



Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

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

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	7
3.	Reference Configuration	8
4.	Equipment and Software Validated	10
5.	Configure Avaya Communication Server 1000E	13
5.1.	Login to the CS1000 System.....	13
5.1.1.	Login to Unified Communications Management (UCM) and Element Manager ..	13
5.1.2.	Login to the Call Server Command Line Interface (CLI).....	16
5.2.	Administer IP Telephony Node	17
5.2.1.	Obtain Node IP address	17
5.2.2.	Administer Terminal Proxy Server	19
5.2.3.	Administer Quality of Service (QoS)	20
5.3.	Administer Voice Codec	21
5.3.1.	Enable Voice Codec, Node IP Telephony.	21
5.3.2.	Synchronize the New Configuration.....	24
5.3.3.	Enable Voice Codec on Media Gateways.....	26
5.4.	Administer Zones and Bandwidth.....	28
5.4.1.	Create a zone for IP phones (zone 5).....	28
5.4.2.	Create a zone for virtual SIP trunks (zone 4).....	29
5.5.	Administer SIP Trunk Gateway	30
5.5.1.	Administer the SIP Trunk Gateway to Session Manager	32
5.5.2.	Administer Virtual D-Channel.....	34
5.5.3.	Administer Virtual Superloops	38
5.5.4.	Administer Virtual SIP Routes	39
5.5.5.	Administer Virtual Trunks.....	42
5.5.6.	Administer Calling Line Identification Entries.....	45
5.6.	Administer Dialing Plans	48
5.6.1.	Define ESN Access Codes and Parameters (ESN)	48
5.6.2.	Associate NPA and SPN call to ESN Access Code 1	49
5.6.3.	Digit Manipulation Block Index (DMI).....	50
5.6.4.	Route List Block (RLB).....	52
5.6.5.	Inbound Digit Translation.....	53
5.6.6.	Outbound Call - Special Number Configuration.	56
5.6.7.	Outbound Call - Numbering Plan Area Code (NPA)	57
5.7.	Administer Phone.....	58
5.7.1.	Phone creation.....	58
5.7.2.	Enable Privacy for Phone.....	60
5.7.3.	Enable Call Forward for the Phone.....	62
5.7.4.	Enable Call Waiting for the Phone	66

6.	Configure Avaya Aura® Session Manager	67
6.1.	System Manager Login and Navigation	68
6.2.	Specify SIP Domain	69
6.3.	Add Location	70
6.4.	Add Adaptation Module	73
6.5.	Add SIP Entities	75
6.6.	Add Entity Links	79
6.7.	Add Routing Policies	81
6.8.	Add Dial Patterns	82
6.9.	Add/View Session Manager	85
7.	Configure Avaya Session Border Controller for Enterprise (Avaya SBCE)	87
7.1.	Log in Avaya SBCE	87
7.2.	Global Profiles	90
7.2.1.	Server Interworking - Avaya-SM	90
7.2.2.	Server Interworking - SP-General	92
7.2.3.	Routing Profiles	93
7.2.4.	Signaling Manipulation	96
7.2.5.	Server Configuration	98
7.2.6.	Topology Hiding	107
7.3.	Domain Policies	109
7.3.1.	Signaling Rules	109
7.3.2.	End Point Policy Groups	115
7.4.	Device Specific Settings	117
7.4.1.	Network Management	117
7.4.2.	Media Interface	119
7.4.3.	Signaling Interface	121
7.4.4.	End Point Flows	123
8.	Bell Aliant SIP Trunk Service Configuration	127
9.	Verification Steps	128
9.1.	General	128
9.2.	Protocol Traces	130
10.	Conclusion	132
11.	References	133
12.	Appendix A: SigMa Script	135

1. Introduction

These Application Notes describe the procedures necessary for configuring Session Initiation Protocol (SIP) trunk service between Bell Aliant and an Avaya SIP-enabled enterprise solution. The Avaya SIP-enabled enterprise solution consists of Avaya Communication Server 1000E Release 7.6 (hereafter referred to as CS1000), Avaya Aura® Session Manager Release 6.3 (hereafter referred to as Session Manager), Avaya Session Border Controller for Enterprise Release 6.2.1 (hereafter referred to as Avaya SBCE), and various Avaya endpoints.

During the interoperability testing, feature test cases were executed to ensure interoperability between Bell Aliant and the Avaya Communication Server 1000E.

The Bell Aliant SIP Trunk Service referenced within these Application Notes is designed for enterprise business customers. Customers using this service with the Avaya SIP-enabled enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI.

During the interoperability testing, a VPN connection was used to connect the sample Avaya enterprise network to Bell Aliant's network via the public Internet. The connection could also be done without the use of VPN, by directly connecting the Avaya SBCE to a public facing SBC located in Bell Aliant's network. This is accomplished by assigning public IP addresses, capable of being reached across the public internet, to the Avaya SBCE (interface B1) and to the Bell Aliant's SBC.

The terms "Service Provider" and "Bell Aliant" will be used interchangeable throughout these Application Notes.

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 Bell Aliant's network via SIP trunks. Various call types were made from the CS1000 to Bell Aliant and vice versa to verify interoperability between the CS1000 and Bell Aliant.

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 Bell Aliant network. The following interoperability areas were covered:

- Response to SIP OPTIONS queries.
- SIP Trunk Registration (Dynamic) Authentication with Bell Aliant.
- Incoming calls from the PSTN were routed to DID numbers assigned by Bell Aliant. 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 Bell Aliant's network.
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect during normal active call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voice mail off).
- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Proper Codec negotiation and two way speech-path. Testing was performed with codecs: G.711MU, G.711A and G.729A, the Bell Aliant preferred codec order.
- No matching codecs.
- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- Call Pilot Voice Mail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with Interactive Voice Response systems (IVR).
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Consultative Call transfers.
- Station Conference.
- G.711Mu fax pass-through (T.38 fax is not supported by Bell Aliant).
- Long duration calls (one hour).
- Early Media transmission.
- Mobility: Mobil X and Personal Call Assistance (PCA).

2.2. Test Results

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

- **No Ring-Back tone after execution of Blind Transfers to the PSTN:** Ring back tone is not heard (only silence) on PSTN phones after the execution of Blind Transfers to the PSTN from CS1000 phones (PSTN_1→CS1000_IP_Phone →Blind Transfer →PSTN_2). **Plug-in 501** has to be enabled in order for Blind Transfers to the PSTN to function properly. If **Plug-in 501** is not enabled, the CS1000 will prevent the execution of Blind Transfers from one PSTN endpoint to another PSTN endpoint by disabling the

Trans key on the CS1000 phone doing the transfer. This is a known CS1000 limitation when **Plug-in 501** is enabled.

- **No Ring Back tone when calling an internal extension or a PSTN number after accessing the CS1000 system remotely from a MobileX mobile telephone via the Mobile Service Access (MSA):** **Scenario:** MobileX mobile phone dials the MSA (Mobile Service Access) number to access the CS1000 system, enters the authorization code, and receives dial tone from the CS1000 system, then proceeds to dial an internal CS1000 extension or a PSTN number. **Result:** Ring back tone is not heard (only silence) on the MobileX mobile telephone while the internal extension or the PSTN telephone are ringing. Audio is good in both directions once the call is answered, the issue is that the MobileX user will not hear ring back tone after dialing the number and while the internal extension of the PSTN telephone are ringing. This issue is under investigation.
- **Blind Call Transfer to the PSTN using SIP phones do not complete until after the transferee answers the call:** When Blind Transfers to the PSTN are executed from CS1000 SIP phones, the transfer does not complete until after the end user (transferee) answers the call. **Scenario:** A PSTN user calls an enterprise SIP extension (**CS1000 SIP phone**) and the call is answered. The enterprise user then proceeds to do a blind transfer to another PSTN endpoint. **Result:** The expected behavior on the enterprise SIP phone is to display “**transfer completed**” after answering “**No**” to the question “**Consultative transfer with party?**” which implies a blind transfer. Instead, the SIP phone continues to display “**transferring**” until the transferee (PSTN user) answers the call. The work around is to hang up the SIP phone. There is no user impact, the transfer completes successfully. This issue is only seen with SIP phones, UniStim phones do not display this behavior.
- **Caller-ID on re-directed calls to the PSTN:** Caller ID works properly between the CS1000 and Bell Aliant 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. Under 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., transferor) and not the Caller ID of the extension that originated the call. This is a known limitation.
- **Outbound call CS1000 holds/retrieve and Transfer scenarios:** If a CS1000 UniStim phone holds/retrieves an outbound call, the dialed digits are no longer displayed; instead the access code of the trunk route (ACOD) is displayed. Also, the trunk route (ACOD), instead of the Caller ID of the extension that originated the call, is displayed during some call transfer scenarios. These are known CS1000 issues.
- **Outbound Calling Party Number (CPN) Block:** To support outbound privacy calls (calling party number blocking), the CS1000 sends “anonymous” as the calling number in the SIP **From** header and includes “Privacy: id” in the INVITE message. During testing, Bell Aliant’s network was configured to ignore the SIP **From** header for this purpose, thus the Calling Party Number (CPN) was not blocked. If Outbound Calling Name (CNAM) is blocked in the CS1000 instead, the name, nor the number, is displayed at the PSTN. For Privacy, blocking the name could be used as a work around; this is accomplished by assigning **NAMD** to the CS1000 extension.

- **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) and Anonymous (e.g., **7916-1 Anonymous**). This is a known CS1000 issue.
- **No matching codec on outbound calls:** If an unsupported audio codec is received by Bell Aliant on the SIP Trunk (e.g., 722), Bell Aliant will respond with “487 Request Terminated” instead of “488 Not Acceptable Here”, the user will hear re-order. This issue does not have any user impact, it is listed here simply as an observation.
- **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. Refer to **Sections 7.3.1** for the list of headers that were removed by the Avaya SBCE. 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. Refer to **Section 6.4** (Session Manager Adaptation Module to remove MIME types).

Items not supported or not tested included the following:

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

2.3. Support

For support on Bell Aliant systems visit the corporate Web page at:

<http://www.bellaliant.ca/index.shtml>

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

3. Reference Configuration

Figure 1 below illustrates the test configuration used. The test configuration simulates an enterprise site with the Avaya components connected to Bell Aliant SIP Trunk Service through an IPSec VPN Tunnel.

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.
- Desktop PC with administration interfaces.
- VPN Firewall.

Located at the edge of the enterprise is a VPN Firewall, followed by the Avaya SBCE. The Avaya SBCE has two physical interfaces, interface **B1** was used to connect to the public network via an IPSec VPN Tunnel, interface **A1** was used to connect to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE and through the VPN Firewall. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Bell Aliant, through the IPSec VPN Tunnel, and across the public internet, is SIP over UDP. The transport protocol between the Avaya SBCE and Session Manager across the enterprise network is SIP over TCP. The transport protocol between Session Manager and the CS1000 across the enterprise 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.

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 Bell Aliant to the Avaya SBCE through the IPSec VPN Tunnel, 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 Bell Aliant through the IPsec VPN Tunnel.

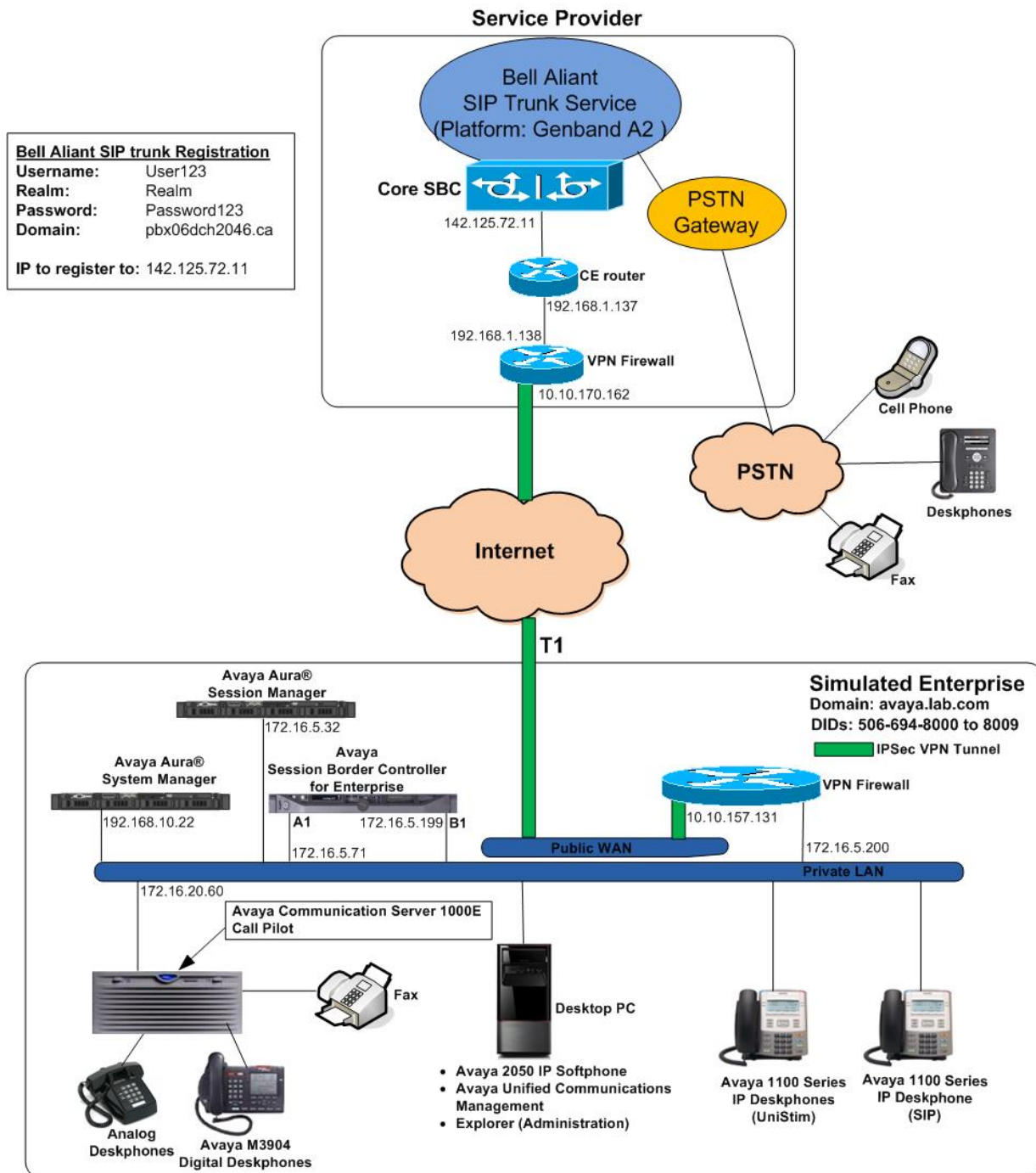


Figure 1: Bell Aliant SIP Trunk service with Avaya CS1000E

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 + Call Server: DepList 1: core Issue: 01 (created: 2013-12-17 04:32:53 (est)) Signaling Server: 7.65.16.00 (Service Pack 4) (See Service Updates & Patches below)
Avaya Call Pilot 202i	05.00.41.20 Service Update 11 (CP50041SU11S)
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.8 (Service Pack 8) (6.3.8.0.638018)
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.8 Build No. 6.3.0.8.5682-6.3.8.4219 Software Update Rev. No. 6.3.8.5.2376
Avaya Session Border Controller for Enterprise running on a DELL R210 V2 Server	6.2.1.Q16
Avaya Deskphones	1110: 0623C8T (UniStim) 1120: 0624C8T (UniStim) 1150: 0627C8T (UniStim) 1165: 0626C8T (UniStim) 1120: 04.04.10.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.02.0062
Lucent Analog Phone	N/A
Fax Machines	N/A
Bell Aliant	
Equipment	Release/Version
Genband A2	17.0.12.16
ACME Session Border Controller (4500)	6.3.7 MR-1 Patch 3

