



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Bright House Networks SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Bright House Networks SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2.

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.

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

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	9
5.	Configure Avaya Communication Server 1000E	12
5.1.	Login to the CS1000 System.....	12
5.1.1.	Login to Unified Communications Management (UCM) and Element Manager ..	12
5.1.2.	Login to the Call Server Command Line Interface (CLI).....	15
5.2.	Administer an IP Telephony Node.....	16
5.2.1.	Obtain Node IP address	16
5.2.2.	Administer Terminal Proxy Server	17
5.2.3.	Administer Quality of Service (QoS)	18
5.2.4.	Synchronize the New Configuration.....	19
5.3.	Administer Voice Codec	20
5.3.1.	Enable Voice Codec, Node IP Telephony.	20
5.3.2.	Enable Voice Codec on Media Gateways.....	22
5.4.	Administer Zones and Bandwidth.....	24
5.4.1.	Create a zone for IP phones (zones 5)	24
5.4.2.	Create a zone for virtual SIP trunks (zone 4).....	26
5.5.	Administer SIP Trunk Gateway	26
5.5.1.	Administer the SIP Trunk Gateway to Session Manager	29
5.5.2.	Administer Virtual D-Channel.....	31
5.5.3.	Administer Virtual Super-Loop	35
5.5.4.	Administer Virtual SIP Routes	36
5.5.5.	Administer Virtual Trunks.....	39
5.5.6.	Enable External Trunk to Trunk Transfer.....	42
5.6.	Administer Dialing Plans	42
5.6.1.	Define ESN Access Codes and Parameters (ESN)	42
5.6.2.	Associate NPA and SPN call to ESN Access Code 1	43
5.6.3.	Digit Manipulation Block Index (DMI).....	44
5.6.4.	Route List Block (RLB).....	46
5.6.5.	Outbound Call - Special Number Configuration.	47
5.6.6.	Outbound Call - Numbering Plan Area Code (NPA)	49
5.7.	Administer Phone.....	49
5.7.1.	Phone creation.....	49
5.7.2.	Enable Privacy for Phone.....	50
5.7.3.	Enable Call Forward for the Phone.....	51
5.7.4.	Enable Call Waiting for the Phone	56
6.	Configure Session Manager.....	57

6.1.	System Manager Login and Navigation.....	58
6.2.	Specify SIP Domains	59
6.3.	Add Location.....	60
6.4.	Add Adaptation Module.....	61
6.5.	Add SIP Entities	65
6.6.	Add Entity Links	69
6.7.	Add Routing Policies	71
6.8.	Add Dial Patterns	72
6.9.	Add/View Session Manager.....	74
7.	Configure the Avaya Session Border Controller for Enterprise (Avaya SBCE).....	76
7.1.	Log in the Avaya SBCE.....	76
7.2.	Global Profiles.....	76
7.2.1.	Server Interworking Avaya-SM.....	76
7.2.2.	Server Interworking SP-General.....	77
7.2.3.	Routing Profiles	78
7.2.4.	Server Configuration.....	80
7.2.5.	Topology Hiding.....	83
7.2.6.	Signaling Manipulation.....	84
7.3.	Domain Policies	86
7.3.1.	Create Application Rules	86
7.3.2.	Media Rules	87
7.3.3.	Signaling Rules	88
7.3.4.	End Point Policy Groups.....	91
7.4.	Device Specific Settings.....	93
7.4.1.	Network Management.....	93
7.4.2.	Media Interface	95
7.4.3.	Signaling Interface	95
7.4.4.	End Point Flows.....	96
8.	Bright House Networks SIP Trunk Service Configuration.....	100
9.	Verification Steps.....	100
9.1.	General	100
9.2.	Verify Call Establishment on the CS1000 Call Server	101
9.3.	Protocol Traces.....	103
10.	Conclusion	105
11.	References.....	106

1. Introduction

These Application Notes provide the procedure for configuring Bright House Networks SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise Release 6.2. During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between the Bright House Networks and Avaya Communication Server 1000E.

In the sample configuration, the Avaya solution consists of a Communication Server 1000E Rel. 7.6 (hereafter referred to as CS1000), Avaya Aura® Session Manager Rel. 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Rel. 6.2 (hereafter referred to as 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 Bright House Networks via SIP trunks. Various call types were made from the CS1000 to Bright House Networks and vice versa to verify interoperability between the CS1000 and the Bright House Networks.

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

2.1. Interoperability Compliance Testing

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

- Incoming calls from the PSTN were routed to DID numbers assigned by Bright House Networks. 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 Bright House Networks.
- 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 end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codec G.711Mu with Voice Activity Detection (VAD) disabled (Bright House Networks only supports codec G.711Mu).

- 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).
- International calls.
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Call Park.
- Consultative Call transfers.
- Station Conference.
- T.38 fax support.
- G.711Mu fax pass-through support.
- Long duration calls (one hour).
- Early Media transmission.

2.2. Test Results

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

- **No audio on calls from the PSTN to the CS1000 Voice Mail system (Call Pilot):** During incoming call re-direction scenarios to Call Pilot Voice Mail (PSTN→CS1000 Call Pilot Voice Mail) there is NO audio (cannot hear the CS1000 voice mail system greetings provided by Call Pilot). The same problem was observed with direct calls from the PSTN to the CS1000 voice mail system (with no call re-direction). The problem is only seen if calls are originated from PSTN phones with particular area codes and that are located within a particular region. The same calls made from other PSTN phones and area codes did NOT experience this audio problem. Traces captured show the carrier sending the last 200 OK with SDP in the call with **connection information 0.0.0.0** and **Media Attribute: inactive**. The problem is being investigated by Bright House Networks.
- **No Ring-Back tone after Blind Transfers to the PSTN:** No ring back tone is heard (only silence) on PSTN phones after execution of Blind Transfers to the PSTN from CS1000 phones (PSTN_1→CS1000_IP_Phone →Blind Transfer →PSTN_2 or CS1000_IP_Phone_1→CS1000_IP_Phone_2 → Blind Transfer →PSTN). The default operation of the CS1000 is as follows: If the Service provider **does not** support SIP UPDATE, the CS1000 will prevent execution of Blind Transfers from one PSTN end point to another PSTN endpoint by disabling the **Trans** key on the CS1000 phone. As a work around **Plug-in 501** can be enabled to allow Blind Transfer when SIP UPDATE is not supported, but with a known limitation that there will be **NO** ring-back tone provided after execution of the Blind Transfer. Bright House Networks does not support SIP UPDATE, compliance testing was done with **Plug-in 501** enabled to allow Blind Transfers to be executed to PSTN endpoints.

- **One way audio, sometime NO audio in both directions, on PSTN phones after Blind Transfers to the PSTN:** One way audio, sometimes NO audio in both directions of the call was observed on PSTN phones after execution of Blind Transfers to the PSTN from CS1000 phones (CS1000_IP_Phone → PSTN_1 then CS1000_IP_Phone Blind Transfer to PSTN)_2). This problem is under investigated by Bright House Networks.
- **Outbound (CS1K→PSTN) T.38 fax:** Outbound (CS1K→PSTN) T.38 fax calls are not supported by Bright House Networks. Inbound (PSTN→CS1K) T.38 fax calls were successfully tested. The options to the customer are to use G.711Mu Pass-Through for inbound and outbound fax calls or T.38 for inbound calls (PSTN→CS1000) and G.711Mu Fax Pass-Through for outbound calls (CS1000→PSTN). G.711Mu Fax Pass-Through was successfully tested in both directions.
- **Caller-ID on re-directed calls to PSTN:** Caller ID works properly between the CS1000 and Bright House Networks 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. The CS1000 is not sending UPDATE or re-INVITE to update the true connected Calling Party. This is a CS1000 known issue.
- **CS1000 phone holds/retrieves an outbound call:** If a CS1000 phone holds/retrieves an outbound call, the dialed digits are no longer displayed; instead the access code of the trunk route (ACOD) is displayed. Also, the trunk route (ACOD), instead of the Caller ID of the extension that originated the call, is displayed during some call transfer scenarios. These are CS1000 known issues.
- **PSTN to CS1000 calls with Privacy enabled:** Calls from the PSTN to the CS1000 with Privacy enabled (Calling Party Name/Number Block) will display the access code of the trunk route (ACOD) instead of **Anonymous**. This is a CS1000 known issue.
- **SIP Header Optimization:** SIP header rules were implemented in the Avaya SBCE and in Session Manager to streamline the SIP header and remove any unnecessary parts. The following headers were removed: X_nt_e164_clid, Alert-Info if they were present in the INVITE. Also the multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-nt-esn5-frag-hex, and x-nt-epid-frag were stripped out. These particular headers and MIME have no real use in the service provider network. If an issue is being investigated on the service provider network, the presence of these headers may add unnecessary confusion.
- Items not supported or not tested included the following:
 - Inbound toll-free calls.
 - 0, 0+10

2.3. Support

For support on Bright House Networks systems, call:

Visit the corporate Web page at:

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

3. Reference Configuration

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

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

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

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

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

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

For inbound calls, the calls flowed from Bright House Networks 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 Bright House Networks.

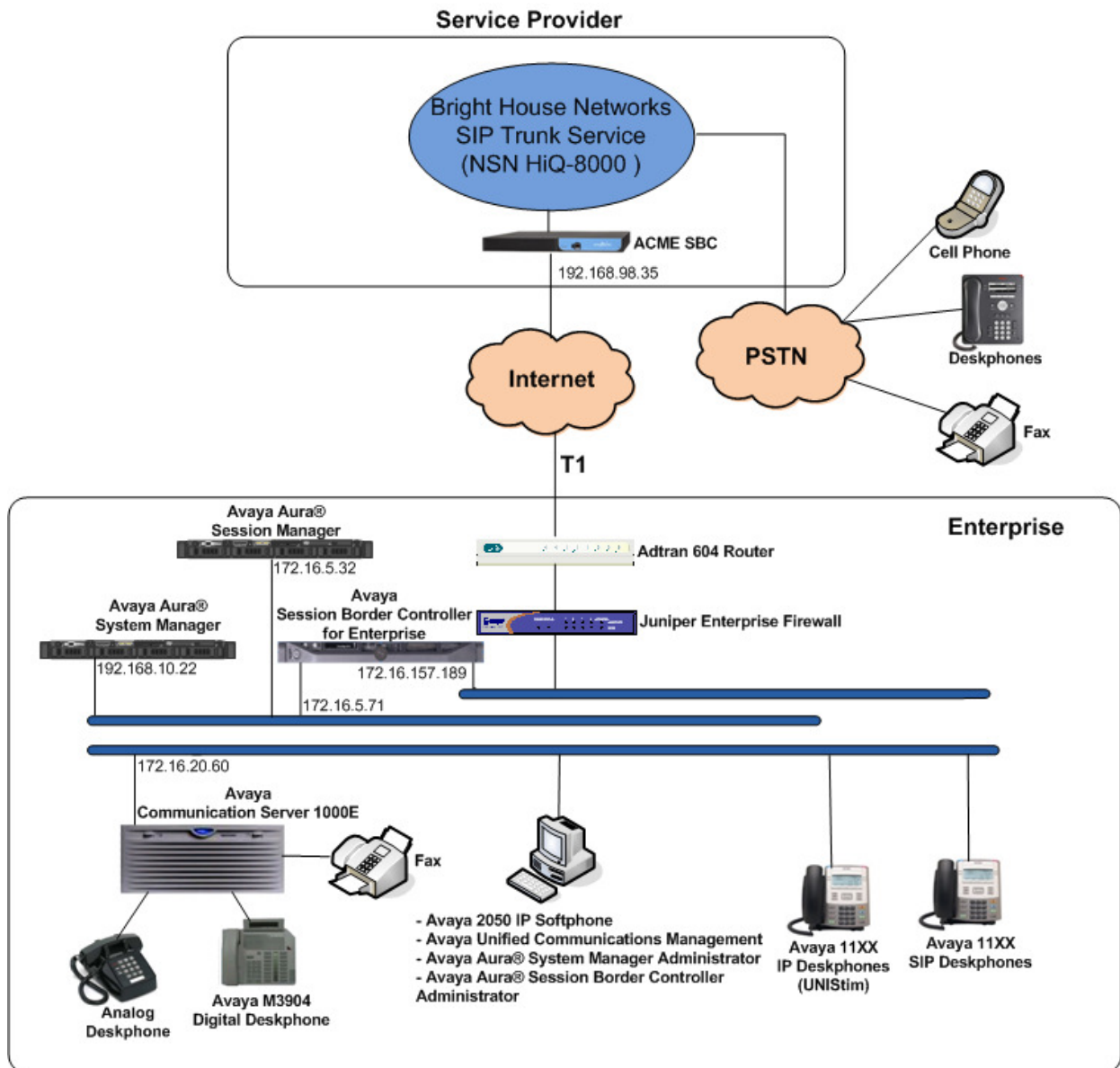


Figure 1: Bright House Networks SIP Trunk service with Avaya CS1000E

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 + DepList 1: core Issue: 01(created: 2013-05-28 04:19:50 (est)) Signaling Server: 7.65.16.00 (Service Pack 2) **See Service Updates & Patches below**
Avaya Call Pilot 202i	Call Pilot Manager Version: 05.00.41.156
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 2 (6.3.2.0.632023)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.0-FP2 Build No. 6.3.0.8.5682-6.3.8.1628 Software Update Rev. No. 6.3.2.4.1529
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.0.Q48
Avaya Deskphones	1110: 0623C8G (UniStim) 1120: 0624C8G (UniStim) 1165: 0626C8G (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.4 Service Pack 1 (Build 067)
Lucent Analog Phone	N/A
Fax Machines	N/A
Bright House Networks:	
Equipment	Release/Version
NSN HiQ-8000 Soft Switch	17 SP3
ACME Session Border Controller	SCX 6.2.0 MR11

