	,	Roman characters
3	786 758309	8050	,	Roman characters
4	786 758310	8020	,	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 2.1.

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.

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

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN)

### Electronic Switched Network (ESN)

- Customer 00
  - + Network Control & Services
  - + Coordinated Dialing Plan (CDP)
  - Numbering Plan (NET)
    - Access Code 1
      - Home Location Code (HLOC)
      - Location Code (LOC)
      - Numbering Plan Area Code (NPA)
      - Exchange (Central Office) Code (NXX)
      - Special Number (SPN)
      - Network Speed Call Access Code (NSCL)
    - + Access Code 2



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.

CS1000 Element Manager

- 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 -- 69

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 RCBF
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 OCBF FLXD FTTC DNDY DNO3 MCBN
FDSF NOVD VOLA VOFD 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 was provisioned as follows:**

**Analog Station Provisioning** (this setting is required for **T.38** fax):

TYPE 500 .....Analog Station Type  
DN 3500.....Extension Number  
CLS DTN .....Digitone (DTMF)  
CLS FAXA .....Fax Class of Service  
CLS MPTD.....Will force T.38 codec selection when FAX V.21 preamble is detected.

### 5.7.2. Enable Privacy for the 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. On the left is a navigation pane with a tree structure: UCM Network Services, Home, Links, Virtual Terminals, System, Customers (highlighted with a red box), Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Customers' and shows a table with columns 'Customer Number' and 'Total Routes'. The first row shows '1000' with a total of '3' routes. The '00' part of the customer number is highlighted with a red box. Above the table are 'Add...' and 'Delete' buttons. At the top of the main area, it says 'Managing: 172.16.21.61' and 'Username: admin'.

Customer Number	Total Routes
1000	3

Select **Call Redirection** as shown below.

The screenshot displays the Avaya CS1000 Element Manager web interface. On the left is a navigation menu with the following items: - UCM Network Services, - Home, - Links (with a sub-item - Virtual Terminals), + System, - Customers (highlighted with a red box), + Routes and Trunks, + Dialing and Numbering Plans, + Phones, + Tools, and + Security. The main content area at the top shows 'Managing: 172.16.21.61' and 'Username: admin', with a breadcrumb trail: Customers » Customer 00 » Customer Details. Below this is the 'Customer Details' section, which contains a list of configuration options: Basic Configuration, Application Module Link, Attendant, Call Detail Recording, Call Party Name Display, Call Redirection (highlighted with a red box), 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** (not shown).

**AVAYA** CS1000 Element Manager

Days for day option 2:   
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:

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 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
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 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
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 EXR0
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
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:

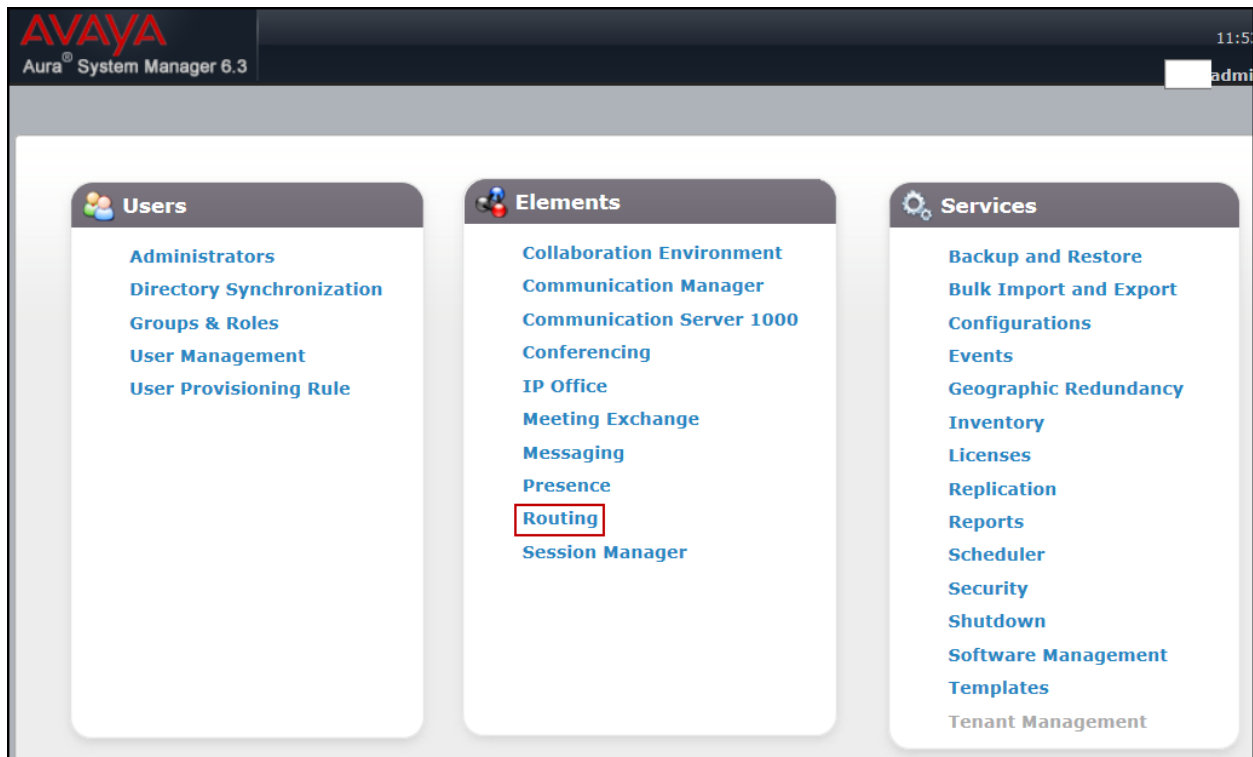
- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to the CS1000, the Avaya SBCE, and Session Manager itself.
- Entity Links, which define the SIP trunk parameters used by Session Manager 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.
- 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.