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

cs1000-dmWeb-7.65.16.22-1.i386.000
tzdata-2013c-2.el5.i386.001
cs1000-linuxbase-7.65.16.22-02.i386.000
cs1000-cs1000WebService_6-0-7.65.16.21-00.i386.000
cs1000-Jboss-Quantum-7.65.16.22-3.i386.000
cs1000-pd-7.65.16.21-00.i386.000
cs1000-shared-carrdtct-7.65.16.21-01.i386.000
cs1000-shared-tpselect-7.65.16.21-01.i386.000
cs1000-dbcom-7.65.16.21-00.i386.000
cs1000-patchWeb-7.65.16.22-1.i386.000
cs1000-shared-xmsg-7.65.16.21-00.i386.000
cs1000-cs-7.65.P.100-02.i386.000
cs1000-tps-7.65.16.21-11.i386.000
cs1000-mscAnnc-7.65.16.21-02.i386.001
cs1000-mscAttn-7.65.16.21-04.i386.001
cs1000-mscConf-7.65.16.21-02.i386.001
cs1000-mscMusc-7.65.16.21-02.i386.001
cs1000-mscTone-7.65.16.21-03.i386.001
cs1000-sps-7.65.16.21-8.i386.000
cs1000-shared-omm-7.65.16.21-2.i386.000
cs1000-baseWeb-7.65.16.22-1.i386.000
cs1000-csmWeb-7.65.16.22-1.i386.000
cs1000-gk-7.65.16.21-01.i386.000
cs1000-csoneksvrMgr-7.65.16.22-1.i386.000
cs1000-snmp-7.65.16.21-00.i686.000
cs1000-emWebLocal_6-0-7.65.16.22-1.i386.000
cs1000-ftpkg-7.65.16.22-1.i386.000
cs1000-ipsec-7.65.16.22-1.i386.000
cs1000-vtrk-7.65.16.22-4.i386.000
cs1000-cppmUtil-7.65.16.22-1.i686.000
cs1000-oam-logging-7.65.16.22-3.i386.000
cs1000-bcc-7.65.16.22-6.i386.000
cs1000-emWeb_6-0-7.65.16.22-5.i386.000

Signaling Server Patches:

p31484_1

MGC Loadware:

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

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

Enable Plug-In 501 as follows:

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

ENABLED PLUGINS:

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

5. Configure Avaya Communication Server 1000E

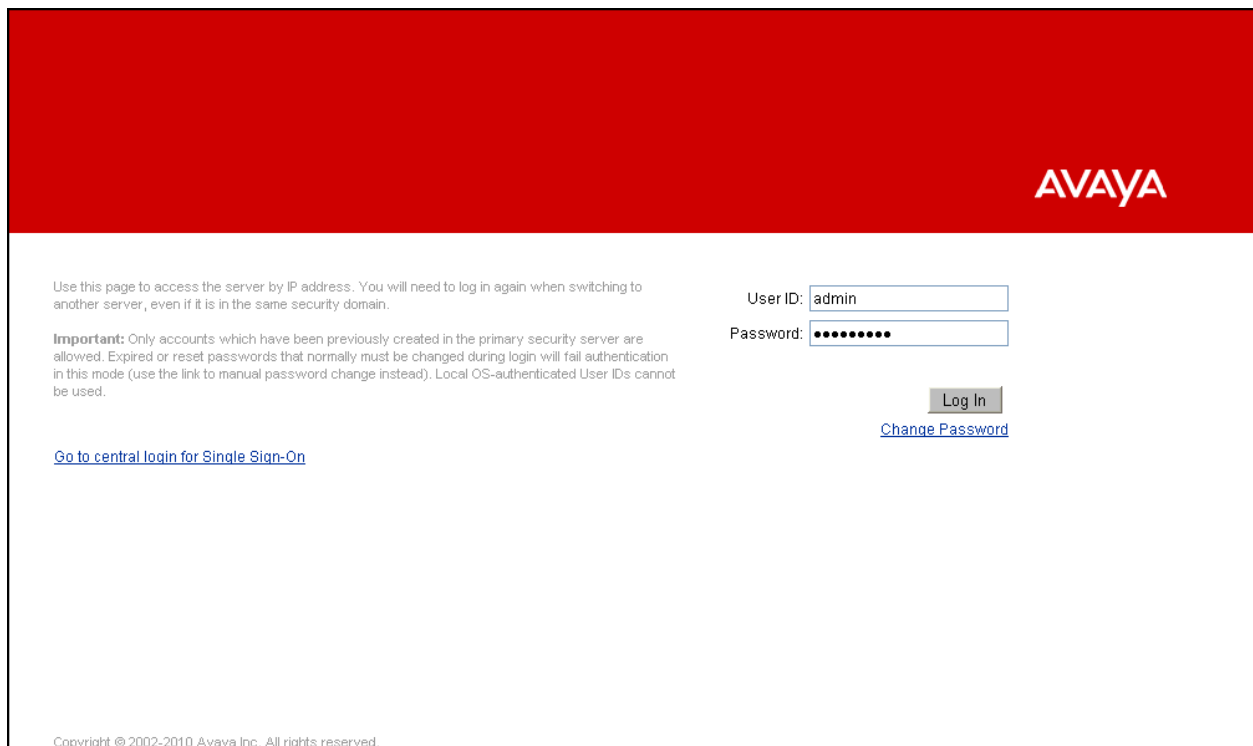
These Application Notes assume that the basic Avaya Communications Server 1000 configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 11**.

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

5.1. Login to the CS1000 System

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

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

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

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

Avaya Unified Communications Management
Help | Logout

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

Host Name: 172.16.20.60 Software Version: 02.30.0086.00(6653) User Name admin

Elements

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

<input type="checkbox"/>	Element Name	Element Type ^	Release	Address	Description
<input type="checkbox"/>	EM on cs1k	CS1000	7.6	172.16.21.61	New element.
<input type="checkbox"/>	cs1k.avaya.lab.com (primary)	Linux Base	7.6	172.16.20.61	Base OS element.
<input type="checkbox"/>	172.16.21.62	Media Gateway Controller	7.6	172.16.21.62	New element.

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

AVAYA

CS1000 Element Manager

Help | Logout

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

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

System Overview

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

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

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

```
login as: admin

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

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

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

TTY 15 SCH MTC BUG OSN    10:24
OVL111 IDLE    0
>logi
USERID? admin
PASS?
.
TTY #15 LOGGED IN ADMIN 1
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only to
authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
0:25  28/2/2014

>
```

5.2. Administer 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 Bell Aliant.

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

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar shows a navigation tree with 'Nodes: Servers, Media Cards' selected. The main content area is titled 'IP Telephony Nodes' and includes a table of nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. Node 1006 is highlighted, showing components like SIP Line, LTPS, IP Media Services, and Gateway (SIPGw). The status is Synchronized.

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

The **Node Details** screen is displayed below with the IP address of the CS1000 node. The **Node IPv4 address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IPv4 address** to communicate with other components for call processing.

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Peripheral Equipment

IP Network

Nodes, Servers, Media Cards

Maintenance and Reports

Media Gateways

Zones

Host and Route Tables

Network Address Translation (

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Software

Customers

Routes and Trunks

Dialing and Numbering Plans

Phones

Tools

Security

Managing: 172.16.21.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

Node ID: 1006 * (0-9999)

Call server IP address: 172.16.21.61 *

TLAN address type: ☒ IPv4 only ☐ IPv4 and IPv6

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

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

Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value.

Save Cancel

Associated Signaling Servers & Cards

Select to add

Add

Remove

Make Leader

Print | Refresh

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

Show: ☐ IPv6 address

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

HG; Reviewed:
SPOC 9/16/2014

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

18 of 136
BellACS1KSMSBCE

5.2.2. Administer Terminal Proxy Server

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

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

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

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

Show: ☐ IPv6 address

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

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

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

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

Firmware | DTLS | Network Connect Server

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

Firmware

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

DTLS

DTLS policy: Off
Options: ☐ Client authentication
☐ Periodic re-keying

Network Connect Server

Primary network connect server / TLAN IP address: 0.0.0.0

* Required Value. Save Cancel

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

5.2.3. Administer Quality of Service (QoS)

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

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

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

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

Show: ☐ IPv6 address

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

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

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

Node ID: 1006 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☒

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

* Required Value. Save Cancel

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

5.3. Administer Voice Codec

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

5.3.1. Enable Voice Codec, Node IP Telephony.

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

AVAYA CS1000 Element Manager Help | Logout

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

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

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

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

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

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

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

Show: ☐ IPv6 address

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

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

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

AVAYA CS1000 Element Manager

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

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

General | Voice Codes | Fax

Voice Codes

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

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

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

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

AVAYA CS1000 Element Manager

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

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

General | Voice Codes | Fax

Voice Codes

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

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

Fax
Codec name: T.38 FAX

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

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

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

The screenshot displays the CS1000 Element Manager web interface. The left sidebar shows a navigation tree with categories like UCM Network Services, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, and Nodes. The 'Nodes' category is expanded, and 'Nodes: Servers, Media Cards' is selected. The main content area shows the configuration for 'Node ID: 1006 - Voice Gateway (VGW) and Codecs'. The 'General' tab is active, showing various settings. Under 'Signaling options', the 'Modem/Fax pass-through' checkbox is checked and highlighted with a red box. The 'V.21 Fax tone detection' checkbox is unchecked. Other settings include 'Echo cancellation' (checked), 'Dynamic attenuation' (checked), 'Voice activity detection threshold' (-17), 'Idle noise level' (-65), 'DTMF tone detection' (checked), 'Low latency mode' (unchecked), 'Remove DTMF delay' (checked), and 'R factor calculation' (unchecked). The 'Voice Codes' section shows 'Codec G711' as 'Enabled (required)' with a 'Voice payload size' of 20 milliseconds per frame and a 'Voice playout (litter buffer) delay' of 40 milliseconds. A 'Save' button is at the bottom right.

5.3.2. Synchronize the New Configuration

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

AVAYA CS1000 Element Manager Help | Logout

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

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

Node ID: * (0-9999)

Call server IP address: * TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

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

Telephony LAN (TLAN) Node IPv4 address: * Subnet mask: *

Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value. **Save** Cancel

Associated Signaling Servers & Cards

Select to add Print | Refresh

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

Show: ☐ IPv6 address

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

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

AVAYA CS1000 Element Manager Help | Logout

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

Node Saved

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

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

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

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

The **Synchronize Configuration Files** screen is displayed. Check the **Signaling_Server** check box (**cs1K**) and click on the **Start Sync** button.

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

Synchronize Configuration Files (Node ID <1006>)

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

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

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

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

When the synchronization completes, check the Signaling Server (**cs1K**) check box again and click on **Restart Applications** button.

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

Synchronize Configuration Files (Node ID <1006>)

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

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

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

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

5.3.3. Enable Voice Codec on Media Gateways.

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

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

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

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

The screenshot displays the Avaya CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, Core Equipment, IP Network, Media Gateways, and others. The 'Media Gateways' category is selected. The main content area is titled 'VGW and IP phone codec profile'. It features a 'Hostname' field set to 'DB1'. Below this, various configuration options are listed with checkboxes and input fields. Two options are highlighted with red boxes: 'Enable modem/fax pass through mode' (checked) and 'Enable V.21 FAX tone detection' (unchecked). Other visible settings include 'Enable echo canceller' (checked), 'Echo canceller tail delay' (128 ms), 'Enable dynamic attenuation' (checked), 'Voice activity detection threshold' (1), 'Idle noise level' (0), 'R factor calculation' (unchecked), 'DTMF tone detection' (checked), 'Enable low latency mode' (unchecked), 'Remove DTMF delay' (checked), 'Fax TCF method' (2), 'FAX maximum rate' (14400 bps), 'FAX playout nominal delay' (100 ms), 'FAX no activity timeout' (20 s), and 'FAX packet size' (30). At the bottom, there is a table for codecs: G711 (Select checked), G729A (Select checked), G723.1 (Select unchecked), and T38 FAX (Select checked). Below the table are sections for '+ QoS', '+ Media Based CLID', and '+ Call Server LAN'. At the very bottom, there are 'Save', 'Cancel', and 'VGW Channels' buttons.

Option	Value/Status
Enable echo canceller	Checked
Echo canceller tail delay	128 (milliseconds)
Enable dynamic attenuation	Checked
Voice activity detection threshold	1 (0 - 4 dBm)
Idle noise level	0 (0 - 1 dBm)
R factor calculation	Unchecked
DTMF tone detection	Checked
Enable low latency mode	Unchecked
Remove DTMF delay (squelch DTMF from TDM to IP)	Checked
Enable modem/fax pass through mode	Checked
Enable V.21 FAX tone detection	Unchecked
Fax TCF method	2
FAX maximum rate	14400 (bps)
FAX playout nominal delay	100 (0 - 300 milliseconds)
FAX no activity timeout	20 (10 - 32000 milliseconds)
FAX packet size	30

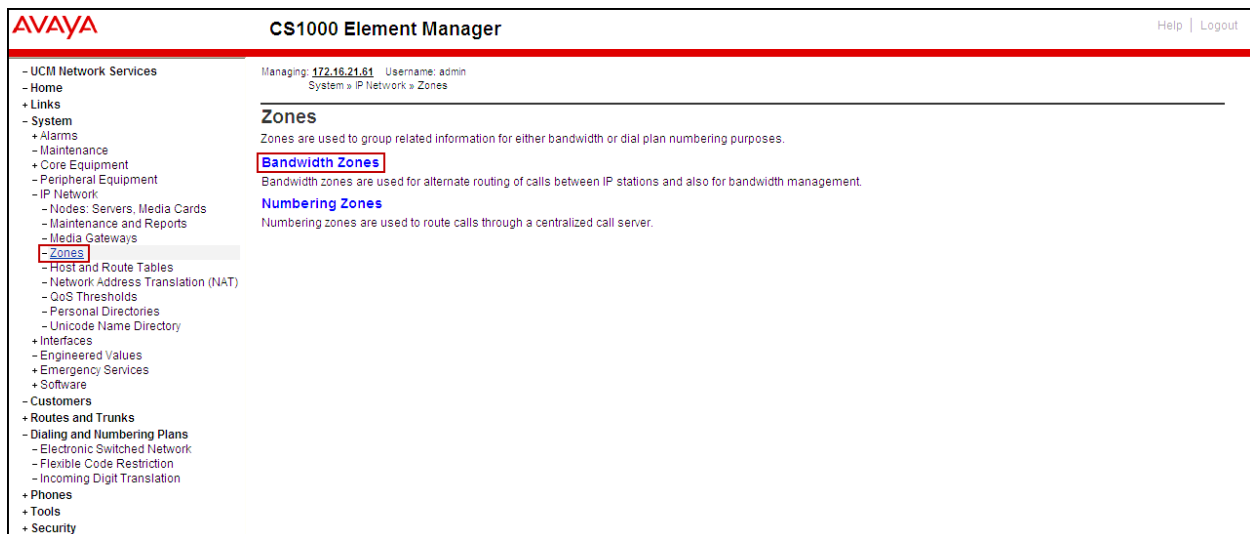
Codec	Select
G711	Checked
G729A	Checked
G723.1	Unchecked
T38 FAX	Checked

5.4. Administer Zones and Bandwidth

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

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

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



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

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

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 5 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

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

Submit Refresh Cancel

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

Follow Section 5.4.1 to create a zone for the Virtual SIP Trunks with the following change. The difference is in the **Zone Intent (ZBRN)** field; For **ZBRN** select **VTRK** for virtual trunk, and then select **Best Quality (BQ)** for both **INTRA_STGY** and **INTER_STGY**, as shown below. Click on the **Submit** button. For Bell Aliant, **Zone 4** was created for the Virtual SIP Trunks.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 4 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE)	4 (1 - 8000)
Intrazone Bandwidth (INTRA_BW)	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY)	Best Quality (BQ)
Interzone Bandwidth (INTER_BW)	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY)	Best Quality (BQ)
Resource Type (RES_TYPE)	Shared (SHARED)
Zone Intent (ZBRN)	VTRK (VTRK)
Description (ZDES)	VTRKZONE_G711_FIRST
Location Name (ZNAME)	
Reserved BW Block Size (RESERVED_BW_SIZE)	0 (200 - 9999999)

Submit Refresh Cancel

5.5. Administer SIP Trunk Gateway

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

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

The screenshot shows the 'Customers' page in the CS1000 Element Manager. The left navigation pane has 'Customers' highlighted. The main area shows a table with columns 'Customer Number', 'Total Routes', and 'Total Trunks'. A single row is visible with '00' in the first column, '3' in the second, and '17' in the third. The '00' is highlighted with a red box. Above the table are 'Add...' and 'Delete' buttons. A 'Refresh' button is in the top right of the table area. The top of the page shows the Avaya logo, 'CS1000 Element Manager', and 'Help | Logout' link. Below the header, it says 'Managing: 172.16.21.61 Username: admin Customers'.

