



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Virgin Media SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura[®] Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2.1 – Issue 1.0

Abstract

These Application Notes describe the procedure for configuration of the Virgin Media SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura[®] Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2.1.

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

Virgin Media SIP Trunk Service provides PSTN access via SIP trunks between the enterprise and the Virgin Media SIP Trunk Service's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	9
5.	Configure Avaya Communication Server 1000.....	11
5.1.	Log into Communication Server 1000 System	11
5.1.1.	Log into System Manager and Element Manager (EM).....	11
5.1.2.	Log into Call Server by Using Overlay Command Line Interface (CLI).....	13
5.2.	Administer IP Telephony Node	14
5.2.1.	Obtain Node IP address	14
5.2.2.	Administer Terminal Proxy Server (TPS)	16
5.2.3.	Administer Quality of Service (QoS)	17
5.2.4.	Synchronize New Configuration.....	17
5.3.	Administer Voice Codec	19
5.3.1.	Enable Voice Codec G.711, G.729.....	19
5.3.2.	Enable Voice Codec on Media Gateways.....	20
5.4.	Zones and Bandwidth Management.....	21
5.4.1.	Create Zone for IP Phones (Zone 10)	21
5.4.2.	Create Zone for Virtual SIP Trunk (Zone 255)	22
5.5.	Administer SIP Trunk Gateway	23
5.5.1.	Integrated Services Digital Network (ISDN).....	23
5.5.2.	Administer SIP Trunk Gateway to Avaya Communication Server 1000	25
5.5.3.	Administer Virtual D-Channel.....	27
5.5.4.	Administer Virtual Super-Loop	31
5.5.5.	Administer Virtual SIP Routes	31
5.5.6.	Administer Virtual Trunks.....	33
5.5.7.	Administer Calling Line Identification Entries.....	36
5.5.8.	Enable External Trunk to Trunk Transfer.....	38
5.6.	Administer Dialing Plans	39
5.6.1.	Define ESN Access Codes and Parameters (ESN).....	39
5.6.2.	Associate NPA and SPN Call to ESN Access Code 1	40
5.6.3.	Digit Manipulation Block Index (DMI).....	41
5.6.4.	Route List Block (RLB) (RLB 14)	42
5.6.5.	Inbound Call – Incoming Digit Translation Configuration	44
5.6.6.	Outbound Call - Special Number Configuration	46
5.7.	Administer a Phone	47
5.7.1.	Phone creation.....	47
5.7.2.	Enable Privacy for the Phone.....	48
5.7.3.	Enable Call Forward for Phone.....	49
6.	Configure Avaya Aura [®] Session Manager	51

6.1.	Avaya Aura® System Manager Login and Navigation.....	52
6.2.	Specify SIP Domain	54
6.3.	Add Location.....	54
6.4.	Configure Adaptations	56
6.5.	Add SIP Entities.....	57
6.5.1.	Configure Session Manager SIP Entity	58
6.5.2.	Configure Communication Server 1000 SIP Entity.....	59
6.5.3.	Configure Avaya SBCE SIP Entity	60
6.6.	Add Entity Links	61
6.7.	Configure Time Ranges	63
6.8.	Add Routing Policies	63
6.9.	Add Dial Patterns	65
7.	Configure Avaya Session Border Controller for Enterprise	68
7.1.	Log into the SBCE	68
7.2.	Global Profiles.....	69
7.2.1.	Configure Server Interworking - Avaya Site	69
7.2.2.	Configure Server Interworking – Virgin Media Site	70
7.2.3.	Configure URI Groups.....	72
7.2.4.	Configure Routing – Avaya Site.....	73
7.2.5.	Configure Routing – Virgin Media Site.....	74
7.2.6.	Configure Signaling Manipulation	76
7.2.7.	Configure Server – Session Manager	77
7.2.8.	Configure Server – Virgin Media SBC A.....	79
7.2.9.	Configure Server – Virgin Media SBC B.....	83
7.2.10.	Configure Topology Hiding – Avaya Site	87
7.2.11.	Configure Topology Hiding – Virgin Media Site.....	88
7.3.	Domain Policies	89
7.3.1.	Create Signaling Rules.....	89
7.3.2.	Create End Point Policy Groups	91
7.3.3.	Create Session Policy.....	93
7.4.	Device Specific Settings.....	95
7.4.1.	Manage Network Settings.....	95
7.4.2.	Create Media Interfaces	97
7.4.3.	Create Signaling Interfaces	98
7.4.4.	Configuration End Point Flows	99
7.4.5.	Create Session Flows	104
8.	Virgin Media SIP Trunk Service Configuration.....	105
9.	Verification Steps.....	106
9.1.	General	106
9.2.	Verification of an Active Call on Communication Server 1000.....	106
9.3.	Protocol Trace	108
10.	Conclusion	109
11.	References.....	110
12.	Appendix A: SigMa Script.....	111

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 and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2.1 with Virgin Media SIP Trunk Service. Virgin Media SIP Trunk Service provides PSTN access via SIP Trunks between the enterprise and the Virgin Media SIP Trunk Service's network as an alternative to legacy analog or digital trunks.

2. General Test Approach and Test Results

CS1000 was connected to Avaya SBCE via Session Manager by using SIP Trunks. Avaya SBCE was connected to Virgin Media SIP Trunk Service's network via SIP trunks. Various call types were made from CS1000 to Virgin Media SIP Trunk Service and vice versa to verify 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:

- General call processing between CS1000 and Virgin Media SIP Trunk Service, including the following:
 - Codec/ptime (G.711 a-law/10ms, G.711 mu-law/10ms, and G.729/10ms), no Voice Activity Detection (VAD).
 - Calling Line Identification Display (CLID).
 - Ring-back tone.
 - Speech (audio) path.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya IP Softphone 2050.
- Dialing plan support: local, long distance, international, outbound toll-free, UK Emergency 999, 112, 18000-Text Direct.
- Fallback outbound calls to both Virgin Media SBC A and SBC B.
- User features such as Hold and Resume, Call Park, Call Waiting.

- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference). Call redirection was performed from both ends. Note: Virgin Media SIP Trunk Service supports Diversion Header for off-net call forwarding.
- Response to SIP OPTIONS queries.
- Response to incomplete call attempts and trunk errors.
- Fax T.38 and G.711 pass-through.
- Inbound and outbound long hold time call stability.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF (RFC2833) in inbound and outbound calls.
- SIP Transport UDP, port 5060.
- Voicemail navigation for inbound and outbound calls.
- CS1000 Mobile-X feature.
- Authentication Support.

The following are items not supported or not tested:

- Inbound toll-free, Operator-assisted call, Local directory.
- Do not Disturb feature.
- Inbound call with G.729 as the first priority.
- DTMF transmission from/to Avaya PBX – In-band.

The following assumptions were made for the compliance tested configuration:

- CS1000 R7.6 software with latest patches.
- Virgin Media SIP Trunk Service provides support to setup, configure and troubleshoot on carrier switch during testing execution.

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

- Calls were checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing were checked.
- Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
- Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
- 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.
- The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
- The call server maintenance terminal window was open during the test execution for the monitoring of BUG(s), ERROR and AUD messages (See **Section 5.1.2**).
- Speech path was checked before and after calls were put on/off hold from each end.
- Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs (Voice Gateways) were released when calls were ended (See SIP Trunk monitoring in **Section 9.2**).