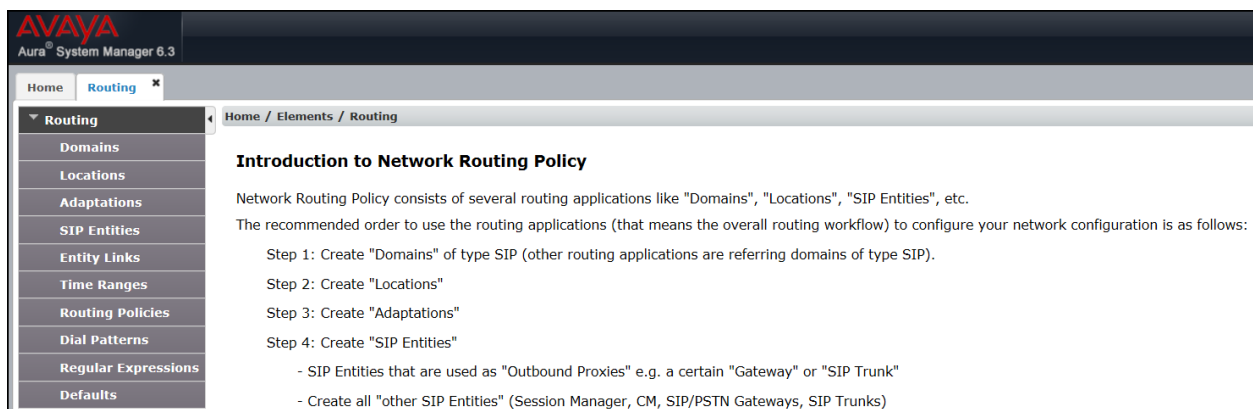
**Note:** Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

## 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**.

AVAYA  
Aura® System Manager 6.3

Home Routing

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

Home / Elements / Routing / Domains

Domain Management

Commit Cancel

1 Item

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

Commit Cancel

### 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 top header shows the Avaya logo and 'Aura® System Manager 6.3'. Below the header, there are tabs for 'Home' and 'Routing'. The 'Routing' tab is active, and a sub-menu on the left lists various routing-related items: 'Routing', 'Domains', 'Locations' (highlighted with a red box), 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area shows the 'Location Details' page for 'HG Session Manager'. The breadcrumb trail at the top reads 'Home / Elements / Routing / Locations'. The 'General' section contains a red-bordered box around the '\* Name:' field, which is filled with 'HG Session Manager'. Below it is a 'Notes:' field. At the top right of the form are 'Commit' and 'Cancel' buttons. Further down, there is a section titled 'Dial Plan Transparency in Survivable Mode' with an 'Enabled:' checkbox (unchecked) and fields for 'Listed Directory Number:' (containing a hyphen) and 'Associated CM SIP Entity:'.

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 'Home' and 'Routing' (with a close icon). A left-hand menu lists various configuration options: Routing, Domains, Locations (highlighted with a red box), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the breadcrumb 'Home / Elements / Routing / Locations' and the title 'Location Details' with 'Commit' and 'Cancel' buttons. Under the 'General' section, the 'Name' field (marked with a red asterisk) contains 'CS1k Node' and the 'Notes' field contains 'CS1K7.6', both highlighted with red boxes. Below this, the 'Dial Plan Transparency in Survivable Mode' section includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field (empty), and an 'Associated CM SIP Entity' field (empty).

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 and the text 'Aura® System Manager 6.3'. Below this, a breadcrumb trail reads 'Home / Elements / Routing / Locations'. The left sidebar contains a menu with 'Routing' expanded, showing sub-items: Domains, Locations (highlighted with a red box), Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, the 'Name' field is set to 'HG ASBCE' and the 'Notes' field is set to 'HG Avaya SBCE', both highlighted with red boxes. The 'Dial Plan Transparency in Survivable Mode' section shows an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field (empty), and an 'Associated CM SIP Entity' field (empty).



## 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 shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a menu with 'Routing' expanded, and 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and 'General'. It includes a 'Commit' button and a 'Cancel' button. The 'Adaptation Name' field is set to 'CS1K76', and the 'Module Name' dropdown is set to 'CS1000Adapter'. The 'Module Parameter Type' dropdown is empty, and the 'Egress URI Parameters' and 'Notes' fields are also empty.

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 OneStream.

- **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 web interface. The left sidebar shows a navigation menu with 'Adaptations' highlighted. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The 'Adaptation Name' field is set to 'HG SBCE'. The 'Module Name' is set to 'DigitConversionAdapter' and the 'Module Parameter Type' is set to 'Name-Value Parameter'. Below these fields are 'Add' and 'Remove' buttons. A table lists parameters, with 'MIME' set to 'no'. 'Commit' and 'Cancel' buttons are at the top right. A red box highlights the adaptation details section.

Name	Value
MIME	no

## 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' highlighted. The main content area is titled 'SIP Entity Details' and includes a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. There are 'Commit' and 'Cancel' buttons at the top right.

**General**

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

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration (dropdown)

**Port**

TCP Failover port: (text field)  
TLS Failover port: (text field)  
Add Remove

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

Select : All, None

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**.
- Type: **Other**.
- For Adaptation select the **CS1K76** adaptation defined in **Section 6.4**.
- For Location select the **CS1k Node** location defined in **Section 6.3**.
- **Time Zone:** Select the time zone which the entity belongs to.

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 left sidebar shows a navigation menu with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. A red box highlights the form fields for creating a new SIP entity. The fields are as follows:

Field	Value
* Name	CS1K7.6
* FQDN or IP Address	172.16.20.60
Type	Other
Notes	CS1000 Rel. 7.6
Adaptation	CS1K76
Location	CS1k Node
Time Zone	America/New_York

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

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**).
- **Type:** **Other**.
- For Adaptation select the **HG SBCE** adaptation defined in **Section 6.4**.
- For Location select the **HG ASBCE** location defined **Section 6.3**.
- **Time Zone:** Select the time zone which the entity belongs to.

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 top navigation bar includes the Avaya logo and the text 'Aura System Manager 6.3'. Below this, there are tabs for 'Home' and 'Routing'. The 'Routing' tab is active, and a sub-menu on the left lists various routing-related options: 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 the entity named 'HG ASBCE'. The form is titled 'SIP Entity Details' and has a 'General' tab selected. The fields are as follows: '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). The form is enclosed in a red rectangular border. At the top right of the form, there are 'Commit' and 'Cancel' buttons.

## 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 7.2.3**.
- **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 Routing

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

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item

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

Select : All, None

Commit Cancel

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

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
* HG Session Manager	* HG Session Manager	TCP	* 5060	* HG ASBCE	<input type="checkbox"/>	* 5060	trusted

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.

