



**Application Notes for Configuring Bell Canada SIP Trunking Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 – Issue 1.0**

**Abstract**

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 with the Bell Canada SIP Trunking service.

The Bell Canada SIP Trunking service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The Bell Canada SIP Trunking service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

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.....	5
2. General Test Approach and Test Results.....	5
2.1. Interoperability Compliance Testing.....	5
2.2. Test Results .....	6
2.3. Support .....	7
3. Reference Configuration .....	8
4. Equipment and Software Validated .....	9
5. Configure Avaya Communication Server 1000.....	10
5.1. Log in to Communication Server 1000 System .....	10
5.1.1. Log in to System Manager and Element Manager (EM).....	10
5.1.2. Log in to Call Server.....	12
5.2. Administer an IP Telephony Node.....	12
5.2.1. Obtain Node IP address .....	12
5.2.2. Administer Terminal Proxy Server (TPS) .....	14
5.2.3. Administer Quality of Service (QoS) .....	14
5.2.4. Synchronize New Configuration.....	14
5.3. Administer Voice Codec .....	15
5.3.1. Enable Voice Codec G.711 .....	15
5.3.2. Enable Voice Codec on Media Gateways.....	16
5.4. Zones and Bandwidth Management.....	17
5.4.1. Create a Zone for IP Telephones (Zone 10).....	17
5.4.2. Create a Zone for Virtual SIP Trunk (Zone 255).....	18
5.5. Administer SIP Trunk Gateway .....	19
5.5.1. Integrated Services Digital Network (ISDN).....	19
5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Manager.....	20
5.5.3. Administer Virtual D-Channel.....	22
5.5.4. Administer Virtual Super-Loop .....	25
5.5.5. Administer Virtual SIP Routes .....	25
5.5.6. Administer Virtual Trunks .....	27
5.5.7. Administer Calling Line Identification Entries.....	29
5.5.8. Enable External Trunk to Trunk Transfer.....	31
5.6. Administer Dialing Plans .....	31
5.6.1. Define ESN Access Codes and Parameters (ESN).....	31
5.6.2. Associate NPA and SPN call to ESN Access Code 1.....	32
5.6.3. Digit Manipulation Block (DMI).....	33

5.6.4.	Digit Manipulation Block Index (DMI) for Outbound Call .....	34
5.6.5.	Route List Block (RLB) (RLB 14) .....	34
5.6.6.	Inbound Call – Incoming Digit Translation Configuration .....	35
5.6.7.	Outbound Call - Special Number Configuration .....	36
5.6.8.	Outbound Call - Numbering Plan Area (NPA).....	37
5.7.	Administer Telephone .....	38
5.7.1.	Telephone creation.....	38
5.7.2.	Enable Privacy for the Telephone.....	40
5.7.3.	Enable Call Forward for Telephone.....	41
5.7.4.	Enable Call Waiting for Telephone .....	43
6.	Configure Avaya Aura® Session Manager .....	44
6.1.	System Manager Login and Navigation.....	44
6.2.	Specify SIP Domain .....	45
6.3.	Add Adaptations.....	46
6.4.	Add Location.....	48
6.5.	Add SIP Entities .....	49
6.6.	Add Entity Links .....	51
6.7.	Add Routing Policies .....	52
6.8.	Add Dial Patterns .....	54
6.9.	Add/View Session Manager.....	56
7.	Configure Avaya Session Border Controller .....	58
7.1.	Log in Avaya Session Border Controller .....	58
7.2.	Global Profiles.....	59
7.2.1.	Uniform Resource Identifier (URI) Groups.....	59
7.2.2.	Routing Profiles .....	59
7.2.3.	Topology Hiding .....	60
7.2.4.	Server Interworking .....	62
7.2.5.	Configure Signaling Manipulation .....	68
7.2.6.	Server Configuration.....	68
7.3.	Domain Policies .....	71
7.3.1.	Signaling Rules .....	71
7.3.2.	Endpoint Policy Groups.....	72
7.4.	Device Specific Settings.....	74
7.4.1.	Network Management.....	74
7.4.2.	Media Interface .....	75
7.4.3.	Signaling Interface .....	75
7.4.4.	End Point Flows - Server Flow .....	76
8.	Bell Canada SIP Trunking Service Configuration.....	78

9.	Verification Steps.....	78
9.1.	General .....	78
9.2.	Verification of an Active Call on CS1000 .....	78
	Conclusion .....	80
10.	Additional References.....	80

# 1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 (CS1000) Release 7.6, Avaya Aura® Session Manager Release 6.3 (SM) and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.3 with Bell Canada SIP Trunking service (Bell). Bell provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

## 2. General Test Approach and Test Results

The CS1000 connects to Avaya SBCE via SM SIP trunk connectivity. The Avaya SBCE connects to Bell system using SIP trunks. Various call types were made from CS1000 to and from Bell system to verify the interoperability.

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

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Response to SIP OPTIONS queries.
- Registration and Authentication.
- General call processing between CS1000 and Bell system including:
  - Codec/ptime G.711 u-law/20ms.
  - Hold/Resume on both ends.
  - Calling Line Identification Display (CLID).
  - Ring-back tone.
  - Speech path.
  - Dialing plan support (Local, long distance, international, outbound toll-free, Assisted Operator, 411 and 911 services).
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends.
- FAX G.711 pass through.
- Inbound and outbound long hold time call stability.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF (RFC2833) in both directions.
- SIP transport UDP, port 5060.
- Voice Mail Server Call Pilot (hosted on Avaya CS1000 system).

The following assumptions were made for these compliance tested configuration:

1. CS1000CS1000 R7.6 software with latest patches.
2. Bell provides support to setup, configure and troubleshoot on carrier switch during testing execution.

During testing, the following activities were made to each test scenario:

1. Calls were checked for the correct call progress tones and cadences.
2. During the ringing state the ring back tone and destination ringing were checked.
3. Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
5. The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. Speech path was checked before and after calls were put on/off hold from each end.

## 2.2. Test Results

The objectives outlined in **Section 2.1** were verified. All the applicable test cases were executed. However, the following observations were noted during the compliance testing:

1. **Calling Line ID is not available after hold/resume** – If the CS1000 telephone holds/resumes an outbound call, the dialed digits are no longer displayed. This is a CS1000CS1000 known issue.
2. **SIP Telephone Conference** – During a conference call hosted by the CS1000 SIP telephone, if the SIP telephone is hanged up/dropped out of the conference, the conference call is dropped. This is known CS1000 SIP telephone limitation.
3. **Calling Line ID (CLID) is not correctly displayed** – After call redirection, namely blind/consultative transfers, is completed with two way voice paths, the CLID on the CS1000 transferee's telephone is not updated accordingly. This is known CS1000 limitation.
4. **Blind Call Transfer to PSTN using SIP telephone does not completed until transferee pick up the call** – Call scenario is when PSTN telephone calls to enterprise SIP extension (CS1000 SIP telephone), CS1000 answers the call and performs blind transfer the call to another PSTN endpoint. The expected behavior of the enterprise SIP telephone is after transfer, the telephone should display “transfer completed”. But in this case, user press “transfer” button, answer question of “Consultative transfer with party?”, and the answer is “No”, which implies the blind transfer, as the transferee PSTN telephone is ringing and the SIP telephone should be released and displayed “transfer successfully”. Instead, the SIP telephone still displayed “transferring” and not released until the transferee PSTN telephone answered the call. The work around is to hang up the SIP telephone. This is a minor and known limitation on CS1000 SIP telephone without any user impact. Transfer is still completed with two way speech paths.

5. **SIP Options** - Bell was configured to send SIP OPTIONS messages with Max-Forwards header with value equal to 0. This was by design from Bell. Avaya SBCE responded correctly with 483 Too Many Hops. However, Bell would accept this and keep the trunk up.

## 2.3. Support

For technical support on the Avaya products described in these Application Notes visit:  
<http://support.avaya.com>

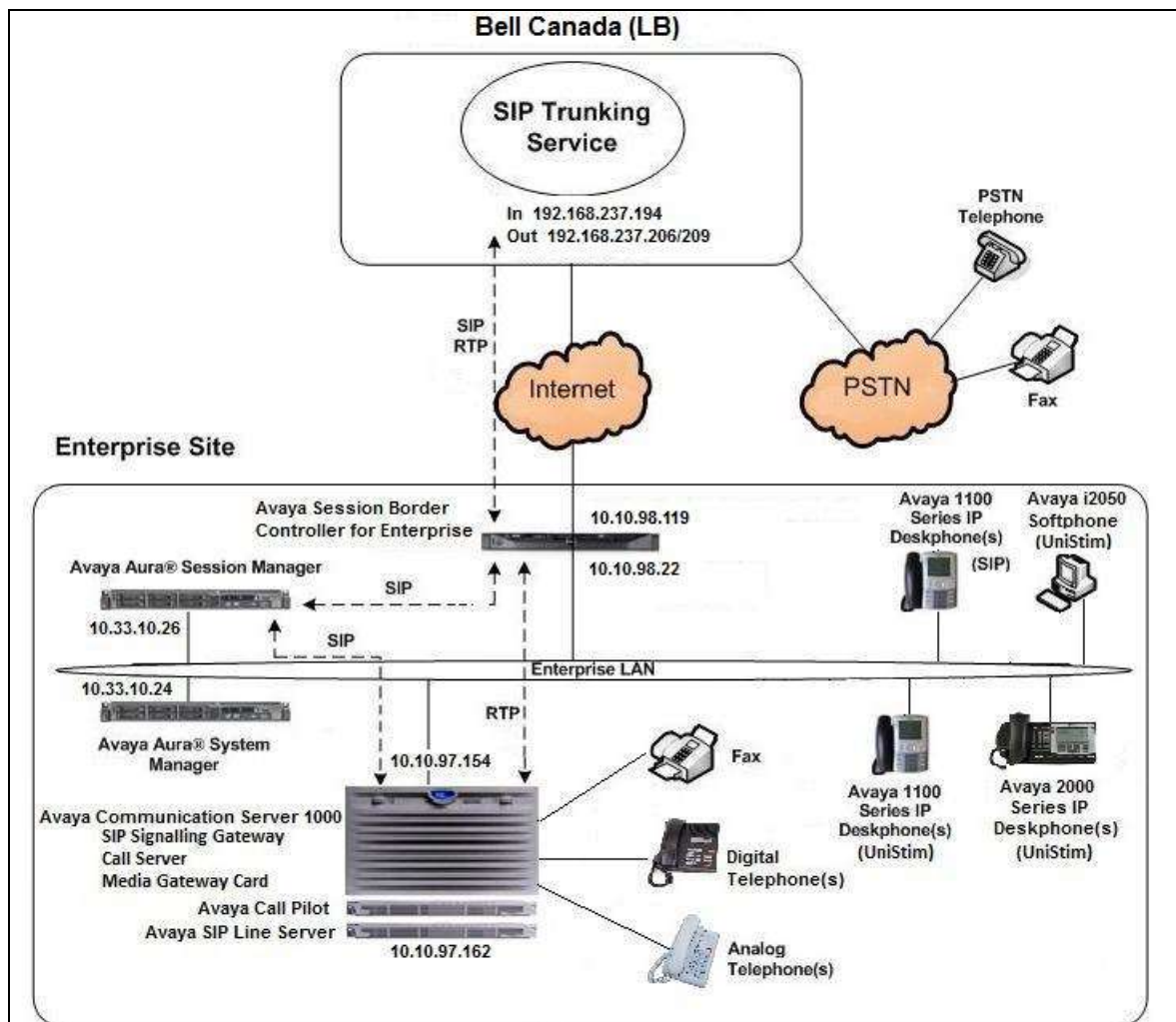
For technical support on the Bell Canada SIP Trunking service, please contact customer service or visit [http://www.bell.ca/enterprise/EntPrd\\_SIP\\_Trunking.page](http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page)

### 3. Reference Configuration

**Figure 1** illustrates the test configuration used during the compliance test between CS1000, SM, Avaya SBCE and Bell system. In this configuration, Avaya SBCE on enterprise side is configured to periodically perform OPTIONS ping to Bell system. Also outbound calls from enterprise CS1000 to PSTN will require authentication with Bell system.

Additionally, external interface of Avaya SBCE is connecting to Bell's load balancer over the internet for outbound call from the enterprise to PSTN via single IP address. For inbound from PSTN to enterprise, calls will coming in to enterprise via two IP addresses as shown in **Figure 1**.

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.



**Figure 1- Network diagram for Avaya and Bell SIP Trunking Service**



## 4. Equipment and Software Validated

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

Avaya Telephony Components	
Equipment/Software	Release/Version
Avaya Communication Server 1000 (CPPM)	Call Server: 7.65 P + Signaling Server: 7.65.16 GA SIP Line Server: 7.65.16 GA
Avaya Call Pilot C201i	Call Pilot Voice Mail Manager: 05.00.41.143
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.10 (6.3.4.4.1830) (Build No. 6.3.0.8.5682-6.3.8.2631)
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3.7 (Build No. 6.3.0.0.630002-6.3.4.634012)
Avaya Session Border Controller for Enterprise	6.3.000-19-4338
Avaya IP Deskphones: 2050 (Soft) 1140 (SIP) 1140 (UniStim) 2007 (UniStim) 3904 (Digital) Analog	4.04.0106 04.03.12.00 0625C8Q 0621C8Q N/A N/A
HP Officejet 4500 Fax	N/A
Bell Canada SIP Trunking Components	
Component	Release
F5 Load Balancer	11
Oracle ACME Packet Net-Net 4500	6.3.7 MR-3 Patch 1
BroadSoft Broadworks	18
Legacy Nortel CS2K Media Gateway	SN10 PVG/IW-SPM

Additional patch lineup for CS1000 listed as below:

**Call Server:** 7.65 P+ GA plus latest DEPLIST – CPL\_7.6\_5.zip

**Signaling Server:** 7.65.16 GA plus latest DEPLIST – SP\_7.6\_5.ntl

## 5. Configure Avaya Communication Server 1000

These Application Notes use the Incoming Digit Translation feature to receive the calls, the Numbering Plan Area Code (NPA), and Special Number (SPN) features to route calls from the CS1000, over a SIP trunk via Bell system, to PSTN.