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:

- **Virgin Media could not change the configuration during this testing** - If Virgin Media change the configuration during this testing, it would impact other solutions. Therefore, some test cases which required Virgin Media to change the configuration could not be executed (such as inbound call with G.729 as the first priority, DTMF transmission from/to Avaya PBX – In-band) even both Virgin Media and Avaya supported them.
- **The Calling Line Identification Display (CLID) was not available after hold/resume** – If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed. This is a CS1000 known limitation.
- **The CLID was not correctly displayed after call redirection/ blind/consultative transfers** – After call redirection, namely blind/consultative transfers, was completed with two way voice paths, the CLID on the transferee’s telephone was not updated accordingly. This is known CS1000 limitation.
- **The CLID was not displayed correctly for outbound call to Canada phone numbers** - Virgin Media system was set up to send CLID as long as it passes screening as a Presentation Number. There are some (very few now) operators who do not support Presentation Number services and in those unusual cases the Network Number (0118XXX4140) might be presented. Since Virgin Media used the Telco network to pass the Presentation Number through the DevConnect Lab in Belleville, Canada, the Telco might insert the Network Number (0118XXX4140) on the CLID.
- **The CLID was always displayed on Emergency agent phone as 0118XXX4140 for outbound call to UK Emergency (999/112)** - The CLID was always displayed as 0118XXX4140 for testing purpose. This was the expected number by the Emergency service during this testing.
- **Off-net blind transfer did not work properly** - In a scenario where PSTN1 phone called an Avaya Communication Server 1000 phone, the user could not press the transfer button on the Avaya Communication Server 1000 phone to complete a blind transfer to PSTN2. In this particular scenario, SIP UPDATE support was required on the Communication Server 1000 for blind transfer, but for some reason, the SIP UPDATE on the PSTN-to-SIP gateway that Virgin Media service used for this interoperability testing did not work properly. In order to resolve this, plug-in 501 was enabled on the Communication Server 1000 to allow blind transfer to work without the UPDATE method (On CS1000 Element Manager, select **System** → **Software** → **Plug-ins** and then click on number **501** to enable plug-in 501). After the user was able to press the transfer button on the Avaya Communication Server 1000 to complete blind transfer, the PSTN1 phone still could not hear ring-back-tone from the PSTN2. In order to resolve this, the Avaya SBCE was configured to translate the SIP 183 with SDP, to SIP 180 without SDP (see **Sections 7.2.1 and 7.3.1**), so that PSTN1 could hear the local ring-back-tone. However, if this translation was performed on Avaya SBCE, early media was not

supported in this configuration. Please communicate the specific site requirement to Virgin Media SIP Trunk Service before implementing this translation on the Avaya SBCE.

- **SIP Telephone Conference** – During a conference call hosted by a 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.

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 Virgin Media SIP Trunk Service, please contact customer service or visit: <http://www.virginmediabusiness.co.uk/Products-and-solutions/Telephony-Solutions/SIP-Trunking/> .

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance test between CS1000 and Virgin Media SIP Trunk Service. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked and replaced with fictitious IP addresses throughout the document.

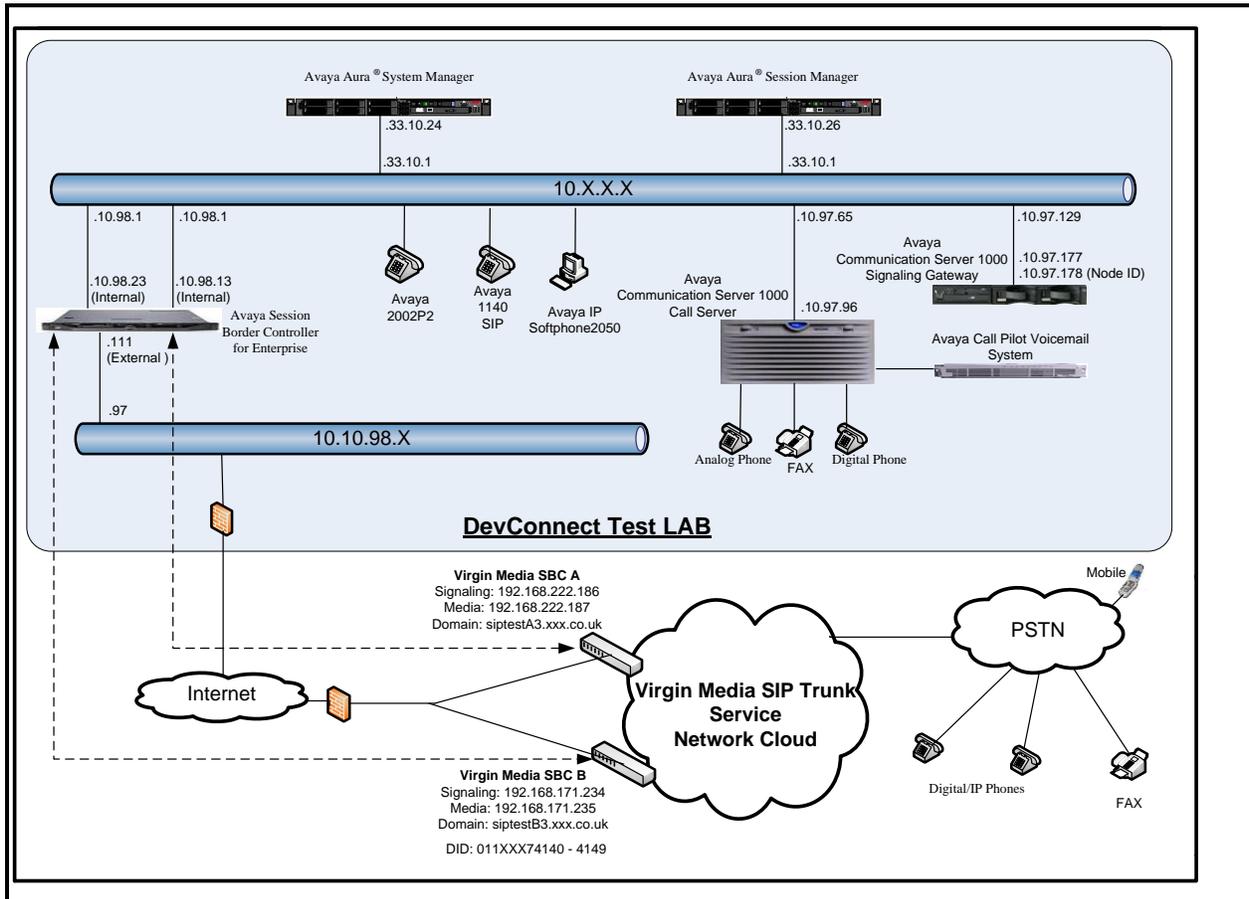


Figure 1- Network diagram for Avaya and Virgin Media SIP Trunk Service

4. Equipment and Software Validated

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

Avaya systems:

Equipment/Software	Release/Version
Avaya Communication Server 1000 (CPPM)	Call Server: 765 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 S8800 Server	Avaya Aura [®] Session Manager R6.3.7 – 6.3.7.0.637008
Avaya S8800 Server	Avaya Aura [®] System Manager R6.3.9 Build No. - 6.3.0.8.5682-6.3.8.4417 Software Update Revision No: 6.3.9.1.2538
Avaya Session Border Controller for Enterprise	6.2.1 Q18
Avaya Phones: 2002 p2 (UNISim) 1140E SIP	0604DCO 04.03.12.00
Avaya 3904 Digital Phone	N/A
Avaya IP Softphone 2050	4.04.0067
Analog Symphony 2000	N/A
HP Office jet 4500 Fax	N/A

Virgin Media SIP Trunk Service systems:

System	Software
Genband Softswitch with Q20 Network SBC	8.1

Additional patch lineup for the configuration is listed as follows:

Call Server: 7.65 P+ GA plus latest DEPLIST – CPL_7.6S4.zip (X2107.65P)

Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_4.ntl (7.65.16.00)

CS1000 Signaling Server patch list:

```
[admin@car3-ssg-carrier ~]$ pstat
```

```
Product Release: 7.65.16.00
```

```
In system patches: 1
```

```
PATCH# NAME IN_SERVICE DATE SPECINS TYPE RPM
```

```
37 p31484_1 Yes 20/10/14 NO FRU cs1000-shared-general-7.65.16-00.i386
```

```
In System service updates: 26
```

```
PATCH# IN_SERVICE DATE SPECINS REMOVABLE NAME
```

```
9 Yes 20/10/14 YES YES cs1000-dmWeb-7.65.16.22-1.i386.000
```

```
12 Yes 19/10/14 NO YES cs1000-linuxbase-7.65.16.22-02.i386.000
```