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
<a href="#">HG Session Manager AAC 5060 TCP</a>	HG Session Manager	TCP	5060	AAC	<input type="checkbox"/>	5060	trusted
<a href="#">HG Session Manager Acme Packet sip1 5060 TCP</a>	HG Session Manager	TCP	5060	Acme Packet sip1	<input type="checkbox"/>	5060	trusted
<a href="#">HG Session Manager CS1K7.6 5085 UDP</a>	HG Session Manager	UDP	5085	CS1K7.6	<input type="checkbox"/>	5085	trusted
<a href="#">HG Session Manager EdgeMarc SBC 5060 UDP</a>	HG Session Manager	UDP	5060	EdgeMarc SBC	<input type="checkbox"/>	5060	trusted
<a href="#">HG Session Manager HG AA-SBC 5060 TCP</a>	HG Session Manager	TCP	5060	HG AA-SBC	<input type="checkbox"/>	5060	trusted
<a href="#">HG Session Manager HG ASBCE 5060 TCP</a>	HG Session Manager	TCP	5060	HG ASBCE	<input type="checkbox"/>	5060	trusted



## 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.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- \* Name:** To CS1K76
- Disabled:** ☐
- \* Retries:** 0
- Notes:** Inbound Calls to CS1K76

The 'SIP Entity as Destination' section has a 'Select' button. Below this is a table with the following data:

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 shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Routing Policies' selected. The main area is titled 'Routing Policy Details' and contains a 'General' section. In the 'General' section, the 'Name' field is set to 'To HG ASBCE', 'Disabled' is unchecked, 'Retries' is set to 0, and the 'Notes' field contains 'Outbound calls via ASBCE'. Below this is a 'SIP Entity as Destination' section with a 'Select' button. At the bottom, a table lists the configured policy:

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 OneStream 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).

The screenshot shows the 'Dial Pattern Details' form in the Avaya Aura System Manager 6.3. The 'General' tab is active. The 'Pattern' field is set to '1', with 'Min' set to '1' and 'Max' set to '11'. The 'SIP Domain' is set to '-ALL-'. The 'Emergency Call' checkbox is unchecked. The 'Emergency Priority' is set to '1'. The 'Emergency Type' is set to 'None'. The 'Notes' field is empty. Below the form, the 'Originating Locations and Routing Policies' table shows 5 items. The first item is highlighted with a red border:

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

The next example shown below is for dial pattern **786075** to route inbound calls to DID numbers provided by OneStream (DID numbers assigned to extensions in the CS1000). For calls that begin with 786075, are between **6** 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.

The screenshot shows the 'Dial Pattern Details' form in the Avaya Aura System Manager 6.3. The 'General' tab is active. The 'Pattern' field is set to '786075', with 'Min' set to '6' and 'Max' set to '10'. The 'SIP Domain' is set to 'avaya.lab.com'. The 'Emergency Call' checkbox is unchecked. The 'Emergency Priority' is set to '1'. The 'Emergency Type' is set to 'None'. The 'Notes' field is empty. Below the form, the 'Originating Locations and Routing Policies' table shows 1 item. The first item is highlighted with a red border:

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

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, etc.

## 6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This should have been done as part of the initial Session Manager installation. If Session Manager needs to be added, 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 **Commit** (not shown) to add Session Manager.

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar contains a navigation menu with the following items: Home, Session Manager, Session Manager Administration (highlighted with a red box), Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, System Tools, and Performance. The main content area is titled 'View Session Manager' and includes a 'Return' button. Below the title, there is a breadcrumb trail: Home / Elements / Session Manager / Session Manager Administration. The interface is divided into two main sections: 'General' and 'Security Module'. The 'General' section contains the following fields: 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), and VMware Virtual Machine (checkbox). The 'Security Module' section contains the following fields: SIP Entity IP Address (172.16.5.32), Network Mask (255.255.255.0), Default Gateway (172.16.5.254), Call Control PHB (46), QOS Priority (6), Speed & Duplex (Auto), and VLAN ID (dropdown). At the bottom of the Security Module section, there is a note: \*SIP Firewall Configuration Rule Set for HG Session Manager.

AVAYA  
Aura® System Manager 6.3

Home / Session Manager

Home / Elements / Session Manager / Session Manager Administration

### View Session Manager

Return

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

#### General

SIP Entity Name: 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: 6

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 OneStream'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. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

### 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**.

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

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar lists 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The main content area is titled 'Dashboard' and contains three sections: 'Information', 'Installed Devices', and 'Alarms (past 24 hours)'. The 'Information' section shows system time, version, build date, license state, and licensing overages. The 'Installed Devices' section shows a table with one device, 'Avaya SBCE'. The 'Alarms (past 24 hours)' section shows a table with five incidents, all with the message 'Avaya SBCE: No Server Flow Matched for Incoming Message'. There is also a 'Notes' section at the bottom, which is empty.

Information	
System Time	09:25:34 PM CST <a href="#">Refresh</a>
Version	6.3.000-19-4338
Build Date	Fri Sep 26 09:14:23 EDT 2014
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS
Avaya SBCE

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message
Avaya SBCE: No Server Flow Matched for Incoming Message

Notes
No notes found.

To view the system information that was 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 **Avaya SBCE** was already added. To view the configuration of this device, click on **View** as shown in the screenshot below.

The screenshot shows the 'Session Border Controller for Enterprise' system management page. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'PPM Services', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The main content area is titled 'System Management' and contains a tabbed interface with 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is active, showing a table with one device, 'Avaya SBCE'. The 'View' button for this device is highlighted with a red box.

Device Name	Management IP	Version	Status	Actions
Avaya SBCE	10.10.10.10	6.3.000-19-4338	Commissioned	<a href="#">Reboot</a> <a href="#">Shutdown</a> <a href="#">Restart Application</a> <a href="#">View</a> <a href="#">Edit</a> <a href="#">Uninstall</a>

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: Avaya SBCE

General Configuration

Appliance Name

Avaya SBCE

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 2000

2000

Advanced Sessions

Requested: 2000

2000

Scopia Video Sessions

Requested: 500

500

Encryption

☒

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
10.10.157.187	10.10.157.187	255.255.255.192	64.197.157.129	B1
10.10.157.188	10.10.157.188	255.255.255.192	64.197.157.129	B1
10.10.157.189	10.10.157.189	255.255.255.192	64.197.157.129	B1
10.10.157.190	10.10.157.190	255.255.255.192	64.197.157.129	B1
10.10.157.191	10.10.157.191	255.255.255.192	64.197.157.129	B1
10.10.157.192	10.10.157.192	255.255.255.192	64.197.157.129	B1

DNS Configuration

Primary DNS

172.16.5.102

Secondary DNS

DNS Location

DMZ

DNS Client IP

172.16.5.71

Management IP(s)

IP

172.16.5.71

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 OneStream. 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).**



## 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:

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

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main title is "Session Border Controller for Enterprise".