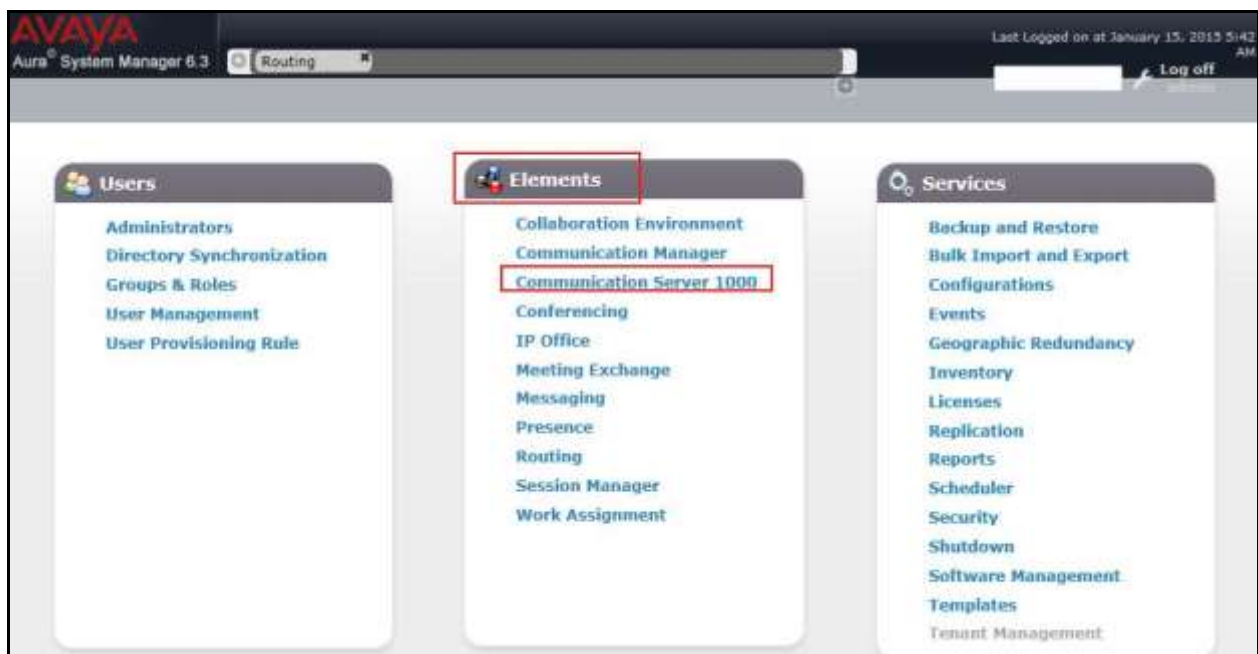
These application notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 10**

The procedures below describe the configuration details of configuring a CS1000 SIP trunk.

### 5.1. Log in to Communication Server 1000 System

#### 5.1.1. Log in to System Manager and Element Manager (EM)

Open an instance of a web browser and connect to the Avaya Aura® System Manager using the following address: <https://<System Manager IP address>/SMGR/>. Log in using an appropriate user ID and password (not shown). Select **Elements** → **Communication Server 1000**.



The **Elements** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in red box as below:

**AVAYA** Avaya Aura® System Manager 6.3 [Help](#) | [Logout](#)

Host Name: smgr.bvwdev.com 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"/>	smgr.bvwdev.com (primary)	Base OS	7.6	10.33.10.24	Base OS element.
<input checked="" type="checkbox"/>	EM on car1-sip	CS1000	7.6	10.10.97.80	New element.
<input checked="" type="checkbox"/>	EM on car2-mas	CS1000	7.6	10.10.97.90	New element.
<input checked="" type="checkbox"/>	EM on car3-sip-ucm	CS1000	7.6	10.10.97.95	New element.
<input checked="" type="checkbox"/>	car1-cores1.bvwdev.com (member)	Linux Base	7.6	10.10.97.153	Base OS element.
<input checked="" type="checkbox"/>	car1-sip.bvwdev.com (member)	Linux Base	7.6	10.10.97.151	Base OS element.

The CS1000 Element Manager **System Overview** page is as bellow.

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

Managing: 10.10.97.80 Username: admin  
System Overview

### System Overview

IP Address: 10.10.97.80  
Type: Avaya Communication Server 1000E CPPM Linux  
Version: 4121  
Release: 765 P +

### 5.1.2. Log in to Call Server

Use Putty, and SSH to the IP address of the CS1000 Signaling Server using an account with administrator credentials.

Run command **cslogin** and log in with the appropriate user account and password. Sample output is shown below.

Note: This screen can be used for monitoring of BUG(s), ERROR and AUD messages.

```
login as: < --- enter an account with administrator credentials

Nortel Networks 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@10.10.97.154's password: <----enter the password
Last login: Thu Feb 20 16:02:14 2014 from 10.10.98.78
[admin2@car3-ssg-carrier ~]$ cslogin

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

USERID? < --- enter the user account
PASS? <----enter the password
.
TTY #09 LOGGED IN ADMIN 11:09 24/02/2014
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 log out immediately. This system may be monitored
for operational purposes at any time.

>
```

## 5.2. Administer an IP Telephony Node

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

### 5.2.1. Obtain Node IP address

These application notes assume that the basic CS1000 configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 1000) in CS1000 IP network to work with Bell. For further

information on CS1000, please consult the references in **Section 11**. Select **System → IP Network → Nodes: Servers, Media Cards** and then click on the **Node ID** as shown.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System (highlighted), Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network (highlighted), Nodes: Servers, Media Cards (highlighted), Maintenance and Reports, Media Gateways, Zones, and Host and Route Tables. The main content area displays the 'IP Telephony Nodes' page. At the top, it shows 'Managing: 10.10.97.80' and 'Username: admin'. Below this, there's a breadcrumb trail: 'System > IP Network > IP Telephony Nodes'. The page title is 'IP Telephony Nodes'. A sub-header says 'Click the Node ID to view or edit its properties.' There are buttons for 'Add', 'Import', 'Export', and 'Delete'. A table lists the nodes:

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1000	1	LTPS, Gateway ( SIPGw )	-	10.10.97.154	-	Synchronized
1001	1	LTPS, Gateway ( SIPGw )	-	10.10.97.221	-	Synchronized
1002	1	SIP Line	-	10.10.97.162	-	Synchronized

At the bottom of the table, there are checkboxes for 'Show' and 'Nodes', and a checkbox for 'IPv6 address' which is checked.

The **Node Details** screen is displayed with the IP address of the CS1000 node. **Call server IP address: 10.10.97.80**. The **Node IPv4 address 10.10.97.154** is a virtual address which corresponds to the **TLAN IPv4 10.10.97.153** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls. The **Node Details** screen is displayed below with the IP Telephony Node Properties and Applications.

The screenshot shows the AVAYA CS1000 Element Manager interface, specifically the 'Node Details' screen for Node ID 1000. The left sidebar is the same as the previous screenshot. The main content area displays the 'Node Details (ID: 1000 - LTPS, Gateway ( SIPGw ))' page. At the top, it shows 'Managing: 10.10.97.80' and 'Username: admin'. Below this, there's a breadcrumb trail: 'System > IP Network > IP Telephony Nodes > Node Details'. The page title is 'Node Details (ID: 1000 - LTPS, Gateway ( SIPGw ))'. The form contains the following fields:

- Node ID: 1000 (required)
- Call server IP address: 10.10.97.80 (required)
- TLAN address type: ☒ IPv4 only, ☐ IPv4 and IPv6
- Embedded LAN (ELAN): Gateway IP address: 10.10.97.65 (required), Subnet mask: 255.255.255.192 (required)
- Telephony LAN (TLAN): Node IPv4 address: 10.10.97.154 (required), Subnet mask: 255.255.255.192 (required), Node IPv6 address: (empty)
- IP Telephony Node Properties:
  - Voice Gateway (VGVW) and Codec
  - 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

At the bottom of the form, there are 'Save' and 'Cancel' buttons. Below the form, there's a section titled 'Associated Signaling Servers & Cards'. It contains a table with the following data:

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
car1-cores1	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.80	10.10.97.153	Leader

### 5.2.2. Administer Terminal Proxy Server (TPS)

Continuing from Section 5.2.1, on the **Node Details** page select **Terminal Proxy Server (TPS)**. Check the **UNISim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click **Save** (not shown).

AVAYA CS1000 Element Manager

Managing: 10.10.97.88 Username: admin

System > IP Network > IP Telephony Nodes > Node Details > UNISim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 1000 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware | DTLs | Network Connected Server

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

Firmware

IP address: 0.0.0.0

Full file path: download/firmwa

Server Account/User ID:

Password:

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

Continuing from Section 5.2.1, on the **Node Details** page select **Quality of Service (QoS)**. The default Diffserv values are as shown. Click **Save**.

AVAYA CS1000 Element Manager

Managing: 10.10.97.88 Username: admin

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

Node ID: 1000 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☐

Control packets: 40 (0-63)

Voice packets: 46 (0-63)

VLAN tagging: ☒ 802.1Q support

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

\* Required Value

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

Save Cancel

### 5.2.4. Synchronize New Configuration

Continuing from Section 5.2.3, return to the **Node Details** page and click the **Save** button. The **Node Saved** screen is displayed. Click **Transfer Now** (not shown). The **Synchronize Configuration Files (Node ID <1000>)** screen is displayed (not shown). Check the **Signaling Server** checkbox and click **Start Sync** (not shown). When the synchronization completes, check the **Signaling Server** checkbox and click **Restart Applications** (not shown).



## 5.3. Administer Voice Codec

### 5.3.1. Enable Voice Codec G.711

On the **Node Details** page shown in **Section 5.2.1**, click on **Voice Gateway (VGW) and Codecs** and then under **Voice Codecs** section.

The Bell system supports **G.711/time 20ms** with **Voice Activity Detection (VAD)** checkbox unchecked. Ensure **Codec G.729** is unchecked. Click **Save**.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar shows a navigation tree with 'System' and 'Nodes, Servers, Media Cards' highlighted. The main content area is titled 'Node ID: 1000 - Voice Gateway (VGW) and Codecs'. The 'Voice Codecs' tab is active, showing a table of codec configurations. The table has columns for 'Codec', 'Enabled', 'Voice payload size', and 'Voice playout (jitter buffer) delay'. The configurations are as follows:

Codec	Enabled	Voice payload size	Voice playout (jitter buffer) delay
Codec G.711	<input checked="" type="checkbox"/> Enabled (required)	20 (milliseconds per frame)	40 - 80 (milliseconds)
Codec G.722	<input checked="" type="checkbox"/> Enabled	20 (milliseconds per frame)	40 - 80 (milliseconds)
Codec G.729	<input type="checkbox"/> Enabled	20 (milliseconds per frame)	

Additional settings for Codec G.711 include 'Voice Activity Detection (VAD)' which is unchecked. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' The 'Save' button is highlighted in red.

Synchronize the new configuration (please refer to **Section 5.2.4**).

### 5.3.2. Enable Voice Codec on Media Gateways

From the left menu of the Element Manager page, select **System** → **IP Network** → **Media Gateways**. The Media Gateways page will appear (not shown). Click on **MGC** which is located on the right of the page (not shown). In the following screen, scroll down to select **Codec G.711** and deselect **Codec G.729A** and uncheck both **VAD** as shown below. Scroll down to the bottom of the page and click the **Save** button (not shown).

**AVAYA CS1000 Element Manager**

**- VGW and IP phone codec profile**

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

**- Codec G711** Select ☒  
Codec name G711  
Voice payload size 20 (ms/frame)  
Voice playout (jitter buffer) nominal delay 40  
Modifications may cause changes to dependent settings  
Voice playout (jitter buffer) maximum delay 80  
Modifications may cause changes to dependent settings  
VAD ☐

**- Codec G729A** Select ☐  
Codec name G729A  
Voice payload size 20 (ms/frame)  
Voice playout (jitter buffer) nominal delay 40  
Modifications may cause changes to dependent settings  
Voice playout (jitter buffer) maximum delay 80  
Modifications may cause changes to dependent settings  
VAD ☐

**+ Codec G723.1** Select ☐

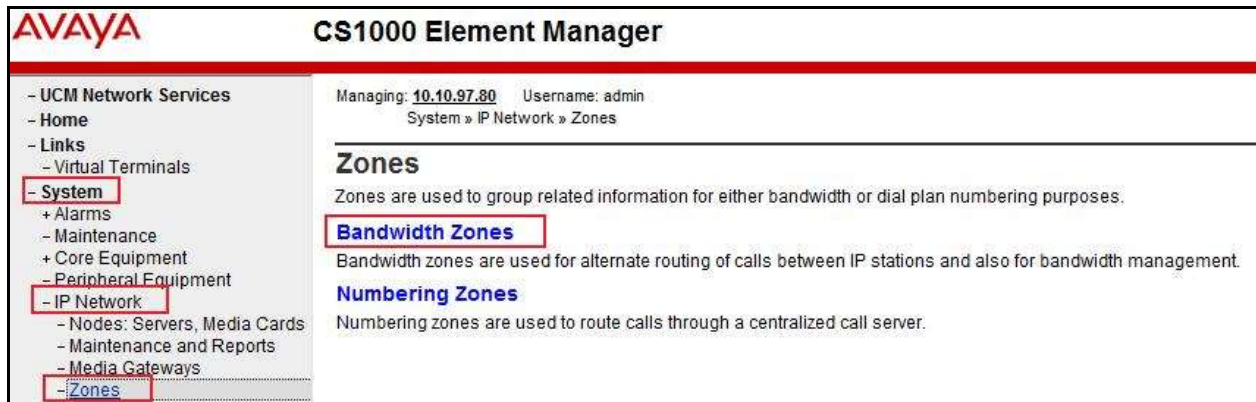


## 5.4. Zones and Bandwidth Management

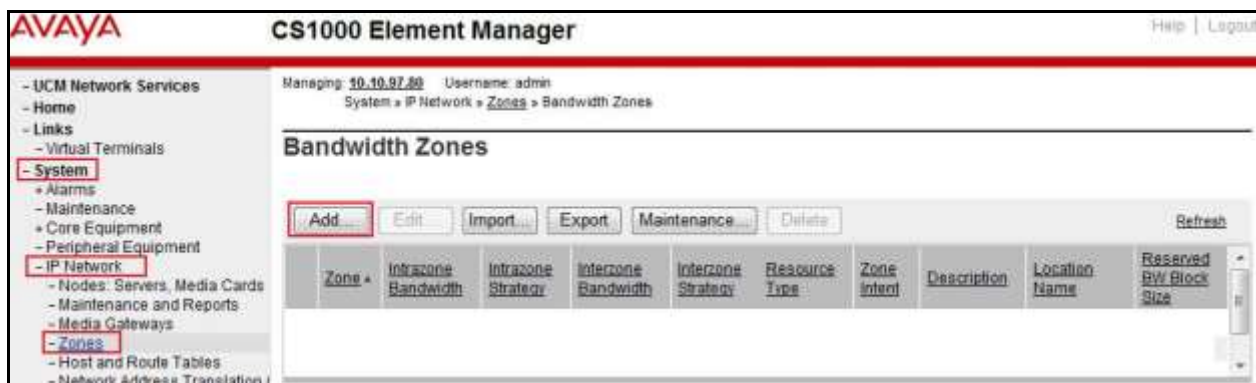
This section describes the steps to create two zones: zone 10 for the VGW and IP sets, and zone 255 for the SIP Trunk.