Customer Number	Total Routes	Total Trunks
10 00	3	17

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

The screenshot shows the 'Customer Details' page in the CS1000 Element Manager. The left navigation pane has 'Customers' highlighted. The main area shows a list of options under the heading 'Customer Details'. The 'Feature Packages' option is highlighted with a red box. The top of the page shows the Avaya logo, 'CS1000 Element Manager', and 'Help | Logout' link. Below the header, it says 'Managing: 172.16.21.61 Username: admin Customers » Customer 00 » Customer Details'.

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

The screen is updated with a list of **Feature Packages** populated. Select **Integrated Services Digital Network** to edit its parameters (not shown). The screen is updated with parameters shown below under **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** button.

AVAYA CS1000 Element Manager Help | Logout

Package: 145

Integrated Services Digital Network: ☒

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

- Private network identifier: 1 (1 - 16383)

- Node DN:

Multi-location business group: 0 (0 - 65535)

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

Prefix 1:

Prefix 2:

Home number plan area code: (200 - 999)

Prefix for central office: (100 - 9999)

Local steering code:

Calling number type: CLID feature displays the set's Prime DN

Redirection count for ISDN calls: 5

CLID information for incoming/outgoing calls: No manipulation is done

Public service telephone networks: ☐

+ Network Attendant Service Package: 159

+ Flexible Numbering Plan Package: 160

+ Trunk Failure Monitor Package: 182

+ 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

Save Cancel

5.5.1. Administer the SIP Trunk Gateway to Session Manager

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

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

Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below. The parameters (highlighted in red boxes) are filled in to match values entered under SIP Entity Link in Session Manager (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 shows the AVAYA CS1000 Element Manager interface. The left pane contains a navigation tree with the following items: UCM Network Services, Home, Links, System (with sub-items: Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network), IP Network (with sub-items: Nodes: Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory), Interfaces (with sub-items: Engineered Values, Emergency Services, Software), Customers, Routes and Trunks (with sub-items: Dialing and Numbering Plans, Electronic Switched Network, Flexible Code Restriction, Incoming Digit Translation), Phones, Tools, and Security. The main pane displays the 'Node ID: 1006 - Virtual Trunk Gateway Configuration Details' screen. The 'General' tab is selected, and the 'Vtrk gateway application' is set to 'SIP Gateway (SIPGw)'. The 'SIP domain name' is 'avaya.lab.com', the 'Local SIP port' is '5085', the 'Gateway endpoint name' is 'CS1KGateway', and the 'Application node ID' is '1006'. The 'Virtual Trunk Network Health Monitor' section is also visible, with a checkbox for 'Monitor IP addresses (listed below)' and a list of 'Monitor addresses'.

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

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

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

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

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

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

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

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

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

SIP URI Map:

Public E.164 domain names

National:

Subscriber:

Special number:

Unknown:

Private domain names

UDP:

CDP:

Special number:

Vacant number:

Unknown:

SIP Gateway Services

SIP Converged Desktop: ☐ Enable CD service

Service DN: Used for making VTRK call from agent.

Converged telephone call forward DN:

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

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

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

Save Cancel

5.5.2. Administer Virtual D-Channel

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

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin

Routes and Trunks » D-Channels

D-Channels

Maintenance

[D-Channel Diagnostics \(LD 96\)](#)

[Network and Peripheral Equipment \(LD 32, Virtual D-Channels\)](#)

[ISDL Diagnostics \(LD 96\)](#)

[TMDI Diagnostics \(LD 96\)](#)

[D-Channel Expansion Diagnostics \(LD 48\)](#)

Configuration

Choose a D-Channel Number: and type:

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

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

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

AVAYA CS1000 Element Manager Help | Logout

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

D-Channels 0 Property Configuration

- Basic Configuration

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

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

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

Release ID of the switch at the far end: 2.2

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

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

Signalling server resource capacity: 3700 Range: 0 - 3700

+ Basic options (BSCOPT)

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

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

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

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

- Remote Capabilities: Edit

+ - Change protocol timer value (TMR)

- Advanced options (ADVOPT)

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

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

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

+ H323 Overlap Signaling Settings (H323)

--Overlap Timer:

- Multilocation Business Group Allowed: ☐

- Network Attendant Service Allowed: ☒

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

+ Feature Packages

Submit Refresh Delete Cancel

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

AVAYA **CS1000 Element Manager** Help | Logout

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

- Basic options (BSCOPT)

PRI loop number for Backup D-channel:
 User: Integrated Services Signaling Link Dedicated (ISLD) *
 Interface type for D-channel: Meridian Meridian1 (SL1)
 Country: ETS 300 102 basic protocol (ETSI)
 D-Channel PRI loop number:
 Primary Rate Interface: [more PRI](#)
 Secondary PRI2 loops:
 Meridian 1 node type: Slave to the controller (USR)
 Release ID of the switch at the far end: 25
 Central Office switch type: 100% compatible with Bellcore standard (STD)
 Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000
 Signalling server resource capacity: 3700 Range: 0 - 3700
 Primary D-channel for a backup DCH: Range: 0 - 254
 - PINX customer number:
 - Progress signal:
 - Calling Line Identification:
 - Output request Buffers: 32
 - D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)
 - Channel Negotiation option: No alternative acceptable, exclusive. (1)
 - Remote Capabilities: [Edit](#)
 - B channel Service messaging: ☐

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

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

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

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

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

CS1000 Element Manager

Help | Logout

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

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

Return - Remote Capabilities Cancel

5.5.3. Administer Virtual Superloops

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

CS1000 Element Manager

Help | Logout

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

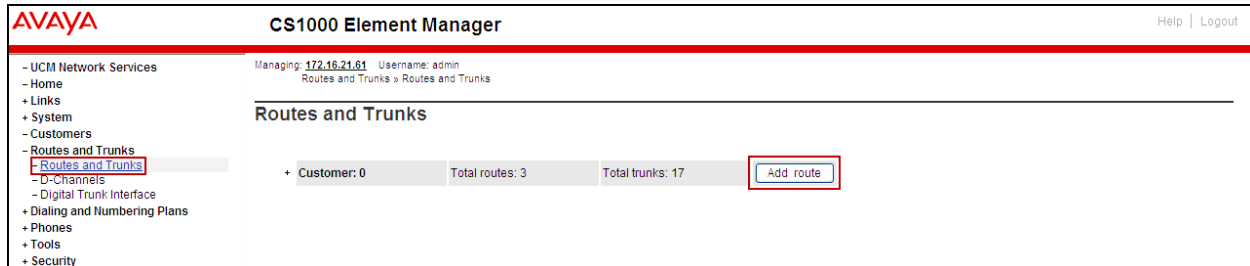
Superloops

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

5.5.4. Administer Virtual SIP Routes

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



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

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

AVAYA CS1000 Element Manager Help | Logout

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

Customer 0, Route 0 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE): RDB
Customer number (CUST): 00

Route number (ROUT): 0
Designator field for trunk (DES): SERVICE PROVIDE
Trunk type (TKTP): TIE
Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD): 7916

Trunk type M911P (M911P): ☐

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

- Zone for codec selection and bandwidth management (ZONE): 00004 (0 - 8000)
- Node ID of signalling server of this route (NODE): 1006 (0 - 9999)
- Protocol ID for the route (PCID): SIP (SIP)

- Print correlation ID in CDR for the route (CRID): ☐
- Enable Shared Bandwidth Management for the route (SBWM): ☐

Integrated services digital network option (ISDN): ☒

- Mode of operation (MODE): Route uses ISDN Signalling Link (ISLD)
- D channel number (DCH): 0 (0 - 254)
- Interface type for route (IFC): Meridian M1 (SL1)
- Private network identifier (PNI): 00001 (0 - 32700)
- Network calling name allowed (NCNA): ☒
- Network call redirection (NCRD): ☒

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

AVAYA CS1000 Element Manager

Help | Logout

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

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

Integrated services digital network option (ISDN): ☒

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

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

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

- 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) (dropdown)

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

- 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) (dropdown)

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

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

+ Basic Route Options

+ Network Options

+ General Options

+ Advanced Configurations

Submit Refresh Delete Cancel

Click on **Basic Route Options**,

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

AVAYA CS1000 Element Manager

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

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

+ Basic Configuration

- Basic Route Options

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

Billing number required (BILN): ☐

Call detail recording (CDR): ☐

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

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

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

- Display external dialed digits (DEXT): ☐

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

Process notification networked calls (PNINC): ☐

+ Network Options

+ General Options

+ Advanced Configurations

Submit Refresh Delete Cancel

5.5.5. Administer Virtual Trunks

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

AVAYA CS1000 Element Manager

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

Routes and Trunks

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

+ Route: 0	Type: TIE	Description: SERVICE PROVIDER	Edit	Add trunk
+ Route: 1	Type: IMUS	Description: MUSIC	Edit	Add trunk
+ Route: 96	Type: TIE	Description: SIP_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 of the basic trunk configuration page. Click on the **Edit** button as shown below.

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

- **Trunk data block (TYPE): IP Trunk (IPTI).**
- **Terminal Number (TN):** Available terminal number (use virtual 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):** 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 top navigation bar includes the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. The left sidebar contains a tree view of network services, with 'Routes and Trunks' selected. The main content area displays the 'Customer 0, Route 0, Trunk 1 Property Configuration' page. The 'Basic Configuration' tab is active, and a red box highlights the configuration fields. The fields are as follows:

Field	Value
Auto increment member number:	<input checked="" type="checkbox"/>
Trunk data block:	IPTI
Terminal number:	048 0 00 00
Designator field for trunk:	VIR_TRK
Extended trunk:	VTRK
Member number:	1
Level 3 Signaling:	[Dropdown]
Card density:	8D
Start arrangement Incoming:	Immediate (IMM)
Start arrangement Outgoing:	Immediate (IMM)
Trunk group access restriction:	1
Channel ID for this trunk:	1
Class of Service:	Edit

At the bottom of the configuration area, there are buttons for 'Save', 'Delete', and 'Cancel'.

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

AVAYA

CS1000 Element Manager

Help | Logout

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

Class of Service Configuration

- Class of Service

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

5.5.6. Administer Calling Line Identification Entries

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

AVAYA CS1000 Element Manager

Help | Logout

General Properties

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

Flexible orbiting prevention timer: **5**

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

Code for processing the called number

National access code: **1**

International access code: **011**

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

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

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

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

Extended Local Calls: ☐

Extended Local Calls for IMS Line user: ☐

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

Calling Line Identification

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

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

Country code: (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Save Cancel

Click on **Add** as shown below.

AVAYA CS1000 Element Manager

Help | Logout

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

Calling Line Identification Entries

Search for CLID

Start range :

End range :

'End range' should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add... Delete Refresh

Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
1 0	506	6948000			NO	
2 1	506	6948001			NO	
3 2	506	6948002			NO	
4 3	506	6948003			NO	
5 4	506	6948004			NO	
6 5	506	6948005			NO	
7 6	506	6948006			NO	

Add entry **0** as shown below.

- **National Code:** Input the three digit area code prefix of the DID number assigned by the service provider, in this case **506**.
- **Local Code:** input the seven digit number of the DID assigned by Service Provider, in this case it is **6948000**.
- **Use DN as DID:** Select **NO**.
- **Calling Party Name Display:** Uncheck for **Roman characters**.

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

AVAYA CS1000 Element Manager

Managing: 172.18.21.61 Username: admin
Customers > Customer 00 > Customer Details > ISDN and ESN Networking > Calling Line Identification Entries > New Calling Line Identification

New Calling Line Identification

General Properties

Entry Id: 0 (0 - 255)

National Code: 506 (0 - 999999)
Code for national home number

Local Code: 6948000 (1-12 digits)
Code for home local number or listed DN

Local Steering Code: (1-7 digits)

Use DN as DID: NO

Emergency Services Access

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

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

Calling Party Name Display

Roman characters: ☐

CPND Name:
first name, last name

Expected Length:

Display Format: First name, Last name

Copyright © 2002-2014 Avaya Inc. All rights reserved.

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

The screenshot displays the Avaya CS1000 Element Manager interface. The left sidebar contains a navigation menu with options: UCM Network Services, Home, Links, System, Customers (highlighted), Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled 'Calling Line Identification Entries'. It features a search section with 'Start range' and 'End range' input fields, a 'Search' button, and a note: 'End range should not exceed the CLID size specified'. Below the search section is a table of entries. The table has columns: Entry Id, National Code, Local Code, Home location code, Local steering code, Use DN as DID, and Emergency Local Code. The table contains 7 entries, all with National Code 506 and Local Code 6948000 through 6948006. The 'Use DN as DID' column for all entries is 'NO'. The table is enclosed in a red border.

Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
0	506	6948000			NO	
1	506	6948001			NO	
2	506	6948002			NO	
3	506	6948003			NO	
4	506	6948004			NO	
5	506	6948005			NO	
6	506	6948006			NO	

Enable External Trunk to Trunk Transfer:

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

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

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

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

5.6. Administer Dialing Plans

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

5.6.1. Define ESN Access Codes and Parameters (ESN)

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

The screenshot 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** (selected), Electronic Switched Network (selected), Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area displays the 'Electronic Switched Network (ESN)' configuration for 'Customer 00'. The configuration is organized into several sections: Network Control & Services (including Network Control Parameters (NCTL), ESN Access Codes and Parameters (ESN) (highlighted), 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), 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 **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**

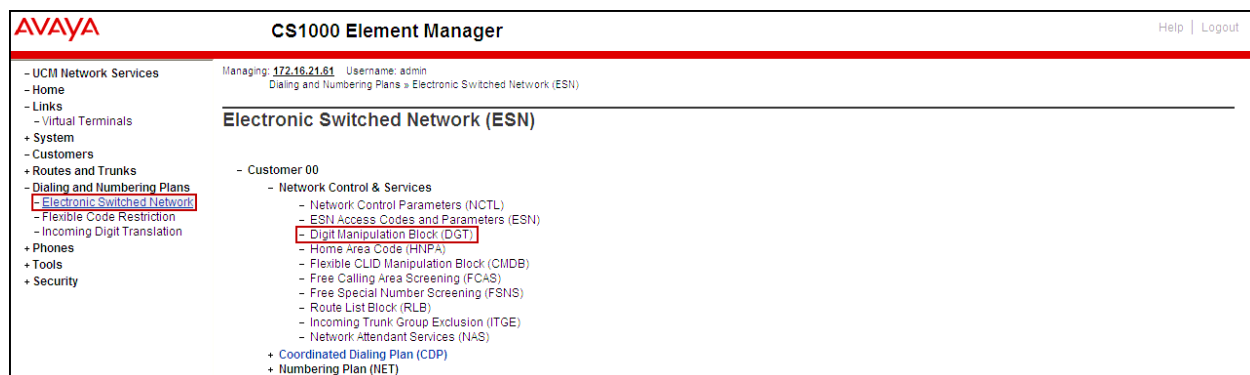
```
>ld 21
PT1000

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.



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

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

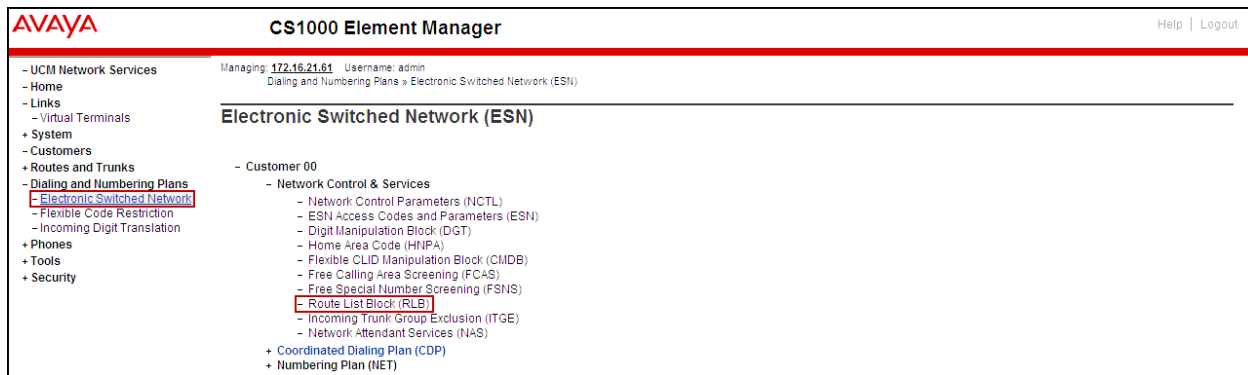
The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Electronic Switched Network (highlighted), Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. The main content area is titled "Digit Manipulation Block List". It shows a management path: Managing: 172.16.21.61 Username: admin, Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List. Below the title, there is a prompt "Please choose the" followed by a dropdown menu showing "Digit Manipulation Block Index 3" and a "to Add" button. Below this, there is a list of two items: "Digit Manipulation Block Index -- 1" with an "Edit" button, and "Digit Manipulation Block Index -- 2" with an "Edit" button.

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

The screenshot shows the AVAYA CS1000 Element Manager interface with the "Digit Manipulation Block" configuration form. The left sidebar is the same as the previous screenshot, with "Electronic Switched Network" highlighted. The main content area is titled "Digit Manipulation Block". It shows the same management path. The form contains the following fields: "Digit Manipulation Index numbers:" with a value of "1"; "Number of leading digits to be deleted:" with a value of "0" and a range "(0 - 19)"; "Insert:" with an empty text field; "IP Special Number:" with a checkbox; and "Call Type to be used by the manipulated digits:" with a dropdown menu showing "NPA (NPA)". At the bottom right, there are four buttons: "Submit", "Refresh", "Delete", and "Cancel".

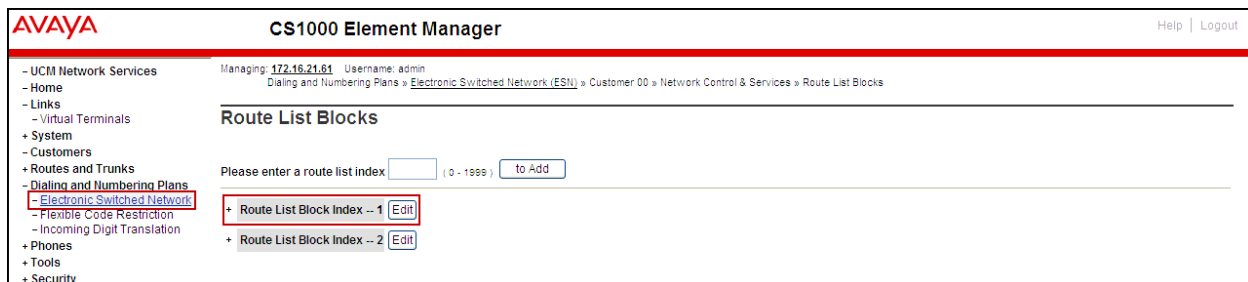
5.6.4. Route List Block (RLB)

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, **Edit** was chosen instead.



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 (not shown).

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

AVAYA CS1000 Element Manager Help | Logout

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

Data Entry of a Route List Block

Route List Block Index: 1

General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 1

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

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: ☐

Incoming CLID Table: 0 (0 - 255)

Options

Local Termination entry: ☐

Route Number: 0

Skip Conventional Signaling: ☐

Display Originator's Information: ☐

Use Tone Detector: ☐

Conversion to LDN: ☐

Expensive Route: ☐

5.6.5. Inbound Digit Translation

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

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

AVAYA CS1000 Element Manager Help | Logout

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

Incoming Digit Translation

- Customer: 00 **Edit IDC**

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

AVAYA

CS1000 Element Manager

Help | Logout

– UCM Network Services

– Home

– Links

– Virtual Terminals

+ System

– Customers

+ Routes and Trunks

– Dialing and Numbering Plans

– Electronic Switched Network

– Flexible Code Restriction

– Incoming Digit Translation

+ Phones

+ Tools

+ Security

Managing: 172.16.21.81 Username: admin

Dialing and Numbering Plans » Incoming Digit Translation » Customer 00

Customer 00 Incoming Digit Conversion Property

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

Refresh

Cancel

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

In the following configuration, the incoming call from the PSTN with the prefix 5066948000 will be translated to the CS1000 extension number 8001.

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

System

Customers

Routes and Trunks

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Tools

Security

Managing 172.16.21.61 Username: admin

Dialing and Numbering Plans > Incoming Digit Translation > Customer 00 > Digit Conversion Tree 0 Configuration > Add Incoming Digits

Add Incoming Digits

Incoming Digits: 5066948000

Converted digits: 8001

(0 - 99999999)

Force storage or removal of data:

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

CPND language:

☒ Roman characters

CPND Name:

first name, last name

Expected length:

Display format: First name, Last name

☐ Katakana characters

CPND Name:

first name, last name

Expected length:

Display format: First name, Last name

Save

Cancel

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

The following screen shows the Incoming Digit Translations used during the compliance testing.

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

System

Customers

Routes and Trunks

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Tools

Security

Managing 172.16.21.61 Username: admin

Dialing and Numbering Plans > Incoming Digit Translation > Customer 00 > Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree

Send calling party DID disabled

Add...

Delete IDC

Delete IDC tree

Refresh

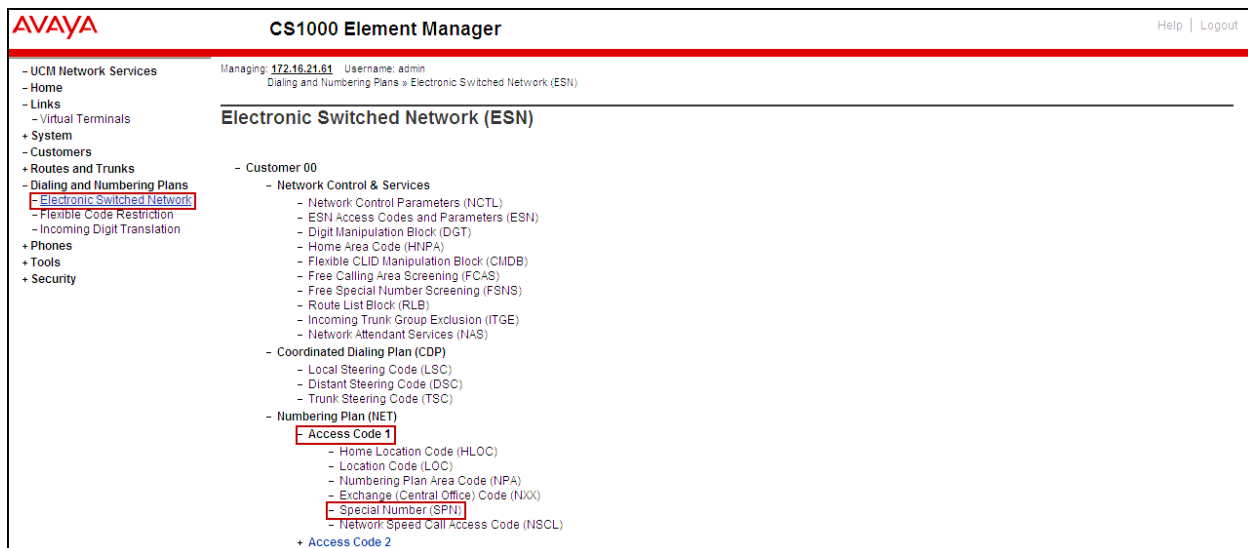
	Incoming Digits	Converted Digits	CPND Name	CPND language
1	5066948000	8001	,	Roman characters
2	5066948001	8002	,	Roman characters
3	5066948002	8007	,	Roman characters
4	5066948003	8020	,	Roman characters
5	5066948004	8011	,	Roman characters
6	5066948005	8017	,	Roman characters
7	5066948006	8004	,	Roman characters
8	5066948007	8056	,	Roman characters

5.6.6. Outbound Call - Special Number Configuration.

There are special numbers which are configured to be used for this testing, such as **0** to reach the Service Provider operator, **0+10** digits to reach the Service Provider operator assistant, **011** prefix for international calls, **1** for national long distance calls, **411** for Directory assistance, **911** for emergency, **69** for seven digit local calls, and so on. Calls to special numbers shown here are for reference only and may not have been tested for various reasons. Refer to **Items not supported or not tested** in **Section 2.2**.

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

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



Enter **SPN** and then click on the **to Add** button (not shown).

Following is a subset of Special Numbers that were added for the testing:

Special Number: 0

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

Special Number: 011

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

Special Number: 1

- **Flexible length:** 11.
- **CallType:** NATL.
- **Route list index:** 1, created in **Section 5.6.4.**

Special Number: 411

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

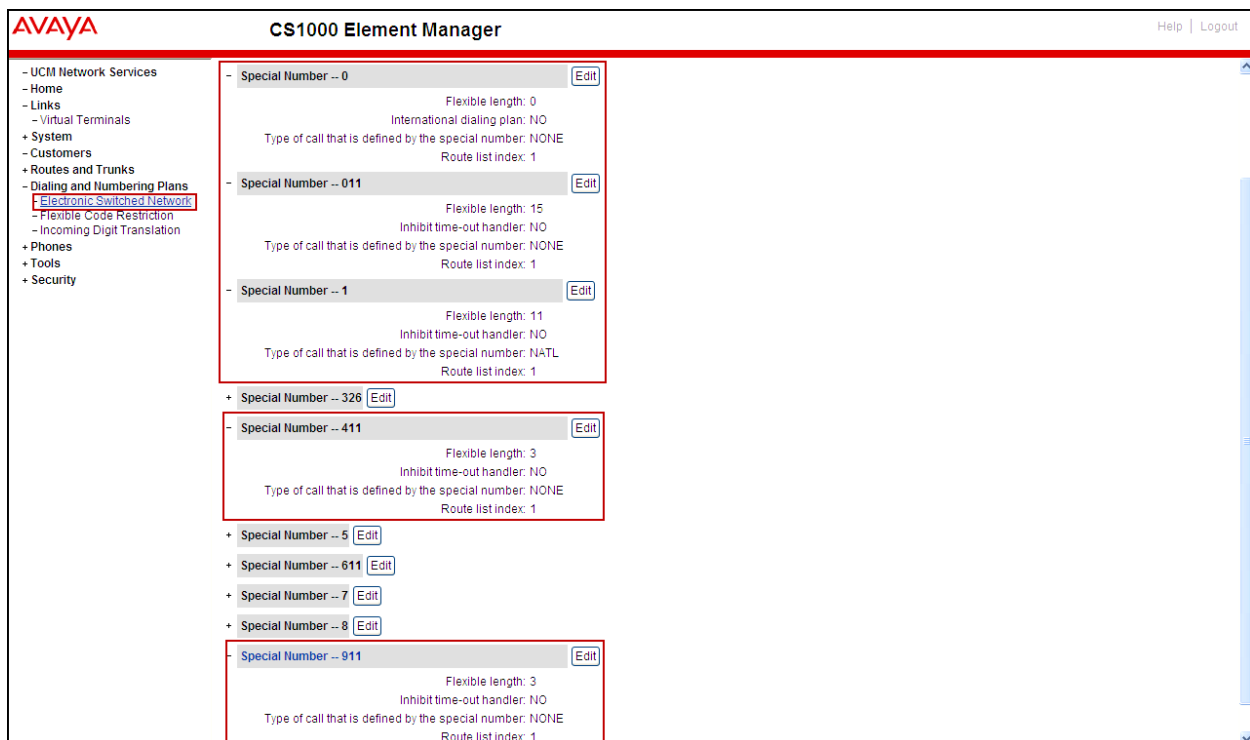
Special Number: 911

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

Special Number: 69

- **Flexible length:** 7.
- **CallType:** LOCL.
- **Route list index:** 1, created in **Section 5.6.4.**

Add any other special numbers as required, a subset of special numbers used during testing are shown below.



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

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

5.7. Administer Phone

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

5.7.1. Phone creation

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

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

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

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

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