On the left, a sidebar menu lists various configuration categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking (highlighted), Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding, Signaling Manipulation, URI Groups, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Interworking Profiles: Avaya-SM" and features an "Add" button. Below this, a list of interworking profiles is shown, including cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, **Avaya-SM** (highlighted), SP-General, Avaya-CS1000, Avaya-IPO, and Avaya-CM.

The configuration for the selected "Avaya-SM" profile is displayed in the "General" tab. The tabs available are General, Timers, URI Manipulation, Header Manipulation, and Advanced. The "General" tab contains the following settings:

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
<b>T.38 Support</b>	<b>Yes</b>
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

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

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. The top navigation bar includes 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', and 'Users'. The left sidebar shows a tree view with 'Global Profiles' expanded, and 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: Avaya-SM' and features a list of profiles on the left, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM' (highlighted), 'SP-General', 'Avaya-CS1000', 'Avaya-IPO', and 'Avaya-CM'. An 'Add' button is located above the list. The right pane shows the 'Advanced' tab with a table of configuration parameters.

General	Timers	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both
Topology Hiding: Change Call-ID				No
Call-Info NAT				No
Change Max Forwards				Yes
Include End Point IP for Context Lookup				Yes
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

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

## 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, clicking **Next**:

On the **General** tab:

- Check **T.38 Support**.
- Leave other fields with their default values.
- Click **Next** until the Advanced tab is reached, then click **Finish** on the Advanced tab.

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

The screenshot displays the 'Session Border Controller for Enterprise' management interface. On the left is a navigation pane with categories like Dashboard, Administration, System Management, and Global Profiles. Under 'Global Profiles', 'Server Interworking' is selected. The main area shows 'Interworking Profiles: SP-General' with a list of profiles including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-cm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-CS1000', 'Avaya-IPO', and 'Avaya-CM'. An 'Add' button is present. The 'General' tab is active, showing a table of settings. The 'T.38 Support' setting is checked (Yes). Other settings include Hold Support (NONE), 180 Handling (None), 181 Handling (None), 182 Handling (None), 183 Handling (None), Refer Handling (No), URI Group (None), Send Hold (No), 3xx Handling (No), Diversion Header Support (No), Delayed SDP Handling (No), Re-Invite Handling (No), URI Scheme (SIP), and Via Header Format (RFC3261). The 'Privacy' section shows Privacy Enabled (No), User Name, P-Asserted-Identity (No), P-Preferred-Identity (No), and Privacy Header. The 'DTMF' section shows DTMF Support (None). An 'Edit' button is at the bottom right.

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

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

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

AlarmsIncidentsStatusLogsDiagnosticsUsers

## Session Border Controller for Enterprise

DashboardAdministrationBackup/RestoreSystem Management▸ Global Parameters▸ **Global Profiles**▸ Domain DoSFingerprint**Server Interworking**Phone InterworkingMedia ForkingRoutingServer ConfigurationTopology HidingSignaling ManipulationURI Groups▸ PPM Services▸ Domain Policies▸ TLS Management▸ Device Specific Settings

Interworking Profiles: SP-GeneralAdd

Interworking Profiles

cs2100avaya-ruOCS-Edge-Servercisco-cmcupsSipera-HaloOCS-FrontEnd-ServerAvaya-SM**SP-General**Avaya-CS1000Avaya-IPOAvaya-CM

Click here to add a description

GeneralTimersURI ManipulationHeader Manipulation**Advanced**

Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
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

Edit

HG; Reviewed:  
SPOC 3/2/2015

Solution & Interoperability Test Lab Application Notes  
©2015 Avaya Inc. All Rights Reserved.

101 of 144  
OneStCS1KSMSBCE

### 7.2.3. Server Configuration

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

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

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

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

IP Address / FQDN	Port	Transport
172.16.5.32	5060	TCP

- Click **Next** on the **Authentication** window.
- Click **Next** on the **Heartbeat** window.

On the **Advanced** tab:

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

**Add Server Configuration Profile - Advanced**

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya-SM

Signaling Manipulation Script None

Connection Type SUBID

Back Finish

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

Alarms Incidents Status 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 PPM Services Domain Policies TLS Management Device Specific Settings

### Server Configuration: Session Manager

Add Rename Clone Delete

Server Profiles

Session Manager

Service Provider

Com Manager

CS1000

IP Office

General Authentication Heartbeat Advanced

Server Type Call Server

IP Address / FQDN	Port	Transport
172.16.5.32	5061	TLS
172.16.5.32	5060	TCP

Edit

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main header reads "Session Border Controller for Enterprise".

On the left, a sidebar menu lists various configuration areas: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Server Configuration: Session Manager" and features an "Add" button. Below this, a list of server profiles is shown: Session Manager (highlighted), Service Provider, Com Manager, CS1000, and IP Office.

The "Advanced" tab is selected, showing the following configuration options:

General	Authentication	Heartbeat	Advanced
Enable DoS Protection <input type="checkbox"/>			
Enable Grooming <input checked="" type="checkbox"/>			
Interworking Profile Avaya-SM			
TLS Client Profile AvayaSBCCClient			
Signaling Manipulation Script None			
Connection Type SUBID			

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



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**.

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

- **Server Type:** Select **Trunk Server**.
- **IP Address / FQDN:** **192.168.45.227** (IP Address of the Service Provider SIP Proxy).
- **Port:** **5060** (This port must match the port number defined in **Section 6.6**).
- **Transports:** Select **UDP**.
- Click **Next**.

IP Address / FQDN	Port	Transport
192.168.45.227	5060	UDP

- Click **Next** on the **Authentication** window.
- Click **Next** on the **Heartbeat** window.

On the **Advanced** tab:

- Select **SP-General** from the **Interworking Profile** drop down menu.
- Leave the **Signaling Manipulation Script** at the default **None**, a signaling manipulation script will be assigned latter.
- Click **Finish**.