13	Yes	20/10/14	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
14	Yes	20/10/14	NO	YES	cs1000-Jboss-Quantum-7.65.16.22-3.i386.000
15	Yes	20/10/14	YES	YES	cs1000-patchWeb-7.65.16.22-1.i386.000
16	Yes	20/10/14	NO	YES	cs1000-shared-carrdtct-7.65.16.21-01.i386.000
17	Yes	20/10/14	NO	YES	cs1000-shared-tpselect-7.65.16.21-01.i386.000
18	Yes	20/10/14	NO	YES	cs1000-dbcom-7.65.16.21-00.i386.000
19	Yes	20/10/14	NO	YES	cs1000-shared-xmsg-7.65.16.21-00.i386.000
20	Yes	20/10/14	NO	YES	cs1000-mscAnnc-7.65.16.21-02.i386.001
21	Yes	20/10/14	NO	YES	cs1000-mscAttn-7.65.16.21-04.i386.001
22	Yes	20/10/14	NO	YES	cs1000-mscConf-7.65.16.21-02.i386.001
23	Yes	20/10/14	NO	YES	cs1000-mscMusc-7.65.16.21-02.i386.001
24	Yes	20/10/14	NO	YES	cs1000-mscTone-7.65.16.21-03.i386.001
25	Yes	20/10/14	NO	YES	cs1000-gk-7.65.16.21-01.i386.000
26	Yes	20/10/14	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
27	Yes	20/10/14	YES	YES	tzdata-2013c-2.el5.i386.001
28	Yes	20/10/14	YES	YES	cs1000-tps-7.65.16.21-11.i386.000
29	Yes	20/10/14	NO	YES	cs1000-sps-7.65.16.21-8.i386.000
30	Yes	20/10/14	NO	YES	cs1000-shared-omm-7.65.16.21-2.i386.000
31	Yes	20/10/14	YES	YES	cs1000-baseWeb-7.65.16.22-1.i386.000
32	Yes	20/10/14	YES	YES	cs1000-csoneksvrmgr-7.65.16.22-1.i386.000
33	Yes	20/10/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
34	Yes	20/10/14	YES	YES	cs1000-vtrk-7.65.16.22-4.i386.000
35	Yes	20/10/14	NO	YES	cs1000-cppmUtil-7.65.16.22-1.i686.000
36	Yes	20/10/14	YES	YES	cs1000-oam-logging-7.65.16.22-3.i386.000

5. Configure Avaya Communication Server 1000

These Application Notes use the Incoming Digit Translation feature to receive calls and the Special Number (SPN) features to route calls from the CS1000 to the PSTN, via SIP trunks to the Virgin Media SIP Trunk Service network.

These Application Notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 11**.

The procedures below describe the configuration details for configuring the CS1000.

5.1. Log into Communication Server 1000 System

5.1.1. Log into System Manager and Element Manager (EM)

Open an instance of a web browser and connect to the 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**.

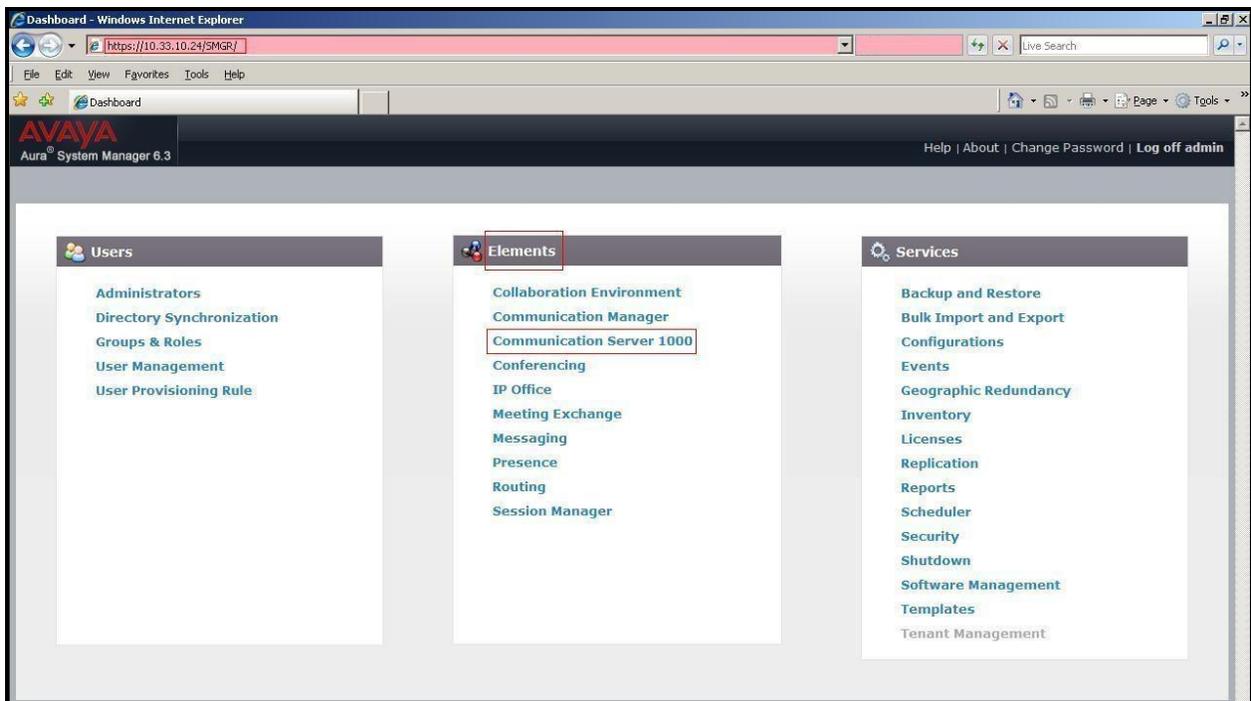


Figure 2 –System Manager Home Screen

The **Avaya Communication Server 1000 Management** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in red box below:

The screenshot shows the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and links for 'Help | About | Change Password | Log off admin'. The left sidebar contains a tree view with categories like 'Network', 'CS 1000 Services', 'User Services', and 'Security'. The main content area displays the 'Elements' management screen. At the top, it shows 'Host Name: 10.33.10.24' and 'User Name: admin'. Below this is a search bar with 'Search' and 'Reset' buttons. A table lists several elements, with the second row, 'EM on car3-sip-ucm', highlighted in red. The table columns are: Element Name, Element Type, Release, Address, and Description.

Element Name	Element Type	Release	Address	Description
smgr.bwdev.com (primary)	Base OS	7.6	10.33.10.24	Base OS element
EM on car3-sip-ucm	CS1000	7.6	10.10.97.96	New element
car3-cores.bwdev.com (member)	Linux Base	7.6	10.10.97.179	Base OS element
car3-sip-ucm.bwdev.com (member)	Linux Base	7.6	10.10.97.175	Base OS element
car3-ssq-carrier.bwdev.com (member)	Linux Base	7.6	10.10.97.177	Base OS element
10.10.97.97	Media Gateway Controller	7.6	10.10.97.97	New element

Figure 3 – Communication Server 1000 Management

Log into the CS1000 using an appropriate **User ID** and **Password**.

The screenshot shows the Avaya Communication Server 1000 Log In screen. The top header is red with the Avaya logo on the right. Below the header, there is a login form with two input fields: 'User ID' containing 'admin' and 'Password' containing a masked password. A 'Log In' button is positioned below the password field. To the left of the form, there is a small text block providing instructions and an important note about account authentication. At the bottom left, there is a link for 'Go to central login for Single Sign-On', and at the bottom right, there is a 'Change Password' link.

Figure 4 – Communication Server 1000 Log In Screen

The CS1000 Element Manager **System Overview** page is displayed as shown in **Figure 5**.