```

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

```

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

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

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

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

5.7.2. Enable Privacy for Phone

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

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

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

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

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


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

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

Note: Privacy did not worked as expected, setting CLS to **ddgd** to hide the display of the number, as described above, did not blocked the number from being displayed. Setting CLS to **namd** to hide the display of the name did blocked the name and the number from being displayed, thus setting CLS to **namd** could be used for privacy. Refer to **Section 2.2**.

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: Check Originating.**
- **Number of normal ring cycles of CFNA: 4.**
- Click on **Save**.

AVAYA CS1000 Element Manager Help | Logout

Days for day option 3:

Redirection Holidays

Do not disturb hunting: ☐

Total redirection count limit:

Options:

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

Call forward: ☒ Originating ☐ Forwarding

Number of normal ringing cycles for CFNA

Option 0:

Option 1:

Option 2:

Number of distinctive ringing cycles for CFNA

Option 0:

Option 1:

Option 2:

Calls routed to message center

No answer DID calls: ☐

No answer non-DID calls: ☐

DID calls to busy telephones: ☐

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

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

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

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

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

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

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

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

5.7.4. Enable Call Waiting for the Phone

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

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

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

6. Configure Avaya Aura® Session Manager

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

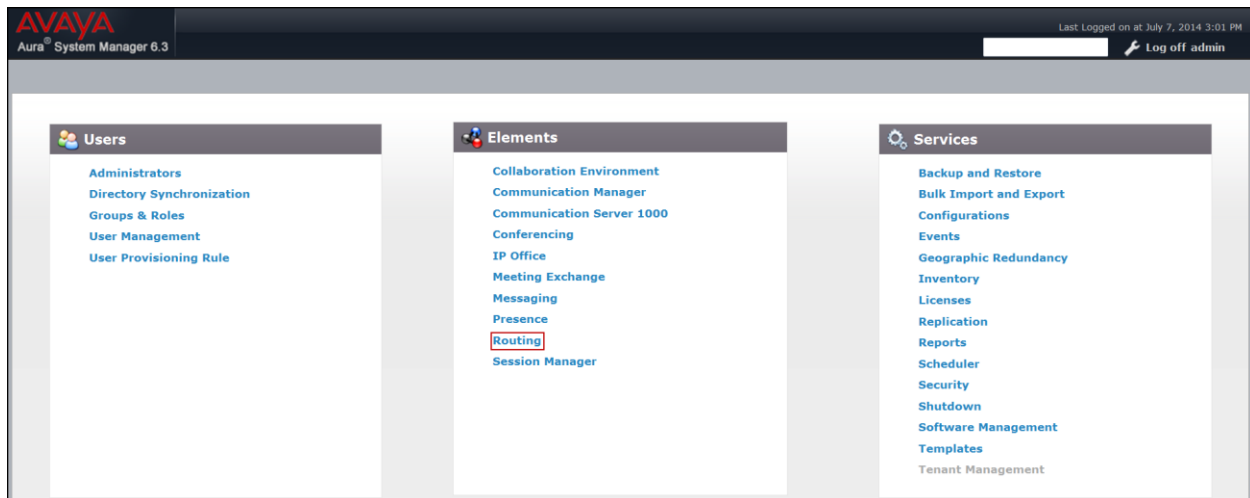
- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to the CS1000, the Avaya SBCE, and Session Manager itself.
- Entity Links, which define the SIP trunk parameters used by Session Manager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

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

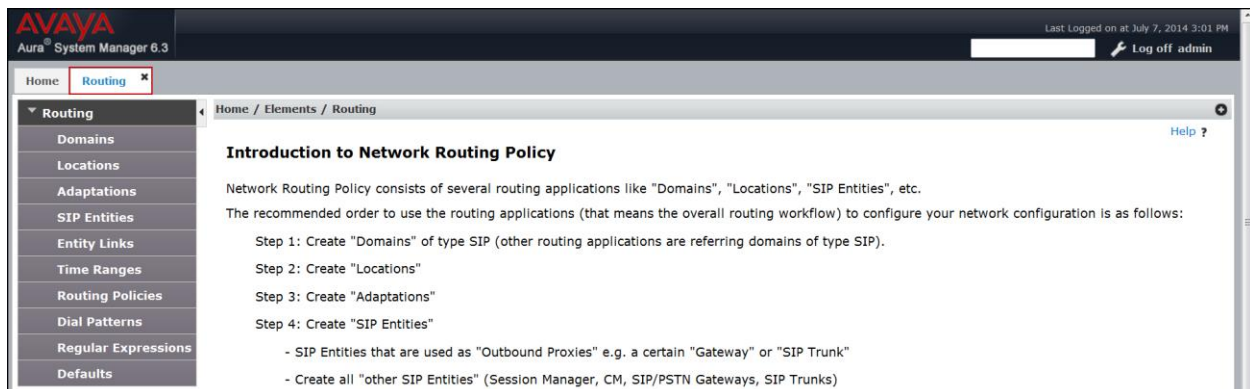
Note: Some of the default information in the screenshots that follow may have been cut out (not included) for brevity
--

6.1. System Manager Login and Navigation

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



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



6.2. Specify SIP Domain

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

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

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

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

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

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

6.3. Add Location

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

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

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

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains a 'Location Details' form for a new location named 'HG Session Manager'. The form includes sections for 'General' (Name, Notes), 'Dial Plan Transparency in Survivable Mode' (Enabled checkbox, Listed Directory Number, Associated CM SIP Entity), 'Overall Managed Bandwidth' (Managed Bandwidth Units, Total Bandwidth, Multimedia Bandwidth, Audio Calls Can Take Multimedia Bandwidth checkbox), 'Per-Call Bandwidth Parameters' (Maximum and Minimum Multimedia Bandwidth, Default Audio Bandwidth), 'Alarm Threshold' (Overall and Multimedia Alarm Threshold, Latency before Overall and Multimedia Alarm Trigger), and 'Location Pattern' (Add, Remove buttons, 0 Items, Filter: Enable, IP Address Pattern, Notes). The 'Name' field is highlighted with a red box. The 'Commit' and 'Cancel' buttons are visible at the bottom right of the form.

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and a 'Log off admin' link. The left sidebar shows a tree view with 'Routing' expanded and 'Locations' selected. The main content area is titled 'Home / Elements / Routing / Locations' and contains the 'Location Details' form for 'CS1k Node'. The form includes sections for 'General' (Name: CS1k Node, Notes: CS1K7.6), 'Dial Plan Transparency in Survivable Mode' (Enabled checkbox), 'Overall Managed Bandwidth' (Managed Bandwidth Units: Kbit/sec, Total Bandwidth, Multimedia Bandwidth, and Audio Calls Can Take Multimedia Bandwidth checkbox), 'Per-Call Bandwidth Parameters' (Maximum and Minimum Multimedia Bandwidth fields), 'Alarm Threshold' (Overall and Multimedia Alarm Thresholds, and Latency before Alarm Trigger fields), and 'Location Pattern' (Add/Remove buttons and a table with 0 items). The 'Commit' and 'Cancel' buttons are visible at the bottom right.

AVAYA
Aura System Manager 6.3

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: CS1k Node

Notes: CS1K7.6

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/Sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items

Filter: Enable

IP Address Pattern	Notes
--------------------	-------

Commit Cancel

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

AVAYA
Aura® System Manager 6.3

Last Logged on at July 7, 2014 3:01 PM
Log off admin

Home Routing

Home / Elements / Routing / Locations

Location Details Commit Cancel

General

* Name: HG ASBCE
Notes: HG Avaya SBCE

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

0 Items Filter: Enable

IP Address Pattern	Notes
--------------------	-------

Commit Cancel

6.4. Add Adaptation Module

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

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation.

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

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

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

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

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with 'Routing' selected. Under 'Routing', 'Adaptations' is highlighted. The main content area is titled 'Adaptation Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section is active, showing the following fields:

- Adaptation Name:** CS1K76
- Module Name:** CS1000Adapter
- Module Parameter Type:** (empty dropdown)
- Egress URI Parameters:** (empty text field)
- Notes:** (empty text field)

Below the 'General' section, there are two sections for digit conversion:

- Digit Conversion for Incoming Calls to SM:** Includes an 'Add' button and a table with 0 items. The table has columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. A 'Filter: Enable' button is on the right.
- Digit Conversion for Outgoing Calls from SM:** Includes an 'Add' button and a table with 0 items. The table has columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. A 'Filter: Enable' button is on the right.

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

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

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

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

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

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

6.5. Add SIP Entities

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

Add the SIP entity for Session Manager, as follows:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling, in this case the IP address of the Session Manager Security Module Interface.
- **Type:** Enter **Session Manager** for Session Manager, **Other** for the CS1000 and the Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** defined in **Section 6.4**.
- **Location:** Select one of the locations defined in **Section 6.3**.
- **Time Zone:** Select the time zone which the entity belongs to.

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

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

For the compliance test, only two Ports were used:

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

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

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

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

Below the form is the 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. The 'Port' section includes input fields for 'TCP Failover port' and 'TLS Failover port', with 'Add' and 'Remove' buttons. A table below shows 9 items:

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

Below the table is a 'SIP Responses to an OPTIONS Request' section with 'Add' and 'Remove' buttons. A table below shows 0 items:

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

The interface includes 'Commit' and 'Cancel' buttons at the top right and bottom right. The top right corner shows 'Last Logged on at July 7, 2014 3:01 PM' and a 'Log off admin' link.

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

For the compliance testing, the following values were used:

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

The following screen shows the addition of the **CS1K7.6** SIP entity. This SIP Entity will be assigned later to the Entity Link corresponding to the CS1000.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. A red rectangular box highlights the following fields: 'Name' (CS1K7.6), '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 this box, the 'SIP Timer B/F (in seconds)' is set to 4. Other visible fields include 'Credential name', 'Call Detail Recording' (none), 'CommProfile Type Preference', 'Loop Detection Mode' (Off), and 'SIP Link Monitoring' (Use Session Manager Configuration). The top of the interface shows the Avaya logo, 'Aura System Manager 6.3', and a 'Log off admin' button. The breadcrumb trail indicates the path: Home / Elements / Routing / SIP Entities.

A separate SIP entity for the Avaya SBCE is required in order to route calls to the service provider.

For the compliance test, the following values were used:

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

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. A red box highlights the following fields: 'Name' (HG ASBCE), 'FQDN or IP Address' (172.16.5.71), 'Type' (Other), 'Notes' (HG ASBCE), 'Adaptation' (HG SBCE), 'Location' (HG ASBCE), and 'Time Zone' (America/New_York). Below this box, other fields include 'SIP Timer B/F (in seconds)' (4), 'Credential name', 'Call Detail Recording' (none), 'CommProfile Type Preference', 'Loop Detection Mode' (Off), and 'SIP Link Monitoring' (Use Session Manager Configuration). The top right corner shows the user is logged in as 'admin' on July 8, 2014.

6.6. Add Entity Links

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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select Session Manager Entity configured in **Section 6.5**.
- **Protocol:** Select the transport protocol used for this link. This must match the protocol defined in **Section 6.5**.
- **Port:** Port number on which Session Manager will receive SIP requests. This must match the port defined in **Section 6.5**.
- **SIP Entity 2:** Select the name of the other system. For the CS1000 and the Avaya SBCE, select the CS1000 or the Avaya SBCE SIP entity defined in **Section 6.5**.
- **Port:** Port number on which the far-end will receive SIP requests. For the CS1000 this must match the port defined under **SIP Gateway Settings** tab, under **Proxy or Redirect Server** in **Section 5.5.1**. For the Avaya SBCE, this must match the port defined under **Server Configuration** in **Section 7.2.5**.
- **Connection Policy:** Select **Trusted** from the pull-down menu.
- Click **Commit** to save.

The following screen illustrates the Entity Link to the CS1000.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Entity Links' selected. The main area shows the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons. Below them, there is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The row shows: 'HG Session Manager' (Name), 'HG Session Manager' (SIP Entity 1), 'UDP' (Protocol), '5085' (Port), 'CS1K7.6' (SIP Entity 2), 'None' (DNS Override), '5085' (Port), 'trusted' (Connection Policy), 'None' (Deny New Service), and 'None' (Notes). Below the table, there is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
* HG Session Manager	* HG Session Manager	UDP	* 5085	* CS1K7.6		* 5085	trusted		

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

Avaya Aura System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item

Filter: Enable

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

Select : All, None

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

Avaya Aura System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

New Edit Delete Duplicate More Actions

21 Items

Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
HG Session Manager_AAC_5060_TCP	HG Session Manager	TCP	5060	AAC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	AAC Entity Link
HG Session Manager_Acme Packet_s1p1_5060_TCP	HG Session Manager	TCP	5060	Acme Packet s1p1	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager_CS1K7.6_5085_UDP	HG Session Manager	UDP	5085	CS1K7.6	<input type="checkbox"/>	5085	trusted	<input type="checkbox"/>	
HG Session Manager_EdgeMarc_SBC_5060_UDP	HG Session Manager	UDP	5060	EdgeMarc SBC	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
HG Session Manager_HG ASBCE_5060_TCP	HG Session Manager	TCP	5060	HG ASBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

6.7. Add Routing Policies

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

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

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).
- In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields.
- Click **Commit** to save.

The following screen shows the Routing Policy for the CS1000.

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

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

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

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

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

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

- Name:** To HG ASBCE
- Disabled:** ☐
- Retries:** 0
- Notes:** Outbound calls via ASBCE

Below these fields is the 'SIP Entity as Destination' section with a 'Select' button. At the bottom, there is a table with the following data:

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 Bell Aliant and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

AVAYA
Aura System Manager 6.3

Last Logged on at July 8, 2014 10:55 AM
Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: 1
* Min: 1
* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-
Notes:

Originating Locations and Routing Policies

[Add] [Remove]

6 Items [Filter: Enable]

	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 **506** to route inbound calls to DID numbers provided by Bell Aliant (DID numbers assigned to extensions in the CS1000). For calls that begin with 506, are between **3** and **10** digits in length, have a SIP Domain of **avaya.lab.com** and an Originating Location Name of **HG ASBCE**, Routing Policy **To CS1K76** will be used.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Routing' selected, and 'Dial Patterns' is highlighted. The main area is titled 'Dial Pattern Details' and contains the following fields:

- Pattern:** 506
- Min:** 3
- Max:** 10
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** avaya.lab.com
- Notes:** (empty)

Below these fields is a section titled 'Originating Locations and Routing Policies' with an 'Add' button and a table showing 1 item:

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

The next example shown below is for dial pattern “**69**” for outbound seven digits local calls, have a SIP Domain of **avaya.lab.com**, Originating Location Name of **CS1k Node**, uses Routing Policy Name of **To HG ASBCE**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar has a menu with 'Routing' selected, and 'Dial Patterns' is highlighted. The main area is titled 'Dial Pattern Details' and contains the following fields:

- Pattern:** 69
- Min:** 2
- Max:** 7
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** avaya.lab.com
- Notes:** (empty)

Below these fields is a section titled 'Originating Locations and Routing Policies' with an 'Add' button and a table showing 1 item:

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

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

6.9. Add/View Session Manager

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

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

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

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

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

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

AVAYA
Aura® System Manager 6.3

Last Logged on at: July 8, 2014 10:55 AM
Log off admin

Home / Session Manager

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

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

General

SIP Entity Name: HG Session Manager
Description: Lab-HG SM
Management Access Point Host Name/IP: 172.16.5.31
Direct Routing to Endpoints: Enable
VMware Virtual Machine: ☐

Security Module

SIP Entity IP Address: 172.16.5.32
Network Mask: 255.255.255.0
Default Gateway: 172.16.5.254
Call Control PHB: 46
QOS Priority: 6
Speed & Duplex: Auto
VLAN ID:
*SIP Firewall Configuration: Rule Set for HG Session Manager

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

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

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

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

7.1. Log in Avaya SBCE

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

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



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

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

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

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

The screenshot shows the 'Session Border Controller for Enterprise' dashboard. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists navigation options: 'Dashboard', 'Administration', 'Backup/Restore', 'System Management', 'Global Parameters', 'Global Profiles', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. The main content area is titled 'Dashboard' and contains three panels: 'Information' (System Time: 09:12:10 AM GMT, Version: 6.2.1.Q16, Build Date: Wed May 28 09:21:02 UTC 2014), 'Installed Devices' (listing EMS and Sipera), and 'Incidents (past 24 hours)' (showing five incidents with the message 'Sipera: No Server Flow Matched for Incoming Message'). A 'Notes' section is at the bottom right.

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

The screenshot shows the 'System Management' page. The left sidebar is the same as the dashboard. The main content area is titled 'System Management' and has tabs for 'Devices', 'Updates', 'SSL VPN', and 'Licensing'. The 'Devices' tab is selected, showing a table of installed devices. The table has columns: 'Device Name (Serial Number)', 'Management IP', 'Version', 'Status', and 'Actions'. The first row shows 'Sipera (PCS31030132)' with Management IP '10.10.10.10', Version '6.2.1.Q16', and Status 'Commissioned'. The 'Actions' column for this device includes 'Reboot', 'Shutdown', 'Restart Application', 'View', 'Edit', and 'Delete'. The 'View' button is highlighted with a red box.

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

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

The screenshot shows a window titled "System Information: Sipera" with a close button (X) in the top right corner. The window is divided into several sections:

- General Configuration:**
 - Appliance Name: Sipera
 - Box Type: SIP
 - Deployment Mode: Proxy
- Device Configuration:**
 - HA Mode: No
 - Two Bypass Mode: No
- Network Configuration:** A table with 5 columns: IP, Public IP, Netmask, Gateway, and Interface.

IP	Public IP	Netmask	Gateway	Interface
172.16.5.71	172.16.5.71	255.255.255.0	172.16.5.254	A1
172.16.5.199	172.16.5.199	255.255.255.0	172.16.5.200	B1
- DNS Configuration:**
 - Primary DNS: 172.16.5.102
 - Secondary DNS: (empty)
 - DNS Location: DMZ
 - DNS Client IP: 172.16.5.71
- Management IP(s):**
 - IP: (blurred out)

On the previous screen, note that the **A1** corresponds to the inside interface (toward Session Manager) and **B1** corresponds to the outside interface (toward the Service Provider) of the Avaya SBCE. The management IP was blurred out for security reasons.

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

7.2. Global Profiles

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

7.2.1. Server Interworking - Avaya-SM

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

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

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

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

For the newly created **Avaya-SM** profile, click **Edit** at the bottom of the **Advanced** tab:

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

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

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

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

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

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

Advanced	
Record Routes	Both
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

7.2.2. Server Interworking - SP-General

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

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

Enter the new profile name, the name of **SP-General** was chosen in this example. Accept the default values for all fields by clicking **Next** and then Click **Finish**.

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

The screenshot displays the 'Session Border Controller for Enterprise' web interface. The left navigation pane shows 'Global Profiles' expanded, with 'Server Interworking' selected. The main content area is titled 'Interworking Profiles: SP-General' and includes an 'Add' button. Below this is a list of existing profiles: cs2100, avaya-ru, OCS-Edge-Server, cisco-ccm, cups, Sipera-Halo, OCS-FrontEnd-Server, Avaya-SM, **SP-General** (highlighted), Avaya-CS1000, Avaya-IPO, Avaya-CM, and Test. The 'General' tab is active, showing a table of configuration parameters.

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with 'Global Profiles' expanded to show 'Server Interworking' and 'SP-General' highlighted. The main content area is titled 'Interworking Profiles: SP-General' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' options. Below this, a list of interworking profiles is shown, including 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', 'OCS-FrontEnd-Server', 'Avaya-SM', 'SP-General' (highlighted), 'Avaya-CS1000', 'Avaya-IPO', 'Avaya-CM', and 'Test'. The 'Advanced' tab is selected, displaying a table of configuration parameters:

Parameter	Value
Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

7.2.3. Routing Profiles

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

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

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

- Select **Routing**.
- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SM**.
- Click **Next**.

On the next screen, complete the following:

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

Edit Routing Rule
X

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

Next Hop Routing

URI Group

*

Next Hop Server 1

IP, IP:Port, Domain, or Domain:Port

172.16.5.32

Next Hop Server 2

IP, IP:Port, Domain, or Domain:Port

Routing Priority based on Next Hop Server

☒

Use Next Hop for In Dialog Messages

☐

Ignore Route Header for Messages Outside Dialog

☐

NAPTR

☐

SRV

☐

Outgoing Transport

☐ TLS
☒ TCP
☐ UDP

Finish

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

Alarms
Incidents
Statistics
Logs
Diagnostics
Users

Settings
Help
Log Out

Session Border Controller for Enterprise
AVAYA

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

Routing Profiles: Route_to_SM

Add
Rename
Clone
Delete

Click here to add a description.

Routing Profile

Add

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

Similarly, for the outbound route:

- Click **Add** in the **Routing Profiles** section.
- Enter Profile Name: **Route_to_SP**
- Click **Next**.
- **Next Hop Server 1: 142.125.72.11** (Service Provider SIP Proxy IP address)
- Check **Routing Priority Based on Next Hop Server**.
- **Outgoing Transport:** select **UDP**.
- Click **Finish**.

Edit Routing Rule X

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

Next Hop Routing

URI Group: *

Next Hop Server 1: 142.125.72.11
IP, IP:Port, Domain, or Domain:Port

Next Hop Server 2:
IP, IP:Port, Domain, or Domain:Port

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

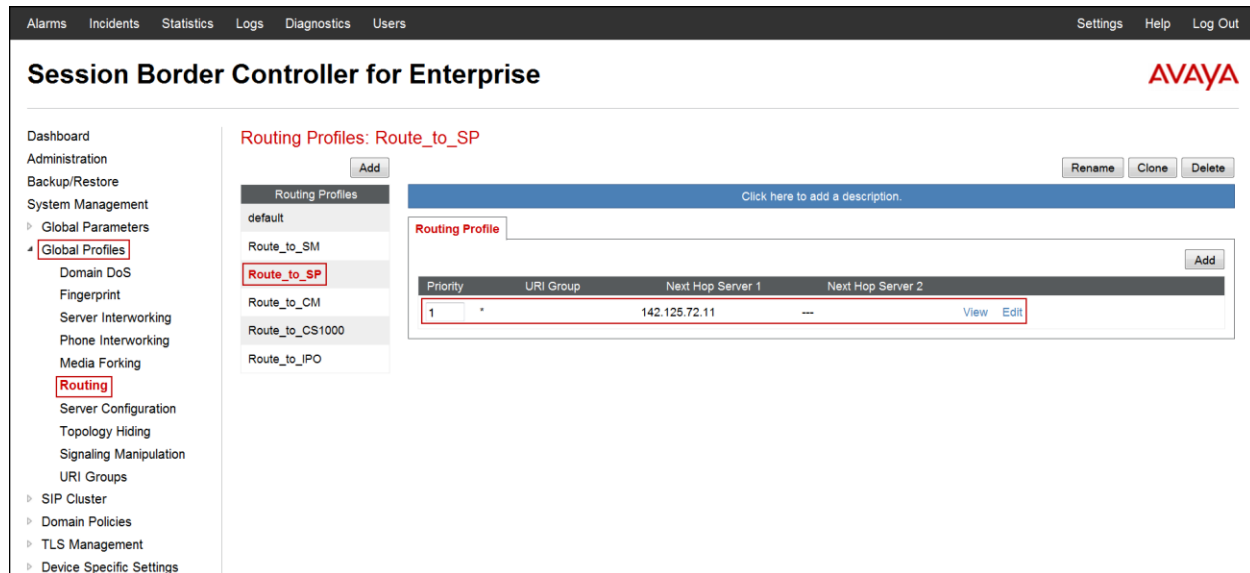
NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☐ TCP ☒ UDP

Finish

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



7.2.4. Signaling Manipulation

The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform a granular header manipulation on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script 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. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [12] on the **References** section for more information on this topic.

A Sigma script was created during the compliance test to hardcode the PAI with the first DID number in the DID group provided by Bell Aliant. This was required in order to make outbound calls from the CS1000 to the PSTN and for the correct number to be displayed at the PSTN (CallID).

Note: Additional Avaya SBCE header manipulation will be performed by implementing Signaling Rules, in **Section 7.3.1** later in this document.

On the left navigation pane, select **Global Profiles** → **Signaling Manipulation**. From the **Signaling Manipulation Scripts** list, select **Add**.

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

Signaling Manipulation Editor AVAYA

Title: Save