Signaling Server Service Updates & Patches:

CS1000 Linux SU's included in Service Pack 2:

cs1000-linuxbase-7.65.16.21-04.i386.000
cs1000-patchWeb-7.65.16.21-04.i386.000
cs1000-dmWeb-7.65.16.21-01.i386.000
cs1000-snmp-7.65.16.00-01.i686.000
cs1000-oam-logging-7.65.16.01-01.i386.000
cs1000-cs1000WebService_6-0-7.65.16.21-00.i386.000
cs1000-sps-7.65.16.21-01.i386.000
cs1000-pd-7.65.16.21-00.i386.000
cs1000-shared-carrrdtct-7.65.16.21-01.i386.000
cs1000-shared-tpselect-7.65.16.21-01.i386.000
cs1000-emWebLocal_6-0-7.65.16.21-01.i386.000
cs1000-dbcom-7.65.16.21-00.i386.000
cs1000-csmWeb-7.65.16.21-05.i386.000
cs1000-shared-xmsg-7.65.16.21-00.i386.000
cs1000-vtrk-7.65.16.21-29.i386.000
cs1000-tps-7.65.16.21-05.i386.000
cs1000-mscAnnc-7.65.16.21-02.i386.001
cs1000-mscAttn-7.65.16.21-04.i386.001
cs1000-mscConf-7.65.16.21-02.i386.001
cs1000-mscMusc-7.65.16.21-02.i386.001
cs1000-mscTone-7.65.16.21-03.i386.001
cs1000-bcc-7.65.16.21-21.i386.000
cs1000-Jboss-Quantum-7.65.16.21-3.i386.000
cs1000-emWeb_6-0-7.65.16.21-06.i386.000
cs1000-cs-7.65.P.100-01.i386.001

#####

Patches:

#####

Loadware:

INSTALLED LOADWARE PEPS : 5

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

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

Enable Plug-Ins 201 and 501 as follows:

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

ENABLED PLUGINS : 2

PLUGIN	STATUS	PRS/CR_NUM	MPLR_NUM	DESCRIPTION

201	ENABLED	Q00424053	MPLR08139	PI:Cant XFER OUTG TRK TO OUTG TRK
501	ENABLED	Q02138637	MPLR30070	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end

5. Configure Avaya Communication Server 1000E

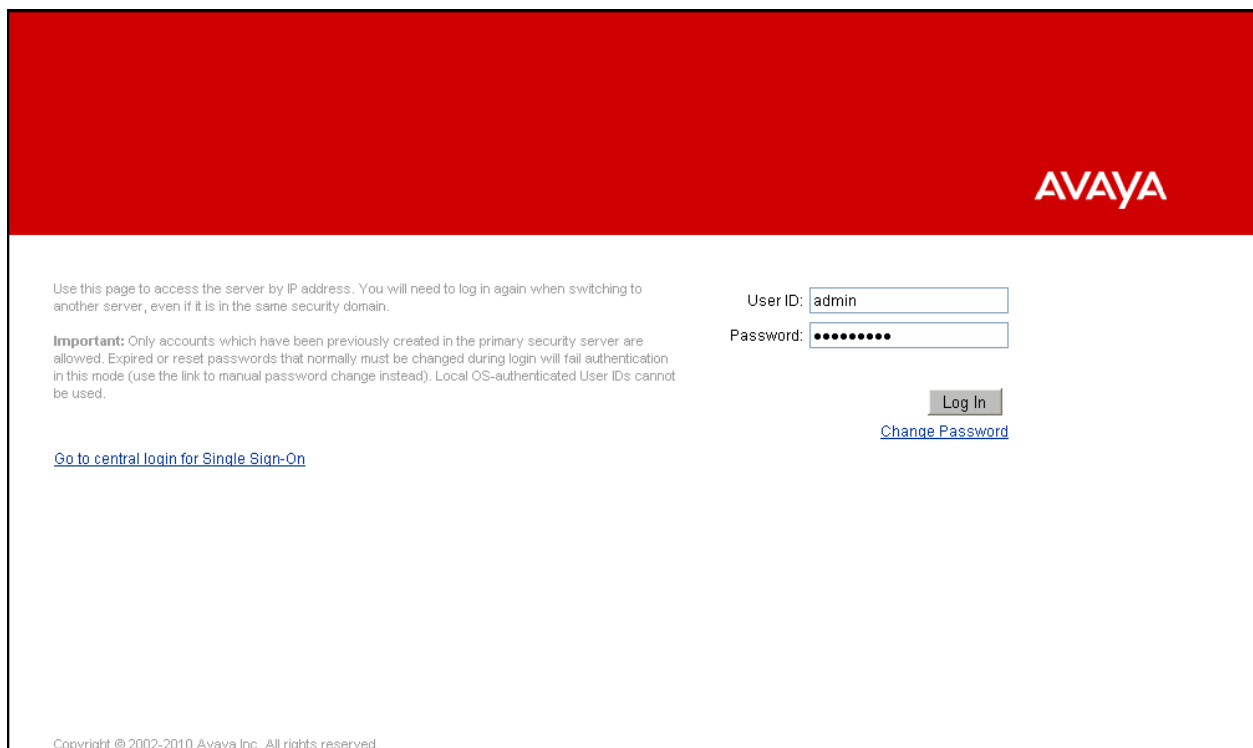
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11**.

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

5.1. Login to the CS1000 System

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

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



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

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

The screenshot displays the Avaya Unified Communications Management web interface. The top header shows the Avaya logo and the title 'Avaya Unified Communications Management'. Below the header, there is a navigation sidebar on the left with categories like Network, Elements, CS 1000 Services, IPsec, Patches, SNMP Profiles, Secure FTP Token, Software Deployment, User Services, Administrative Users, External Authentication, Password, Security, Roles, Policies, Certificates, Active Sessions, and Tools. The main content area is titled 'Elements' and contains a search bar with 'Search' and 'Reset' buttons. Below the search bar are 'Add...', 'Edit...', and 'Delete' buttons. A table lists the elements with columns for Element Name, Element Type, Release, Address, and Description. The first row, 'EM on cs1k', is highlighted with a red box. The table also includes a checkbox for each element.

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

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

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

AVAYA CS1000 Element Manager Help | Logout

Managing: 172.16.21.61 Username: admin
System Overview

System Overview

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

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

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

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

```
login as: admin

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

admin@172.16.20.60's password:
Last login: Wed Aug 28 15:59:22 2013 from 172.16.5.250
[admin@cs1k ~]$ cslogin

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

TTY 14 SCH MTC BUG OSN    10:44
OVL111 IDLE    0
>logi
USERID? admin
PASS?
.
TTY #14 LOGGED IN ADMIN 10:44  29/8/2
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only to
authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
013

>
```

5.2. Administer an IP Telephony Node

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

5.2.1. Obtain Node IP address

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

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

AVAYA CS1000 Element Manager

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

IP Telephony Nodes

Click the Node ID to view or edit its properties.

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

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

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

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

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

AVAYA CS1000 Element Manager Help | Logout

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

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

Node ID: 1006 * (0-9999)

Call server IP address: 172.16.21.61 *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 172.16.21.254 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 172.16.20.60 *

Subnet mask: 255.255.255.0 *

Node IPv6 address: *

* Required Value. [Save] [Cancel]

Associated Signaling Servers & Cards

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

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

Show: ☐ IPv6 address

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

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

5.2.2. 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 Help | Logout

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

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

Subnet mask: 255.255.255.0 *

Subnet mask: 255.255.255.0 *

Node IPv6 address: *

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value. [Save] [Cancel]

Associated Signaling Servers & Cards

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

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

Show: ☐ IPv6 address

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

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

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'Nodes: Servers, Media Cards' highlighted. The main content area is titled 'Node ID: 1006 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details'. It features a 'Firmware | DTLS | Network Connect Server' tab set. The 'Firmware' section has a checkbox for 'Enable proxy service on this node' which is checked. Below this are fields for 'IP address' (0.0.0.0), 'Full file path' (download/firmware), 'Server Account/User ID', and 'Password'. The 'DTLS' section has a 'DTLS policy' dropdown set to 'Off' and two unchecked options: 'Client authentication' and 'Periodic re-keying'. The 'Network Connect Server' section has a 'Primary network connect server (T1 and) IP address' field set to '0.0.0.0'. At the bottom, there are 'Save' and 'Cancel' buttons. A note states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

5.2.3. Administer Quality of Service (QoS)

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway (SIPGW))'. It features a 'Subnet mask' field set to '255.255.255.0' and a 'Node IPv6 address' field. Below this is a section titled 'IP Telephony Node Properties' with a list of links: 'Voice Gateway (V/GW) and Codecs', 'Quality of Service (QoS)', 'LAN', 'SNTP', 'Numbering Zones', and 'MCDN Alternative Routing Treatment (MALT) Causes'. The 'Quality of Service (QoS)' link is highlighted. To the right of this list is a section titled 'Applications (click to edit configuration)' with links: 'SIP Line', 'Terminal Proxy Server (TPS)', 'Gateway (SIPGW)', 'Personal Directories (PD)', 'Presence Publisher', and 'IP Media Services'. Below these sections is a table titled 'Associated Signaling Servers & Cards'. The table has columns: 'Hostname', 'Type', 'Deployed Applications', 'ELAN IP', 'TLAN IPv4', and 'Role'. The table contains one row for 'cs1k' with the following details: Type is 'Signaling_Server', Deployed Applications is 'SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services', ELAN IP is '172.16.21.61', TLAN IPv4 is '172.16.20.61', and Role is 'Leader'. At the bottom, there are 'Save' and 'Cancel' buttons. A note states: 'Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are'.

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

System > IP Network > IP Telephony Nodes > Node Details > Quality of Service (QoS)

Node ID: 1006 - Quality of Service (QoS)

DiffServ Codepoint (DSCP)

Enable Avaya automatic QoS: ☐

Control packets: 40 (0-63)

Voice packets: 46 (0-63)

VLAN tagging: ☒ 802.1Q support

802.1Q bits value (802.1P): 6 (0-7)

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

Save Cancel

5.2.4. Synchronize the New Configuration

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

System > IP Network > IP Telephony Nodes > Node Details

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

Node ID: 1006 * (0-9999)

Call server IP address: 172.16.21.61 *

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 172.16.21.254 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 172.16.20.60 *

Subnet mask: 255.255.255.0 *

Node IPv6 address: *

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIPH323), PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

Show: ☐ IPv6 address

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

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

5.3. Administer Voice Codec

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

5.3.1. Enable Voice Codec, Node IP Telephony.

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

System > IP Network > IP Telephony Nodes > Node Details

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

Subnet mask: 255.255.255.0 Subnet mask: 255.255.255.0

Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cs1k	Signaling_Server	SIP Line, LTPS, Gateway (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

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

The **Voice Gateway (VGW) and Codec** screen is displayed below. Bright House Networks only supports codec **G711Mu** with **Voice Activity Detection (VAD)** disabled. Disable **codec G.729** by unchecking. Codec G.711A is NOT supported by Bright House Networks and cannot be disabled at the CS1000, Bright House Networks will ignore codec G.711A when is included in the list of codecs the CS1000 will send to Bright House Networks.

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

AVAYA **CS1000 Element Manager** Help | Logout

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

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

General | Voice Codecs | Fax

Voice Codecs

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

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

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

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

Save Cancel

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

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

AVAYA **CS1000 Element Manager** Help | Logout

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

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

General | Voice Codecs | Fax

Fax

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

Codec name: T.38 FAX
Maximum rate: 14400 (bps)
Fax TCF method: 2
Fax playback 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

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

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

AVAYA CS1000 Element Manager

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

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

General | Voice Codecs | Fax

General

Echo cancellation: ☒ Use canceller, with tail delay: 128

☒ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection

☐ Low latency mode

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

☒ **Modem/Fax pass-through**

☒ **V.21 Fax tone detection**

☐ R factor calculation

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

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

* Required Value.