IP Address: 10.10.97.96
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 765 P +



Figure 5 – Element Manager System Overview

5.1.2. Log into Call Server by Using Overlay Command Line Interface (CLI)

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

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

```
login as: ← Enter an account with administrator credentials
```

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@10.10.97.177's password: ← Enter the password
```

```
Last login: Mon Oct 20 07:20:18 2014 from 10.10.98.78
```

```
[admin@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 #08 LOGGED IN ADMIN 07:39 10/20/2014
```

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.

>

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

5.2. Administer 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 3000) in CS1000 IP network to work with Virgin Media SIP Trunk Service. 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 in **Figure 6**.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with the following items: UCM Network Services, Home, Links, Virtual Terminals, System (highlighted), Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network (highlighted), Nodes: Servers, Media Cards (highlighted), Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), and QoS Thresholds. The main content area is titled "CS1000 Element Manager" and shows the "IP Telephony Nodes" configuration page. The page header indicates "Managing: 10.10.97.96 Username: admin" and "System » IP Network » IP Telephony Nodes". Below the header, there is a table of IP Telephony Nodes. The table has columns for Node ID, Components, Enabled Applications, ELAN IP, Node/TLAN IPv4, Node/TLAN IPv6, and Status. Two nodes are listed: Node ID 3000 (Components: 1, Enabled Applications: LTPS, Gateway (SIPGw), ELAN IP: -, Node/TLAN IPv4: 10.10.97.178, Node/TLAN IPv6: -, Status: Synchronized) and Node ID 3002 (Components: 1, Enabled Applications: SIP Line, LTPS, ELAN IP: -, Node/TLAN IPv4: 10.10.97.176, Node/TLAN IPv6: -, Status: Synchronized). The table also includes buttons for Add, Import, Export, and Delete, and a Print/Refresh link. At the bottom of the table, there are checkboxes for "Show: Nodes" (checked), "Component servers and cards" (unchecked), and "IPv6 address" (checked).

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
3000	1	LTPS, Gateway (SIPGw)	-	10.10.97.178	-	Synchronized
3002	1	SIP Line, LTPS	-	10.10.97.176	-	Synchronized

Figure 6 – IP Telephony Nodes

The **Node Details** screen is displayed in **Figure 7** with the IP address of the CS1000 node. **Call server IP address: 10.10.97.96**. The **Node IPv4 address 10.10.97.178** is a virtual address which corresponds to the **TLAN IPv4 address 10.10.97.177** 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.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: IPv4 only
 IPv4 and IPv6

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

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

Node IPv6 address:

* Required Value.

Associated Signaling Servers & Cards

Select to add [Print](#) | [Refresh](#)

<input type="checkbox"/>	Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/>	car3-ssg-carrier	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: IPv6 address

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

Figure 7 –Node Details 1

The **Node Details** screen is displayed in **Figure 8** with the IP Telephony Node Properties and Applications.

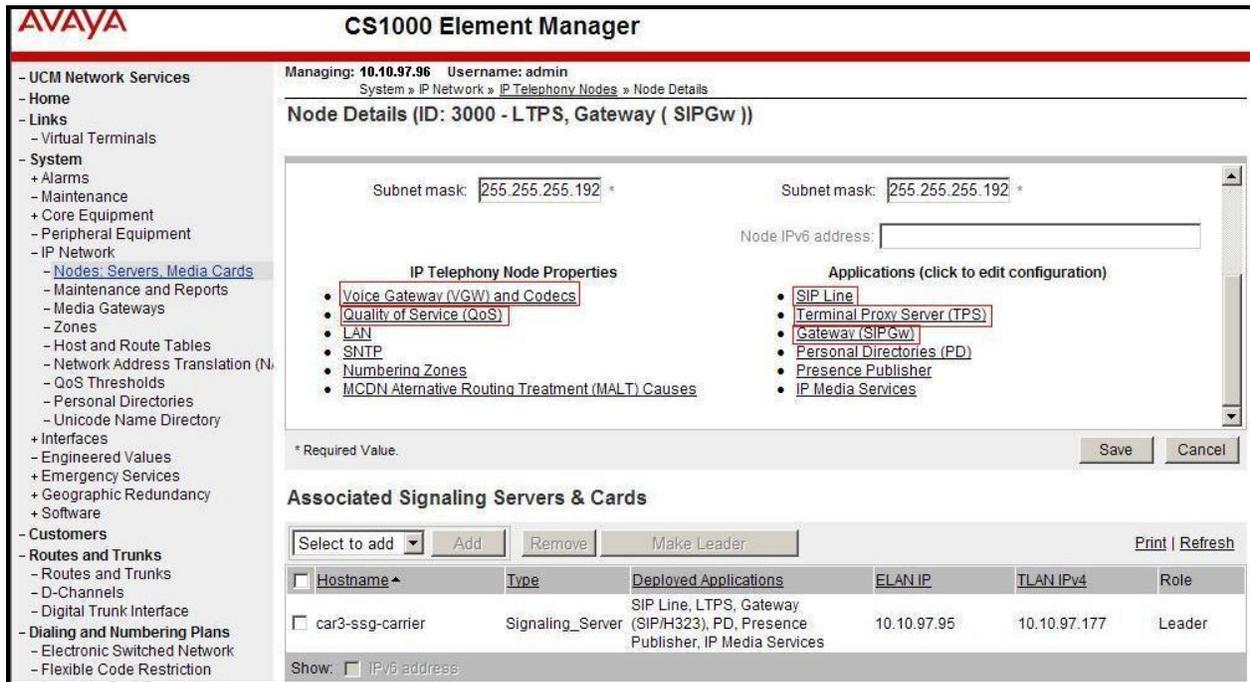


Figure 8 –Node Details 2

5.2.2. Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in **Figure 8**. Check the **UNISim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click the **Save** button as shown in **Figure 9**.

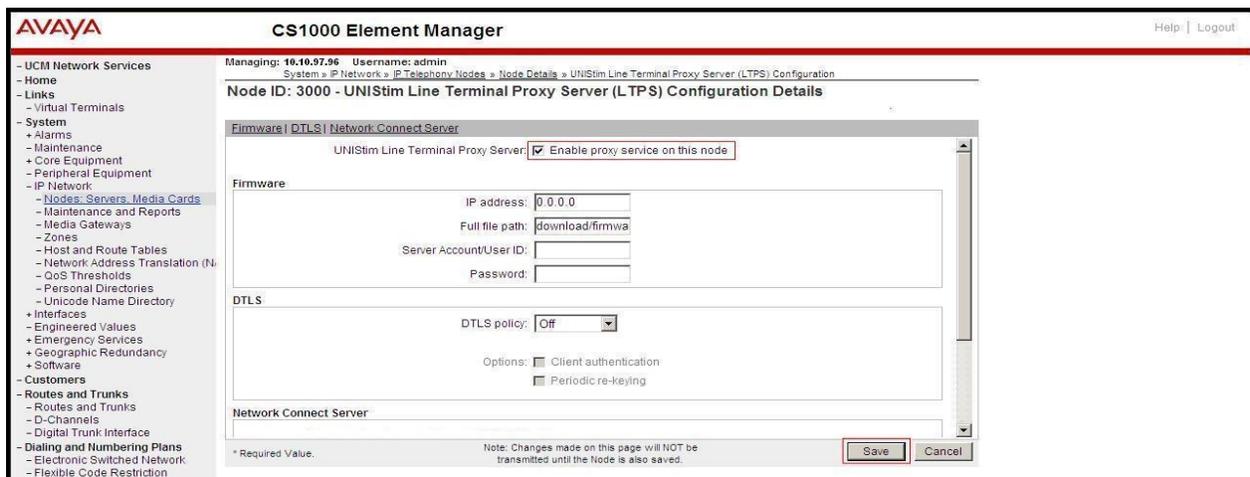


Figure 9 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 8**. The default Diffserv values are as shown in **Figure 10**. Click on the **Save** button.

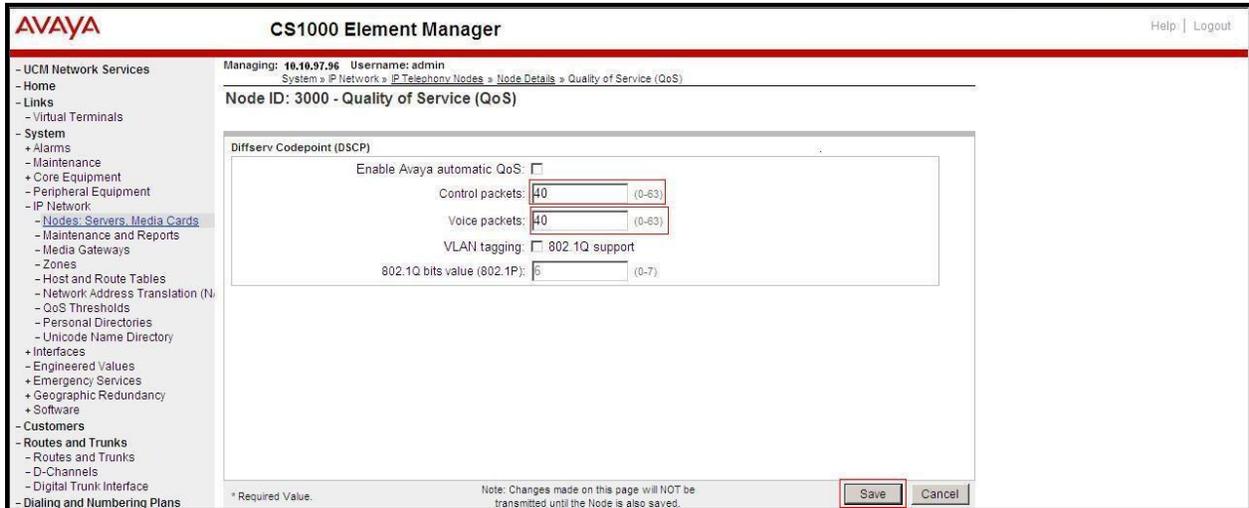


Figure 10 – QoS Configuration Details

5.2.4. Synchronize New Configuration

Continuing from **Section 5.2.3**, return to the **Node Details** page (**Figure 7**) and click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now**.



Figure 11 – Node Saved Screen

The **Synchronize Configuration Files (Node ID <3000>)** screen is displayed. Check the **car3-ssg-carrier** checkbox and click on **Start Sync**. When the synchronization completes, check the **car3-ssg-carrier** checkbox and click on the **Restart Applications**.

Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <3000>)

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

Start Sync Cancel Restart Applications Print Refresh

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	car3-ssg-carrier	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	Sync required

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

Figure 12 – Node Synchronized Screen

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G.711, G.729

Select **IP Network** → **Nodes: Servers, Media Cards** from the left pane and on the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed (see **Section 5.2.1** for more details). On the **Node Details** page shown in **Figure 8**, click on **Voice Gateway (VGW) and Codecs**.

Virgin Media SIP Trunk Service supports **G.711 a-law**, **G.711 mu-law** and **G.729** with **Voice payload size 10 milliseconds per frame**. Uncheck **Voice Activity Detection (VAD)** checkbox. Click on the **Save** button.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left-hand navigation pane shows a tree structure with 'IP Network' expanded to 'Nodes: Servers, Media Cards'. The main content area is titled 'Node ID: 3000 - Voice Gateway (VGW) and Codecs' and has three tabs: 'General', 'Voice Codecs', and 'Fax'. The 'Voice Codecs' tab is selected. The configuration area shows three codec settings:

- Codec G711:** Enabled (required). Voice payload size: 10 (milliseconds per frame). Voice playback (jitter buffer) delay: 20 (Nominal) / 40 (Maximum) (milliseconds). A note states: 'Maximum delay may be automatically adjusted based on nominal settings.' The Voice Activity Detection (VAD) checkbox is unchecked.
- Codec G722:** Enabled. Voice payload size: 20 (milliseconds per frame). Voice playback (jitter buffer) delay: 40 (Nominal) / 80 (Maximum) (milliseconds). A note states: 'Maximum delay may be automatically adjusted based on nominal settings.'
- Codec G729:** Enabled. Voice payload size: 10 (milliseconds per frame). Voice playback (jitter buffer) delay: 20 (Nominal) / 40 (Maximum) (milliseconds).

At the bottom of the configuration area, there is a note: '* Required Value.' and another note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are 'Save' and 'Cancel' buttons at the bottom right.

Figure 13 – Voice Gateway and Codec Configuration Details

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 in **Figure 13**, select **IP Network** → **Media Gateways**. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page. In the following screen, scroll down to select the **Codec G711** and **Code G729A** with **Voice payload size 10 ms/frame** and uncheck **VAD** as shown in **Figure 14**. Scroll down to the bottom of the page and click on the **Save** button (not shown).

AVAYA CS1000 Element Manager

- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation (NAT)
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ 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

- 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 10 (ms/frame)

Voice playout (jitter buffer) nominal delay 20

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 40

Modifications may cause changes to dependent settings

VAD

- Codec G729A Select

Codec name G729A

Voice payload size 10 (ms/frame)

Voice playout (jitter buffer) nominal delay 20

Figure 14 – Media Gateways Configuration Details

5.4. Zones and Bandwidth Management

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

5.4.1. Create Zone for IP Phones (Zone 10)

The following figures show how to configure a zone for VGW and IP phones for bandwidth management purposes. The bandwidth strategy can be adjusted to preference.

Select **IP Network** → **Zones** from the left pane (not shown), click on **Bandwidth Zones** as shown in **Figure 15**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The main content area is titled 'ZONES' and contains the following text: 'Zones are used to group related information for either bandwidth or dial plan numbering purposes.' Below this, there are two sections: 'Bandwidth Zones' and 'Numbering Zones'. The 'Bandwidth Zones' section states: 'Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.' The 'Numbering Zones' section states: 'Numbering zones are used to route calls through a centralized call server.'