### 5.4.1. Create a Zone for IP Telephones (Zone 10)

The following figures show how to configure a zone for VGW and IP sets for bandwidth management purposes. The bandwidth strategy can be adjusted to preference. Select **IP Network** → **Zones** configuration from the left pane (not shown), click **Bandwidth Zones**.



The **Bandwidth Zones** screen is displayed as shown below. Click **Add** to create new zone for IP Telephones.



Select and input the values as shown below (in the red boxes), and click on **Submit** button.

- **Intrazone Bandwidth (INTRA\_BW): 1000000**
- **Intrazone Strategy (INTRA\_STGY): Select Best Quality (BQ)** to use G.711 as the first priority codec for negotiation of local calls.
- **Interzone Bandwidth (INTER\_BW): 1000000**
- **Interzone Strategy (INTER\_STGY): Select Best Quality (BQ)** to use G.711 as the first priority codec for negotiation of calls over trunks.
- **Zone Intent (ZBRN): Select MO (MO)** for IP telephones, and VGW.

**AVAYA CS1000 Element Manager**

Managing: 10.10.97.80 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	10 (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):	
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 Trunk (Zone 255)

Follow the steps described in Section 5.4.1 to create a zone for the virtual SIP trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK (VTRK)** for virtual trunk as shown and then click **Submit** button.

**AVAYA CS1000 Element Manager**

Managing: 10.10.97.80 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 (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):	

**Submit** Refresh Cancel

## 5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Avaya SBCE.

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

Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00** (not shown). The system can support more than one customer with different network settings and options. The **Customer 00 Edit** page will appear (not shown). Select the **Feature Packages** option from **Customer 00 Edit** page (not shown). The screen is updated with a listing of available **Feature Packages** (not all features are shown in capture below). Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click the **Save** button (not shown).

The screenshot displays the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System (highlighted with a red box), + Alarms, - Maintenance, + Core Equipment, - Peripheral Equipment, + IP Network, + Interfaces, - Engineered Values, + Emergency Services, + Geographic Redundancy, + Software, and - Customers (highlighted with a red box). The main content area is titled 'Integrated Services Digital Network' (highlighted with a red box) and 'Package: 145'. Below the title is a checkbox 'Integrated Services Digital Network:' which is checked (highlighted with a red box). Under this checkbox are two fields: '- Virtual private network identifier: 1' and '- Private network identifier: 1', both with '(1 - 16383)' to their right. Below these are fields for '- Node DN:', 'Multi-location business group: 0' (with '(0 - 65535)' to its right), 'Business sub group consult-only: 65535' (with '(0 - 65535)' to its right), 'Prefix 1:', and 'Prefix 2:'.

### 5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Manager

On the **Node Details** page as shown in **Section 5.2.1**, select **Gateway (SIPGw)**. 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.

- **SIP domain name:** Create a domain name, which will be used for enterprise network.
- **Local SIP port: 5060** is used.
- **Gateway endpoint name:** SIP gateway endpoint name during set up of CS1000 system.
- **Application node ID:** Node ID that is used in **Section 5.2.1**.
- Click **Save**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Car, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translators, QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, and Routes and Trunks. The main content area is titled 'Node ID: 1000 - Virtual Trunk Gateway Configuration Details'. It has tabs for General, SIP Gateway Settings, and SIP Gateway Services. The General tab is active, showing the 'Vtrk.gateway application' dropdown set to 'SIP Gateway (SIPGw)'. Below this are fields for 'SIP domain name' (avayalab.com), 'Local SIP port' (5060), 'Gateway endpoint name' (car1-cores1), 'Gateway password', and 'Application node ID' (1000). A checkbox 'Vtrk.gateway application' is checked with the label 'Enable gateway service on this node'. On the right, the 'Virtual Trunk Network Health Monitor' section is visible, with a checkbox 'Monitor IP addresses (listed below)' and a table for monitoring IP addresses. At the bottom, there are 'Save' and 'Cancel' buttons.

Click on the **SIP Gateway Services** tab, under **Proxy or Redirect Server**, and enter the following values (highlighted in red boxes) for the specified fields, retaining the default values for the remaining fields as shown in capture below. Enter the internal interface IP address of SM in the **Primary TLAN IP address** field (This IP address pattern is defined in **Section 6.4**). Enter **Port: 5060** and **Transport protocol: UDP**. Uncheck **Support registration** checkbox. Click **Save**.



AVAYA CS1000 Element Manager

Node ID: 1000 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | **SIP Gateway Services**

☐ Enable Shared Bandwidth Management

**Proxy Or Redirect Server:**

Proxy Server Route to:

Primary TLAN IP address: 10.33.10.26  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration  
☐ Primary CDS proxy

\* Required Value.

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

**Save** Cancel

Continue with **Virtual Trunk Gateway Configuration Details** page above, scroll to the **SIP URI Map** section.

Under the **Public E.164 domain names**, enter the following:

- **National:** Empty this field
- **Subscriber:** Empty this field
- **Special Number:** Empty this field
- **Unknown:** Empty this field

Under the **Private domain names**, enter the following:

- **UDP:** Empty this field
- **CDP:** Empty this field
- **Special Number:** Empty this field
- **Vacant number:** Empty this field
- **Unknown:** Empty this field

The remaining fields can be left at their default values. Click **Save**.

AVAYA CS1000 Element Manager

Managing: 10.10.87.80 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > Virtual Trunk Gateway Configuration

Node ID: 1000 - 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:

\* Required Value.

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

**Save** Cancel

Synchronize the new configuration (refer to **Section 5.2.4**).

### 5.5.3. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list (in this case is **100**) and type **DCH** as shown. Click to **Add** button.



The **D-Channels 100 Property Configuration** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D channel Card Type:** D-Channel is over IP (DCIP)
- **Designator:** A descriptive name
- **User:** Integrated Services Signaling Link Dedicated (ISLD)
- **Interface type for D-channel:** Meridian Meridian1 (SL1)
- **Meridian 1 node type:** Slave to the controller (USR)
- **Release ID of the switch at the far end:** 25

Click on **Advanced options (ADVOPT)**. Check on the **Network Attendant Service Allowed** checkbox as shown. Other fields are left as default. Click **Submit** button.

AVAYA

CS1000 Element Manager

Help | Logout

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

D-Channels 100 Property Configuration

- Basic Configuration

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

+ Basic options (BSCOPT)

+ Advanced options (ADVOPT)

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

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

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

+ H323 Overlap Signaling Settings (H323)

-Overlap Timer:

- Multilocation Business Group Allowed: ☐

- Network Attendant Service Allowed: ☒

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

+ Feature Packages

On the same page, choose the **Basic Options (BSCOPT)** and click **Edit** button on the **Remote Capabilities** field.

QT; Reviewed:  
SPOC 3/9/2015

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

23 of 81  
BCS76SM63ASBC63

**AVAYA CS1000 Element Manager** Help | Logout

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Geographic Redundancy
  - + Software
- Customers
  - Routes and Trunks
    - Routes and Trunks
    - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction

**- 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 (TIMR)**

- B channel Service messaging: ☐

**+ Advanced options (ADVOPT)**

**+ Feature Packages**

Submit Refresh Delete Cancel

The **Remote Capabilities Configuration** page appears as shown below. Check **Network name display method (ND2)** and **Message waiting interworking with DMS-100 (MWI)** checkboxes.

**AVAYA CS1000 Element Manager** Help | Logout

**- Remote Capabilities Configuration**

Input Description	Input Value
Basic rate interface (BRI)	<input type="checkbox"/>
Call completion on busy using integer value (CCBI)	<input type="checkbox"/>
Call completion on busy using object identifier (CCBO)	<input type="checkbox"/>
Call transfer notification and invocation to EuroISDN (ECTO)	<input type="checkbox"/>
Malicious call identification (MCID)	<input type="checkbox"/>
MCDN QSIG conversion (MQC)	<input type="checkbox"/>
Remote D-channel is on a MSDL card (MSL)	<input type="checkbox"/>
Message waiting interworking with DMS-100 (MWI)	<input checked="" type="checkbox"/>
Network access data (NAC)	<input type="checkbox"/>
Network call trace supported (NCT)	<input type="checkbox"/>
Network name display method 1 (ND1)	<input type="checkbox"/>
Network name display method 2 (ND2)	<input checked="" type="checkbox"/>
Network name display method 3 (ND3)	<input type="checkbox"/>

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

Click **Submit** button (not shown).



#### 5.5.4. Administer Virtual Super-Loop

Select **System** → **Core Equipment** → **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click **Add** button to create a new one as shown below. In this example, **Superloop Numbers 4, 96, 100, and 104** have been added and are being used.



#### 5.5.5. Administer Virtual SIP Routes

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



The **Customer 0**, new **Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed to put the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of Basic Configuration section of existing route 100 is displayed to edit as shown in capture below.

- **Route number (ROUT):** Select an available route number (example: route **100**).
- **Designator field for trunk (DES):** A descriptive text (**SP**).
- **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 (example: **8001**).
- Check the **The route is for a virtual trunk route (VTRK)** field, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter **255** (created in **Section 5.4.2**). Note: The Zone value is filled out as **255**, but after it is added, the screen is displayed with prefix **00**.

- For the **Node ID of signaling server of this route (NODE)** field, enter the node number **1000** (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. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
  - **Route data block (RDB):** Type **RDB** is used as default
  - **Customer number (CUST):** Customer **00** is used
  - **Mode of operation (MODE):** Select **Route uses ISDN Signalling Link (ISLD)**
  - **D channel number (DCH):** Enter **100** (created in **Section 5.5.3**)
  - **Network calling name allowed (NCNA):** Check the field.
  - **Network call redirection (NCRD):** Check the field.
  - **Insert ESN access code (INAC):** Check the field.
  - **Enable Shared Bandwidth Management for the route (SBWM):** uncheck.
  - **Interface type for route (IFC):** Select **Meridian M1 (SL1)**.
  - **Private network identifier (PNI):** **00001** is used.

**AVAYA CS1000 Element Manager** Help | Logout

**Customer 0, Route 100 Property Configuration**

**- Basic Configuration**

Route data block (RDB) (TYPE): RDB

Customer number (CUST): 00

Route number (ROUT): 100

Designator field for trunk (DES): SP

Trunk type (TKTP): TIE

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

Access code for the trunk route (ACOD): 8001

Trunk type M911P (M911P): ☐

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

- Zone for codec selection and bandwidth management (ZONE): 00255 (0 - 8000)

- Node ID of signaling server of this route (NODE): 1000 (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): 100 (0 - 254)

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

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

- Network calling name allowed (NCNA): ☒

- Network call redirection (NCRD): ☒

- Trunk route optimization (TRO): ☐

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

- Channel type (CHTY): B-channel (BCH)

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

- Insert ESN access code (INAC): ☒

Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** checkboxes. Enter **0** for both **Day IDC tree number** and **Night IDC tree number**. Click **Submit** button.

**AVAYA CS1000 Element Manager** Help | Logout

- UCM Network Services
  - Home
  - Links
    - Virtual Terminals
  - + System
  - Customers
    - **Routes and Trunks**
      - **Routes and Trunks**
      - D-Channels
      - Digital Trunk Interface
  - Dialing and Numbering Plans
    - Electronic Switched Network
    - Flexible Code Restriction
    - Incoming Digit Translation
  - Phones
    - Templates
    - Reports
    - Views
    - Lists
    - Properties
    - Migration
  - Tools
    - + Backup and Restore
    - Date and Time
    - + Logs and reports
  - Security
    - + Passwords
    - + Policies
    - + Login Options

**- Basic Route Options**

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

Billing number required (BILN): ☐

Call detail recording (CDR): ☐

**North American toll scheme (NATL): ☒**

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

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

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

- Display external dialed digits (DEXT): ☐

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

Process notification networked calls (PNNC): ☐

**+ Network Options**

**+ General Options**

**+ Advanced Configurations**

**Submit** Refresh Delete Cancel

### 5.5.6. Administer Virtual Trunks

Select **Routes and Trunks** → **Route and Trunks**. The Route list is now updated with the newly added routes. In the example, the **Route 100** was added. Click **Add trunk** button as shown below.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: 10.10.97.80 Username: admin  
Routes and Trunks » Routes and Trunks

**Routes and Trunks**

- Customer: 0 Total routes: 3 Total trunks: 66 Add route

Route	Type	Description	Edit	Add trunk
+ Route: 1	MUS	Description: MUS	Edit	Add trunk
+ Route: 100	TIE	Description: SP	Edit	<b>Add trunk</b>
+ Route: 101	TIE	Description: SIPL	Edit	Add trunk

The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service** at the bottom of the page. Click **Edit** button as shown in capture below.

Note: The **Multiple trunk input number (MTINPUT)** field (not shown) may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created (not shown). In the screen capture bellow, Trunk 1 is used in this testing.