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

Save Cancel

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

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

5.3.2. Enable Voice Codec on Media Gateways.

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

AVAYA CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes: Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Software

Customers

Routes and Trunks

Dialing and Numbering Plans

Phones

Tools

Security

Media Gateways

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

Modifications may cause changes to dependent settings

☒ **VAD**

Codec: G729A Select ☐

Codec: G723,1 Select ☐

Codec: T38 FAX Select ☒

QoS

Media Based CLID

Call Server LAN

Embedded LAN (ELAN) configuration

Primary call server IP address: 172.16.21.61

Primary call server hostname: Primary_CS

Signaling port: 15000

Broadcast port: 15001 (1024 - 65535)

Telephony LAN (TLAN) configuration

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

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.

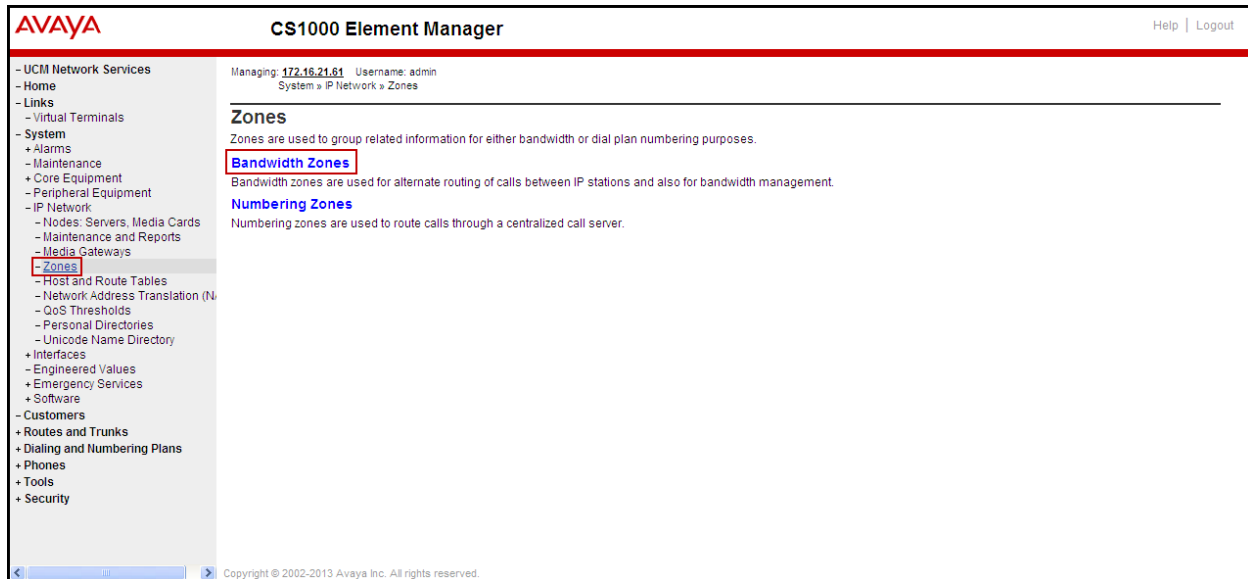
23 of 109
BHNC51KSMASBCE

5.4. Administer Zones and Bandwidth

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

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

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



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

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

Note: **BQ** will use **G711**, **BB** will use **G729**, Bright House Networks only supports G.711, only **BQ** was used.

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The top header includes the AVAYA logo, 'CS1000 Element Manager', and 'Help | Logout'. The breadcrumb trail is: 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.

The main section is titled 'Zone Basic Property and Bandwidth Management'. It contains a table with two columns: 'Input Description' and 'Input Value'.

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

At the bottom of the form are three buttons: 'Submit', 'Refresh', and 'Cancel'.

The footer of the page includes a copyright notice: 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

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

Follow Section 5.4.1 to create a zone for the Virtual SIP Trunks. The difference is in the **Zone Intent (ZBRN)** field, For **ZBRN** select **VTRK** for virtual trunk and **Best Quality (BQ)** for both, **INTRA_STGY** and **INTER_STGY** as shown below and then click on the **Save** button. For Bright House Networks 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 - 100000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 100000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	VTRKZONE_G711_FIRST

Submit Refresh Cancel

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

Note: Bright House Networks only supports codec G.711Mu, non supported codec's sent by the CS1000 (i.e., G.711A) will be ignored by Bright House Networks.

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.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin
Customers

Customers

Add... Delete Refresh

Customer Number	Total Routes	Total Trunks
1 00	3	17

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

The screenshot displays the Avaya CS1000 Element Manager web interface. The top header bar is red and contains the Avaya logo on the left, the title "CS1000 Element Manager" in the center, and "Help | Logout" on the right. Below the header, the left sidebar contains a navigation menu with the following items: "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 "Customer Details" and lists various configuration options: "Basic Configuration", "Application Module Link", "Attendant", "Call Detail Recording", "Call Party Name Display", "Call Redirection", "Centralized Attendant Service", "Controlled Class of Service", "Features", "Feature Packages" (highlighted 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". The top of the main content area also displays "Managing: 172.16.21.61 Username: admin" and 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 Help | Logout

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

- Integrated Services Digital Network Package: 145

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier: (1 - 16383)

- Private network identifier: (1 - 16383)

- Node DN:

Multi-location business group: (0 - 65535)

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

Prefix 1:

Prefix 2:

Home number plan area code: (200 - 999)

Prefix for central office: (100 - 9999)

Local steering code:

Calling number type:

Redirection count for ISDN calls:

CLID information for incoming/outgoing calls:

Public service telephone networks: ☐

+ Network Attendant Service Package: 159

+ Flexible Numbering Plan Package: 160

+ Trunk Failure Monitor Package: 182

+ Radio Paging Package: 187

+ Commonwealth of Independent States -Trunk Package: 221

+ Called Party Control on Internal Calls Package: 310

+ M3900 Product Enhancement Package: 386

+ IP Media Services Package: 422

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

5.5.1. Administer the SIP Trunk Gateway to Session Manager

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

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

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

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

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

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

Port: 5085 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0

Port: 5060 (1 - 65535)

Transport protocol: UDP

* Required Value.

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

Save Cancel

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

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

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

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

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

Note: The SIP URI Map entries shown above were used during the compliance testing; it is possible that in a customer environment other values are use or that these fields are left blank with no entries.

Then click on the **Save** button.

AVAYA **CS1000 Element Manager** Help | Logout

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

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

SIP URI Map:

Public E.164 domain names		Private domain names	
National:	<input type="text"/>	UDP:	<input type="text" value="udp"/>
Subscriber:	<input type="text"/>	CDP:	<input type="text" value="cdp.udp"/>
Special number:	<input type="text" value="PublicSpecial"/>	Special number:	<input type="text" value="PrivateSpecial"/>
Unknown:	<input type="text" value="PublicUnknown"/>	Vacant number:	<input type="text" value="PrivateUnknown"/>
		Unknown:	<input type="text" value="UnknownUnknown"/>

SIP Gateway Services

SIP Converged Desktop: ☐ Enable CD service

Service DN: Used for making VTRK call from agent.

Converged telephone call forward DN:

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

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

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

5.5.2. Administer Virtual D-Channel

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

AVAYA **CS1000 Element Manager** Help | Logout

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

D-Channels

Maintenance

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

Configuration

Choose a D-Channel Number: and type:

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

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

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

AVAYA CS1000 Element Manager

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

D-Channels 0 Property Configuration

- Basic Configuration

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

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

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

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

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

Retain the default values for the remaining fields.

AVAYA CS1000 Element Manager

Help | Logout

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	more PRI
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700
+ Basic options (BSCOPT)	
- Advanced options (ADVOPT)	
- Layer 3 call control message count per 5 second time interval:	300 Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms:	1
- Map channel number to timeslots on a PRI2 loop:	<input checked="" type="checkbox"/>
+ H323 Overlap Signaling Settings (H323)	
--Overlap Timer:	
- Multilocation Business Group Allowed:	<input type="checkbox"/>
- Network Attendant Service Allowed:	<input checked="" type="checkbox"/>
+ - Link Access Protocol for D-channel (LAPD)	

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

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

AVAYA

CS1000 Element Manager

Help | Logout

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

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian 1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	more PRI
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700
Primary D-channel for a backup DCH:	Range: 0 - 254
- PINX customer number:	
- Progress signal:	
- Calling Line Identification:	
- Output request Buffers:	32
- D-channel transmission Rate:	56 kb/s when LCMT is AMI (56K)
- Channel Negotiation option:	No alternative acceptable, exclusive. (1)
- Remote Capabilities:	Edit
- B channel Service messaging:	<input type="checkbox"/>

- Basic options (BSCOPT)

+ - Change protocol timer value (TMR)

+ Advanced options (ADVOPT)

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

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

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

AVAYA CS1000 Element Manager Help | Logout

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

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

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

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

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

Network call park (CPK) ☐

Connected line identification presentation (COLP) ☐

Call transfer integer (CTI) ☐

Call transfer object (CTO) ☐

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

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

Rerouting requests processed using integer value (DV2I) ☐

Rerouting requests processed using object identifier (DV2O) ☐

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

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

Call transfer notification and invocation to EuroISDN (ECTO) ☐

Malicious call identification (MCID) ☐

MCDN QSIG conversion (MQC) ☐

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

Message waiting interworking with DMS-100 (MWI) ☒

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

Network name display method 2 (ND2) ☒

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

5.5.3. Administer Virtual Super-Loop

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

AVAYA CS1000 Element Manager Help | Logout

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

Superloops

Add... Delete Refresh

Superloop Number	Superloop Type
1 4	IPMG
2 8	Virtual
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/MISF Cards
 - Conference/TDS/Multifrequency
 - Tone Senders and Detectors
 - Peripheral Equipment
 - + IP Network
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Software
- Customers
 - + Routes and Trunks
 - Routes and Trunks
 - Dialing and Numbering Plans
 - + Phones
 - + Tools
 - + Security

5.5.4. Administer Virtual SIP Routes

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



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

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

AVAYA CS1000 Element Manager Help | Logout

Managing: 172.16.21.51 Username: admin
Routes and Trunks » Routes and Trunks » Customer 0, Route 0 Property Configuration

Customer 0, Route 0 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE): RDB

Customer number (CUST): 00

Route number (ROUT): 0

Designator field for trunk (DES): SERVICE PROVIDER

Trunk type (TKTP): TIE

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

Access code for the trunk route (ACOD): 7916

Trunk type M911P (M911P): ☐

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

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

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

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

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

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

Integrated services digital network option (ISDN): ☒

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

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

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

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

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

-- Trunk route optimization (TRO): ☐

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

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

AVAYA CS1000 Element Manager

Help | Logout

UCM Network Services

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

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

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

Integrated services digital network option (ISDN): ☒

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

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

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

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

Network calling name allowed (NCNA): ☒

Network call redirection (NCRD): ☒

Trunk route optimization (TRO): ☐

Recognition of 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

- In **Basic Route Options**, check the **North American toll scheme (NATL)**.

AVAYA CS1000 Element Manager

Help | Logout

Managing: 172.16.21.61 Username: admin

Routes and Trunks > Routes and Trunks > Customer 0, Route 0 Property Configuration

Customer 0, Route 0 Property Configuration

Basic Configuration

Basic Route Options

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

Billing number required (BILN): ☐

Call detail recording (CDR): ☐

North American toll scheme (NATL): ☒

Controls or timers (CNLT): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

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

Process notification networked calls (PNNC): ☐

Network Options

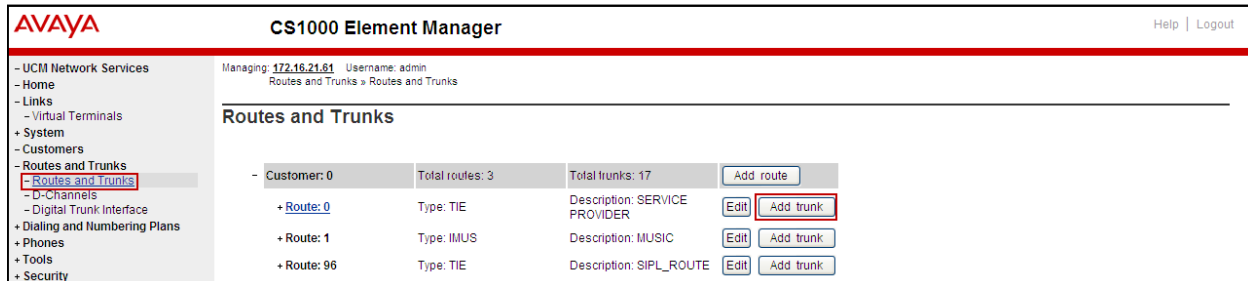
General Options

Advanced Configurations

Submit Refresh Delete Cancel

5.5.5. Administer Virtual Trunks

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



The screenshot displays the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks (highlighted), D-Channels, Digital Trunk Interface, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Routes and Trunks' and shows a table of routes for Customer 0. The table has columns for Customer, Route, Type, and Description. The routes listed are Route 0 (Type: TIE, Description: SERVICE PROVIDER), Route 1 (Type: IMUS, Description: MUSIC), and Route 96 (Type: TIE, Description: SIPL_ROUTE). Each route has an 'Edit' button and an 'Add trunk' button. The 'Add trunk' button for Route 0 is circled in red. The top header shows the Avaya logo and 'CS1000 Element Manager'. The top right corner has 'Help' and 'Logout' links. The top left corner shows the managing IP address '172.16.21.61' and the username 'admin'.