Figure 15 – Zones Page

The **Bandwidth Zones** screen is displayed as shown in **Figure 16**. Click **Add** to create a new zone for IP Phones.

The screenshot shows the AVAYA CS1000 Element Manager interface for the 'Bandwidth Zones' page. The page title is 'Bandwidth Zones'. Below the title, there are several buttons: 'Add...', 'Edit...', 'Import...', 'Export', 'Maintenance...', and 'Delete'. A 'Refresh' button is located on the right side. Below the buttons is a table with the following columns: 'Zone', 'Intrazone Bandwidth', 'Intrazone Strategy', 'Interzone Bandwidth', 'Interzone Strategy', 'Resource Type', 'Zone Intent', and 'Description'. The table contains five rows of data:

Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1000000	BQ	1000000	BQ	SHARED	MO	
2	1000000	BQ	1000000	BQ	SHARED	MO	
3	1000000	BB	1000000	BB	SHARED	MO	
4	1000000	BQ	1000000	BQ	SHARED	MO	
5	1000000	BQ	1000000	BQ	SHARED	VTRK	

Figure 16 – Bandwidth Zones

Select and input the values as shown below (in the red boxes) in **Figure 17**, and click on the **Submit** button.

- **Intrazone Bandwidth (INTRA_BW): 1000000.**
- **Intrazone Strategy (INTRA_STGY):** Set codec for local calls. Select **Best Quality (BQ)** to use G.711 as the first priority codec for negotiation or select **Best Bandwidth (BB)** to use G.729 as the first priority codec for negotiation.
- **Interzone Bandwidth (INTER_BW): 1000000.**
- **Interzone Strategy (INTER_STGY):** Set codec for the calls over trunk. Select **Best Quality (BQ)** to use G.711 as the first priority codec for negotiation or select **Best Bandwidth (BB)** to use G.729 as the first priority codec for negotiation.
- **Zone Intent (ZBRN):** Select **MO (MO)** for IP phones, and VGW.

The screenshot shows the 'Zone Basic Property and Bandwidth Management' configuration page for Zone 10. The form is structured as follows:

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):	

Buttons: Submit, Refresh, Cancel

Figure 17 – Bandwidth Management Configuration Details – IP phone

5.4.2. Create 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** for virtual trunk as shown in **Figure 18** and then click on the **Submit** button.

The screenshot shows the 'Zone Basic Property and Bandwidth Management' configuration page for Zone 255. The form is structured as follows:

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):	

Buttons: Submit, Refresh, Cancel

Figure 18 – Bandwidth Management Configuration Details – Virtual SIP trunk

5.5. Administer SIP Trunk Gateway

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

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**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane is expanded to 'Customers'. The main content area displays a table with the following data:

Customer Number	Total Routes	Total Trunks
1 00	7	125
2 01	0	0

Figure 19 – Customer – ISDN Configuration 1

The system can support more than one customer with different network settings and options. The **Customer Details** page will appear. Select the **Feature Packages** option from **Customer Details** page.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane is expanded to 'Customers' and then to 'Customer 00' and 'Customer Details'. The main content area displays a list of configuration options, with 'Feature Packages' highlighted.

Figure 20 – Customer – ISDN Configuration 2

The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 21** 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 on the **Save** button (not shown).

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
 Customers » Customer 00 » Customer Details » Feature Packages

Feature Packages

+ Do Not Disturb Individual	Package: 9
+ End-to-End Signaling	Package: 10
+ Message Waiting Center	Package: 46
+ New Flexible Code Restriction	Package: 49
+ Set Relocation	Package: 53
+ Network Alternate Route Selection	Package: 58
+ Distinctive Ringing	Package: 74
+ Departmental Listed Directory Number	Package: 76
+ Command Status Link	Package: 77
+ Pretranslation	Package: 92
+ Dialed Number Identification System	Package: 98
+ Malicious Call Trace	Package: 107
+ Incoming Digit Conversion	Package: 113
+ Directed Call Pickup	Package: 115
+ Enhanced Music	Package: 119
+ Station Camp-On	Package: 121
+ Integrated Digital Access	Package: 122
+ Digital Private Network Signaling System 1	Package: 123
+ Flexible Tones and Cadences	Package: 125