```

1 //The SBC will hardcode the PAI with the first DID number in the DID group,
2 //Which is also used for SIP Trunk Registration.
3 //This is required in order to make outbound calls (CS1K-->PSTN) and for
4 //the correct number to be displayed at the PSTN.
5
6 within session "INVITE"
7 {
8   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
9   {
10     %HEADERS["P-Asserted-Identity"][1].URI.USER = "5066948000";
11   }
12 }

```

The following screen capture shows the Hardcode PAI SigMa script after it was added.

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Signaling Manipulation Scripts: Hardcode PAI

Upload Add Download Clone Delete

Click here to add a description.

Signaling Manipulation

```

//The SBC will hardcode the PAI with the first DID number in the DID group,
//Which is also used for SIP Trunk Registration.
//This is required in order to make outbound calls (CS1K-->PSTN) and for
//the correct number to be displayed at the PSTN.

within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["P-Asserted-Identity"][1].URI.USER = "5066948000";
  }
}

```

Edit

7.2.5. Server Configuration

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

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

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

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

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

The screenshot displays the 'Edit Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Call Server'. The 'IP Addresses / Supported FQDNs' text area contains '172.16.5.32'. Under 'Supported Transports', the 'TCP' checkbox is checked, while 'UDP' and 'TLS' are unchecked. The 'TCP Port' field is set to '5060'. There are empty input fields for 'UDP Port' and 'TLS Port'. A 'Finish' button is located at the bottom center of the window.

On the **Advanced** window:

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

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

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Avaya-SM

Signaling Manipulation Script None

TCP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

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

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise AVAYA

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

Server Configuration: Session Manager

Add

Session Manager Service Provider Com Manager CS1000 IP Office

General Authentication Heartbeat Advanced

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

Edit

Rename Clone Delete

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

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with "Global Profiles" expanded to show "Session Manager" and "Server Configuration" highlighted. The main content area is titled "Server Configuration: Session Manager" and features an "Add" button. Below this, a list of server profiles includes "Session Manager", "Service Provider", "Com Manager", "CS1000", and "IP Office". The "Session Manager" profile is selected, and its configuration is shown in the "Advanced" tab. The configuration table lists the following settings:

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

An "Edit" button is located at the bottom right of the configuration table. The "Session Manager" profile name and the "Advanced" tab are also highlighted with red boxes in the original image.

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

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

- **Server Type:** select **Trunk Server**.
- **IP Address:** **142.125.72.11** (service provider's SIP Proxy IP address).
- **Supported Transports:** check **UDP**.
- **UDP Port:** enter **5060**.
- Click **Next**.

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

The screenshot displays the 'Add Server Configuration Profile - General' window. The 'Server Type' dropdown is set to 'Trunk Server'. The 'IP Addresses / Supported FQDNs' field contains '142.125.72.11'. Under 'Supported Transports', the 'UDP' checkbox is checked, while 'TCP' and 'TLS' are unchecked. The 'UDP Port' field is set to '5060'. The 'Back' and 'Next' buttons are at the bottom.

Server Type	Trunk Server
IP Addresses / Supported FQDNs <small>Separate entries with commas</small>	142.125.72.11
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
<input type="button" value="Back"/> <input type="button" value="Next"/>	

On the **Authentication** tab:

- Check the **Enable Authentication** box.
- Enter the **User Name** credential information supplied by the service provider for the authentication of the SIP trunk.
- Enter the **Realm** information supplied by the service provider for the authentication of the SIP trunk. (Must be entered, currently cannot be detected automatically from the challenge)
- Enter **Password** credential information supplied by the service provider for the authentication of the SIP trunk.
- Click **Next**.

The screenshot shows a dialog box titled "Add Server Configuration Profile - Authentication". It contains the following fields and controls:

- Enable Authentication:** A checkbox that is checked, highlighted by a red box.
- User Name:** A text input field containing "User123", highlighted by a red box.
- Realm:** A text input field containing "Realm", highlighted by a red box. Below the field is the text "(Leave blank to detect from server challenge)".
- Password:** A password input field with masked characters (dots), highlighted by a red box.
- Confirm Password:** A password input field with masked characters (dots), highlighted by a red box.
- Buttons:** "Back" and "Next" buttons are located at the bottom of the dialog.

On the **Heartbeat** tab:

- Check the **Enable Heartbeat** box.
- Under **Method**, select **REGISTER** from the drop down menu.
- **Frequency**: Enter the amount of time (in seconds) between REGISTER messages that will be sent from the enterprise to the Service Provider Proxy Server to refresh the registration binding of the SIP trunk. This value should be chosen in consultation with the service provider, **60** seconds was the value used during the compliance test.
- The **From URI** and **To URI** entries for the REGISTER messages are built using the following:
 - **From URI**: use the **User Name** entered above in the **Authentication** screen and the Service Provider's domain name, as shown on the screen below.
 - **To URI**: Use the **User Name** entered above in the **Authentication** screen and the Service Provider Proxy Provider's domain name, as shown on the screen below.
 - Click **Next**.

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER
Frequency	60 seconds
From URI	User123@pbx06dch204
To URI	123@pbx06dch2046.ca

Back Next

On the **Advanced** tab:

- Select **SP-General** from the **Interworking Profile** drop down menu.
- Under **Signaling Manipulation Script**, select the **Hardcode PAI** script created in **Section 7.2.4**.
- Click **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile SP-General

Signaling Manipulation Script Hardcode PAI

UDP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Back Finish

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

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Server Configuration: Service Provider

Add Rename Clone Delete

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

Server Type	Trunk Server
IP Addresses / FQDNs	142.125.72.11
Supported Transports	UDP
UDP Port	5060

Edit

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

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Global Profiles" and "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 "Authentication" tab is active, showing a table with the following data:

Authentication	
Enable Authentication	<input checked="" type="checkbox"/>
User Name	User123
Realm	Realm

Buttons for "Rename", "Clone", and "Delete" are located at the top right of the configuration area. An "Add" button is at the top left, and an "Edit" button is at the bottom right of the table.

The following screen capture shows the **Heartbeat** tab of the newly created **Service Provider** Profile.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface, showing the "Heartbeat" tab for the "Service Provider" profile. The top navigation bar and sidebar menu are consistent with the previous screenshot. The main content area is titled "Server Configuration: Service Provider -" and features a tabbed interface with "General", "Authentication", "Heartbeat", and "Advanced" tabs. The "Heartbeat" tab is active, showing a table with the following data:

Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	REGISTER
Frequency	60 seconds
From URI	User123@pbx06dch2046.ca
To URI	User123@pbx06dch2046.ca

Buttons for "Rename", "Clone", and "Delete" are located at the top right of the configuration area. An "Add" button is at the top left, and an "Edit" button is at the bottom right of the table.

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

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration categories, with "Global Profiles" expanded to show "Domain DoS", "Fingerprint", "Server Interworking", "Phone Interworking", "Media Forking", "Routing", "Server Configuration", "Topology Hiding", "Signaling Manipulation", "URI Groups", "SIP Cluster", "Domain Policies", "TLS Management", and "Device Specific Settings". The "Server Configuration" section is highlighted. The main content area is titled "Server Configuration: Service Provider -" and features an "Add" button and "Rename", "Clone", and "Delete" buttons. A list of server profiles is shown, including "Session Manager", "Service Provider", "Com Manager", "CS1000", "IP Office", and "Service Provider" (which is highlighted). The "Advanced" tab is selected, displaying a table of configuration parameters: "Enable DoS Protection" (checkbox), "Enable Grooming" (checkbox), "Interworking Profile" (set to "SP-General"), "Signaling Manipulation Script" (set to "Hardcode PAI"), and "UDP Connection Type" (set to "SUBID"). An "Edit" button is located at the bottom right of the table.

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

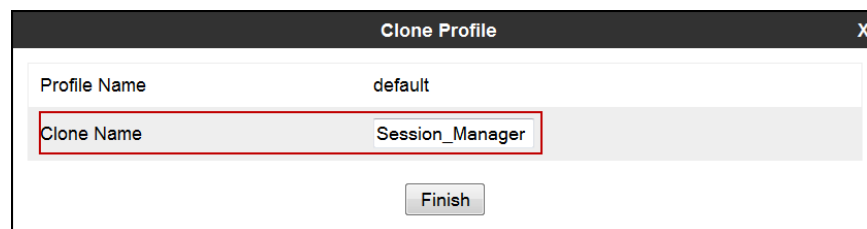
7.2.6. Topology Hiding

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.

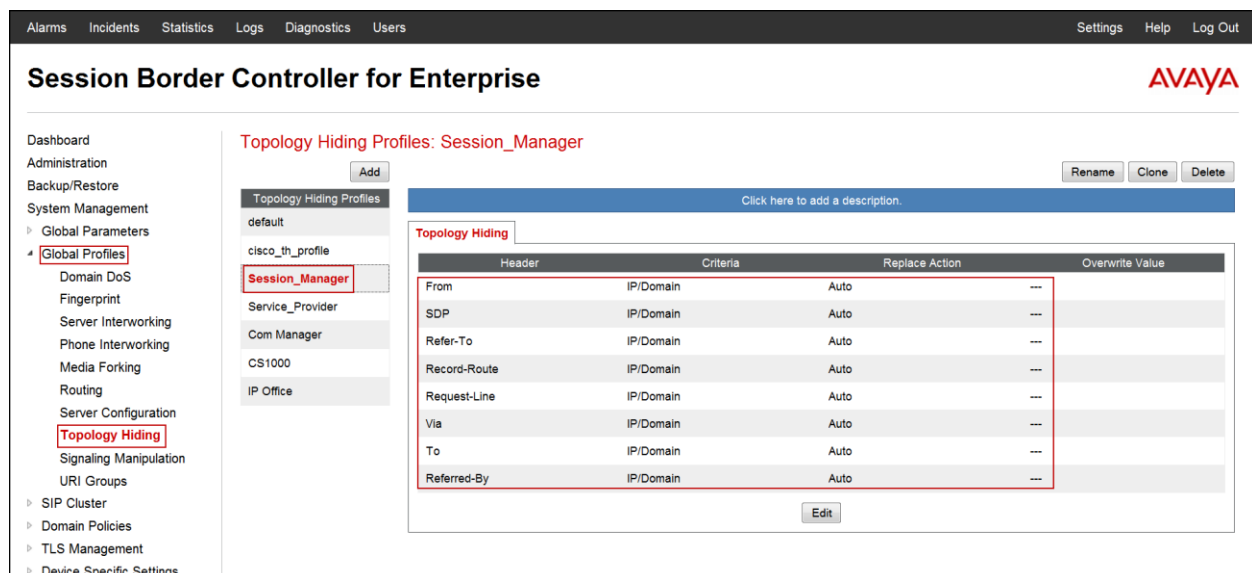
To add the Topology Hiding Profile in the Enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

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



A dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two input fields: "Profile Name" with the value "default" and "Clone Name" with the value "Session_Manager". The "Clone Name" field is highlighted with a red border. Below the fields is a "Finish" button.

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

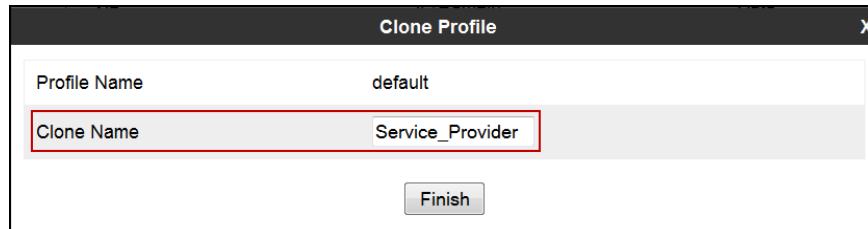


The screenshot shows the "Session Border Controller for Enterprise" web interface. The left sidebar contains a navigation menu with "Global Profiles" selected. The main area displays "Topology Hiding Profiles: Session_Manager". A list of profiles is shown on the left, with "Session_Manager" highlighted. On the right, a table titled "Topology Hiding" shows the configuration for the selected profile. The table has four columns: Header, Criteria, Replace Action, and Overwrite Value. The "From" header is highlighted with a red border.

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

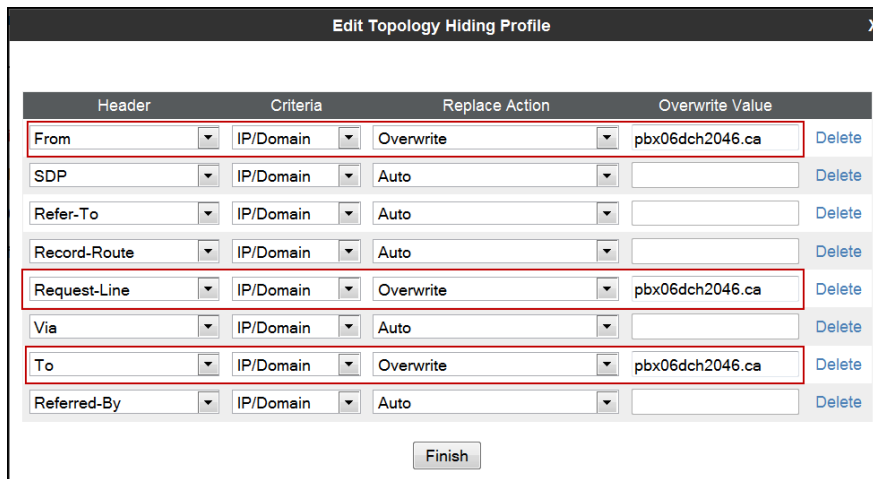
To add the Topology Hiding Profile in the Service Provider direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side:

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



The 'Clone Profile' dialog box shows the 'Profile Name' as 'default' and the 'Clone Name' as 'Service_Provider'. A red box highlights the 'Clone Name' field. A 'Finish' button is at the bottom.

- Click **Edit** on the newly added **Service_Provider** Topology Hiding profile.
- In the **From** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**pbx06dch2046.ca**) under **Overwrite Value**.
- In the **To** choose **Overwrite** from the pull-down menu under **Replace Action**, enter the domain name for the Service Provider (**pbx06dch2046.ca**) under **Overwrite Value**.
- In the **Request-Line** choose **Overwrite** from the pull-down menu under **Replace Action**; enter the domain name for the Service Provider (**pbx06dch2046.ca**) under **Overwrite Value**.



The 'Edit Topology Hiding Profile' dialog box shows a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The 'From', 'Request-Line', and 'To' rows are highlighted with red boxes, showing 'Overwrite' as the Replace Action and 'pbx06dch2046.ca' as the Overwrite Value. A 'Finish' button is at the bottom.

Header	Criteria	Replace Action	Overwrite Value	
From	IP/Domain	Overwrite	pbx06dch2046.ca	Delete
SDP	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	pbx06dch2046.ca	Delete
Via	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	pbx06dch2046.ca	Delete
Referred-By	IP/Domain	Auto		Delete

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

The screenshot shows the Avaya Session Border Controller for Enterprise configuration interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (selected), Signaling Manipulation, URI Groups, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Topology Hiding Profiles: Service_Provider' and includes an 'Add' button, a list of profiles (default, cisco_th_profile, Session_Manager, Service_Provider (selected), Com Manager, CS1000, IP Office), and a table for 'Topology Hiding' rules. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The rules listed are: From (IP/Domain, Overwrite, pbx06dch2046.ca), SDP (IP/Domain, Auto, ---), Refer-To (IP/Domain, Auto, ---), Record-Route (IP/Domain, Auto, ---), Request-Line (IP/Domain, Overwrite, pbx06dch2046.ca), Via (IP/Domain, Auto, ---), To (IP/Domain, Overwrite, pbx06dch2046.ca), and Referred-By (IP/Domain, Auto, ---). There are also buttons for Rename, Clone, Delete, and Edit.

7.3. Domain Policies

Domain Policies allow the configuration of 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. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, two new Signaling Rules were defined. All other rules under the Domain Policies menu, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one of the defaults and then make the necessary changes to the new rule.

7.3.1. Signaling Rules

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

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

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

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

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

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

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

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

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

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