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

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

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

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

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like 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 'Customer 0, Route 0, Trunk 1 Property Configuration'. Under the 'Basic Configuration' section, there is a red-bordered box containing the following fields and values:

- Auto increment member number: ☒
- Trunk data block:
- Terminal number:
- Designator field for trunk:
- Extended trunk:
- Member number: *
- Level 3 Signaling:
- Card density:
- Start arrangement Incoming:
- Start arrangement Outgoing:
- Trunk group access restriction:
- Channel ID for this trunk:
- Class of Service:

Below the 'Basic Configuration' section is the 'Advanced Trunk Configurations' section, which is currently empty. At the bottom right of the form, there are three buttons: 'Save', 'Delete', and 'Cancel'.

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

AVAYA CS1000 Element Manager Help | Logout

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

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

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

Return Class of Service **Cancel**

Copyright © 2002-2013 Avaya Inc. All rights reserved

5.5.6. Enable External Trunk to Trunk Transfer

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

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

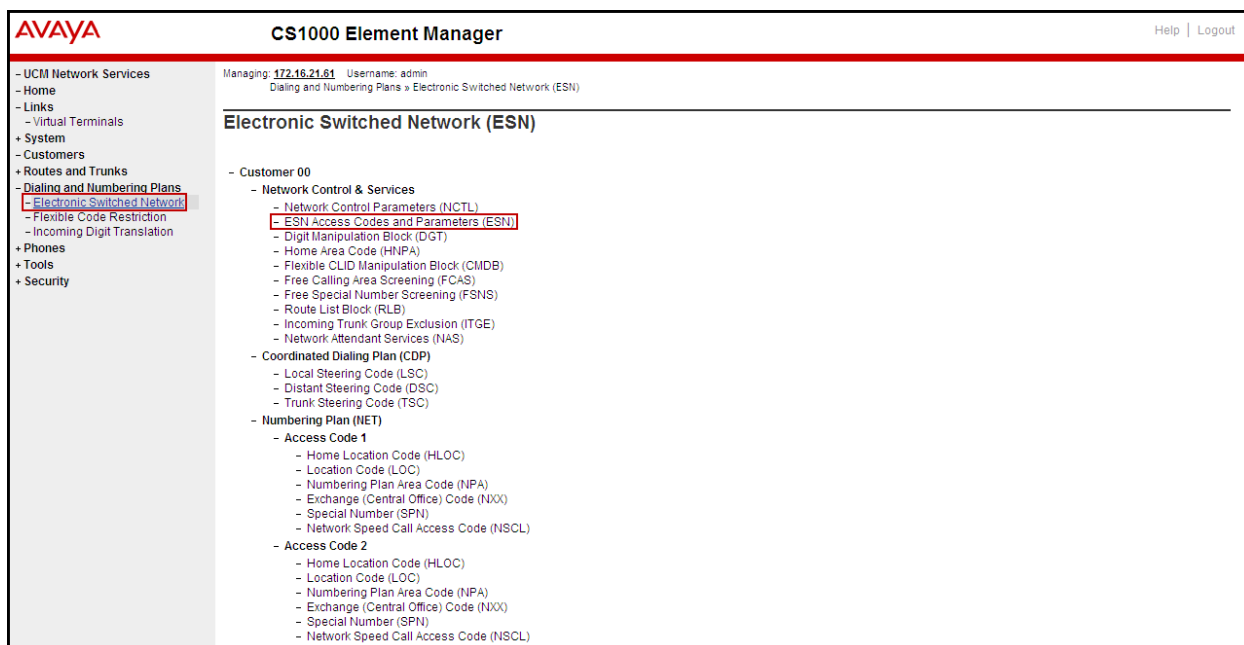
```
>ld 15 CDB000
MEM AVAIL: (U/P): 43552101   USED U P: 371282 939078   TOT: 44862461
DISK SPACE NEEDED: 1713 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
....
TRNX yes
EXTT yes
....
```

5.6. Administer Dialing Plans

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

5.6.1. Define ESN Access Codes and Parameters (ESN)

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



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

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

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

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

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

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

Verify Customer Net_Data block by using LD 21

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.6.3. Digit Manipulation Block Index (DMI)

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

The screenshot shows the Avaya CS1000 Element Manager interface. The top header includes the Avaya logo, 'CS1000 Element Manager', and 'Help | Logout'. The left sidebar contains a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks, Dialing and Numbering Plans (highlighted), Electronic Switched Network (highlighted), Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area displays the 'Electronic Switched Network (ESN)' configuration for 'Customer 00'. The configuration is organized into several sections: Network Control & Services (including Network Control Parameters (NCTL), ESN Access Codes and Parameters (ESN), Digit Manipulation Block (DGT) (highlighted), Home Area Code (HNPA), Flexible CLID Manipulation Block (CMDB), Free Calling Area Screening (FCAS), Free Special Number Screening (FSNS), Route List Block (RLB), Incoming Trunk Group Exclusion (ITGE), and Network Attendant Services (NAS)); Coordinated Dialing Plan (CDP) (including Local Steering Code (LSC), Distant Steering Code (DSC), and Trunk Steering Code (TSC)); and Numbering Plan (NET) (including Access Code 1 and Access Code 2, each with Home Location Code (HLOC), Location Code (LOC), Numbering Plan Area Code (NPA), Exchange (Central Office) Code (NXX), Special Number (SPN), and Network Speed Call Access Code (NSCL)).

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

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

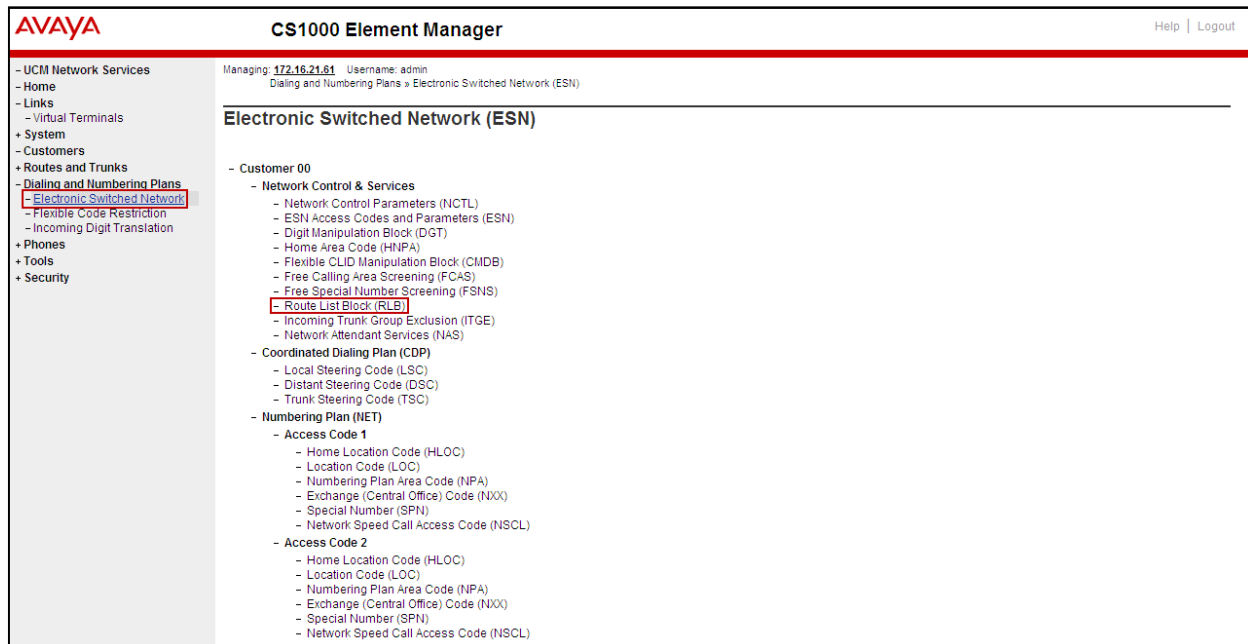
The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main content area is titled "Digit Manipulation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

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

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

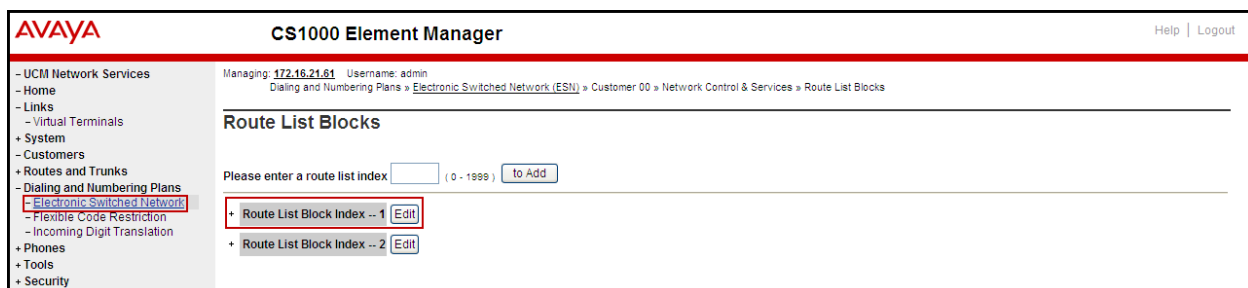
5.6.4. Route List Block (RLB)

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



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

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



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

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

The screenshot shows the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'Dialing and Numbering Plans' expanded, and 'Electronic Switched Network' selected. The main area displays the configuration for 'Route List Block Index: 1'. Under the 'Indexes' section, 'Digit Manipulation Index' is set to 1. Under the 'Options' section, 'Route Number' is set to 0. Other fields like 'Entry Number for the Route List' are set to 0. The bottom of the screen shows a copyright notice: 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

5.6.5. Outbound Call - Special Number Configuration.

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

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

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

AVAYA

CS1000 Element Manager

Help | Logout

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

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

Electronic Switched Network (ESN)

- Customer 00
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)
 - Numbering Plan (NET)
 - Access Code 1
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - **Special Number (SPN)**
 - Network Speed Call Access Code (NSCL)
 - Access Code 2
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)

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

Special Number: 0

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

Special Number: 011

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

Special Number: 1

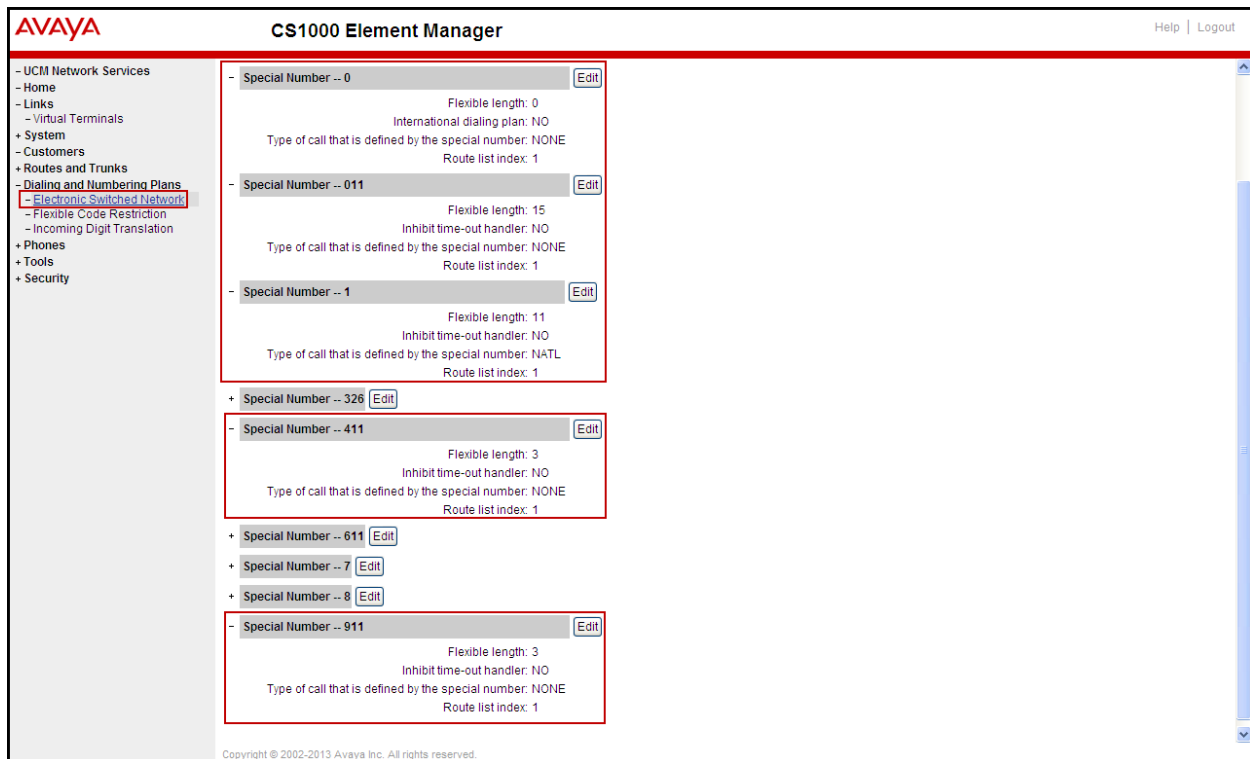
- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number).
- **CallType:** NATL.
- **Route list index:** 1, created in **Section 5.6.4.**

Special Number: 411

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

Special Number: 911

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



5.6.6. 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 5.6.5** allows the user to dial any Numbering Plan Area Code (NPA) when dialing **9+1**.