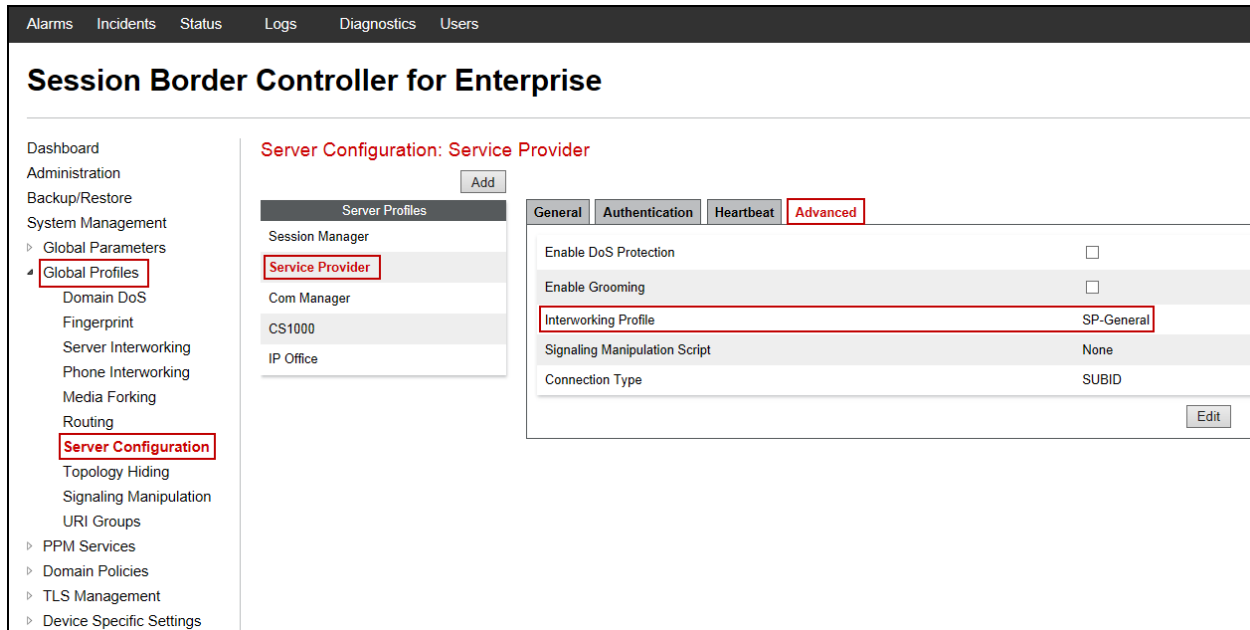
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-General
Signaling Manipulation Script	None
Connection Type	SUBID

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Status, 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 "Server Configuration" highlighted. The main content area is titled "Server Configuration: Service Provider" and features a tabbed interface with "General", "Authentication", "Heartbeat", and "Advanced" tabs. The "General" tab is active, showing a table of Trunk Servers. The table has columns for IP Address / FQDN, Port, and Transport. A single entry is visible: IP Address 192.168.45.227, Port 5060, and Transport UDP. Buttons for "Add", "Rename", "Clone", "Delete", and "Edit" are present.

IP Address / FQDN	Port	Transport
192.168.45.227	5060	UDP

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



#### 7.2.4. 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 Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Session Manager**.
- **Next Hop Address:** Select **172.16.5.32:5060 (TCP)** (Session Manager IP address, Port and Transport).
- Click **Finish**.

X

URI Group \*

Time of Day default

Load Balancing Priority

NAPTR ☐

Transport None

Next Hop Priority ☒

Next Hop In-Dialog ☐

Ignore Route Header ☐

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manage	172.16.5.32:5060 (TCP)	None

Back
Finish

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

Alarms Incidents Status Logs Diagnostics Users
Settings Help Log Out

**Session Border Controller for Enterprise**
AVAYA

Dashboard  
Administration  
Backup/Restore  
System Management  
   > Global Parameters  
   4 Global Profiles  
     Domain DoS  
     Fingerprint  
     Server Interworking  
     Phone Interworking  
     Media Forking  
     **Routing**  
       Server Configuration  
       Topology Hiding  
       Signaling Manipulation  
       URI Groups  
   > PPM Services  
   > 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

Route\_to\_IPO

To SM from Rem W

Routing Profile

Update Priority

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	172.16.5.32	TCP

Edit
Delete

HG; Reviewed:  
SPOC 3/2/2015

Solution & Interoperability Test Lab Application Notes  
©2015 Avaya Inc. All Rights Reserved.

108 of 144  
OneStCS1KSMSBCE

Similarly, for the outbound route:

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route\_to\_SP**.
- Click **Next**.

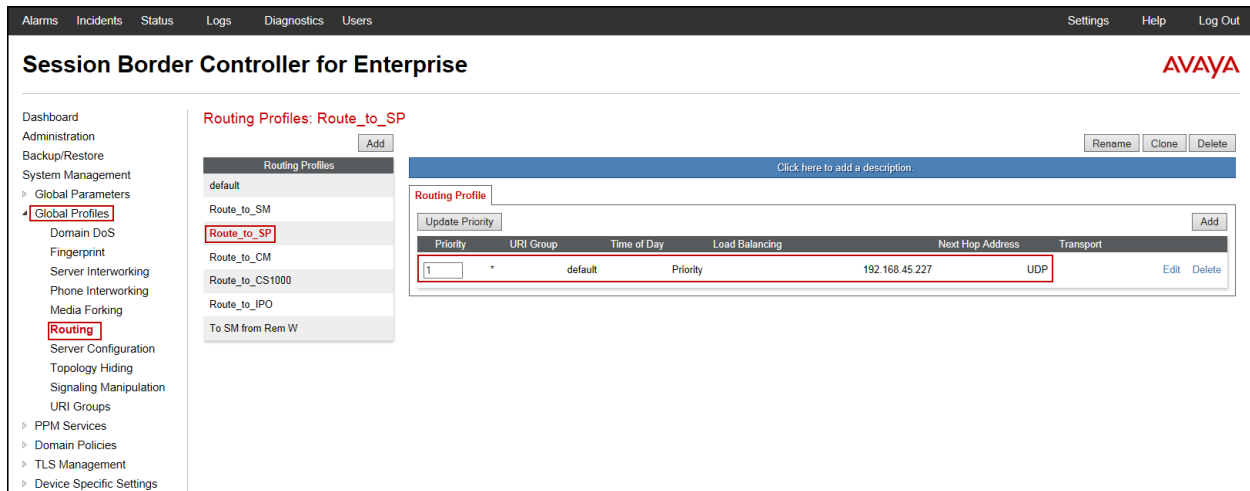
On the Routing Profile screen complete the following:

- Click on the **Add** button to add a **Next-Hop Address**.
- **Priority / Weight: 1**
- **Server Configuration:** Select **Service Provider**.
- **Next Hop Address:** Select **192.168.45.227:5060 (UDP)** (Service Provider SIP Proxy IP address, Port and Transport).
- Click **Finish**.