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

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

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

To add the **P-Charging-Vector** header:

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

To add the **P-Location** header:

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

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

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

The following screen capture shows the **Request Headers** tab of the **SessMgr_SigRule** signaling rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with categories like Dashboard, Administration, System Management, and Domain Policies. The 'Domain Policies' section is expanded, showing 'Signaling Rules' as a sub-option. The main content area is titled 'Signaling Rules: SessMgr_SigRule'. It features a 'Filter By Device...' dropdown and buttons for 'Add', 'Rename', 'Clone', and 'Delete'. Below this is a tabbed interface with tabs for 'General', 'Requests', 'Responses', 'Request Headers' (which is selected), 'Response Headers', 'Signaling QoS', and 'UCID'. The 'Request Headers' tab displays a table with the following data:

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

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

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

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

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

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

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

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

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

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

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

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

To add the **P-Charging-Vector** header:

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

To add the **P-Location** header:

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

To add the **P-Location** header:

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

The following screen capture shows the **Response Headers** tab of the **SessMgr_SigRule** signaling rule

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' and 'Signaling Rules' highlighted. The main content area shows the configuration for the 'SessMgr_SigRule' signaling rule. The 'Response Headers' tab is selected, showing a table of configured headers.

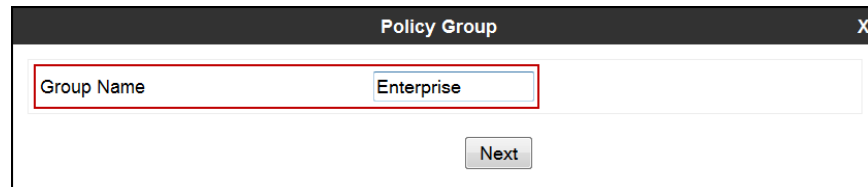
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
2	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
3	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit Delete
4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

7.3.2. 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.**
- Click **Next**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Group Name" which contains the text "Enterprise". This field is highlighted with a red rectangular border. Below the input field, there is a "Next" button.

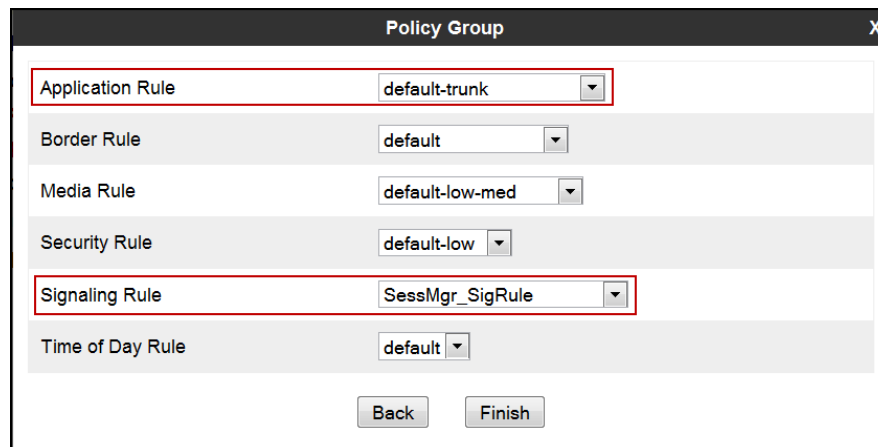
In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the **SessMgr_SigRule** rule created in **Section 7.3.1** was selected.

In the **Policy Group** screen select the following:

- **Application Rule: default-trunk.**
- **Signaling Rule: SessMgr_SigRule.**

All other fields will default to the values shown below.

- Click **Finish**.



The screenshot shows a dialog box titled "Policy Group" with a close button (X) in the top right corner. Inside the dialog, there are several dropdown menus for different rule types. The "Application Rule" dropdown is highlighted with a red box and shows "default-trunk". The "Signaling Rule" dropdown is also highlighted with a red box and shows "SessMgr_SigRule". Other dropdowns include "Border Rule" (default), "Media Rule" (default-low-med), "Security Rule" (default-low), and "Time of Day Rule" (default). At the bottom of the dialog, there are "Back" and "Finish" buttons.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Enterprise'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-subscri...', 'avaya-def-high-server', 'Enterprise', and 'Service Provider'. The 'Enterprise' group is selected. The right pane shows the configuration for the 'Enterprise' group, including a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: 1, default-trunk, default, default-low-med, default-low, SessMgr_SigRule, and default. The 'Enterprise' group is also listed in the 'Policy Groups' list on the left.

A second End Point Policy Group was created for the service provider, repeating the steps described above. Defaults were used for all fields. The name **Service Provider** was chosen in this example.

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: Service Provider'. It features a list of policy groups on the left, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'avaya-def-high-subscri...', 'avaya-def-high-server', 'Enterprise', and 'Service Provider'. The 'Service Provider' group is selected. The right pane shows the configuration for the 'Service Provider' group, including a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row with the following values: 1, default-trunk, default, default-low-med, default-low, default, and default. The 'Service Provider' group is also listed in the 'Policy Groups' list on the left.

7.4. Device Specific Settings

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

7.4.1. Network Management

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

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

Use **Figure 1** as reference for IP address assignments.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with 'Device Specific Settings' expanded, and 'Network Management' selected. The main content area is titled 'Network Management: Sipera' and features two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask 255.255.255.0', 'A2 Netmask', 'B1 Netmask 255.255.255.0', and 'B2 Netmask', with 'Add', 'Save', and 'Clear' buttons. A table lists IP addresses and their associated interfaces:

IP Address	Public IP	Gateway	Interface	
172.16.5.71		172.16.5.254	A1	Delete
172.16.5.199		172.16.5.200	B1	Delete

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

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ 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

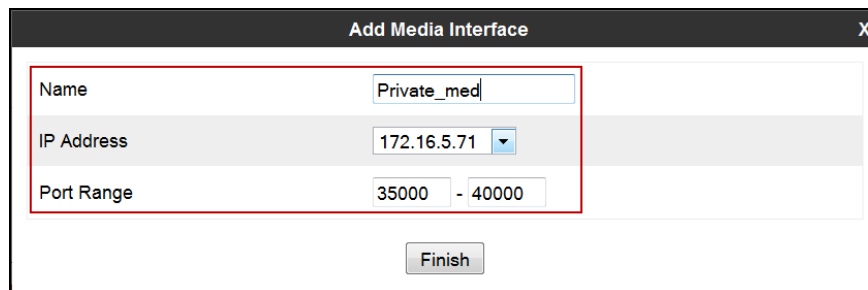
Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

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, port range 35000 to 40000 was used.

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

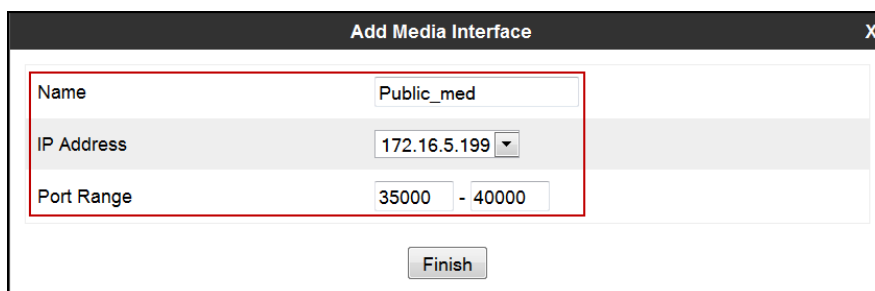
- Select **Add** in the **Media Interface** area (not shown).
- **Name: Private_med.**
- **IP Address: 172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward Session Manager).
- **Port Range: 35000-40000.**
- Click **Finish**.



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

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

- Select **Add** in the **Media Interface** area.
- **Name: Public_med.**
- **IP Address: 172.16.5.199** (Outside or B1 IP Address of the Avaya SBCE, toward the Service Provider via the IPSec VPN Tunnel).
- **Port Range: 35000-40000.**
- Click **Finish**.



The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "Public_med", "IP Address" with a dropdown menu showing "172.16.5.199", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the dialog.

The following screen capture shows the newly created media interfaces.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management sections, with "Device Specific Settings" and "Media Interface" highlighted. The main content area is titled "Media Interface: Sipera" and features a tabbed interface with "Media Interface" selected. A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is a table listing the configured media interfaces:

Name	Media IP	Port Range	
Private_med	172.16.5.71	35000 - 40000	Edit Delete
Public_med	172.16.5.199	35000 - 40000	Edit Delete

An "Add" button is located to the right of the table header.

7.4.3. Signaling Interface

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

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

- Select **Add** in the **Signaling Interface** area.
- **Name: Private_sig.**
- Select **IP Address: 172.16.5.71** (Inside or A1 IP Address of the Avaya SBCE, toward Session Manager).
- **TCP Port: 5060.**
- Click **Finish**.

Name	Private_sig
IP Address	172.16.5.71
TCP Port <small>Leave blank to disable</small>	5060
UDP Port <small>Leave blank to disable</small>	
Enable Stun	<input type="checkbox"/>
TLS Port <small>Leave blank to disable</small>	
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

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

- Select **Add** in the **Signaling Interface** area.
- **Name: Public_sig.**
- **IP Address: 172.16.5.199** (Outside or B1 IP Address of the Avaya SBCE, toward the Service Provider via the IPSec VPN Tunnel).
- **UDP Port: 5060.**
- Click **Finish**.

Name	Public_sig
IP Address	172.16.5.199
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	5060
Enable Stun	<input type="checkbox"/>
TLS Port <small>Leave blank to disable</small>	
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

The following screen capture shows the newly created signaling interfaces.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ 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

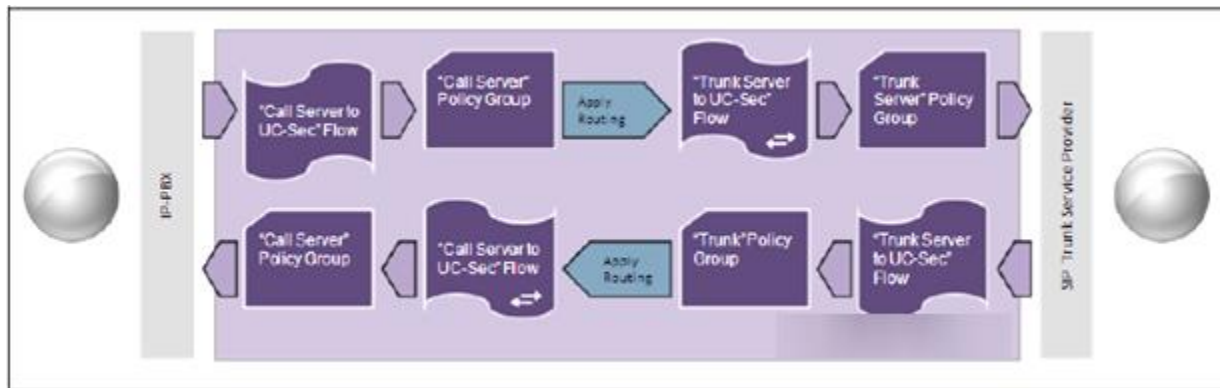
Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	172.16.5.71	5060	---	---	None	Edit Delete
Public_sig	172.16.5.199	---	5060	---	None	Edit Delete

Add

7.4.4. End Point Flows

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



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

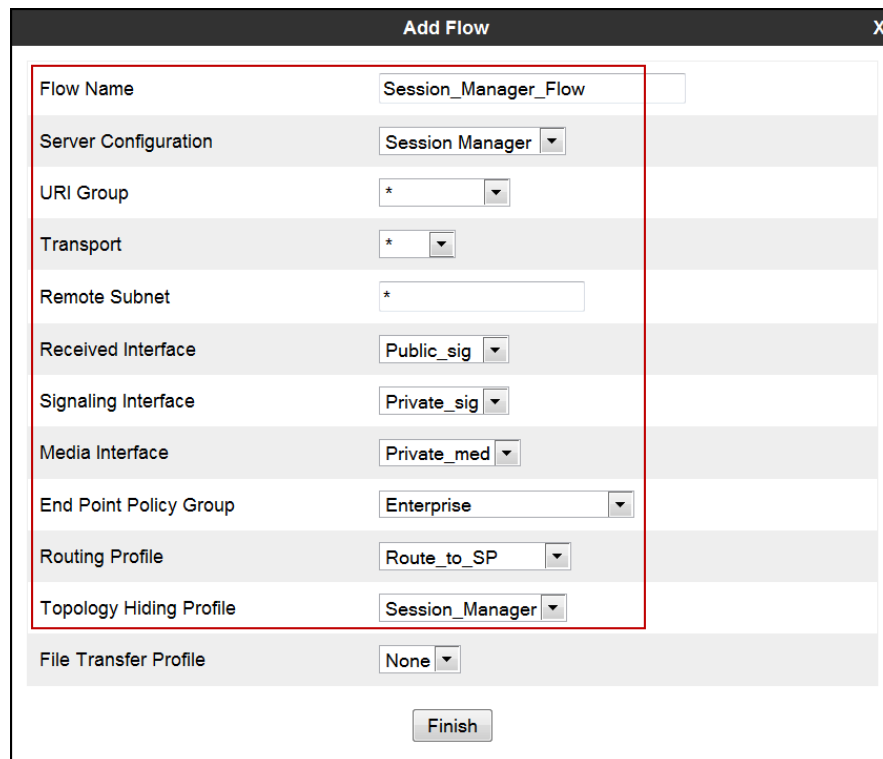
To create the call flow toward the Service Provider SIP trunk, from the **Device Specific Settings** menu, select **End Point Flows**, and then the **Server Flows** tab. Click **Add Flow** (not shown).

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

Add Flow	
Flow Name	SIP_Trunk_Flow
Server Configuration	Service Provider
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private_sig
Signaling Interface	Public_sig
Media Interface	Public_med
End Point Policy Group	Service Provider
Routing Profile	Route_to_SM
Topology Hiding Profile	Service_Provider
File Transfer Profile	None
Finish	

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

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



The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label and a value field. A red rectangular box highlights the first ten fields, from "Flow Name" to "Topology Hiding Profile". The fields and their values are:

Field	Value
Flow Name	Session_Manager_Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	Enterprise
Routing Profile	Route_to_SP
Topology Hiding Profile	Session_Manager

Below the highlighted fields, there is one more field:

Field	Value
File Transfer Profile	None

At the bottom center of the window is a button labeled "Finish".

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management tasks, with 'Device Specific Settings' and 'End Point Flows' highlighted. The main content area is titled 'End Point Flows: Sipera' and contains two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, showing two configuration sections: 'Server Configuration: Service Provider' and 'Server Configuration: Session Manager'. Each section contains a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The 'Service Provider' table has one entry with Priority 1, Flow Name 'SIP_Trunk_Flow', URI Group '*', Received Interface 'Private_sig', Signaling Interface 'Public_sig', End Point Policy Group 'Service Provider', and Routing Profile 'Route_to_SM'. The 'Session Manager' table has one entry with Priority 1, Flow Name 'Session_Manager_Flow', URI Group '*', Received Interface 'Public_sig', Signaling Interface 'Private_sig', End Point Policy Group 'Enterprise', and Routing Profile 'Route_to_SP'. Both entries have 'View', 'Clone', 'Edit', and 'Delete' action links.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ 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.

Server Configuration: Service Provider

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

Server Configuration: Session Manager

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

8. Bell Aliant SIP Trunk Service Configuration

To use Bell Aliant's SIP Trunk service, a customer must request the service from Bell Aliant using the established sales processes. The process can be started by contacting Bell Aliant via the corporate web site at: <http://www.bellaliant.ca/index.shtml> and requesting information.

During the signup process, Bell Aliant and the customer will discuss details about the preferred method to be used to connect the customer's enterprise network to Bell Aliant's network. In the configuration described under these Application Notes, an IPSec VPN Tunnels was used. Bell Aliant will provide IP addresses, Direct Inward Dialed (DID) numbers to be assigned to the enterprise, etc. This information is used to complete the Avaya Communication Server 1000E, Avaya Aura® Session Manager, and the Avaya Session Border Controller for Enterprise configuration discussed in the previous sections.

During the interoperability testing, a VPN connection was used to connect the simulated enterprise site to Bell Aliant's network via the public internet. The connection could also be done without the use of VPN, by directly connecting the Avaya SBCE to a public facing SBC located in Bell Aliant's network. This is accomplished by assigning public IP addresses, capable of being reached across the public internet, to the Avaya SBCE (interface B1) and to the Bell Aliant's SBC.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

Place an inbound/outbound call to/from a PSTN phone and to/from an internal CS1000 phone, answer the call, and verify that two-way speech path exists. Check call displayed number to ensure the correct Call ID is received. Perform hold/retrieve on calls. Verify the call remains stable for several minutes and disconnects properly.

Verify Call Establishment on the CS1000 Call Server

Active Call Trace (LD 80).

The following is an example of one of the commands available on the CS1000 to trace the extension (DN) when the call is active or idle. The call scenario involved the CS1000 extension 8001 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 8001** while the call is active.
- After the call is released, issue command **trac 0 8001** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when extension 8001 is in an active call:

Note that part of the telephone numbers have been blurred out for security reasons.

The following screen shows an example of an active call on extension 8001.