5.7. Administer Phone

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

5.7.1. Phone creation

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

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

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

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

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

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

```
>ld 11
REQ: prt
TYPE: 1165
DES 8000
TN 008 0 00 00 VIRTUAL
TYPE 1165
CDEN 8D
CTYP XDLC
CUST 0
CFG_ZONE 00005
CUR_ZONE 00005
TGAR 0
LDN NO
NCOS 5
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDD
CFTA SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXA ARHD CLTD ASCD
CPFA CPTA ABDD CFHA FICD NAID DNAA BUZZ
UDI RCC HBTB AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXRO
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD VMSA
CPND_LANG ENG
RCO 0
EFD 91786331
HUNT 91786331
EHT 91786331
DNDR 0
KEY 00 SCR 8000 0 MARP
CPND
CPND_LANG ROMAN
NAME Avaya, 1165_Uni
XPLN 14
DISPLAY_FMT FIRST, LAST
ANIE 0
01 CWT
02
31
```

5.7.2. Enable Privacy for Phone

This section shows how to enable or disable Privacy for a phone by changing its class of service (CLS); changes can be made by using **Unified Communications Management (UCM)** or **LD 11**. By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately. The privacy for a single call can be done by

configuring per-call blocking and a corresponding dialing sequence, for example *67. The resulting SIP privacy setting will be the same in either case.

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

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

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

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

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

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

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

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

5.7.3. Enable Call Forward for the Phone

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

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin
Customers

Customers

Add... Delete Refresh

	Customer Number	Total Routes	Total Trunks
1	00	3	17

Select **Call Redirection** as shown below.

AVAYA CS1000 Element Manager

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

Customer Details

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

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

Set the following fields:

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

Click on **Save** (not shown)

The screenshot displays the Avaya CS1000 Element Manager interface. The left sidebar shows a navigation tree with 'Customers' selected. The main content area is titled 'Call Redirection' and contains the following settings:

- Redirection Holidays:**
 - Do not disturb hunting: ☐
 - Total redirection count limit: 0 (dropdown menu)
- 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 (radio button selected), Forwarding (radio button unselected)
- Number of normal ringing cycles for CFNA:**
 - Option 0: 4 (dropdown menu)
 - Option 1: 4 (dropdown menu)
 - Option 2: 4 (dropdown menu)
- Number of distinctive ringing cycles for CFNA:**
 - Option 0: 4 (dropdown menu)
 - Option 1: 4 (dropdown menu)
 - Option 2: 4 (dropdown menu)
- Calls routed to message center:**
 - No answer DID calls: ☐
 - No answer non-DID calls: ☐
 - DID calls to busy telephones: ☐

At the bottom right, there are 'Save' and 'Cancel' buttons. The footer of the page reads 'Copyright © 2002-2013 Avaya Inc. All rights reserved.'

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

```

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

```

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

```

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

```

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

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

5.7.4. Enable Call Waiting for the Phone

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

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

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


6. Configure Session Manager

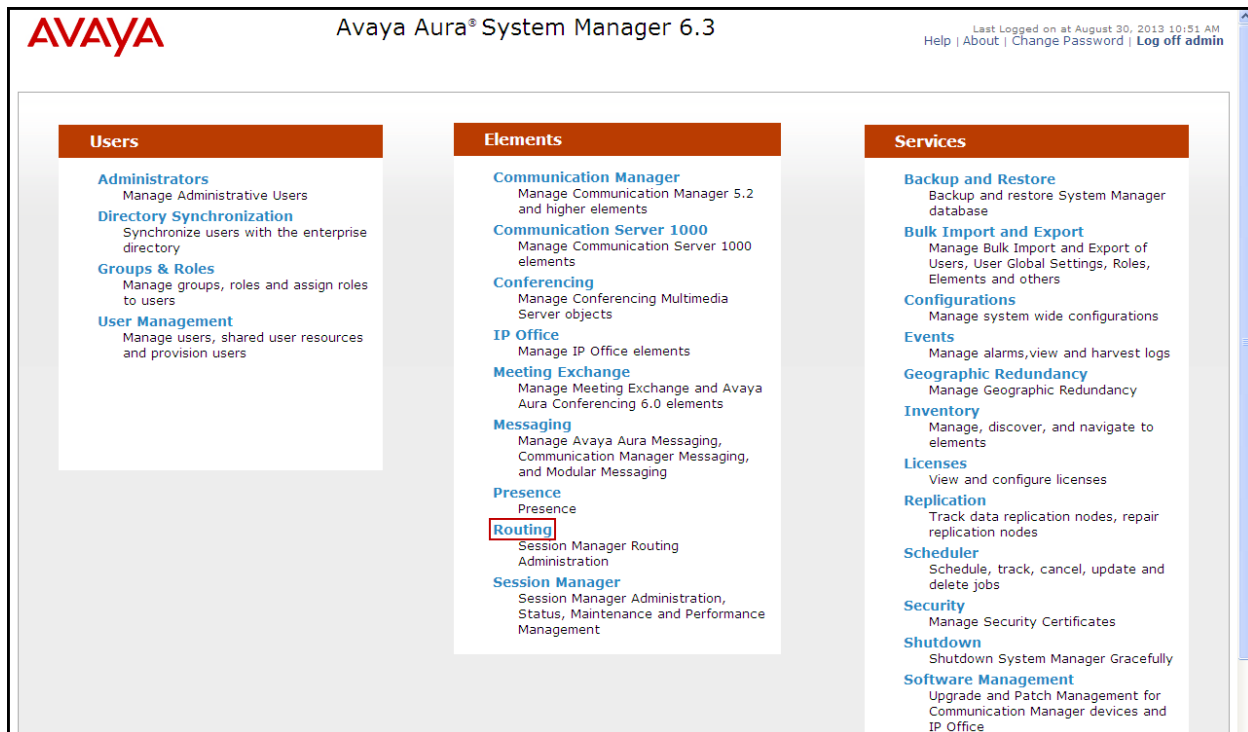
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

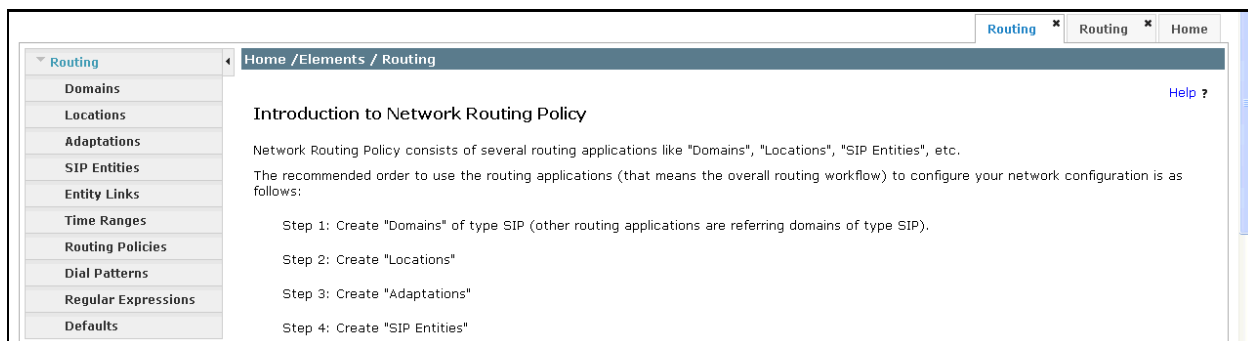
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. System Manager Login and Navigation

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



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



6.2. Specify SIP Domains

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

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

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

Click **Commit**. The screen below shows the entry for the domain name used; this is the **enterprise** domain name.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Domains' highlighted. The main area is titled 'Domain Management' and shows a table with one item. The table has columns for Name, Type, and Notes. The item is 'avaya.lab.com' of type 'sip' with the note 'Lab-HG Domain'. The 'Commit' button is highlighted.

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

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for 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).

Use default values for all remaining fields.

Once all entries have been completed click **Commit** to save.

The **Location Pattern** (not shown) is used to identify a location based on the caller IP address, for location-based routing purposes. If no IP address match is found, Session Manager uses the assigned Location on the sending SIP entity. In the sample configuration, Locations were added to SIP Entities in **Section 6.5**, so it is not necessary to define a pattern here.

The following screen shows the location details for the location named **CS1k Node**. Later, this location will be assigned to the SIP Entity corresponding to the CS1000.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. On the left, a navigation pane shows 'Routing' expanded with 'Locations' selected. The main content area is titled 'Location Details' and shows the configuration for a location named 'CS1k Node'. The 'General' tab is active, displaying two input fields: 'Name' (containing 'CS1k Node') and 'Notes' (containing 'CS1K7.6'). Both fields are highlighted with red boxes. Above these fields are 'Commit' and 'Cancel' buttons, also highlighted with red boxes. Below the input fields, there is a section for 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox (unchecked) and a 'Listed Directory Number' field. The top of the interface shows the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating the last login time and options for help, about, change password, and log off.

The location named **HG ASBCE** shown in the following screen will later be assigned to the SIP Entity corresponding to the Avaya SBCE.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a 'Routing' menu with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations'. Under 'Location Details', the 'General' tab is active. A form contains the following fields: 'Name' (HG ASBCE), 'Notes' (HG Avaya SBCE), 'Dial Plan Transparency in Survivable Mode' (Enabled checkbox), and 'Listed Directory Number' (empty field). 'Commit' and 'Cancel' buttons are at the top right.

The following screen shows the location details for the location named **HG Session Manager**. This location was created during the installation of Session Manager and was assigned to the Session Manager SIP Entity.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a 'Routing' menu with 'Locations' highlighted. The main content area is titled 'Home / Elements / Routing / Locations'. Under 'Location Details', the 'General' tab is active. A form contains the following fields: 'Name' (HG Session Manager), 'Notes' (empty), 'Dial Plan Transparency in Survivable Mode' (Enabled checkbox), and 'Listed Directory Number' (empty field). 'Commit' and 'Cancel' buttons are at the top right.

6.4. Add Adaptation Module

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

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

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at September 13, 2013 6:35 PM
Help | About | Change Password | Log off admin

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Adaptations

Adaptations

New

Edit

Delete

Duplicate

More Actions

7 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	AAC	DigitConversionAdapter		Adaptation For Avaya Aura Conferencing
<input type="checkbox"/>	AA Messaging	DigitConversionAdapter odstd=auramessaging.com osrcd=auramessaging.com iodstd=sil.miami.avaya.com iosrcd=sil.miami.avaya.com		
<input type="checkbox"/>	CS1K76	CS1000Adapter fromto=true		
<input type="checkbox"/>	EdgeMarc	DiversionTypeAdapter iosrcd=avaya.lab.com iodstd=avaya.lab.com odstd=172.16.5.116 MIME=no		
<input type="checkbox"/>	HG SBCE	DigitConversionAdapter iosrcd=avaya.lab.com iodstd=avaya.lab.com odstd=172.16.5.71 MIME=no		
<input type="checkbox"/>	Outbound to AT&T	DigitConversionAdapter odstd=aslab.centivxvoip.net osrcd=aslab.centivxvoip.net		
<input type="checkbox"/>	To MA Lab	DigitConversionAdapter odstd=sil.miami.avaya.com iosrcd=sil.miami.avaya.com		

Select : All, None

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 drop-down menu (or type the adapter name if not previously defined).
- **Module Parameter:** Enter **fromto=true**. By setting this parameter, all digit conversion performed in this adaptation will additionally be applied to the To and From headers. This entry is required if Digit Conversion is performed in Session Manager instead of in the CS1000.
- The **Digit Conversion for Incoming Calls to SM** section of the adaptation is used to modify the digits in origination headers (P-Asserted-Identity, From) on messages coming from the CS1000 to Session Manager. These digits are converted from extension numbers in the CS1000 to the DID numbers assigned by Bright House Networks, before being forwarded to the Avaya SBCE and to Bright House Networks.
- Further down the screen, the **Digit Conversion for Outgoing Calls from SM** section of the adaptation is used to modify the digits in destination headers (Request-URI, To) on messages from Session Manager to the CS1000. These digits are converted from the assigned Bright House Networks DID numbers to the associated destination extension numbers in the CS1000.