- **Trunk data block:** IP Trunk (**IPTI**)
- **Terminal Number:** Available terminal number (Superloop **100** created in **Section 5.5.4**)
- **Designator field for trunk:** A descriptive text
- **Extended trunk:** Virtual trunk (**VTRK**)
- **Member number:** Current route number and starting member
- **Card density:** 8D
- **Start arrangement Incoming:** Immediate (**IMM**)
- **Start arrangement Outgoing:** Immediate (**IMM**)
- **Trunk group access restriction:** Desired trunk group access restriction level
- **Channel ID for this trunk:** An available starting channel ID

AVAYA CS1000 Element Manager

Managing: 10.10.97.80 Username: admin

Routes and Trunks » Routes and Trunks » Customer 0, Route 100, Trunk 1 Property Configuration

### Customer 0, Route 100, Trunk 1 Property Configuration

**- Basic Configuration**

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:  \*

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

**+ Advanced Trunk Configurations**

Save Delete Cancel



For **Media Security**, select **Media Security Never (MSNV)**. Enter the values for the specified fields as shown in capture below. Scroll down to the bottom of the screen, click **Return Class of Service** and then the **Save** button (not shown in capture above).

**AVAYA CS1000 Element Manager** Help | Logout

**Class of Service Configuration**

**- Class of Service**

Input Description	Input Value
- 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:	

Return Class of Service Cancel

### 5.5.7. Administer Calling Line Identification Entries

Select **Customers** (on the left pane) → **00** → **ISDN and ESN Networking** (not shown). Click **Calling Line Identification Entries**.

**AVAYA CS1000 Element Manager** Help | Logout

**ISDN and ESN Networking**

**Calling Line Identification**

Information for incoming/outgoing calls: No manipulation is done

Size: 256 (0 - 4000)

Country code: 1 (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Click **Add** button as shown.

**AVAYA CS1000 Element Manager** Help | Logout

**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

The add entry **0** screen is displayed (not shown). Enter the following values for the specified fields and retain the default values for the remaining fields. The **Edit Calling Line Identification** of existing entry **0** is displayed as shown in capture below:

- **National Code:** left blank.
- **Local Code:** input prefix digits assigned by Bell, in this case it is 6 digits – **613XXX**. This will be used for call display purpose for **Call Type = Unknown**.
- **Home Location Code:** input prefix digits assigned by Bell, in this case it is 6 digits – **613XXX**. This will be used for call display purpose for **Call Type = National (NPA)**.
- **Local Steering Code:** input prefix digits assigned by Bell, in this case it is 6 digits – **613XXX**. This will be used for call display purpose for **Call Type = Local Subscriber (NXX)**.
- **Use DN as DID:** YES.
- **Calling Party Name Display:** Uncheck **Roman characters**.

Click **Save**.

**AVAYA CS1000 Element Manager** Help | Logout

**Edit Calling Line Identification 0**

**General Properties**

National Code:  (0 - 999999)

Code for national home number

Local Code:  613XXX (1-12 digits)

Code for home local number or listed DN

Home Location Code:  613XXX (1-7 digits)

Local Steering Code:  613XXX (1-7 digits)

Use DN as DID:  YES

**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

**Save** **Cancel**

### 5.5.8. Enable External Trunk to Trunk Transfer

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

Log in to the Call Server Overlay CLI (please refer to **Section 5.1.2** for more details). Allow External Trunk to Trunk Transfer for Customer Data Block by using **ld 15**.

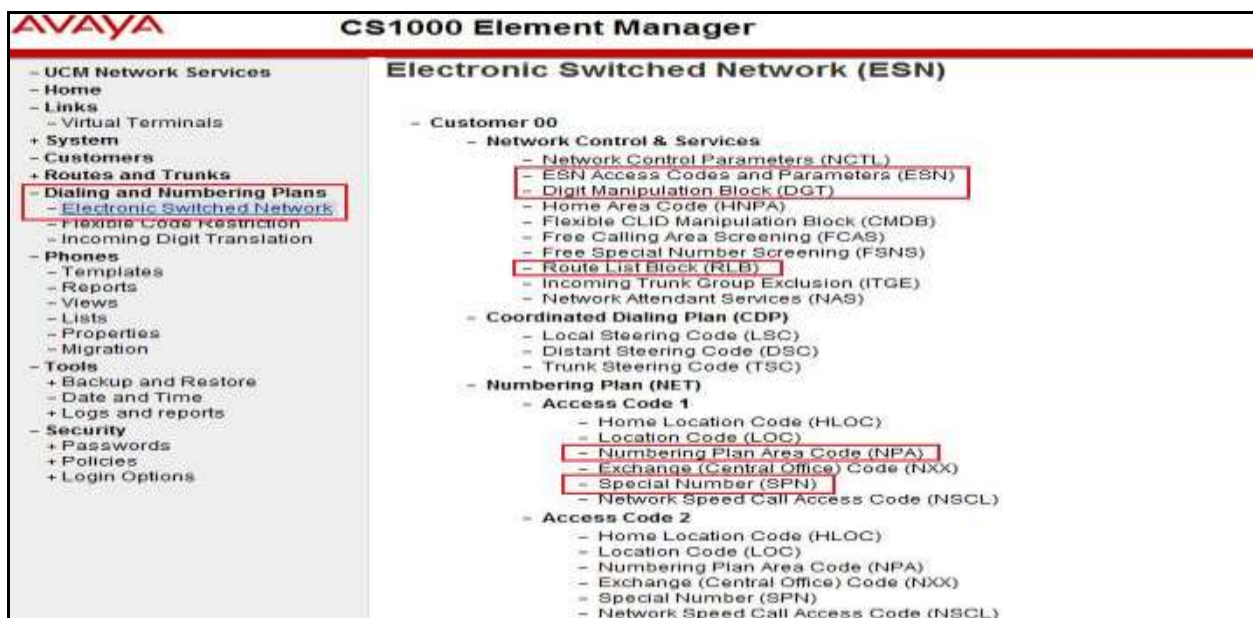
```
>ld 15
CDB000
MEM AVAIL: (U/P): 35359353   USED U P: 8485941 1034575   TOT: 45879869
DISK SPACE NEEDED: 1883 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 0
OPT
...
TRNX YES (←Enable transfer feature)
EXTT YES (← Enable external trunk to trunk Transfer )
...
```

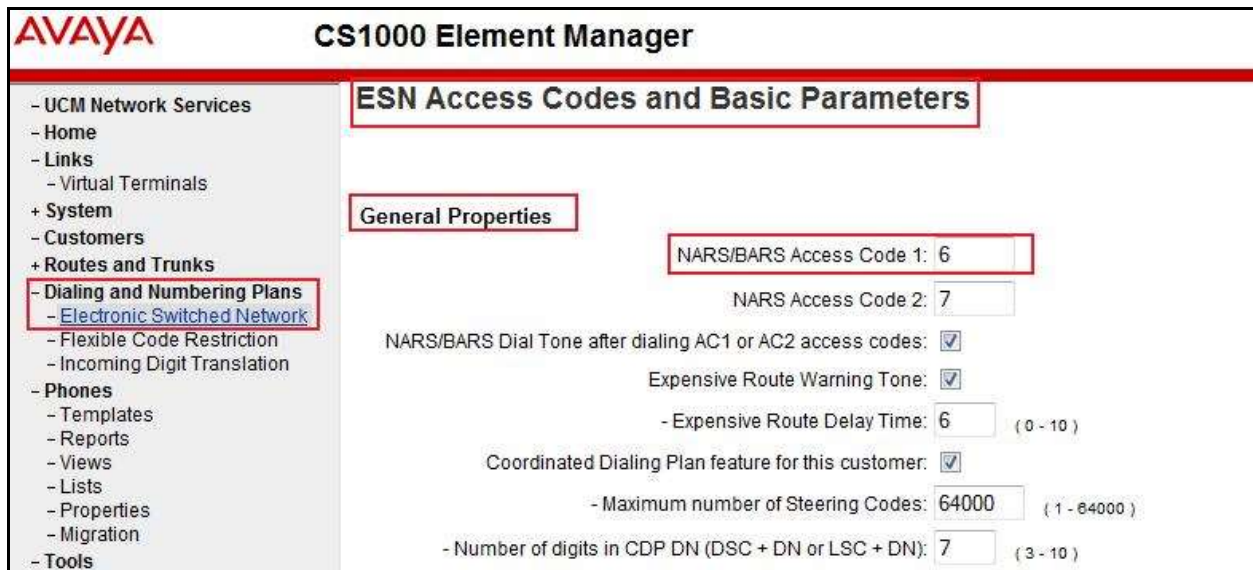
## 5.6. Administer Dialing Plans

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

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen.



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



**AVAYA CS1000 Element Manager**

**ESN Access Codes and Basic Parameters**

**General Properties**

NARS/BARS Access Code 1: 6

NARS Access Code 2: 7

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

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: 6 (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

- Number of digits in CDP DN (DSC + DN or LSC + DN): 7 (3 - 10)

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

Log in to Call Server CLI (please refer to **Section 5.1.2** for more details), change Customer Net Data block by using **ld 15**. In this provisioning, the idea is to disassociate the **NPA** and **SPN** in **AC2** so that the system will be forced to associate **NPA** and **SPN** with **AC1** (not shown).

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35359353   USED U P: 8485941 1034575   TOT: 45879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 0
OPT
AC2 xNPA xSPN   → (Set NPA, SPN not to associate to ESN Access Code 2)
FNP
CLID
...
```



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 ----- > (NPA, SPN are associated to ESN Access Code 1)
AC2
FNP YES
...
```

### 5.6.3. Digit Manipulation Block (DMI)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen (not shown). Select **Digit Manipulation Block** (DGT) as shown in capture **Section 5.6.1**. Select an available DMI from the drop-down list and click **to Add** as shown. In testing example, **Digit Manipulation Block Index 1** is added.



The **DMI\_1** screen will open (not shown). In this testing, there is no leading digit to delete, therefore enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** and then click **Submit** button.



#### 5.6.4. Digit Manipulation Block Index (DMI) for Outbound Call

To add DMI for outbound calls, there is an index, which was added to the **Digit Manipulation Block Index 1** as shown in **Section 5.6.3. Digit Manipulation Block Index 1** is used for outbound calls.

#### 5.6.5. Route List Block (RLB) (RLB 14)

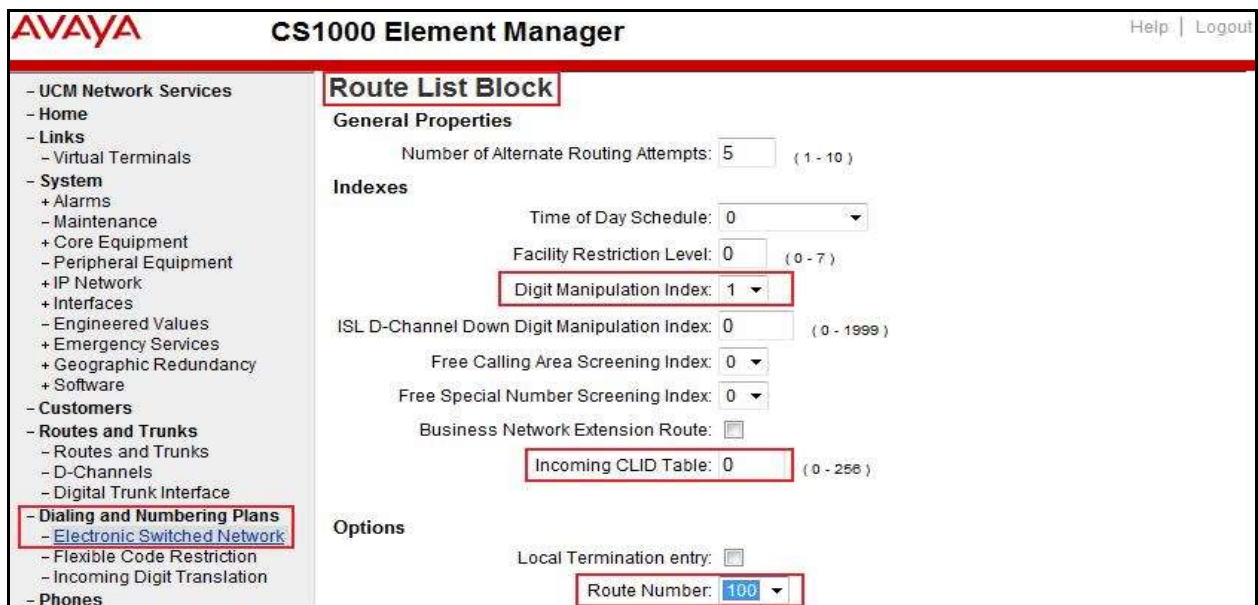
To add a RLB associated with the DMI in **Section 5.6.4**, select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Route List Block (RLB)** as shown in capture of **Section 5.6.1**.

Enter an available value in the textbox for the **Please enter a route list index** (in this case 100) and click to **Add** button as shown.



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, and click **Submit** button (not shown).

- **Digit Manipulation Index: 1** (created in **Section 5.6.4**)
- **Incoming CLID Table: 0** (created in **Section 5.5.7**)
- **Route Number: 100** (created in **Section 5.5.5**)



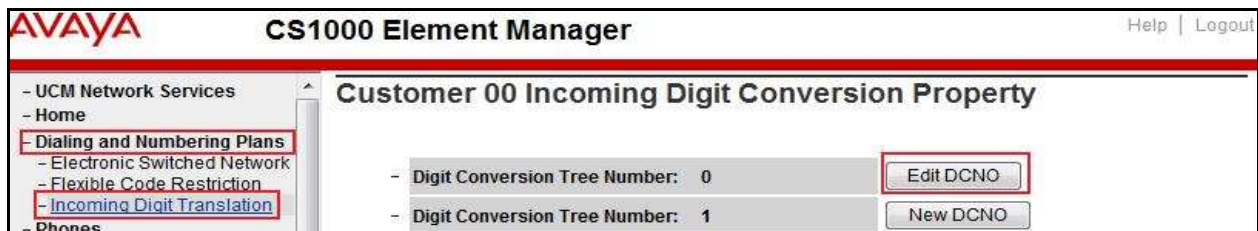
### 5.6.6. Inbound Call – Incoming Digit Translation Configuration

This section describes the steps for receiving the calls from PSTN via Bell system.

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



Click on the **New DCNO** to create the digit translation mechanism. In this example, **Digit Conversion Tree Number 0** has been created.



Detail configuration of the Digit Conversion Tree Configuration is shown in capture below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the associated CS1000 system telephone DN. This **DCNO** has been assigned to route 100.

In the following configuration, the incoming call from PSTN with DID prefix **613XXX** will be translated to associated 4 digits DN. DID number **613XXX6508** is translated to **1700** for Voicemail accessing purpose and **613XXX6507** is translated to **1115** for Mobile Service Access DN.