+ Multifrequency Compelled Signaling	Package: 128
+ International Supplementary Features	Package: 131
+ Enhanced Night Service	Package: 133
- Integrated Services Digital Network	Package: 145

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network:

- Virtual private network identifier: (1 - 16383)

- Private network identifier: (1 - 16383)

- Node DN:

Multi-location business group: (0 - 65535)

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

Figure 21 – Customer – ISDN Configuration 3

5.5.2. Administer SIP Trunk Gateway to Avaya Communication Server 1000

Select **IP Network** → **Nodes: Servers, Media Cards** from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as shown in **Figure 8, Section 5.2.1**.

On the **Node Details** screen, 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 as shown in **Figure 22**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of Avaya SBCE (in **Section 6.2**, and **6.6**).

The screenshot displays the 'AVAYA CS1000 Element Manager' interface. The left sidebar shows a navigation tree with 'Nodes: Servers, Media Cards' selected. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. The 'General' tab is active, showing the following configuration fields:

- Vtrk gateway application:** SIP Gateway (SIPGw) (highlighted in red)
- SIP domain name:** bwdev7.com (highlighted in red)
- Local SIP port:** 5060 (highlighted in red)
- Gateway endpoint name:** car3-ssg-carrier (highlighted in red)
- Application node ID:** 3000 (highlighted in red)
- Enable gateway service on this node:**
- Gateway password:** (empty field)
- Enable failsafe NRS:**

The 'Virtual Trunk Network Health Monitor' section includes a checkbox for 'Monitor IP addresses (listed below)', a 'Monitor IP:' field with an 'Add' button, and a 'Monitor addresses:' list with a 'Remove' button. A note at the bottom states: 'Note: FailSafe NRS will be enabled only on those servers in the node where NRS application is not deployed.' The bottom of the screen features a 'Save' button and a 'Cancel' button.

Figure 22 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown in **Figure 23**. Enter the internal IP address of Session Manager in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **UDP** for **Transport protocol**. This should be matched in the configuration of Session Manager (see to **Section 6.5.1**). Uncheck the **Support registration** checkbox.

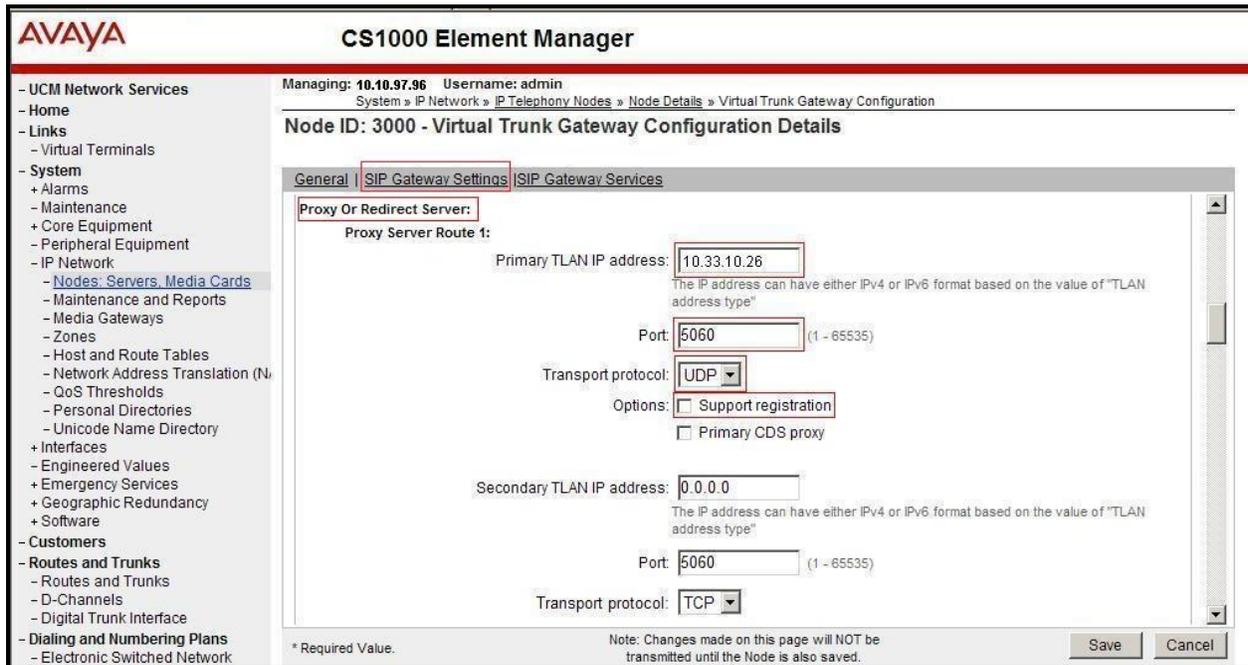


Figure 23 – Virtual Trunk Gateway Configuration Details

On the same page as shown in **Figure 23**, scroll down to the **SIP URI Map** section. Under **Public E.164 domain names**, enter the following:

- **National:** leave this SIP URI field blank.
- **Subscriber:** leave this SIP URI field blank.
- **Special Number:** leave this SIP URI field blank.
- **Unknown:** leave this SIP URI field blank.

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

- **UDP:** leave this SIP URI field blank.
- **CDP:** leave this SIP URI field blank.
- **Special Number:** leave this SIP URI field blank.
- **Vacant number:** leave this SIP URI field blank.
- **Unknown:** leave this SIP URI field blank.

The remaining fields can be left at their default values as shown in **Figure 24**. Click on the **Save** button.

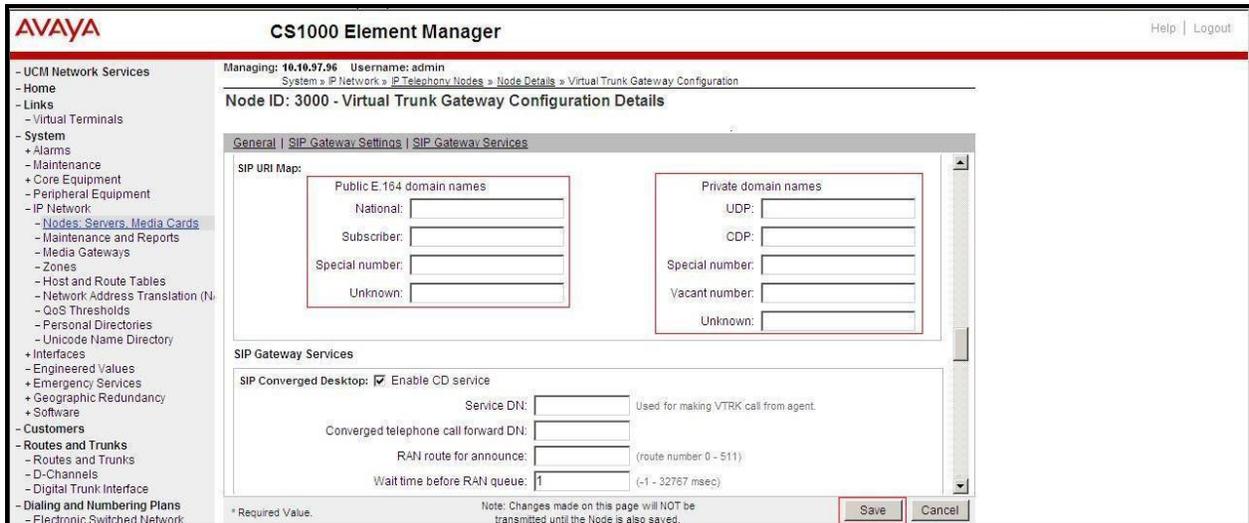


Figure 24 – Virtual Trunk Gateway Configuration Details

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

5.5.3. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** (not shown) 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 and type **DCH** as shown in **Figure 25**. Click on the **to Add** button.

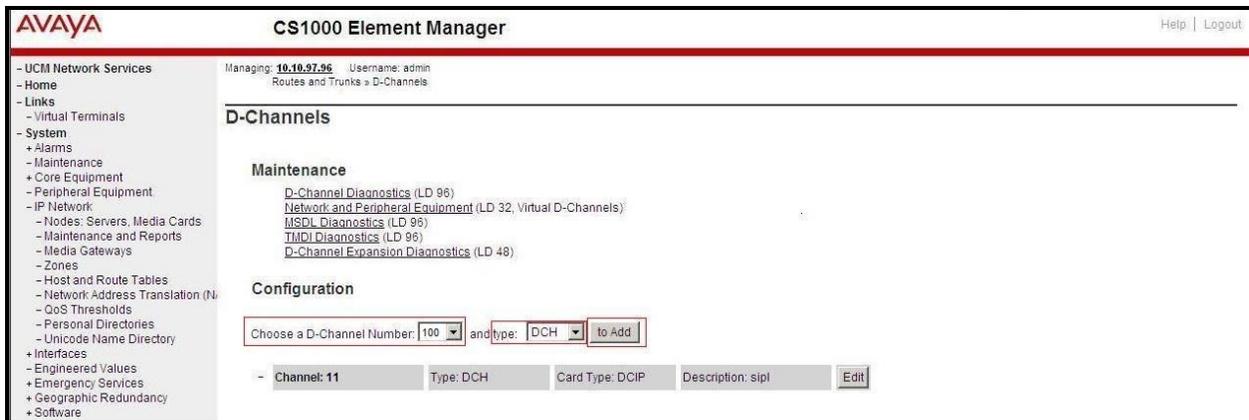


Figure 25 – D-Channels

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 26**. 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 in **Figure 26**. Other fields are left as default.

AVAYA CS1000 Element Manager

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> more PRI
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	1800 Range: 0 - 3700
+ Basic options (BSCOPT)	
- Advanced options (ADVOPT)	
- Layer 3 call control message count per 5 second time interval:	300 Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms:	1
- Map channel number to timeslots on a PRI2 loop:	<input checked="" type="checkbox"/>
- H323 Overlap Signaling Settings (H323)	
- Overlap Receiving:	<input type="checkbox"/>