Note: Digit translation/conversion can be done in the CS1000 instead of in Session Manager, this is accomplished by administering the necessary tables in the CS1000 (i.e., Incoming Digit Translation, Calling Line Identification Entries, checking the option “Incoming DID digit conversion on this route (IDC)” under Routes and Trunks→Basic Route Options.

Once all entries have been completed click **Commit** to save.

The **CS1K76** adaptation shown below will later be assigned to the **CS1K7.6** SIP entity.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at September 18, 2013 11:51 AM
Help | About | Change Password | Log off admin

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Adaptations

Adaptation Details

CommitCancel

Help ?

General

* Adaptation name: CS1K76

Module name: CS1000Adapter

Module parameter: fromto=true

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

AddRemove

6 Items Refresh

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 8000	* 4	* 4		* 4	3525559910	both		
<input type="checkbox"/>	* 8001	* 4	* 4		* 4	3525559911	both		
<input type="checkbox"/>	* 8011	* 4	* 4		* 4	3525559913	both		
<input type="checkbox"/>	* 8017	* 4	* 4		* 4	3525559914	both		
<input type="checkbox"/>	* 8021	* 4	* 4		* 4	3525559915	both		
<input type="checkbox"/>	* 8056	* 4	* 4		* 4	3525559912	both		

Select : All, None

Digit Conversion for Outgoing Calls from SM

AddRemove

6 Items Refresh

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	3525559910	* 10	* 10		* 10	8000	both		
<input type="checkbox"/>	3525559911	* 10	* 10		* 10	8001	both		
<input type="checkbox"/>	3525559912	* 10	* 10		* 10	8056	both		
<input type="checkbox"/>	3525559913	* 10	* 10		* 10	8011	both		
<input type="checkbox"/>	3525559914	* 10	* 10		* 10	8017	both		
<input type="checkbox"/>	3525559915	* 10	* 10		* 10	8021	both		

Select : All, None

CommitCancel

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**. The Module parameter is set to modify the source and destination domains of headers arriving from the Avaya SBCE to be overwritten with the enterprise domain (**avaya.lab.com**) known by Session Manager. The egress destination domain is overwritten with the IP address of the private interface of the Avaya SBCE (**172.16.5.71**). See **Figure 1**. **MIME=no** will remove MIME types inserted by the CS1000 which are not used for call processing and should not be sent to Bright House Networks.

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DigitConversionAdapter**.
- **Module parameter:** Enter **iosrcd=avaya.lab.com iodstd=avaya.lab.com odstd=172.16.5.71 MIME=no**

Click **Commit** to save.

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' section expanded, with 'Adaptations' selected. The main content area is titled 'Home / Elements / Routing / Adaptations'. Under 'Adaptation Details', the 'General' tab is active. A red box highlights the following fields: 'Adaptation name' (HG SBCE), 'Module name' (DigitConversionAdapter), and 'Module parameter' (iosrcd=avaya.lab.com iodstd=avaya.lab.com odstd=172.16.5.71 MIME=no). Below these are fields for 'Egress URI Parameters' and 'Notes'. Further down, there are sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM', each with an 'Add' button and a table of conversion rules. At the bottom right, the 'Commit' button is highlighted with a red box.

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 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 Session Manager. The IP address of Session Manager Security Module Interface is entered for **FQDN or IP Address**.

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 'Name' field (HG Session Manager), 'FQDN or IP Address' field (172.16.5.32), 'Type' dropdown (Session Manager), 'Notes' field (HG Session Manager), 'Location' dropdown (HG Session Manager), 'Outbound Proxy' dropdown, 'Time Zone' dropdown (America/New_York), and 'Credential name' field. Below this, the 'SIP Link Monitoring' section shows a dropdown set to 'Use Session Manager Configuration'. The 'Port' section includes 'TCP Failover port' and 'TLS Failover port' fields, with 'Add' and 'Remove' buttons. A table lists 9 items with columns for 'Port', 'Protocol', 'Default Domain', and 'Notes'. A red box highlights the first two rows: TCP on 5060 and UDP on 5085, both with 'avaya.lab.com' as the default domain. Below the table is a 'SIP Responses to an OPTIONS Request' section with 'Add' and 'Remove' buttons. At the bottom right, 'Commit' and 'Cancel' buttons are visible.

Avaya Aura® System Manager 6.3

Last Logged on at September 13, 2013 6:35 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: HG Session Manager

* FQDN or IP Address: 172.16.5.32

Type: Session Manager

Notes: HG Session Manager

Location: HG Session Manager

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Port

TCP Failover port:

TLS Failover port:

Add Remove

9 Items Refresh Filter: Enable

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

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Refresh Filter: Enable

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

Commit Cancel

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

For the compliance testing, the following values were used:

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at September 13, 2013 6:35 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows a tree view with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing a form for a SIP entity named 'CS1K7.6'. The form fields are: 'FQDN or IP Address' (172.16.20.60), 'Type' (Other), 'Notes' (CS1000 Rel. 7.6), 'Adaptation' (CS1K76), 'Location' (CS1k Node), and 'Time Zone' (America/New_York). Below the form, there are checkboxes for 'Override Port & Transport with DNS SRV' and 'SIP Timer B/F (in seconds)' (4), a 'Credential name' field, 'Call Detail Recording' (none), 'CommProfile Type Preference', 'Loop Detection Mode' (Off), and 'SIP Link Monitoring' (Use Session Manager Configuration).

Avaya Aura® System Manager 6.3

Last Logged on at September 13, 2013 6:35 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* 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

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

For the compliance test the following values were used:

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at September 13, 2013 6:35 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows a tree view with 'Routing' expanded, and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. A red box highlights the 'Name' field (set to 'HG ASBCE'), 'FQDN or IP Address' field (set to '172.16.5.71'), 'Type' dropdown (set to 'Other'), 'Notes' field (set to 'HG ASBCE'), 'Adaptation' dropdown (set to 'HG SBCE'), and 'Location' dropdown (set to 'HG ASBCE'). Below this, the 'Time Zone' is set to 'America/New_York'. The 'Override Port & Transport with DNS SRV' checkbox is unchecked. The 'SIP Timer B/F (in seconds)' is set to '4'. The 'Credential name' field is empty. The 'Call Detail Recording' dropdown is set to 'none'. The 'CommProfile Type Preference' dropdown is set to an empty value. The 'Loop Detection' section shows 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are visible at the top right of the form area.

6.6. Add Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select Session Manager entity configured in **Section 6.5**.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol defined in **Section 6.5**.
- **Port:** Port number on which Session Manager will receive SIP requests. This must match the port defined in **Section 6.5**.
- **SIP Entity 2:** Select the name of the other system. For the CS1000 and the Avaya SBCE, select the CS1000 or the Avaya SBCE SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the far-end will receive SIP requests. For the CS1000 this must match the port defined under **SIP Gateway Settings** tab, under **Proxy or Redirect Server** in **Section 5.5.1**. For the Avaya SBCE, this must match the port defined under **Server Configuration** in **Section 7.2.4**.
- **Connection Policy:** Select **Trusted** from the pull-down menu.

Click **Commit** to save.

The following screens illustrate the Entity Links to the CS1000.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

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

Commit Cancel

The following screens illustrate the Entity Links to the Avaya SBCE.

Avaya Aura® System Manager 6.3

Last Logged on at September 13, 2013 6:35 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing | Home

Home / Elements / Routing / Entity Links

Entity Links [Commit](#) [Cancel](#) [Help ?](#)

1 Item Refresh

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

Select : All, None

[Commit](#) [Cancel](#)

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

Avaya Aura® System Manager 6.3

Last Logged on at September 13, 2013 6:35 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing | Home

Home / Elements / Routing / Entity Links

Entity Links [Help ?](#)

[New](#) [Edit](#) [Delete](#) [Duplicate](#) [More Actions](#)

19 Items Refresh

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

6.7. Add Routing Policies

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

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

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

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

Click Commit to save.

The following screen shows the Routing Policy for the CS1000.

Avaya Aura® System Manager 6.3

Last Logged on at September 13, 2013 6:35 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: To CS1K76

Disabled: ☐

* Retries: 0

Notes: Inbound Calls to CS1K75

SIP Entity as Destination

Select

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

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

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

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

6.8. Add Dial Patterns

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

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain configured in **Section 6.2** used in the matching criteria.
- **Notes:** Add a brief description (optional).

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

Default values can be used for the remaining fields.

Click **Commit** to save.

The example shown below is for dial pattern “1” for the North American Numbering Plan area prefix, have a SIP Domain of **-ALL-**, Originating Location Name of **CS1k Node**, uses Routing Policy Name of **To HG ASBCE**. Note that **ALL** is being used for the SIP Domain since pattern “1” is being shared with other domain being used by other test activities in the lab, the specific domain name could be use instead (i.e., avaya.lab.com)

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, **Dial Patterns** (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes a 'General' tab. The 'General' tab contains the following fields:

- Pattern:** 1
- Min:** 1
- Max:** 11
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** -ALL- (dropdown menu)
- Notes:**

Below the 'General' tab is the 'Originating Locations and Routing Policies' section. It includes an 'Add' button, a 'Remove' button, and a 'Refresh' button. Below these buttons is a table with 4 items. The table has the following columns: ☐ (checkbox), Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The table contains one row with the following data:

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	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 “352” to route inbound calls to DID numbers provided by Bright House Networks (DID numbers assigned to extensions in the CS1000), have a SIP Domain of **-ALL-**, Originating Location Name of **HG ASBCE**, and uses Routing Policy Name of **To CS1K76**. Note that **ALL** is being used for the SIP Domain since pattern **352** is being shared with other domain being used by other test activities in the lab, the specific domain name could be use instead (i.e., avaya.lab.com)

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at September 18, 2013 11:51 AM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 352

* Min: 3

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	HG ASBCE	HG Avaya SBCE	To CS1K76	0	<input type="checkbox"/>	CS1K7.6	Inbound Calls to CS1K75

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

6.9. Add/View Session Manager

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

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

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

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter the IP address of Session Manager signaling interface.

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

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

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at September 16, 2013 2:40 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Session Manager](#) × [Routing](#) × [Home](#)

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

Description

Management Access Point Host Name/IP

Direct Routing to Endpoints ☒ Enable

VMware Virtual Machine ☐

Security Module ▾

SIP Entity IP Address

Network Mask

Default Gateway

Call Control PHB

QOS Priority

Speed & Duplex

VLAN ID

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

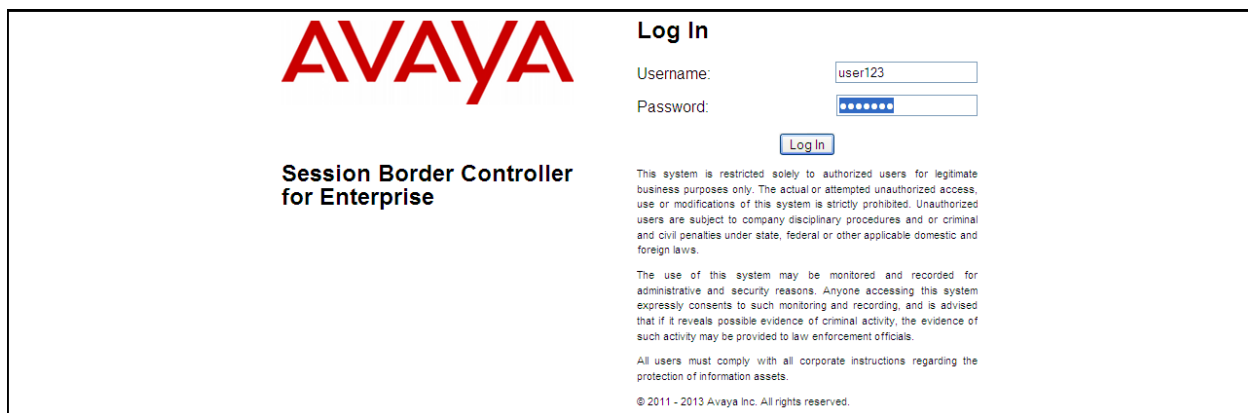
This section describes the required configuration of the Avaya SBCE to connect to Bright House Networks SIP Trunk service.

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

7.1. Log in the Avaya SBCE

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

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

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

7.2. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows 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 the list under **Interworking Profiles** on the screen below. If a different profile is needed, a new Interworking Profile can be created, or an existing default profile can be modified or “cloned”. Since modifying a default profile is generally not recommended, for the test configuration the default **avaya-ru** profile was duplicated, or “cloned”, and then modified to meet specific requirements for the enterprise SIP-enabled solution.