### 5.6.7. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 1866, 411, 911 and so on.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Special Number (SPN)** under **Access Code 1** (not shown). Enter a SPN number and then click **to Add** button (not shown). Capture below shows all the special numbers used for this testing.

The screenshot displays the AVAYA CS1000 Element Manager interface. On the left, a navigation pane shows a tree structure with 'Dialing and Numbering Plans' and its sub-item 'Electronic Switched Network' highlighted. The main content area is titled 'Special Number List'. At the top of this area is a form with the text 'Please enter a Special Number' followed by an input field and a 'to Add' button. Below this, a list of four special numbers is shown, each with an 'Edit' button to its right. The entries are: 'Special Number -- 0' (Flexible length: 0, International dialing plan: NO, Type of call: NONE, Route list index: 100), 'Special Number -- 1866' (Flexible length: 11, Inhibit time-out handler: NO, Type of call: NONE, Route list index: 100), 'Special Number -- 411' (Flexible length: 3, Inhibit time-out handler: NO, Type of call: NATL, Route list index: 100), and 'Special Number -- 911' (Flexible length: 3, Inhibit time-out handler: NO, Type of call: NATL, Route list index: 100).

Special Number	Flexible length	Inhibit time-out handler	Type of call	Route list index
Special Number -- 0	0	NO	NONE	100
Special Number -- 1866	11	NO	NONE	100
Special Number -- 411	3	NO	NATL	100
Special Number -- 911	3	NO	NATL	100

### 5.6.8. Outbound Call - Numbering Plan Area (NPA)

This section describes the creation of NPA used in this test configuration.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Numbering Plan Area Code (NPA)** under **Access Code 1** (not shown). Enter the area code desired in the textbox and click to **Add** button. **416**, **613**, **647** and **905** area codes were used in this configuration.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left-hand navigation pane contains a tree structure with the following items: UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans (highlighted with a red box), Flexible Code Restriction, Incoming Digit Translation, Phones, Tools, and Security. Under 'Dialing and Numbering Plans', the 'Electronic Switched Network' sub-item is also highlighted with a red box. The main content area is titled 'Numbering Plan Area Code List'. It features a form with the text 'Please enter an area code' followed by an empty input field and a 'to Add' button (both highlighted with red boxes). Below this, there is a list of four configured area codes, each with an 'Edit' button: 'Numbering Plan Area Code -- 416', 'Numbering Plan Area Code -- 613', 'Numbering Plan Area Code -- 647', and 'Numbering Plan Area Code -- 905'. Each entry also displays 'Route List Index: 100' and 'Incoming Trunk group Exclusion Index: NONE'.



## 5.7. Administer Telephone

This section describes the creation of CS1000 clients used in this configuration.

### 5.7.1. Telephone creation

Refer to **Section 5.5.4** for creation of virtual superloop **96** and **Section 5.4.1** for creation of bandwidth zone **10** used for IP telephones. Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail). Create an IP telephone by using **ld 11** as shown below:

```
>ld 11
REQ: new
TYPE: 2007
TN 96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED
DES 2007 < --- Describe information for IP Telephone
TN 96 0 0 02 VIRTUAL < --- Set Terminal Number for IP Telephone
TYPE 2007
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010 < --- Set bandwidth zone for IP telephone
CUR_ZONE 00010
MRT
ERL 0
ECL 0
FDN
TGAR 1
LDN NO
NCOS 7
SGRP 0
RNPG 0
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBD WTA LPR MTD FND HTD TDD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
```

UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD  
DRDD EXR0  
USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN  
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD  
MSNV FRA PKCH MWTD DVLD CROD ELCD  
CPND\_LANG ENG  
HUNT  
PLEV 02  
PUID  
UPWD  
DANI NO  
AST  
IAPG 0  
AACS NO  
ITNA NO  
DGRP  
MLWU\_LANG 0  
MLNG ENG  
DNDR 0  
**KEY 00 SCR 1396 0** MARP < --- Set the position of DN 1396 to display on key 0 of the telephone  
CPND  
CPND\_LANG ROMAN  
**NAME Bell1396** < --- Set name to display  
XPLN 13  
DISPLAY\_FMT FIRST, LAST  
01  
<Text removed for brevity>

### 5.7.2. Enable Privacy for the Telephone

This section shows how to enable Privacy for a telephone by changing its class of service (cls) and this feature cannot be enabled or disabled from the telephone. By modifying the configuration of the telephone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately.

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

```
>ld 11
REQ: chg
TYPE: 2007
TN 96 0 0 2
ECHG yes
ITEM cls ddgd
...
```

To allow the display number, set **cls** to **ddga**. CS1000 will not send the Privacy header to the Service Provider.

```
>ld 11
REQ: chg
TYPE: 2007
TN 96 0 0 2
ECHG yes
ITEM cls ddga
...
```



### 5.7.3. Enable Call Forward for Telephone

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

Select **Customers** → **00** → **Call Redirection**. The **Call Redirection** page is shown.

- **Total redirection count limit: 0** (unlimited)
- **Call forward: Originating**
- **Number of normal ringing cycles for CFNA: 3** (for all options)
- Click **Save**.

**AVAYA** CS1000 Element Manager Help | Logout

**Call Redirection**

Redirection Holidays

Do not disturb hunting: ☐

Total redirection count limit: 0

Options:

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

Call forward: ☒ Originating ☐ Forwarding

Number of normal ringing cycles for CFNA

Option 0: 3

Option 1: 3

Option 2: 3

Number of distinctive ringing cycles for CFNA

Option 0: 3

Option 1: 3

Option 2: 3

Calls routed to message center

No answer DID calls: ☐

No answer non-DID calls: ☐

DID calls to busy telephones: ☐

**Save** **Cancel**

To enable Call Forward All Call (CFAC) for a telephone over a trunk, use **ld 11**. Set **cls** to **CFXA**, and **SFA**, then program the forward number on the telephone set. The following is the configuration of a telephone that has CFAC enabled with forwarding number **66139675204**.

**ld 11**  
REQ: chg  
TYPE: 2007  
TN 96 0 0 2  
  
ECHG yes  
ITEM cls **CFXA SFA**  
ITEM key 19 CFW 16 **66139675204**

To enable **Call Forward Busy (CFB)** for telephone over trunk, use **ld 11**. Set **cls** to **FBA**, **HTA**, and **SFA**, then program the forward number as **hunt** and **fdn**. Following is the configuration of a telephone with **CFB** enabled and forward number **66139675204**.

**ld 11**  
REQ: chg  
TYPE: 2007  
TN 96 0 0 2  
ECHG yes  
ITEM cls **FBA HTA SFA**  
ITEM hunt **66139675204**  
ITEM fdn 66139675203

To enable **Call Forward No Answer (FNA)** for a telephone over a trunk, use **ld 11**. Set **cls** to **FNA**, and **SFA**, and program the forward number as **hunt** and **FDN**. Following is the configuration of a telephone that has **FNA** enabled with forward number **66139675204**.

**ld 11**  
REQ: chg  
TYPE: 2007  
TN 96 0 0 4  
ECHG yes  
ITEM cls **FNA SFA**  
ITEM hunt **66139675204**  
ITEM fdn 66139675203

#### 5.7.4. Enable Call Waiting for Telephone

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

Log in to the Call Server CLI (please refer to **Section 5.1.2** for more details), configure Call Waiting feature for telephone by using **ld 11** to change **cls** to **HTD**, and **SWA** and adding a **CWT** key.

```
ld 11
REQ: chg
TYPE: 2007
TN 96 0 0 2
ECHG yes
ITEM cls HTD SWA
ITEM key 2 cwt
...
```

## 6. Configure Avaya Aura® Session Manager

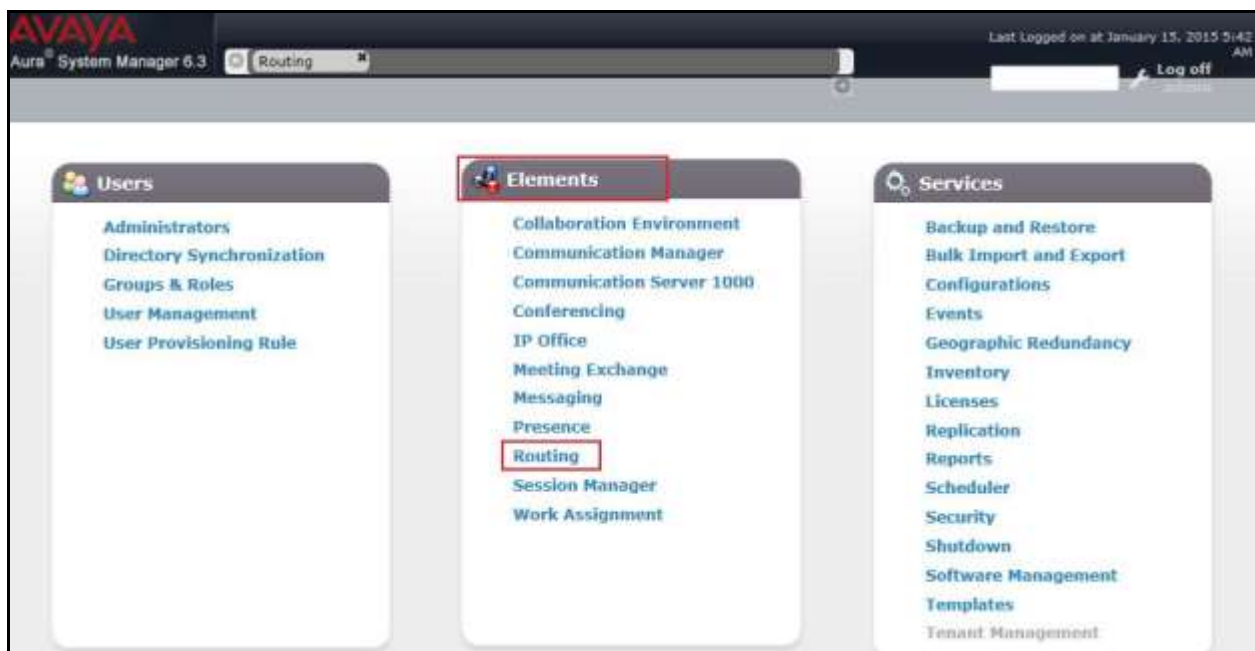
This section provides the procedures for configuring SM. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, SM and the Avaya SBCE
- Entity Links, which define the SIP trunk parameters used by SM 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
- SM, corresponding to the SM 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 SM installation. This includes items such as certain SIP domains, locations, SIP entities, and SM itself. However, each item should be reviewed to verify the configuration.

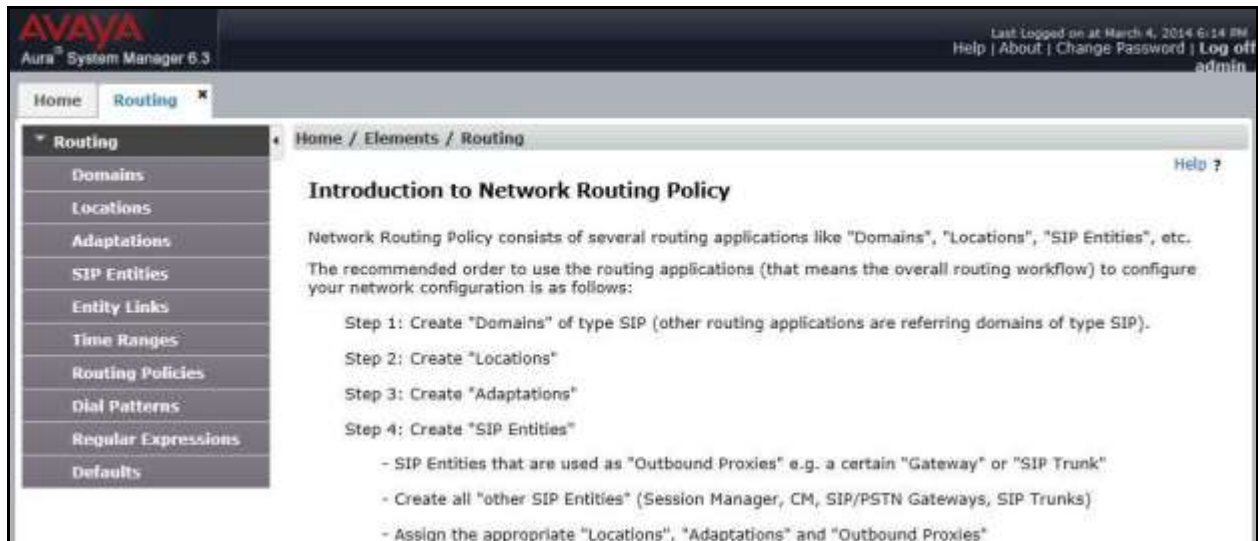
### 6.1. System Manager Login and Navigation

SM configuration is accomplished by accessing the Web GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the **System Manager Log On** screen (not shown), provide the appropriate credentials and click on **Login**. The initial screen shown below is then displayed.



Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column (not shown) to bring up the **Introduction to Network Routing Policy** screen.

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



## 6.2. Specify SIP Domain

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain “avayalab.com” was already created for communication between SM and CS1000. The domain “avayalab.com” is not known to Bell. It will be adapted by the Avaya SBCE to IP address based URI-Host to meet the SIP specification of Bell system.



## 6.3. Add Adaptations

Adaptations can be used to modify SIP messages that are leaving a SM instance (egress adaptation) and that are entering a SM instance (ingress adaptation). This adaptation function is needed to convert strings containing calling and called party numbers from the local dial-plan of a SIP entity to the dial-plan administered on the SM, and vice versa. Adaptation is also needed when other SIP entities require special SIP protocol conventions. Each administered SIP entity may have its own unique adaptation, or one adaptation can be shared among multiple entities.

To add an Adaptation, navigate to **Routing → Adaptations** in the left-hand menu pane and click **New** button in the right pane (not shown).

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Choose predefined Module Name from drop down list.
- **Module Parameter Type:** Choose a module from drop down list.

An Adaptation, using Module Name **CS1000Adapter**, was created to support CS1000 source based routing.