URI Group	Time of Day
*	default
Load Balancing	Priority
Transport	None
Next Hop In-Dialog	Ignore Route Header

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Service Provider	192.168.45.227:5060 (UDP)	None

The following screen capture shows the newly created **Route\_to\_SP** 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 un-trusted 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).

AlarmsIncidentsStatusLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for EnterpriseAVAYA

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

Topology Hiding Profiles: Session\_ManagerAddRenameCloneDelete

Topology Hiding Profilesdefaultcisco\_th\_profileSession\_ManagerService\_ProviderCom ManagerCS1000IP Office

Click here to add a description.

Topology Hiding

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

Edit

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 Status 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

PPM Services Domain Policies TLS Management Device Specific Settings

**Topology Hiding Profiles: Service\_Provider**

Add

Rename Clone Delete

Click here to add a description

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

Edit



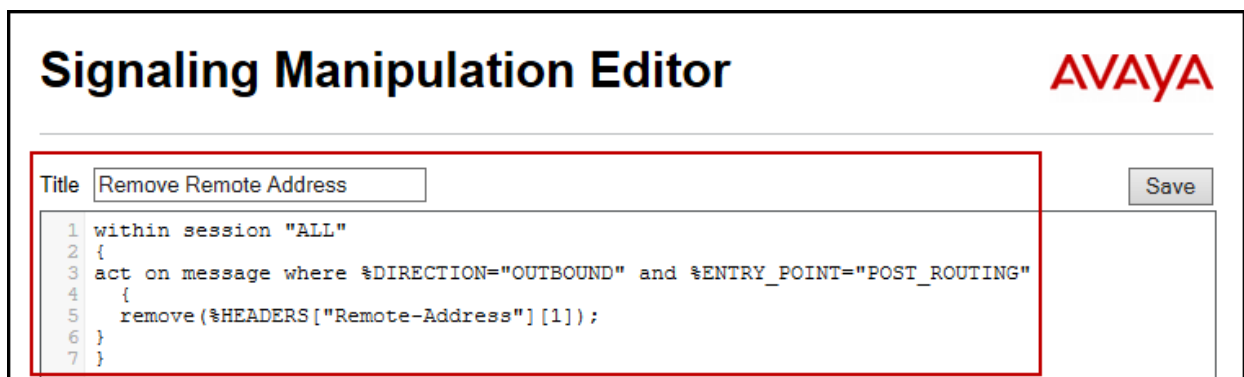
### 7.2.6. Signaling Manipulation

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.

- 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**.



**Signaling Manipulation Editor** AVAYA

Title  Save

```
1 within session "ALL"
2 {
3   act on message where $DIRECTION="OUTBOUND" and $ENTRY_POINT="POST_ROUTING"
4   {
5     remove($HEADERS["Remote-Address"][1]);
6   }
7 }
```

The following screen shows the newly added Signaling Manipulation script.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar contains a navigation menu with 'Global Profiles' expanded, showing 'Signaling Manipulation' as a sub-option. The main content area is titled 'Signaling Manipulation Scripts: Remove Remote Address'. It features a list of scripts on the left, with 'Remove Remote Address' highlighted. The right pane shows the script configuration, including a description field and a code editor containing the following JSON:

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

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

After the Signaling Manipulation Script is created, it should be applied to the **Service Provider Server Configuration Profile** previously created in **Section 7.2.3**.

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 screenshot shows the 'Edit Server Configuration Profile - Advanced' dialog box. It contains several configuration fields: 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown menu set to 'SP-General'), 'Signaling Manipulation Script' (dropdown menu set to 'Remove Remote Address'), and 'Connection Type' (dropdown menu set to 'SUBID'). A 'Finish' button is located at the bottom center of the dialog.

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

The screenshot displays the configuration interface for a Session Border Controller for Enterprise. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main title is "Session Border Controller for Enterprise".

On the left, a sidebar menu lists various configuration categories: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted), Topology Hiding, Signaling Manipulation, URI Groups, PPM Services, Domain Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Server Configuration: Service Provider" and features an "Add" button. Below this, a list of server profiles is shown: Session Manager, Service Provider (highlighted), Com Manager, CS1000, and IP Office.

The "Advanced" tab is selected, showing the following configuration options:

General	Authentication	Heartbeat	Advanced
Enable DoS Protection <input type="checkbox"/>			
Enable Grooming <input type="checkbox"/>			
Interworking Profile SP-General			
Signaling Manipulation Script Remove Remote Address			
Connection Type SUBID			

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

## 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**.

- Click on the **Add** button to add a new rule.
- **Rule Name:** enter the name of the profile, e.g., **2000 Sessions**.
- Under **Audio** check **In** and **Out** and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** was used in the sample configuration.
- Click **Finish**.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	<input checked="" type="radio"/> None <input type="radio"/> CDR w/ RTP <input type="radio"/> CDR w/o RTP
RTCP Keep-Alive	<input type="checkbox"/>

Back Finish

The following screen capture shows the newly created **2000 Sessions** application rule.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'Application Rules' selected. The main content area is titled 'Application Rules: 2000 Sessions'. It features a list of application rules on the left, with '2000 Sessions' highlighted. The right pane shows the configuration for this rule, including a table for application types and miscellaneous settings.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous settings:

- CDR Support: None
- RTCP Keep-Alive: No

### 7.3.2. Media Rules

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left sidebar shows the navigation menu with 'Domain Policies' expanded and 'Media Rules' selected. The main content area is titled 'Media Rules: default-low-med'. It features a list of media rules on the left, with 'default-low-med' highlighted. The right pane shows the configuration for this rule, including a warning message and tabs for various media-related settings.