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

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

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

- Verify that for **Hold Support**, **RFC2543** is selected.
- Check **T.38 Support** (for T.38 fax support refer to **Section 2.2**).
- Click **Next**.
- Click **Finish** on the **Privacy and DTMF** tab.
- Leave other fields with their default values.

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and SIP Cluster. Under 'Global Profiles', 'Server Interworking' is highlighted. The main area is titled 'Interworking Profiles: Avaya-SM' and contains a list of profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, **Avaya-SM** (highlighted), and SP-General. The 'Avaya-SM' profile is selected, and its configuration is shown in a tabbed interface with 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced' tabs. The 'General' tab is active, showing settings for 'Hold Support' (RFC2543), '180 Handling' through '183 Handling' (all set to None), 'Refer Handling' (No), '3xx Handling' (No), 'Diversion Header Support' (No), 'Delayed SDP Handling' (No), 'T.38 Support' (Yes), 'URI Scheme' (SIP), and 'Via Header Format' (RFC3261). Below this, the 'Privacy' section shows 'Privacy Enabled' (No), 'User Name', 'P-Asserted-Identity' (No), 'P-Preferred-Identity' (No), and 'Privacy Header'. The 'DTMF' section shows 'DTMF Support' (None). An 'Edit' button is at the bottom right of the configuration area.

7.2.2. Server Interworking SP-General

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

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

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

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

- Check **T.38 Support** (for T.38 fax support refer to **Section 2.2**).
- Click **Next**.
- Click **Finish** on the **Privacy** tab.
- Leave other fields with their default values.

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

The screenshot displays the 'Session Border Controller for Enterprise' configuration page. The left sidebar shows a navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A list of profiles is shown on the left, with 'SP-General' selected. The configuration tabs are 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table of settings. The 'T.38 Support' setting is highlighted with a red box and set to 'Yes'. Below the 'General' tab is the 'Privacy' tab, which is currently inactive. At the bottom, there is a 'DTMF' tab, also inactive, with an 'Edit' button.

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

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

DTMF	
DTMF Support	None

7.2.3. Routing Profiles

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

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

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

- Select the **Routing** tab.
- Select **Add Profile**.
- Enter Profile Name: **Route_to_SM**.
- Click **Next**.

On the next screen, complete the following:

- **Next Hop Server 1: 172.16.5.32** (Session Manager Security Module IP address).
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: TCP** (not shown).
- Click **Finish**.

The following screen shows the newly added **Route_to_SM** Profile.

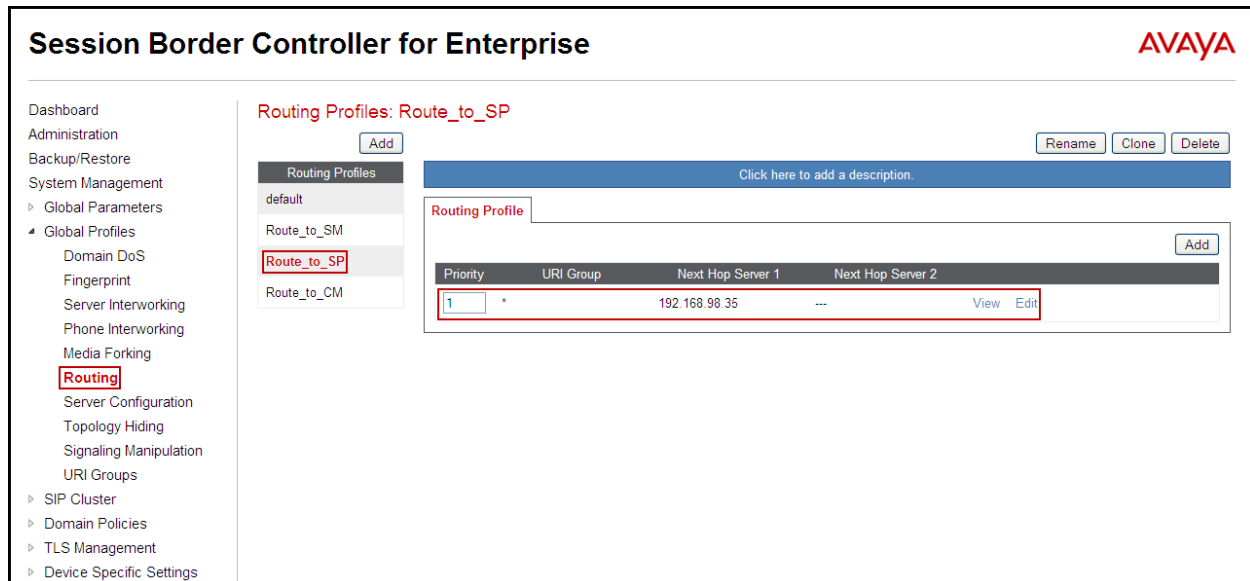
The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, System Management, Global Profiles, and SIP Cluster. The 'Routing' option under Global Profiles is highlighted. The main content area is titled 'Routing Profiles: Route_to_SM'. It features a list of routing profiles on the left: 'default', 'Route_to_SM' (highlighted with a red box), 'Route_to_SP', and 'Route_to_CM'. An 'Add' button is above this list. To the right, the configuration for 'Route_to_SM' is shown. It includes a description field with the placeholder 'Click here to add a description.' and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a table for 'Routing Profile' entries. The table has columns for 'Priority', 'URI Group', 'Next Hop Server 1', and 'Next Hop Server 2'. One entry is visible with 'Priority' 1, 'URI Group' *, 'Next Hop Server 1' 172.16.5.32, and 'Next Hop Server 2' ---. The 'Priority' and 'URI Group' cells are highlighted with a red box. 'View' and 'Edit' buttons are at the end of the row. An 'Add' button is also present at the top right of the table.

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

Similarly, for the outbound route:

- Select **Add Profile**.
- Enter Profile Name: **Route_to_SP**
- Click **Next**.
- **Next Hop Server 1: 192.168.98.35** (IP address for Service Provider's proxy server)
- Check **Routing Priority Based on Next Hop Server** (not shown).
- Check **Outgoing Transport: UDP** (not shown).
- Click **Finish**.

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



7.2.4. Server Configuration

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

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

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

- Select Server Type: **Call Server**.
- **IP Address: 172.16.5.32** (IP Address of Session Manager Security Module).
- **Supported Transports:** Check **TCP**.
- **TCP Port: 5060** (This port must match the port number defined in **Section 6.6**).
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **Avaya-SM** from the **Interworking Profile** drop down menu.
Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, and Routing. The 'Server Configuration' option under Routing is highlighted. The main area is titled 'Server Configuration: Session Manager' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a tabbed interface with 'General', 'Authentication', 'Heartbeat', and 'Advanced' tabs. The 'General' tab is active, showing a table with the following configuration:

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

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

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

This screenshot shows the 'Advanced' tab of the 'Session Manager' profile configuration. The navigation menu on the left is the same as in the previous screenshot. The main area is titled 'Server Configuration: Session Manager' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. The 'Advanced' tab is selected, displaying a table with the following settings:

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

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

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

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

- Select Server Type: **Trunk Server**.
- **IP Address: 192.168.98.35** (service provider's SIP Proxy IP address).
- **Supported Transports: Check UDP**.

- **UDP Port: 5060.**
- Click **Next**.
- Click **Next** on the **Authentication** tab.
- Click **Next** on the **Heartbeat** tab.
- On the **Advanced** tab, select **SP-General** from the **Interworking Profile** drop down menu.
Leave the **Signaling Manipulation Script** at the default **None**.
- Click **Finish**.

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu 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, displaying a table with the following configuration:

Parameter	Value
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.98.35
Supported Transports	UDP
UDP Port	5060

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

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

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

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

The 'Interworking Profile' value 'SP-General' is highlighted with a red box. The 'Edit' button is located at the bottom right of the configuration area.

7.2.5. Topology Hiding

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

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

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

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

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise configuration page. On the left is a navigation menu with categories like Dashboard, Administration, and System Management. Under 'Global Profiles', 'Topology Hiding' is selected. The main area shows 'Topology Hiding Profiles: Session_Manager'. A list of profiles includes 'default', 'cisco_th_profile', 'Session_Manager' (highlighted), 'Service_Provider', and 'Com Manager'. An 'Add' button is above the list. Below the list, a 'Topology Hiding' tab is active, showing a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The table lists six SIP headers: Request-Line, Record-Route, From, To, SDP, and Via, all with 'IP/Domain' as criteria and 'Auto' as replace action. The 'Overwrite Value' column contains dashes. Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible.

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

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

- Click on **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

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

Topology Hiding Profiles: Service_Provider

Click here to add a description.

Topology Hiding

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

7.2.6. Signaling Manipulation

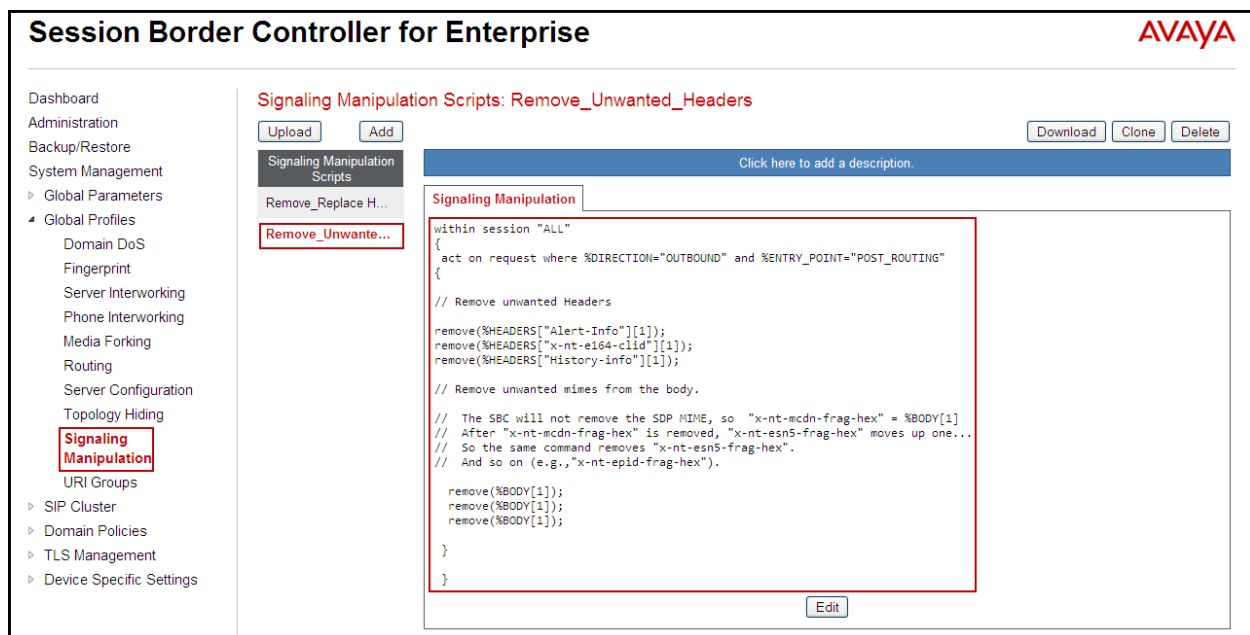
The Avaya SBCE is capable of doing header manipulation by means of Signaling Manipulation (or SigMa) Scripts. The scripts can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. For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

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

- On the **Title**, enter **Remove_Unwanted_Headers**.
- Enter the script as shown on the screen below.
- Click **Save**.



The following screen capture shows the added **Remove_Unwanted_Headers** Script.



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

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

Edit Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile Avaya

Signaling Manipulation Script Remove_Unwanted_Headers

UDP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

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

Session Border Controller for Enterprise AVAYA

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

Server Configuration: Service Provider

Add Rename Clone Delete

Server Profiles
Session Manager
Service Provider
Com Manager

General Authentication Heartbeat **Advanced**

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile Avaya

Signaling Manipulation Script Remove_Unwanted_Headers

UDP Connection Type SUBID

Edit

7.3. Domain Policies

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

7.3.1. Create Application Rules

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

the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is visible, with 'Domain Policies' expanded and 'Application Rules' selected. The main content area is titled 'Application Rules: 1000 Sessions'. It features a list of application rules on the left, with '1000 Sessions' highlighted. The main table displays the configuration for the '1000 Sessions' rule:

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

Below the table, there is a 'Miscellaneous' section with the following settings:

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' are visible at the top. An 'Edit' button is located at the bottom right of the configuration area.

7.3.2. Media Rules

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is visible, 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 main table displays the configuration for the 'default-low-med' rule:

Media Rule	Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS
default-low-med	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons for 'Add', 'Filter By Device...', and 'Clone' are visible at the top. An 'Edit' button is located at the bottom right of the configuration area.