AVAYA  
Aura® System Manager 6.3

Last Logged on at March 18, 2014 12:08 PM  
Help | About | Change Password | Log of admin

Home Routing \*  
Home / Elements / Routing / Adaptations

Adaptation Details

General

\* Adaptation Name: CS1000\_Adaptation

Module Name: CS1000Adapter

Module Parameter Type: Name-Value Parameter

Add Remove

Name	Value
fromto	true

Select : All, None

Egress URI Parameters:

Notes:



An Adaptation, using Module Name **DiversionTypeAdapter**, was created to add Diversion header and to remove MIME (CS1000 proprietary SIP info.).

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header shows the Avaya logo, the version 'Aura System Manager 6.3', and the user 'admin' logged in at 'March 18, 2014 12:08 PM'. The left sidebar contains a navigation menu with options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Routing' section is expanded, and the 'Adaptations' sub-section is selected. The main content area shows the 'Adaptation Details' for 'Diversion\_MIME'. The 'General' tab is active, displaying the following fields: 'Adaptation Name' (Diversion\_MIME), 'Module Name' (DiversionTypeAdapter), and 'Module Parameter Type' (Name-Value Parameter). Below these fields are 'Add' and 'Remove' buttons. A table lists the parameters for the adaptation, with one entry: 'MIME' with a value of 'no'. Below the table is a 'Select' dropdown menu set to 'All'. At the bottom, there is an 'Egress URI Parameters' field and a 'Notes' field containing the text 'Remove MIME and add Diversion'.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

\* Adaptation Name: Diversion\_MIME

Module Name: DiversionTypeAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

Name	Value
MIME	no

Select : All, None

Egress URI Parameters:

Notes: Remove MIME and add Diversion

## 6.4. Add Location

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

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

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

In the **Location Pattern** section (see the screen below), click **Add** and enter following values:

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

Displayed below is the screenshot for location **Belleville**, which includes all equipment on the **10.33.x.x**, **10.10.98.x** and **10.10.97.x** subnets including CS1000, SM and Avaya SBCE. Click **Commit** to save.

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'. The 'Location Details' section includes a 'General' tab with fields for 'Name' (set to 'Belleville') and 'Notes' (set to 'GSSCP Belleville'). Below this is the 'Dial Plan Transparency in Survivable Mode' section, which is currently disabled. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec', 'Total Bandwidth' set to '10000000', and 'Multimedia Bandwidth' set to '10000000'. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked. The 'Location Pattern' section at the bottom shows a table with 3 items, filtered by 'Enable'. The table has columns for 'IP Address Pattern' and 'Notes'. The items listed are '10.33.\*', '10.10.97.\*', and '10.10.98.\*'. The 'Add' and 'Remove' buttons are visible above the table. The top right corner of the interface shows the user 'admin' and the last login time 'March 4, 2014 6:14 PM'.

IP Address Pattern	Notes
* 10.33.*	
* 10.10.97.*	
* 10.10.98.*	

## 6.5. Add SIP Entities

A SIP Entity must be added for SM and for each SIP telephony system connected to it which includes CS1000 and the Avaya SBCE.

To add a new SIP Entity, navigate to **Routing** → **SIP Entities** in the left navigation pane and click **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for SM, **Other** for CS1000 and **Other** for the Avaya SBCE.
- **Location:** Select the location defined previously in **Section Error! Reference source not found.**
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of SM SIP Entity. The IP address of the SM signaling interface is entered for **FQDN or IP Address**.

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'. On the right, it indicates 'Last Logged on at March 4, 2014 6:14 PM' and provides links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left navigation pane is expanded to 'Routing', which includes sub-items like Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the 'SIP Entity Details' form under the 'General' tab. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The form contains the following fields: 'Name' (SM63), 'FQDN or IP Address' (10.33.10.26), 'Type' (Session Manager), 'Notes' (SM R6.3), 'Location' (Belleville), 'Outbound Proxy' (empty), 'Time Zone' (America/Toronto), and 'Credential name' (empty). At the bottom, there is a 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

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

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

- **Port:** Port number on which the SM can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.
- Defaults can be used for the remaining fields.
- Click **Commit** to save (not shown).

The compliance test used **Port** entry **5060** with **UDP** for connecting to CS1000 and **Port** entry **5060** with **UDP** for connecting to the Avaya SBCE.

**Port**

TCP Failover port:

TLS Failover port:

4 Items Filter: Enable

Port	Protocol	Default Domain	Notes
5060	UDP	avayalab.com	

The following screen shows the addition of CS1000 SIP Entities. In order for SM to send SIP traffic on an entity link to CS1000, it is necessary to create a SIP Entity for CS1000. The **FQDN or IP Address** field is set to IP address of CS1000. Select **Other** as **Type**.

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at March 18, 2014 12:08 PM  
Help | About | Change Password | **Log off** admin

Home Routing

Home / Elements / Routing / SIP Entities

**SIP Entity Details** Help ?

**General**

\* Name: CS1K\_car1

\* FQDN or IP Address: 10.10.97.154

Type: Other

Notes:

Adaptation: CS1000\_Adaptation

Location: Belleville

Time Zone: America/New\_York

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

The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of Avaya SBCE's private network interface (see **Figure 1**). Select **Other** as **Type**. Select **Link Monitoring Enabled** as **SIP Link Monitoring** with the interval of 60 seconds (not shown). This setting allows SM to send outbound OPTIONS heartbeat in every 60 seconds to service provider (which is forwarded by the Avaya SBCE) to query for the status of the SIP trunk connecting to service provider.

The screenshot shows the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at March 31, 2014 11:18 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar contains a navigation menu with 'Routing' selected, showing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area displays the 'SIP Entity Details' form for 'SBCE'. The breadcrumb trail is 'Home / Elements / Routing / SIP Entities'. The form has 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing fields for:
 

- Name:** SBCE
- \* FQDN or IP Address:** 10.10.98.22
- Type:** Other (dropdown)
- Notes:** SBCE
- Adaptation:** Diversion\_MIME (dropdown)
- Location:** Belleville (dropdown)
- Time Zone:** America/Toronto (dropdown)
- \* SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown)
- CommProfile Type Preference:** (empty dropdown)

 Below the 'General' tab are two other sections:
 

- Loop Detection:** Loop Detection Mode: Off (dropdown)
- SIP Link Monitoring:** SIP Link Monitoring: Link Monitoring Enabled (dropdown)

## 6.6. Add Entity Links

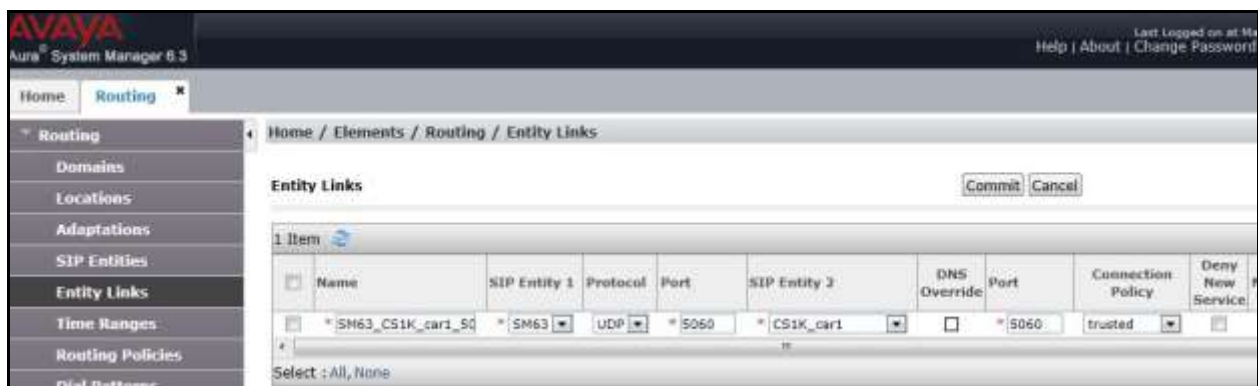
A SIP trunk between SM and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for CS1000 and other for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **New** button in the right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

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link, UDP for the Entity Link to CS1000 and UDP for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which SM will receive SIP requests from the far-end. For CS1000, this must match the **Far-end Listen Port** defined on the CS1000 in **Section 5.5.2**.

- **SIP Entity 2:** Select the name of the other systems. For CS1000, select the CS1000 SIP Entity defined in **Section** Error! Reference source not found.. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section** Error! Reference source not found..
- **Port:** Port number on which the other system receives SIP requests from SM. For CS1000, this must match the **Near-end Listen Port** defined on the CS1000 in **Section 5.5.2**.
- **Connection Policy:** Select **Trusted**. **Note:** If this is not selected, calls from the associated SIP Entity specified in **Section** Error! Reference source not found. will be denied.
- Click **Commit** to save.

The following screens illustrate the Entity Links to CS1000 and to Avaya SBCE.

Below is Entity Link to CS1000.



Below is Entity Link to Avaya SBCE.



## 6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section** Error! Reference source not found.. Two routing policies were added, one for CS1000 and other for Avaya SBCE. To add a routing policy, navigate to **Routing** →



**Routing Policies** in the left navigation pane and click **New** button in the right pane (not shown). The following screen is displayed.

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

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

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

The following screens show the Routing Policies for CS1000.

AVAYA  
Aura® System Manager 6.3

Last Logged on at March 4, 2014 6:14 PM  
Help | About | Change Password | Log off admin

Home Routing x

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

\* Name: Inbound\_To\_CS1K\_Car1

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K_car1	10.10.97.154	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select : All, None

The following screens show the Routing Policies for Avaya SBCE.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane is expanded to 'Routing', and the 'Routing Policies' sub-item is selected. The main content area displays the 'Routing Policy Details' for a policy named 'Outbound\_To\_SBCE'. The 'General' section includes fields for Name, Disabled status, Retries, and Notes. The 'SIP Entity as Destination' section shows a table with one entry for 'SBCE' with FQDN or IP Address '10.10.98.22' and Type 'Other'. The 'Time of Day' section shows a table with one entry for '24/7' with Start Time '00:00' and End Time '23:59'.

**Routing Policy Details**

**General**

\* Name: Outbound\_To\_SBCE

Disabled: ☐

\* Retries: 0

Notes: Outbound to SBCE

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
SBCE	10.10.98.22	Other	SBCE

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

Select: All, None

## 6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through SM. For the compliance testing, dial patterns were needed to route calls from CS1000 to Bell system 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 **New** button in the right pane (not shown).

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

- **Pattern:** Enter a dial string that will be matched against the “Request-URI” of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria, **Section 6.2**.
- **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** (not shown).

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

Two examples of the dial patterns used for the compliance testing were shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows that 10-digit dialed numbers that has a destination domain of “avayalab.com” uses route policy to Avaya SBCE as defined in **Section** Error! Reference source not found..

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at March 4, 2014 6:14 PM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** [Commit] [Cancel] [Help ?]

**General**

\* Pattern: 513

\* Min: 10

\* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes:

**Originating Locations and Routing Policies**

[Add] [Remove]

2 Items [Filter: Enable]

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	GSSCP Belleville	Outbound_To_SBCE	0	<input type="checkbox"/>	ACME	Outbound_To_SBCE

Select : All, None

**Denied Originating Locations**

[Add] [Remove]

0 Items [Filter: Enable]

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

The second example shows that inbound 10-digit numbers that start with 613 to domain “avayalab.com” uses route policy to CS1000 as defined in **Section Error! Reference source not found..8**. These are the DID numbers assigned to the enterprise by Bell.

AVAYA  
Aura® System Manager 6.3

Last Logged on at March 31, 2014 11:18 AM  
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

\* Pattern: 613.XXX

\* Min: 6

\* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avayalab.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	GSSCP Belleville	Inbound_To_CS1K_Car1	0	<input type="checkbox"/>	CS1K_car1	

## 6.9. Add/View Session Manager

The creation of a SM element provides the linkage between System Manager and SM. This is most likely done as part of the initial SM installation. To add a SM, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click **New** button in the right pane (not shown). If the SM Instances 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 SM.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the SM management interface.
- **Direct Routing to Endpoints:** Enable, to enable call routing on the SM.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **Network Mask:** Enter the network mask corresponding to the IP address of SM.

- **Default Gateway:** Enter the IP address of the default gateway for SM.
- Use default values for the remaining fields. Click **Commit** to save (not shown).

The screen below shows the SM values used for the compliance testing.

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at March 5, 2014 11:35 AM  
Help | About | Change Password | **Log off** admin

Home Session Manager x

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

Description

Management Access Point Host Name/IP

Direct Routing to Endpoints ☒ Enable

VMware Virtual Machine ☐

### Security Module

SIP Entity IP Address

Network Mask

Default Gateway

Call Control PHB

QOS Priority

Speed & Duplex

VLAN ID

\*SIP Firewall Configuration

## 7. Configure Avaya Session Border Controller

This section describes the configuration of Avaya SBCE necessary for interoperability with CS1000, SM and Bell system.

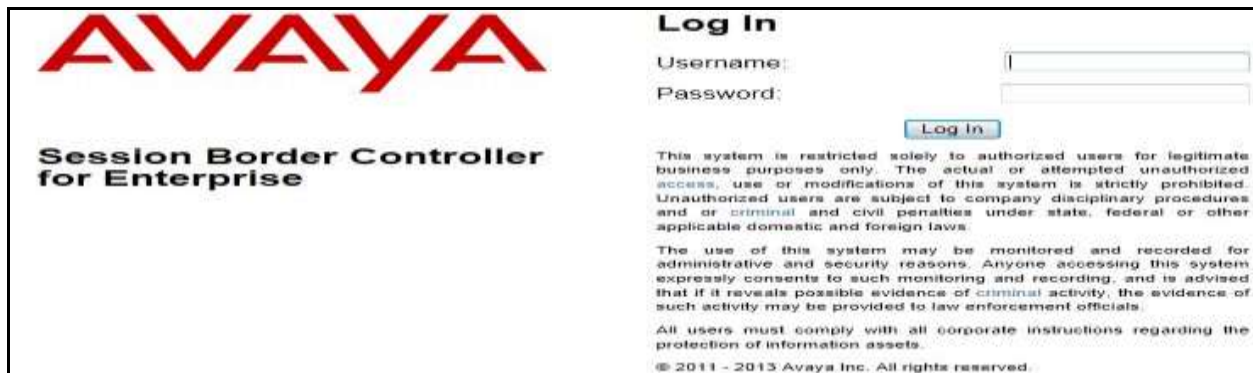
In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Bell system resides on the Public side of the network.