```
.trac 0 8001

ACTIVE VTN 008 0 00 01

ORIG VTN 048 0 00 00 VTRK IPTI RMBR 0 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 172.16.5.71
FAR-END MEDIA ENDPOINT IP: 172.16.5.71 PORT: 35802
FAR-END VendorID: Nortel SESM 17.0.7.4 AVAYA-SM-6.3.8.0.638018
TERM VTN 008 0 00 01 KEY 0 SCR MARP CUST 0 DN 8001 TYPE 1110
SIGNALLING ENCRYPTION: INSEC
FAR-END SIP SIGNALLING IP: 172.16.21.61
FAR-END MEDIA ENDPOINT IP: 10.10.10.1 PORT: 5200
FAR-END SIP SIGNALLING IP: 172.16.21.61
FAR-END MEDIA ENDPOINT IP: 10.10.10.1 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 8001
MAIN_PM ESTD
TALKSLOT ORIG 16 TERM 21 JUNCTOR ORIGO TERMO
EES_DATA:
NONE
QUEU NONE
CALL ID 0 150

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 385
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 786331 NUM_PLAN:PRIVATE TON:ABBREVIATED ESN:CDP
CALLED NO = 506694 NUM_PLAN:PRIVATE TON:ABBREVIATED ESN:CDP
```

The following screen shows an example after the call on extension 8001 was released.

```
.trac 0 8001

IDLE VTN 008 0 00 01 MARP
```

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

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

9.2. Protocol Traces

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

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

The following screen shows an example of a typical capture for a call made from an 1120 Deskphone (DID: 506694xxxx) on the CS1000, to a PSTN number (786331xxxx).

No.	Time	Source	Destination	Protocol	Length	Info
435	17.258638	172.16.5.199	142.125.72.11	SIP/SDP	1282	Request: INVITE sip:1786331@pbx06dch2046.ca;user=phone
436	17.340323	142.125.72.11	172.16.5.199	SIP	374	Status: 100 Trying
437	17.444139	142.125.72.11	172.16.5.199	SIP/SDP	946	Status: 183 Session Description
652	22.226833	142.125.72.11	172.16.5.199	SIP/SDP	1016	Status: 200 OK
656	22.239489	172.16.5.199	142.125.72.11	SIP	836	Request: ACK sip:1786331@142.125.72.11:5060;transport=udp
1649	28.685083	142.125.72.11	172.16.5.199	SIP	699	Request: BYE sip:506694@172.16.5.199:5060;transport=udp;user=phone;gsid=398153b0-0781-11e4-884a-78e3b51bf2d0
1651	28.694186	172.16.5.199	142.125.72.11	SIP	625	Status: 200 OK
1682	32.198735	172.16.5.199	142.125.72.11	SIP	555	Request: OPTIONS sip:pbx06dch2046.ca;transport=udp
1684	32.276197	142.125.72.11	172.16.5.199	SIP	633	Status: 200 OK
[Frame 435: 1282 bytes on wire (10256 bits), 1282 bytes captured (10256 bits) <ul style="list-style-type: none"> Ethernet II, Src: IntelCor_cb:79:91 (00:1b:21:cb:79:91), Dst: Netscreen_90:b4:20 (00:10:db:90:b4:20) Internet Protocol Version 4, Src: 172.16.5.199 (172.16.5.199), Dst: 142.125.72.11 (142.125.72.11) User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060) Session Initiation Protocol (INVITE) <ul style="list-style-type: none"> Request-Line: INVITE sip:1786331@pbx06dch2046.ca;user=phone SIP/2.0 Message Header <ul style="list-style-type: none"> From: "Avaya 1110_uni" <sip:506694@pbx06dch2046.ca;user=phone>;tag=3310050-3c1410ac-13dd-55013-bc7d9-4de8eb88-bc7d9 To: <sip:1786331@pbx06dch2046.ca;user=phone> CSeq: 1 INVITE Call-ID: c63be1545439226bce432d69d6c12800 Contact: <sip:506694@172.16.5.199:5060;transport=udp;user=phone;gsid=398153b0-0781-11e4-884a-78e3b51bf2d0> Record-Route: <sip:172.16.5.199:5060;ipcs-line=2181;r;transport=udp> Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO, SUBSCRIBE, UPDATE Supported: 100rel, x-nortel-sipvc, replaces User-Agent: Nortel CS1000 SIP GW release_7.0 version_sslinux-7.65.16 AVAYA-SM-6.3.8.0.638018 Max-Forwards: 30 Via: SIP/2.0/UDP 172.16.5.199:5060;branch=z9hG4bK-s1632-001786073274-1--s1632- <ul style="list-style-type: none"> Privacy: none P-Asserted-Identity: "Avaya 1110_uni" <sip:506694@pbx06dch2046.ca;user=phone> Content-Type: application/sdp Max-Breadth: 60 Content-Length: 263 Message Body <ul style="list-style-type: none"> Session Description Protocol <ul style="list-style-type: none"> Session Description Protocol Version (v): 0 Owner/Creator, Session Id (o): - 16559 1 IN IP4 172.16.5.199 Session Name (s): Connection Information (c): IN IP4 172.16.5.199 Time Description, active time (t): 0 0 Media Description, name and address (m): audio 35758 RTP/AVP 0 8 18 101 111 Connection Information (c): IN IP4 172.16.5.199 Media Attribute (a): fmtp:18 annexb=no Media Attribute (a): rtptime:101 telephone-event/8000 Media Attribute (a): fmtp:101 0-15 Media Attribute (a): rtptime:111 X-nt-infreq/8000 Media Attribute (a): pttime:20 Media Attribute (a): sendrecv 						

10. Conclusion

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

Bell Aliant 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] *Avaya Communication Server 1000 Network Routing Service Fundamentals*, Release 7.6, Document Number NN43001-130, Issue 04.04, June 2014.
- [2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013.
- [3] *Avaya Communication Server 1000E Overview*, Release 7.6, Document Number NN43041-110, Issue 06.02, June 2014.
- [4] *Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals*, Release 7.6, Document Number NN43001-116, Issue 06.03, June 2014.
- [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*. Document Number PSN003460u, Issue 02, April 05, 2013.
- [8] *Communication Server 1000 Release 7.6 & Service Pack 4 Release Notes*, Issue 2.0 February 2014.

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

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

- [9] *Avaya Aura® System Manager Overview and Specification*, Release 6.3, Issue 4, June 2014.
- [10] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 4, June 2014.
- [11] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3, Issue 5, June 2014.

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

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

- [12] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 3, June 2014.
- [13] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 4, June 2014.

Other resources:

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

12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE, **Section 7.2.4:**

Title: Hardcode PAI

```
//The SBC will hardcode the PAI with the first DID number in the DID group,  
//Which is also used for SIP Trunk Registration.  
//This is required in order to make outbound calls (CS1K-->PSTN) and for  
//the correct number to be displayed at the PSTN.
```

```
within session "INVITE"
```

```
{  
  act on request where %DIRECTION="OUTBOUND" and  
  %ENTRY_POINT="POST_ROUTING"  
  {  
    %HEADERS["P-Asserted-Identity"][1].URI.USER = "5066948000";  
  }  
}
```

©2014 Avaya Inc. All Rights Reserved.

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

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