7.3.3. Signaling Rules

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

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

A Signaling Rules was created, to be later applied in the direction of the Enterprise or the Service Provider. To create a rule to block unwanted headers coming from Session Manager from being propagated to the network, in the **Domain Policies** menu, select **Signaling Rules**:

- Click on **default** Signaling Rule.
- Click on Clone Rule.
- Enter a name: **SessMgr_SigRule**. Click **Finish**.

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

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

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

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

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

To add the **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-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 **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.**

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

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
 Global Parameters
 Global Profiles
 SIP Cluster
 Domain Policies
 Application Rules
 Border Rules
 Media Rules
 Security Rules
 Signaling Rules
 Time of Day Rules
 End Point Policy Groups
 Session Policies
 TLS Management
 Device Specific Settings

Signaling Rules: SessMgr_SigRule

Signaling Rules
default
No-Content-Type-Ch...
SessMgr_SigRule

Request Headers

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
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	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

Select the **Response Headers** tab.

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: 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: 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**.

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

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Signaling Rules' highlighted. The main content area shows the 'Signaling Rules: SessMgr_SigRule' configuration page. The 'Response Headers' tab is selected, showing a table of headers. The table has columns: Row, Header Name, Response Code, Method Name, Header Criteria, Action, Proprietary, and Direction. The table lists five headers, all with a 'Remove Header' action and 'Forbidden' criteria. The 'Add In Header Control' button is highlighted with a red box.

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

7.3.4. End Point Policy Groups

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

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

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

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

Session Border Controller for Enterprise AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ Application Rules
‣ Border Rules
‣ Media Rules
‣ Security Rules
‣ Signaling Rules
‣ Time of Day Rules
End Point Policy Groups
‣ Session Policies
‣ TLS Management
‣ Device Specific Settings

Policy Groups: Enterprise

Policy Groups

Click here to add a description.

Hover over a row to see its description.

Policy Group

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

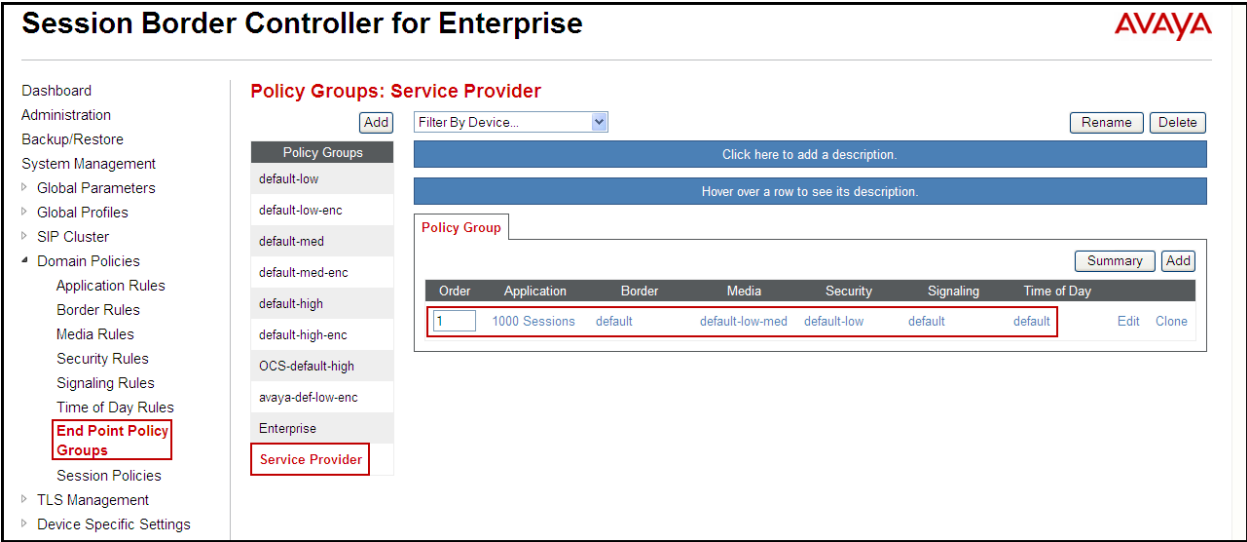
Enterprise

Service Provider

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

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

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



7.4. Device Specific Settings

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

7.4.1. Network Management

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

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

Session Border Controller for Enterprise AVAYA

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

Network Management: Sipera

Devices
Sipera

Network Configuration Interface Configuration

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

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.192 B2 Netmask:
Add Save Clear

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
172.16.157.189		172.16.157.129	B1	Delete

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

Session Border Controller for Enterprise AVAYA

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

Network Management: Sipera

Devices
Sipera

Network Configuration **Interface Configuration**

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

7.4.2. Media Interface

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

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

- Select **Add Media Interface.**
- **Name: Private.**
- Select **IP Address: 172.16.5.71** (Inside IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000.**
- Click **Finish.**
- Select **Add Media Interface.**
- **Name: Public.**
- Select **IP Address: 172.16.157.189** (Outside IP Address of the Avaya SBCE, toward Service Provider).
- **Port Range: 35000-40000.**
- Click **Finish.**

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

Session Border Controller for Enterprise AVAYA

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

Media Interface: Sipera

Media Interface

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

Name	Media IP	Port Range	Edit	Delete
Private	172.16.5.71	35000 - 40000	Edit	Delete
Public	172.16.157.189	35000 - 40000	Edit	Delete

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**

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

- Select **IP Address: 172.16.5.71** (Inside IP Address of the , toward Session Manager).
- **TCP Port: 5060.**
- **UDP Port: 5060.**
- Click **Finish.**
- Select **Add Signaling Interface:**
- **Name: Public**
- Select **IP Address: 172.16.157.189** (Outside IP Address of the Avaya SBCE, toward the Service Provider).
- **TCP Port: 5060.**
- **UDP Port: 5060.**
- Click **Finish.**

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

Session Border Controller for Enterprise AVAYA

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

Signaling Interface: Sipera

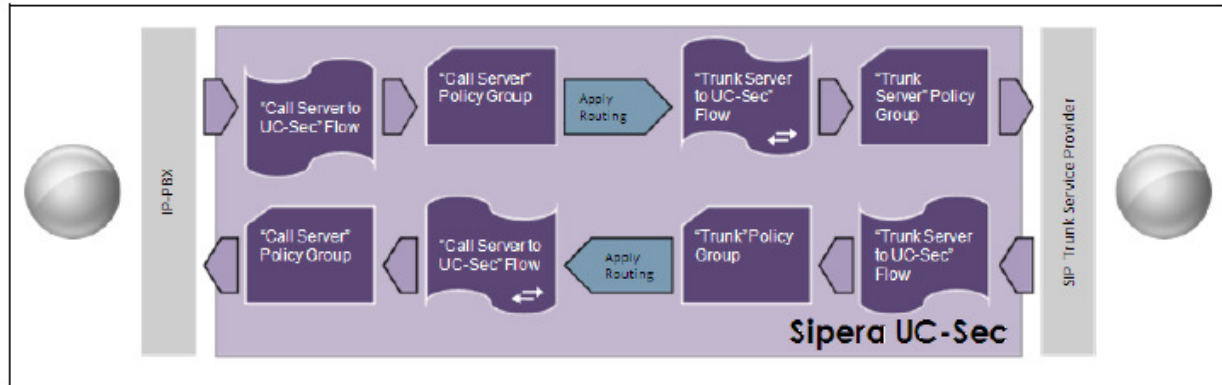
Devices
Sipera

Signaling Interface Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private	172.16.5.71	5060	---	---	None	Edit Delete
Public	172.16.157.189	---	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** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

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

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

View Flow: SIP_Trunk_Flow

X

Criteria	
Flow Name	SIP_Trunk_Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private

Profile	
Signaling Interface	Public
Media Interface	Public
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
File Transfer Profile	None

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

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

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

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

Session Border Controller for Enterprise

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

Network Management

Media Interface

Signaling Interface

Signaling Forking

End Point Flows

Session Flows

Relay Services

SNMP

Syslog Management

Advanced Options

Troubleshooting

End Point Flows: Sipera

Devices

Sipera

Subscriber Flows

Server Flows

Click here to add a row description.

Add

Server Configuration: Service Provider

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

Server Configuration: Session Manager

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

HG; Reviewed:
SPOC 10/14/2013

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

99 of 109
BHNCS1KSMASBCE

8. Bright House Networks SIP Trunk Service Configuration

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

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

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

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

9.2. Verify Call Establishment on the CS1000 Call Server

Active Call Trace (LD 80).

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

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

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

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

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

```
>ld 80
TRA000
.trac 0 8000

ACTIVE VTN 008 0 00 00

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

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

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

```
.trac 0 8000

IDLE VTN 008 0 00 00 MARP
```

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

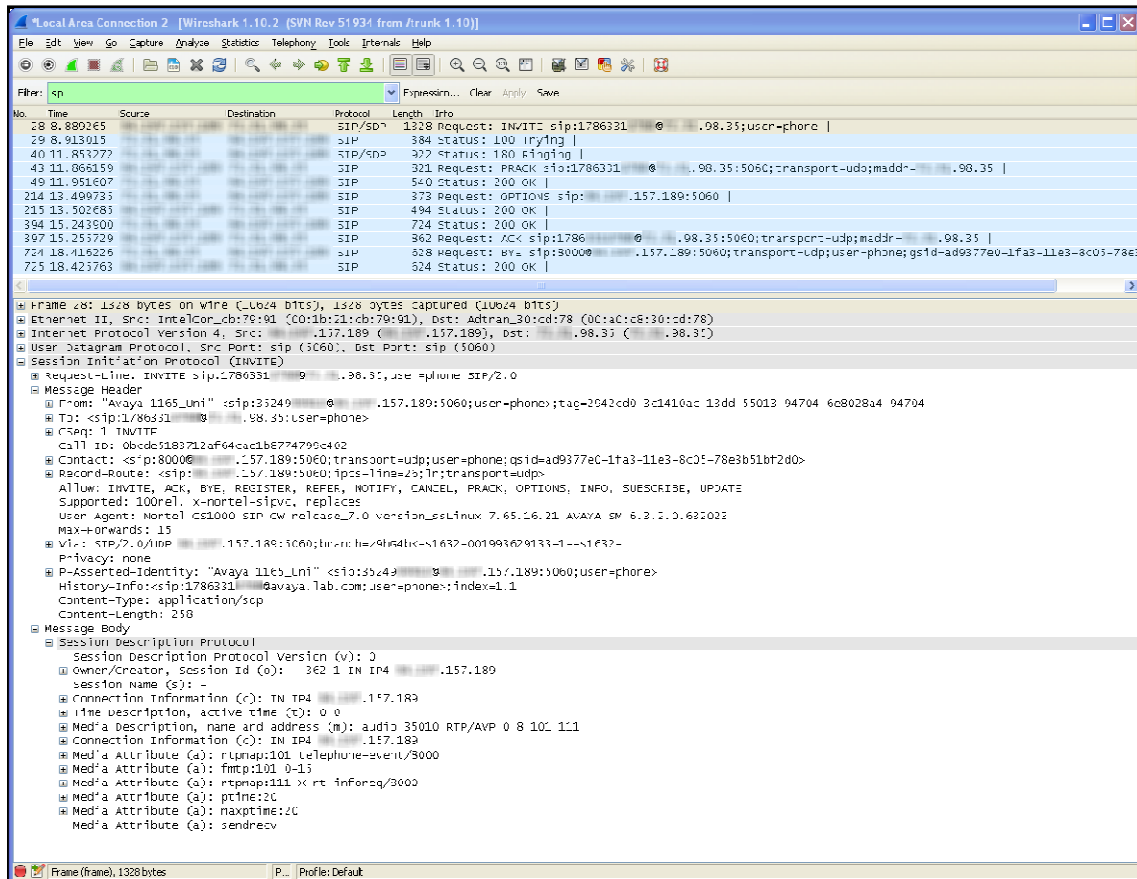
```
>ld 32
NPRO00
.stat 48 0
012 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

9.3. Protocol Traces

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

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

Following screen shows an example of a typical capture for a call made from an 1165 Deskphone (DID: 3525559910) on the CS1000 to a PSTN number (7863311234).



10. Conclusion

These Application Notes describe the procedures necessary to Configuring Bright House Networks SIP Trunk service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 as shown in **Figure 1**.

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

11. References

This section references the documentation relevant to these Application Notes.

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

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

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

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 2, May 2013.
- [10] Administering Avaya Aura® Session Manager, Release 6.3, Issue 2, June 2013.
- [11] Maintaining and Troubleshooting Avaya Aura® Session Manager, Release 6.3, Issue 2, May 2013.

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

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

- [12] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, May 2013.
- [13] Installing Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, June 2013.
- [14] Upgrading Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, July 2013.

Other resources:

[15] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>

[16] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,
<http://www.ietf.org/>

Appendix A: SigMa Script

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

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

    // Remove unwanted Headers

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

    // Remove unwanted mimes from the body.

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

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

  }
}
```

©2013 Avaya Inc. All Rights Reserved.

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

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