**Note:** The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 11** of these Application Notes.

### 7.1. Log in Avaya Session Border Controller


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

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



The login page features the Avaya logo in red at the top left. Below it, the text "Session Border Controller for Enterprise" is displayed. To the right, there is a "Log In" section with input fields for "Username:" and "Password:", followed by a "Log In" button. Below the login fields, there is a disclaimer: "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." Below this, another disclaimer states: "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." At the bottom, it says: "All users must comply with all corporate instructions regarding the protection of information assets." and "© 2011 - 2013 Avaya Inc. All rights reserved."

The main page of the Avaya SBCE will appear as shown below.



The dashboard has a left sidebar with navigation links: "Dashboard", "Administration", "Backup/Restore", "System Management", "Global Parameters", "Global Profiles", "PPM Services", "Domain Policies", "TLS Management", and "Device Specific Settings". The main content area is titled "Dashboard" and contains a warning message: "Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation." Below the warning, there are two panels. The "Information" panel displays system details: System Time (01:55:19 AM CST), Version (6.3.000-19-4338), Build Date (Fri Sep 26 09:14:23 EDT 2014), License State (OK), Aggregate Licensing Overages (0), and Peak Licensing Overage Count (0). The "Installed Devices" panel lists two devices: "EMS" and "SBCE62".



## 7.2. Global Profiles

Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

### 7.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “\*” is used for all incoming and outgoing traffic.

### 7.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

To create a Routing Profile, select **Global Profiles → Routing**. Click on the **Add** button.

In the compliance testing, a Routing Profile **EN-to-SP** was created to use in conjunction with the server flow defined for EN. This entry is to route the outbound call from the enterprise to service provider.

In the opposite direction, a Routing Profile named **SP-to-EN** was created to be used in conjunction with the server flow defined for SP. This entry is to route the inbound call from service provider to the enterprise.

## Routing Profile for SP

The screenshot below illustrates the routing profile from Avaya SBCE to the SP network, **Global Profiles → Routing: EN-to-SP**. As shown in **Figure 1**, the SP SIP trunk is connected with transportation protocol UDP (not shown). If there is a match in the “To” or “Request URI” headers with the URI Group **SP** defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of SP SIP trunk on port 5060.



## Routing Profile for EN

The Routing Profile for SP to EN, **SP-to-EN**, was defined to route call where the “To” header matches the URI Group **SP** defined in **Section 7.2.1** to **Next Hop Server 1** which is the IP address of Session Manager, on port 5060 as a destination. As shown in **Figure 1**, the SIP trunk between EN and the Avaya SBCE is connected with transportation protocol TCP.



## 7.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding**. Click on the **Add** button.

In the compliance testing, two Topology Hiding profiles **EN-to-SP** and **SP-to-EN** were created.

## Topology Hiding Profile for SP

Profile **EN-to-SP** was defined to mask the enterprise SIP domain avayalab.com in “Request-URI” and “To” headers to SP IP address and “From” header to the Avaya SBC external interface IP address; mask the enterprise SIP domain avayalab.com in the “From” and “PAI” headers to IP **10.10.98.119** (the Avaya SBCE public IP address). It is to secure the enterprise network topology and to meet the SIP requirement of the service provider.

### Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header also applies to “Referred-By” and “P-Asserted-Identity” headers.
- The masking applied on “To” header also applies to “Refer-To” header.

The screenshots below illustrate the Topology Hiding profile **EN-to-SP**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with options like 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, and Domain Policies. The main content area is titled "Topology Hiding Profiles: EN-to-SP" and includes buttons for Add, Rename, Clone, and Delete. Below the title, there is a link to add a description. The "Topology Hiding" tab is selected, showing a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sipxxxxxxxx.bell.ca
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	vendor6.xxx.internetworks.ca
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sipxxxxxxxx.bell.ca
SDP	IP/Domain	Auto	---

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

## Topology Hiding Profile for EN

Profile **SP-to-EN** was also created to mask SP URI-Host in “Request-URI”, “From”, “To” headers to the enterprise domain *avayalab.com*, replace Record-Route, Via headers and SDP added by SP to internal IP address known to EN.

### Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header also applies to “Referred-By” and “P-Asserted-Identity” headers.
- The masking applied on “To” header also applies to “Refer-To” header.

The screenshots below illustrate the Topology Hiding profile **SP-to-EN**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Global Profiles' expanded, and 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: SP-to-EN'. It includes an 'Add' button and a list of profiles: 'EN-to-SP' and 'SP-to-EN'. The 'SP-to-EN' profile is selected, showing a table of configuration rules. The table has columns: Header, Criteria, Replace Action, and Overwrite Value. The rules are as follows:

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

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

## 7.2.4. Server Interworking

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles** → **Server Interworking**. Click on the **Add** button.

In the compliance testing, two Server Interworking profiles were created for SP and EN respectively.

## Server Interworking profile for SP

Profile **SP=SI** was defined to match the specification of SP. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

### General settings:

- **Hold Support** = *NONE*. The Avaya SBCE will not modify the hold/ resume signaling from EN to SP.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from EN to SP.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from EN to SP.
- **T.38 Support** = *No*. SP does not support T.38 fax in the compliance testing.
- **Privacy Enabled** = *No*. The Avaya SBCE will not mask the “From” header with anonymous for the outbound call to SP.
- **DTMF Support** = *None*. The Avaya SBCE will send original DTMF method from EN to SP.

The screenshots below illustrate the Server Interworking profile **SP-SI**, **General**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-SI' and includes an 'Add' button. Below this, there are tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, showing a table of settings. The settings are organized into sections: General, Privacy, and DTMF. The 'General' section includes settings like Hold Support, 180 Handling, 181 Handling, 182 Handling, 183 Handling, Refer Handling, URI Group, 3xx Handling, Diversion Header Support, Delayed SDP Handling, Re-Invite Handling, T.38 Support, URI Scheme, and Via Header Format. The 'Privacy' section includes Privacy Enabled, User Name, P-Asserted-Identity, P-Preferred-Identity, and Privacy Header. The 'DTMF' section includes DTMF Support. The values for these settings are: 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), Privacy Enabled (No), User Name, P-Asserted-Identity (No), P-Preferred-Identity (No), Privacy Header, DTMF Support (None). There are 'Rename', 'Clone', and 'Delete' buttons at the top right, and an 'Edit' button at the bottom right.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
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

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

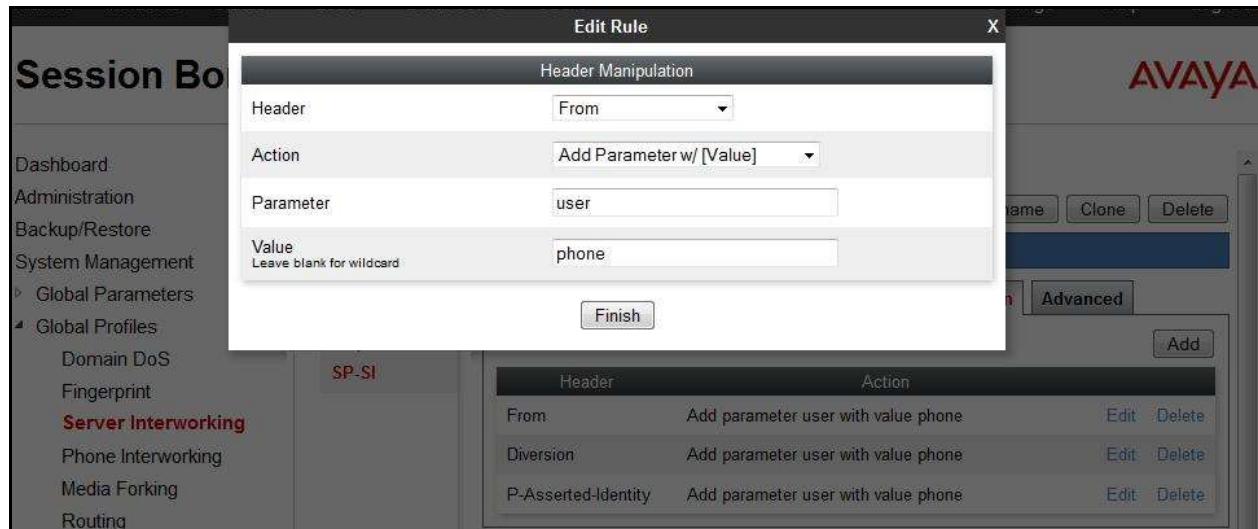
DTMF	
DTMF Support	None

## Header Manipulation:

Header rules are added to include the parameter *user=phone* to the **From**, **Diversion** and **P-Asserted-Identity** headers as Bell required.

- **Header:** This field is where *From*, *Diversion* and *P-Asserted-Identity* is selected.
- **Action:** *Add Parameter w/[value]* is selected.
- **Parameter** = *user*.
- **Value** = *phone*.

The screenshots below illustrate the Server Interworking profile **SP-SI**, **Header Manipulation**.





### Advanced settings:

- **Record Routes = Both** Sides. The Avaya SBCE will send “Record-Route” header to both call and trunk servers.
- **Topology Hiding: Change Call-ID = Yes**. The Avaya SBCE will modify “Call-ID” header for the call toward SP.
- **Change Max Forwards = Yes**. The Avaya SBCE will adjust the original Max-Forwards value from EN to SP by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC = Yes**. SP has a SBC which interfaces its Central Office (CO) to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from SP for the media.

The screenshots below illustrate the Server Interworking profile **SP-SI, Advanced**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SP-SI' and shows a list of profiles with 'SP-SI' selected. The 'Advanced' tab is active, displaying a table of settings.

Setting	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

## Server Interworking profile for EN

Profile **EN-SI** was defined to match the specification of EN. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

### General settings:

- **Hold Support** = *None*.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from SP to EN.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from SP to EN.
- **T.38 Support** = *No*. EN does support T.38 fax, but SP doesn't in the compliance testing.
- **Privacy Enabled** = *No*. The Avaya SBCE will not mask the "From" header with anonymous for an inbound call from SP. It depends on SP to enable/ disable privacy on an individual call basis.
- **DTMF Support** = *None*. The Avaya SBCE will send original DTMF method from SP to EN.

The screenshots below illustrate the Server Interworking profile **EN-SI**, **General**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: EN-SI' and includes an 'Add' button. Below this, there are tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. 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

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

DTMF	
DTMF Support	None

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

### Advanced settings:

- **Record Routes = Both** Sides. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Topology Hiding: Change Call-ID = Yes**. The Avaya SBCE will modify “Call-ID” header for the call toward EN.
- **Change Max Forwards = Yes**. The Avaya SBCE will adjust the original Max-Forwards value from SP to EN by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC = Yes**. This setting allows the Avaya SBCE to always use the SDP received from EN for the media.

The screenshots below illustrate the Server Interworking profile **EN-SI, Advanced**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like 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, and Device Specific Settings. The main content area is titled "Interworking Profiles: EN-SI" and includes buttons for Add, Rename, Clone, and Delete. Below this, there's a section for "Click here to add a description." and a tabbed interface with General, Timers, URI Manipulation, Header Manipulation, and **Advanced** tabs. The Advanced tab is active, showing a table of settings:

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

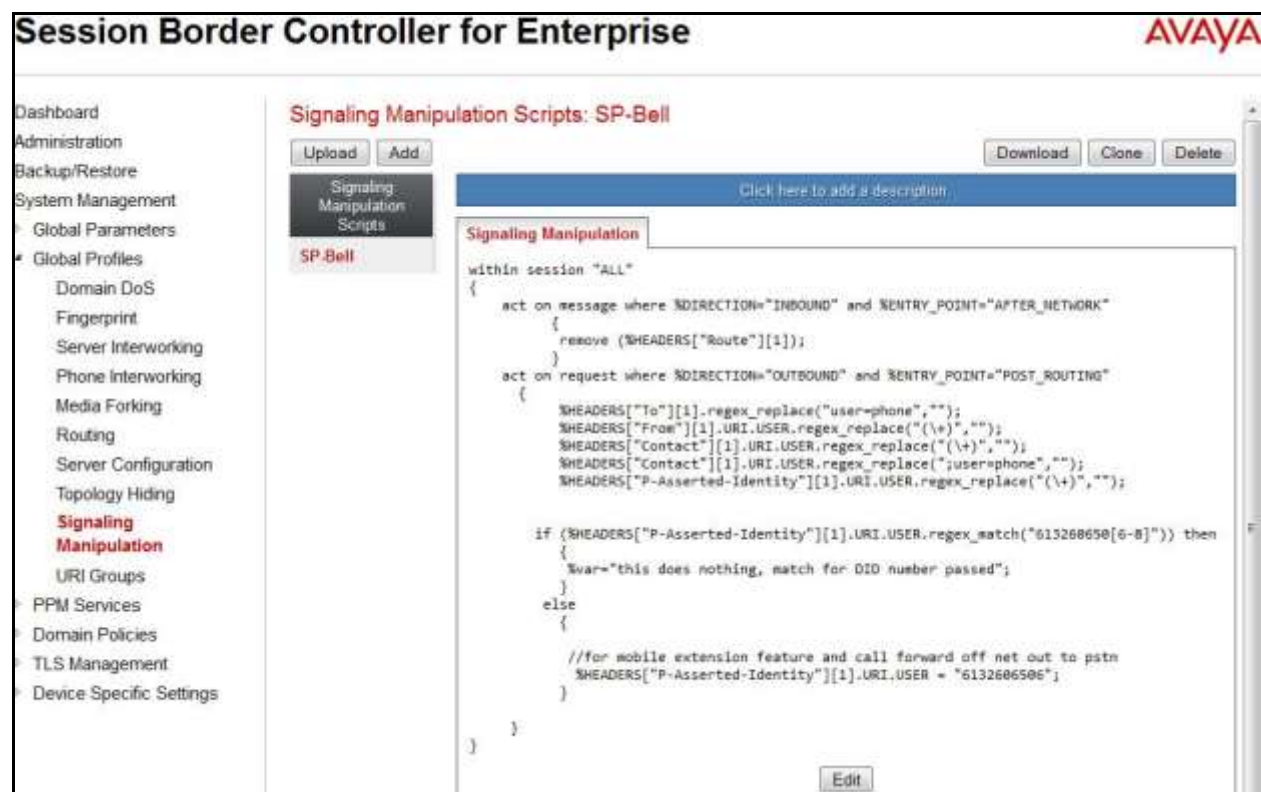
An Edit button is located at the bottom right of the settings table.