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

Media NAT | Media Encryption | Media Silencing | Media QoS | Media BFCP | Media FECC

Media NAT Learn Media IP dynamically Edit

### 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 Rule was created, to later be applied in the direction of the Enterprise to block unwanted headers coming from Session Manager from being propagated to the OneStream network. To add this header, 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 **SessMgr\_SigRule** 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 **Endpoint-View** header:

- Select **Add in Header Control**
- Check the **Proprietary Request Header** box
- **Header Name: Endpoint-View**
- **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 is titled 'Signaling Rules: SessMgr\_SigRule' and features a table of headers. The 'Request Headers' tab is selected, showing a list of 8 headers. The header 'x-nt-e164-clid' is highlighted in red.

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

Select the **Response Headers** tab of the newly created **SessMgr\_SigRule** 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 top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo.

On the left is a sidebar menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies (expanded), Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (highlighted), Time of Day Rules, End Point Policy Groups, Session Policies, TLS Management, and Device Specific Settings.

The main content area is titled "Signaling Rules: SessMgr\_SigRule". It features a list of signaling rules on the left, with "SessMgr\_SigRule" selected. The right pane shows the configuration for this rule, with tabs for General, Requests, Responses, Request Headers, Response Headers (active), Signaling QoS, and UCID. The "Response Headers" tab contains a table of response headers.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
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

A second Signaling Rules was created, to later be applied in the direction of the Service Provider. This Signaling Rule changes the “Contact” header name in “183 response codes” to “180 Ringing”. This change was necessary in order to solve no ring back tones issues on PSTN stations when calls from the PSTN to CS1000 SIP endpoints are transferred back out to the PSTN (Refer to **Section 2.2**). To add this signaling rule, 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: **Contact**.
- Click **Finish**.

Select the **Response Headers** tab of the newly created **Contact** signaling rule.

- Select **Add in Header Control**
- **Header Name: Contact**.
- **Response Code: 183**
- **Method Name: INVITE**
- **Header Criteria: Forbidden**
- **Presence Action: Select: Change response to...**  
Enter: **180 Ringing**
- Click **Finish**

The screenshot shows the 'Add Header Control' dialog box. The fields are as follows:

Field	Value
Proprietary Response Header	<input type="checkbox"/>
Header Name	Contact
Response Code	183
Method Name	INVITE
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	Change response to... 180 Ringing

Finish

### 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: 2000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: SessMgr\_SigRule.**
- Click **Finish**.

Policy Group

Application Rule: 2000 Sessions

Border Rule: default

Media Rule: default-low-med

Security Rule: default-low

Signaling Rule: SessMgr\_SigRule

Back Finish

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

Session Border Controller for Enterprise

Policy Groups: Enterprise

Order	Application	Border	Media	Security	Signaling	
1	2000 Sessions	default	default-low-med	default-low	SessMgr_SigRule	Edit

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

- **Group Name: Service Provider.**
- **Application Rule: 2000 Sessions.**
- **Border Rule: default.**
- **Media Rule: default-low-med.**
- **Security Rule: default-low.**
- **Signaling Rule: Contact.**
- Click **Finish**.

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

## 7.4. Device Specific Settings

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

### 7.4.1. Network Management

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. The left sidebar contains a menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under "Device Specific Settings", "Network Management" is highlighted. The main content area is titled "Network Management: Avaya SBCE" and features two tabs: "Interfaces" and "Networks". The "Networks" tab is active, showing a table with columns for Name, Gateway, Subnet Mask, Interface, and IP Address. Two network entries are listed: Network\_A1 and Network\_B1. Red boxes highlight the IP addresses in the original image.

Name	Gateway	Subnet Mask	Interface	IP Address	
Network_A1	172.16.5.254	255.255.255.0	A1	172.16.5.71	Edit Delete
Network_B1	10.10.157.129	255.255.255.192	B1	10.10.157.187	Edit Delete

On the **Interface** Configuration tab, click the **Disabled** 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 (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. The left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Device Specific Settings. The "Device Specific Settings" category is expanded, and "Network Management" is selected. The main content area is titled "Network Management: Avaya SBCE" and features three tabs: "Devices", "Interfaces", and "Networks". The "Interfaces" tab is active, showing a table with the following data:

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

An "Add VLAN" button is located in the top right corner of the interface table.

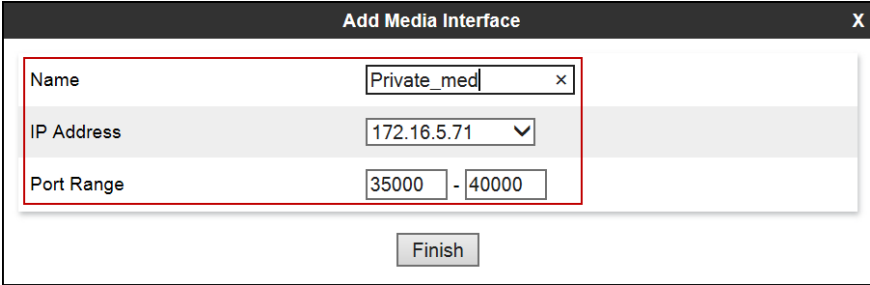


### 7.4.2. Media Interface

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.

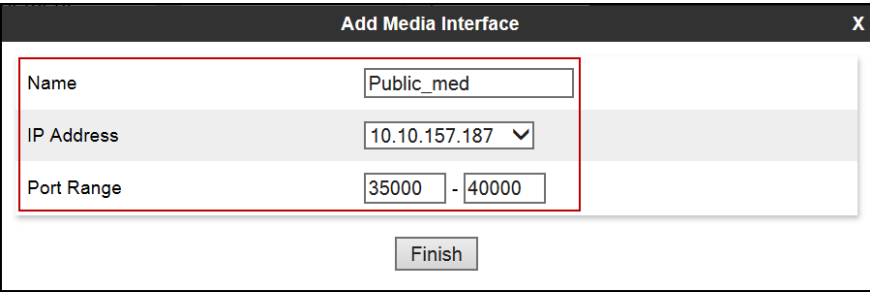
- Select **Add** in the **Media Interface** area (not shown).
- **Name:** **Private\_med**.
- **IP Address:** **172.16.5.71** (Inside or Private IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range:** **35000-40000**.
- Click **Finish**.