### 7.2.5. Configure Signaling Manipulation

Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation**. Click **Add Script** (not shown).

In the compliance testing, a SigMa script is created for Server Configuration for SP and its details are captured below.



### 7.2.6. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **Global Profiles → Server Configuration**. Click on the **Add** button.

In the compliance testing, two separate Server Configurations were created, server entry **SP-SC** for SP and server entry **EN-SC** for EN.

## Server Configuration for SP

Server Configuration named **SP-SC** was created for SP. It will be discussed in detail below. **General** and **Advanced** tabs are provisioned for SP on the SIP trunk for every outbound call from enterprise to PSTN. The additional **DoS Whitelist** and **DoS Protection** tabs are displayed after **DoS Protection** is enabled under **Advanced** tab, the settings for these tabs are kept as default. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from EN to SP to query the status of the SIP trunk.

In the **General** tab, click on the **Edit** button then set **Server Type** for SP as **Trunk Server**. In the compliance testing, SP supported **UDP** and listened on port **5060**.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Global Profiles  
Domain DoS  
Fingerprint  
Server Interworking  
Phone Interworking  
Media Forking  
Routing  
**Server Configuration**

**Server Configuration: SP-SC**

Add Rename Clone Delete

Server Profiles  
SP-SC

**General** Authentication Heartbeat Advanced DoS Whitelist DoS Protection

Server Type Trunk Server

IP Addresses / FQDNs 192.168.237.194, 192.168.237.206, 192.168.237.209

Supported Transports UDP

UDP Port 5060

Edit

In the **Authentication** tab, click on the Edit button and enter following information.

- Check **Enable Authentication** check box.
- Enter **User Name** (provided by SP).
- Enter **Realm** (provided by SP).
- Enter **Password** and **Confirm Password** (provided by SP).
- Click **Finish**.

**Session Border Controller for Enterprise** AVAYA

Dashboard  
Administration  
Global Profiles  
Domain DoS  
Fingerprint  
Server Interworking  
Phone Interworking  
Media Forking  
Routing  
**Server Configuration**

**Server Configuration: SP-SC**

Add Rename Clone Delete

Server Profiles  
SP-SC

**General** **Authentication** Heartbeat Advanced DoS Whitelist DoS Protection

Enable Authentication ☒

User Name VEND6\_6130006506\_01A

Realm sipxxxxxxxxx.bell.ca

Edit



- Under **Advanced** tab, check on **Enable DoS Protection**. From the **Interworking Profile** drop down list, select **SP-SI** as defined in **Section 7.2.4**. For **Signaling Manipulation Script**, select **SP-Bell** as defined above. This configuration applies the specific SIP profile to the SP traffic. The other settings are kept as default.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main content area is titled "Server Configuration: SP-SC" and includes an "Add" button and action buttons (Rename, Clone, Delete). Below the title is a tabbed interface with tabs for General, Authentication, Heartbeat, Advanced, DoS Whitelist, and DoS Protection. The "Advanced" tab is selected, showing the following configuration:

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP-SI
Signaling Manipulation Script	SP-Bell
UDP Connection Type	SUBID

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

## Server Configuration for EN

Server Configuration named **EN-SC** created for EN is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from SP to EN to query the status of the SIP trunk.

In the **General** tab, click on the **Edit** button then specify **Server Type** for EN as **Call Server**. In the compliance testing, the link between the Avaya SBCE and EN was **TCP** and listened on port **5060**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main content area is titled "Server Configuration: EN-SC" and includes an "Add" button and action buttons (Rename, Clone, Delete). Below the title is a tabbed interface with tabs for General, Authentication, Heartbeat, and Advanced. The "General" tab is selected, showing the following configuration:

Server Type	Call Server
IP Addresses / FQDNs	10.33.10.26
Supported Transports	TCP

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



Under **Advanced** tab, click on the **Edit** button, from the **Interworking Profile** drop down list select **EN-SI** as defined in **Section 7.2.4** and from the **Signaling Manipulation Script** drop down list select **None**. The other settings are kept as default.

**Session Border Controller for Enterprise** AVAYA

Dashboard

- Global Parameters
- Global Profiles
  - Domain DoS
  - Fingerprint
  - Server Interworking
  - Phone Interworking
  - Media Forking
  - Routing
  - Server Configuration**

**Server Configuration: EN-SC**

Add Rename Clone Delete

Server Profiles

- SP-SC
- EN-SC**

General Authentication Heartbeat **Advanced**

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

Edit

## 7.3. Domain Policies

Domain Policies configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the Avaya SBCE security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

### 7.3.1. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

To clone a Signaling Rule, navigate to **Domain Policies → Signaling Rules**. With the **default** rule chosen, click on the **Clone** button.

## Signaling Rules for SP

In the compliance testing, created signaling rule **SP-SR** is discussed below. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button then check on **Enable** box. Then select **EF** value for **DSCP** option.



## Signaling Rules for EN

In the compliance testing, created signaling rule **EN-SR** is discussed below. All the tabs are kept as default values except **Signaling QoS** tab.

In **Signaling QoS** tab, click on **Edit** button then check on **Enable** box. Then select **EF** value for **DSCP** option.



## 7.3.2. Endpoint Policy Groups

The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

Endpoint Policy Groups were created for SP and EN.

To create a new policy group, navigate to **Domain Policies** → **Endpoint Policy Groups** and click on **Add**.

## Endpoint Policy Group for SP

The following screen shows **SP-PG** created for SP:

- Set Application Rule to *default-trunk*.
- Set Border Rule to *default*.
- Set Media Rule to *default-low-med*.
- Set Security Rule to *default-high*.
- Set Signaling Rule to *SP-SR* as created in **Section 7.3.1**.
- Set Time of Day Rule to *default*.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: SP-PG'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below these, there are two blue bars with text: 'Click here to add a description.' and 'Click here to add a row description.'. A table titled 'Policy Group' is shown 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-high, SP-SR, and default. There are 'Edit' and 'Clone' buttons for this row. A 'Summary' button and an 'Add' button are also present.

## Endpoint Policy Group for EN

The following screen shows **EN-PG** created for EN:

- Set Application Rule to *default-trunk*.
- Set Border Rule to *default*.
- Set Media Rule to *default-low-med*.
- Set Security Rule to *default-low*.
- Set Signaling Rule to *EN-SR* as created in **Section 7.3.1**.
- Set Time of Day Rule to *default*.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: EN-PG'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below these, there are two blue bars with text: 'Click here to add a description.' and 'Hover over a row to see its description.'. A table titled 'Policy Group' is shown 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-high, EN-SR, and default. There are 'Edit' and 'Clone' buttons for this row. A 'Summary' button and an 'Add' button are also present.

## 7.4. Device Specific Settings

Device Specific Settings allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

### 7.4.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as device IP address (es), public IP address (es), netmask, gateway, etc. to interface the device to the network. This information populates the **Network Management** tab, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings** → **Network Management** and under the **Network Configuration** tab verify the IP addresses assigned to the interfaces. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.

**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

**Network Management: SBCE62**

Devices  
SBCE62

**Network Configuration** Interface Configuration

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

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.10.98.119		10.10.98.97	B1	Delete
10.10.98.22		10.10.98.1	A1	Delete

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface, click its **Toggle** button.

**Network Management: SBCE62**

Devices  
SBCE62

**Network Configuration** **Interface Configuration**

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



### 7.4.2. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will open a connection for RTP on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**.

Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

**Note:** After the media interfaces are created, an application restart is necessary before the changes will take effect.

The screenshot shows the 'Media Interface' configuration page for device 'SBCE62'. The left sidebar contains a navigation menu with 'Media Interface' highlighted. The main content area has a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table of existing media interfaces.

Name	Media IP	Port Range	Edit	Delete
InsideMedia	10.10.98.22	35000 - 40000		
OutsideMedia	10.10.98.119	35000 - 40000		

### 7.4.3. Signaling Interface

The Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to **Device Specific → Settings → Signaling Interface** and click **Add**.

Separate Signaling Interfaces were created for both inside and outside interfaces. The following screen shows the Signaling Interfaces were created in the compliance testing with UDP/5060 for the outside interface to SP and TCP/5060 for the inside interface to EN.

The screenshot shows the 'Signaling Interface' configuration page for device 'SBCE62'. The left sidebar contains a navigation menu with 'Signaling Interface' highlighted. The main content area has a table of existing signaling interfaces.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
InsideSignaling	10.10.98.22	5060	5060	---	None		
OutsideSignaling	10.10.98.119	5060	5060	---	None		

#### 7.4.4. End Point Flows - Server Flow

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 the Avaya SBCE to secure a SIP Trunk call.

In the compliance testing, separate Server Flows were created for SP and EN. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.5** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow.  
**Note:** URI Group can be set to “\*” to match all calls.
- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** that the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.22** to assign to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** that the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 7.2.3** to apply to the Server Configuration.
- Click **Finish**.



The following screen shows the Server Flow **SP-SF** configured for SP.

The screenshot shows a configuration window titled "Edit Flow: SP-SF". It contains the following fields and values:

Field	Value
Flow Name	SP-SF
Server Configuration	SP-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideSignaling
Signaling Interface	OutsideSignaling
Media Interface	OutsideMedia
End Point Policy Group	SP-PG
Routing Profile	SP-to-EN
Topology Hiding Profile	EN-to-SP
File Transfer Profile	None

A "Finish" button is located at the bottom right of the window.

Similarly, the following screen shows the Server Flow **EN-SF** configured for EN.

The screenshot shows a configuration window titled "Edit Flow: EN-SF". It contains the following fields and values:

Field	Value
Flow Name	EN-SF
Server Configuration	EN-SC
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSignaling
Signaling Interface	InsideSignaling
Media Interface	InsideMedia
End Point Policy Group	EN-PG
Routing Profile	EN-to-SP
Topology Hiding Profile	SP-to-EN
File Transfer Profile	None

A "Finish" button is located at the bottom right of the window.

## 8. Bell Canada SIP Trunking Service Configuration

Bell is responsible for network configuration of Bell Canada SIP Trunking system. Bell system will require that customer provide public IP address used to reach Avaya SBCE public interface at the edge of the enterprise. Bell will provide IP address of Bell system SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to enterprise. This information is used to complete configurations for CS1000, Avaya SM and Avaya SBCE discussed in the previous sections.

The configuration between Bell system and Avaya enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to Bell system network.

## 9. Verification Steps

The following steps may be used to verify the configuration.

### 9.1. General

Place an inbound call from a PSTN telephone to an internal Avaya telephone, answer the call, and verify that two-way speech path exists. Verify that the call remains stable for several minutes and disconnects properly.

### 9.2. Verification of an Active Call on CS1000

#### Active Call Trace (LD 80)

The following is an example of one of the commands available on the CS1000 to trace a DN (1396) for which the call is in progress or idle. The call scenario involved PSTN telephone number 6139675203 calling 613XXX6506 (which is mapped to telephone 1396).

- Log in to CS1000 Signaling Server 10.10.97.154 with administrator account and password.
- Issue a command “cslogin” to login on to the CS1000 Call Server.
- Log in to the Overlay command prompt, issue the command **LD 80** and then **trac 0 1396**. It should show the TN is active as show bellow.

Below is the actual output of the CS1000 Call Server Command Line mode when the 1396 is in call state:

```
>ld 80

.trac 0 1396

ACTIVE VTN 096 0 00 02

ORIG VTN 100 0 00 00 VTRK IPTI RMBR 100 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.97.184
FAR-END MEDIA ENDPOINT IP: 10.10.97.184 PORT: 21582
FAR-END SIP SIGNALLING IP: 10.10.97.184
FAR-END MEDIA ENDPOINT IP: 10.10.97.184 PORT: 21582
TERM VTN 096 0 00 02 KEY 0 SCR MARP CUST 0 DN 1396 TYPE 2007
```

```
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.33.5.4 PORT: 5200
MEDIA PROFILE: CODEC G.729A NO-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 1396
MAIN_PM ESTD
TALKSLOT ORIG 10 TERM 15
EES_DATA:
NONE
QUEU NONE
CALL ID 0 34385

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 385
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 6139675203 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
CALLED NO = 613XXX6506 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
```

- After the call is released, issue command **trac 0 1396** again to see if the DN is released back to idle state. It should show the TN is in idle state.

Below is the example after the call to 1396 is finished.

```
.trac 0 1396
IDLE VTN 096 0 00 02 MARP
```

### SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675203) to an internal device (613XXX6506). Then check the SIP trunk status by using LD 32, and verify that one trunk is BUSY.

```
>ld 32
NPR000
.stat 100 0
063 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

After the call is released, check all SIP trunk status changed to IDLE state.

```
.stat 100 0
064 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

## Conclusion

All of the test cases have been executed. The test results met the objectives outlined in **Section 2.1**, within the constraints described in **Section 2.2**. The Bell Canada SIP Trunking service is considered **compliant** with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2.

## 10. Additional References

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

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

- [1] *Network Routing Service Fundamentals, Avaya CS1000, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013.*
- [2] *IP Peer Networking Installation and Commissioning, Avaya CS1000, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013.*
- [3] *CS1000E Overview, Avaya CS1000, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013.*
- [4] *Unified Communications Management Common Services Fundamentals, Avaya CS1000, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013.*
- [5] *Dialing Plans Reference, Avaya CS1000, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.*
- [6] *Product Compatibility Reference, Avaya CS1000, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013.*
- [7] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 4, October 2014*
- [8] *Maintaining and Troubleshooting Avaya Aura® Session Manager, Release 6.3, Issue 6, December 2014*
- [9] *Administering Avaya Aura® System Manager, Release 6.3, Issue 5, October 2014*
- [10] *Avaya Session Border Controller for Enterprise Overview and Specification, Release 6.3, Issue 3, May 2014.*
- [11] *Upgrading Avaya Session Border Controller for Enterprise, Release 6.3, Issue 5, Oct 2014.*

Product services for Bell Canada SIP Trunking Services may be found at:

[http://www.bell.ca/enterprise/EntPrd\\_SIP\\_Trunking.page](http://www.bell.ca/enterprise/EntPrd_SIP_Trunking.page)

---

**©2015 Avaya Inc. All Rights Reserved.**

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

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