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.

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:** **10.10.157.187** (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 "10.10.157.187", 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.

The following screen capture shows the newly created media interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, 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 "Device Specific Settings" and "Media Interface" highlighted. The main content area is titled "Media Interface: Avaya SBCE" and features a tabbed interface with "Media Interface" selected. 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." Below this is a table of media interfaces with columns for Name, Media IP, and Port Range. The table lists two interfaces: "Private\_med" and "Public\_med", both with Media IP 172.16.5.71 and Port Range 35000 - 40000. Each interface has "Edit" and "Delete" links. An "Add" button is located at the top right of the table.

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	10.10.157.187	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**.

Name	Private_sig
IP Address	172.16.5.71
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	
TLS Profile	None
Enable Shared Control	<input type="checkbox"/>
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: 10.10.157.187** (Outside or Public IP Address of the Avaya SBCE, toward the Service Provider).
- **UDP Port: 5060.**
- Click **Finish**.

**Add Signaling Interface** X

Name	Public_sig
IP Address	10.10.157.187 ▼
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	5060 x
TLS Port Leave blank to disable	
TLS Profile	None ▼
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

The following screen capture shows the newly created signaling interfaces.

Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

## Session Border Controller for Enterprise

AVAYA

- Dashboard
- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
  - PPM Services
  - Domain Policies
  - TLS Management
  - Device Specific Settings**
    - Network Management
    - Media Interface
    - Signaling Interface**
    - End Point Flows
    - Session Flows
      - DMZ Services
    - TURN/STUN Service
    - SNMP
    - Syslog Management
    - Advanced Options
    - Troubleshooting

### Signaling Interface: Avaya SBCE

Devices  
Avaya SBCE

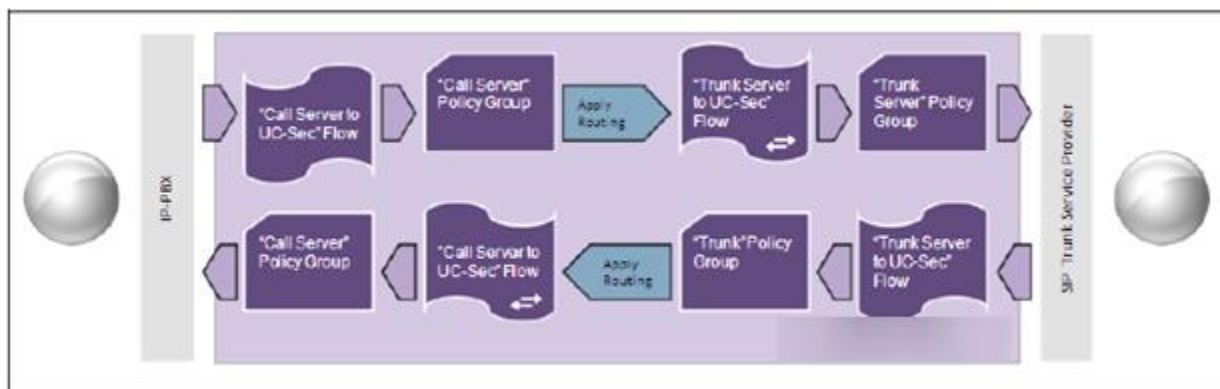
Signaling Interface

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

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.71	5060	---	---	None	Edit Delete
Public_sig	10.10.157.187	---	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.
- **Signaling Manipulation Script:** None
- Click **Finish**.

Edit Flow: SIP_Trunk_Flow	
Flow 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
Topology Hiding Profile	Service_Provider
File Transfer Profile	None
Signaling Manipulation Script	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.
- **Signaling Manipulation Script:** None
- Click **Finish**.

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

Signaling Manipulation Script: None

Finish

The following screen capture shows the newly created **End Point Flows**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Status, 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: Avaya SBCE". It features two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab. An "Add" button is located in the top right corner of the "Server Flows" section.

Below the tabs, there are two configuration sections:

- Server Configuration: Service Provider**: This section contains a table with the following data:

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	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
- Server Configuration: Session Manager**: This section contains a table with the following data:

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
2	Session_Manager_Flow	*	Public_sig	Private_sig	Enterprise	Route_to_SP	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>



## 8. OneStream SIP Trunk Service Configuration

To use OneStream SIP Trunk service, a customer must request the service from OneStream using the established sales processes. The process can be started by contacting OneStream via the corporate web site at: <http://www.onestreamnetworks.com/Default.aspx?RD=3340> or by calling the Toll Free number at 1-800-869-0315 and requesting information.

During the signup process, OneStream will require that the customer provide the public IP address used to reach Avaya SBCE at the edge of the enterprise. OneStream 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 from/to 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.

## 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
TRA000
.trac 0 8000

ACTIVE VTN 008 0 00 00

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

## 9.2. Protocol Traces

Wireshark was used to verify SIP message information for each call. Wireshark traces were captured on the outside or public network side of the SIP Trunk, in between the simulated enterprise and OneStream.

## 10. Conclusion

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) Trunk service for an enterprise solution consisting of Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.3 to support OneStream Global SIP Trunking Services, as shown in **Figure 1**.

Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results 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] *Avaya Communication Server 1000 Network Routing Service Fundamentals*, Release 7.6, Document Number NN43001-130, Issue 04.04, June 2014.
- [2] *Avaya Communication Server 1000 IP Peer Networking Installation and Commissioning*, Release 7.6, Document Number NN43001-313, Issue 06.04, September 2014.
- [3] *Avaya Communication Server 1000E Overview*, Release 7.6, Document Number NN43041-110, Issue 06.02, June 2014.
- [4] *Unified Communications Management Common Services Fundamentals Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.
- [5] *Avaya Communication Server 1000 Dialing Plans Reference*, Release 7.6, Document Number NN43001-283, Issue 06.02, July 2014.
- [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 Release 7.6: An Overview*. Document Number PSN003460u, Issue 02, April 05, 2013.
- [8] *Communication Server 1000 Release 7.6 & Service Pack 5 Release Notes*, Issue 4.0 September 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 4, June 2014.
- [10] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, September 2014.
- [11] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3, Issue 6, December 2014.

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 6.3, Issue 4, October 2014.
- [13] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014.

Other resources:

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

## 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]);
}
}
```

**©2015 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).