- Overlap Sending:	<input type="checkbox"/>
--Overlap Timer:	<input type="text"/>
- Multilocation Business Group Allowed:	<input checked="" type="checkbox"/>
- Network Attendant Service Allowed:	<input checked="" type="checkbox"/>
+ Link Access Protocol for D-channel (LAPD)	
+ Feature Packages	

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

Figure 26 – D-Channel Configuration

Click on **Basic Options (BSCOPT)** and click on the **Edit** button on the **Remote Capabilities** field as shown in **Figures 27**.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories such as UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers, Routes and Trunks, 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, and Login Options. The main content area is titled 'D-Channel Configuration' and includes the following fields and options:

- Action Device And Number (ADAN): DCH
- D channel Card Type: DCIP
- Designator: VoIP
- Recovery to Primary:
- PRI loop number for Backup D-channel:
- User: Integrated Services Signaling Link Dedicated (ISLD)
- Interface type for D-channel: Meridian Meridian1 (SL1)
- Country: ETS 300 =102 basic protocol (ETSI)
- D-Channel PRI loop number:
- Primary Rate Interface: more PRI
- Secondary PRI2 loops:
- Meridian 1 node type: Slave to the controller (USR)
- Release ID of the switch at the far end: 25
- Central Office switch type: 100% compatible with Bellcore standard (STD)
- Integrated Services Signaling Link Maximum: 4000 (Range: 1 - 4000)
- Signalling server resource capacity: 1800 (Range: 0 - 3700)
- Primary D-channel for a backup DCH: (Range: 0 - 254)
- PINX customer number:
- Progress signal:
- Calling Line Identification:
- Output request Buffers: 32
- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)
- Channel Negotiation option: No alternative acceptable, exclusive. (1)
- Remote Capabilities: **Edit**
- B channel Service messaging:

At the bottom of the configuration area, there are buttons for Submit, Refresh, Delete, and Cancel. The footer of the page reads 'Copyright © 2002-2011 Avaya Inc. All rights reserved.'

Figure 27 – D-Channel Configuration

The **Remote Capabilities Configuration** page appears as shown in **Figures 28**. Check the **ND2** and the **MWI** checkboxes.

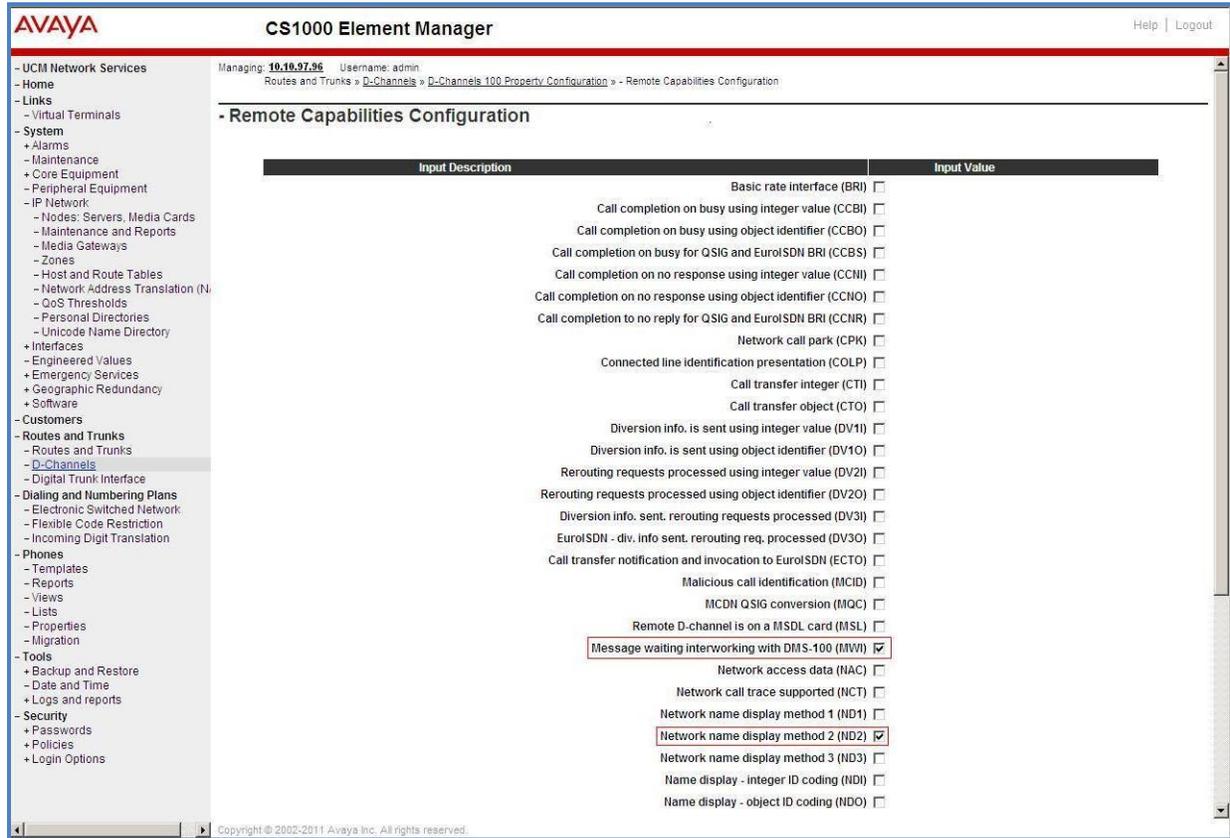


Figure 28 – Remote Capabilities Configuration

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

Click on the **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, please click the **Add** button to create a new one as shown in **Figure 29**. In this example, Superloop 4, 96, 100, and 124 have been added and are being used.

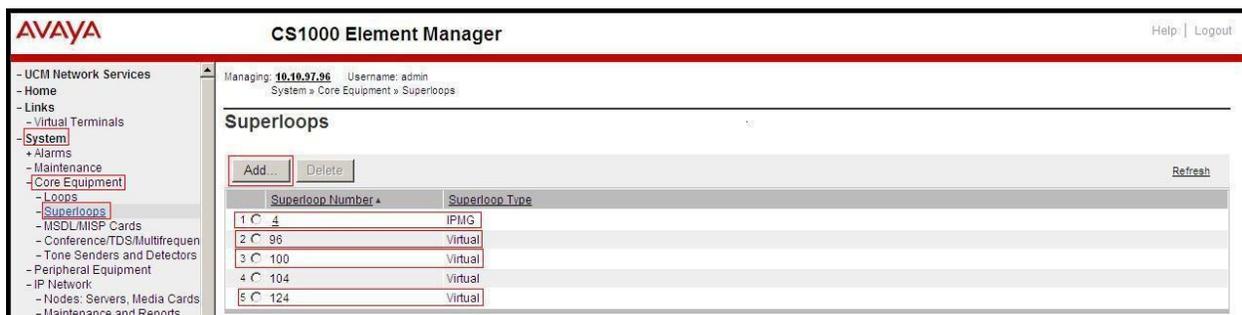


Figure 29 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

Select **Routes and Trunks** → **Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown in **Figure 30**.

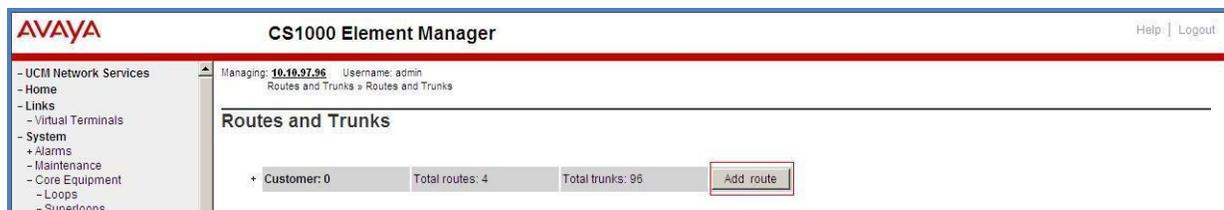


Figure 30 – Add route

The **Customer 0, New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter 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 **Figures 31**.

- **Route data block (RDB) (TYPE):** RDB as default.
- **Customer number (CUST):** 0 as customer 0 is in used.
- **Route number (ROUT):** Enter an available route number (example: route 100).
- **Designator field for trunk (DES):** A descriptive text (100).
- **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: 8100).

- 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 **3000** (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.
 - **Mode of operation (MODE):** Select **Route uses ISDN Signaling Link (ISLD)**.
 - **D channel number (DCH):** Enter **100** (created in Section 5.5.3).
 - **Interface type for route (IFC):** Select **Meridian M1 (SL1)**.
 - **Private network identifier (PNI):** Enter **1**. **Note:** The value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
 - **Network calling name allowed (NCNA):** Check this option to allow calling name display.
 - **Network call redirection (NCRD):** Check this option to allow call redirection.
 - **Insert ESN access code (INAC):** Check this option to insert ESN access code (Refer to Section 5.6.1).

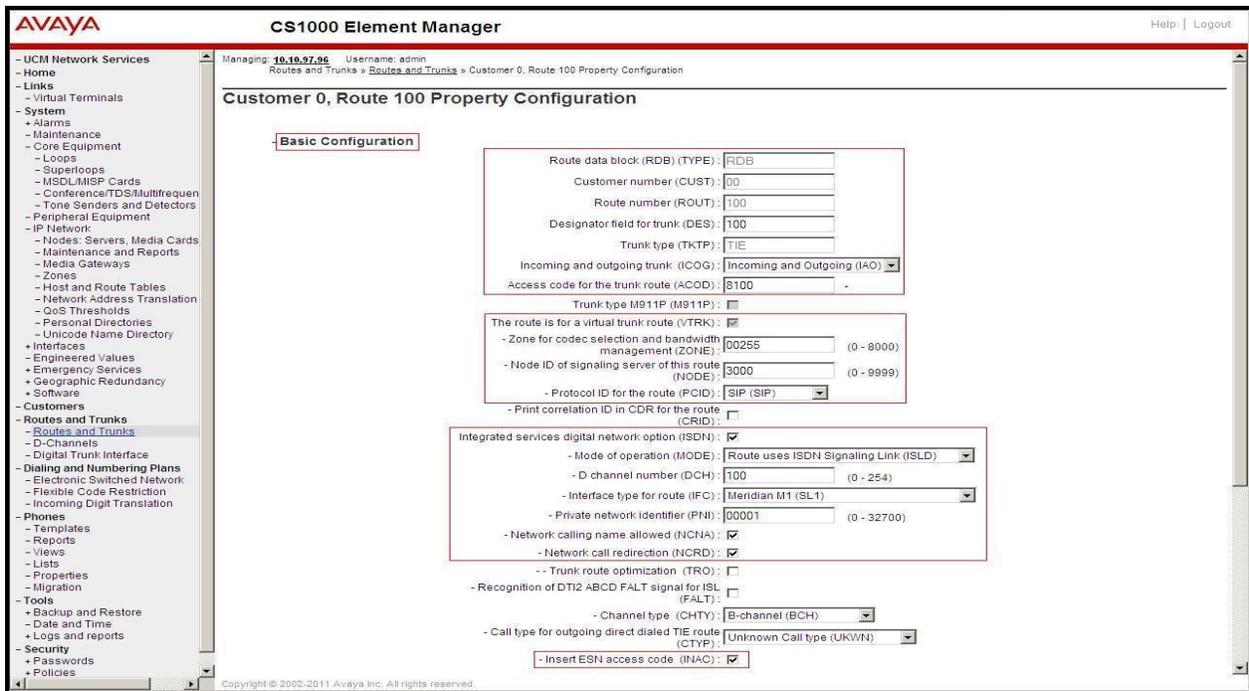


Figure 31 – Route Configuration 1

Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** checkboxes. Enter **1** for both **Day IDC tree number** and **Night IDC tree number** as shown in **Figure 32**.

Click on the **Submit** button.

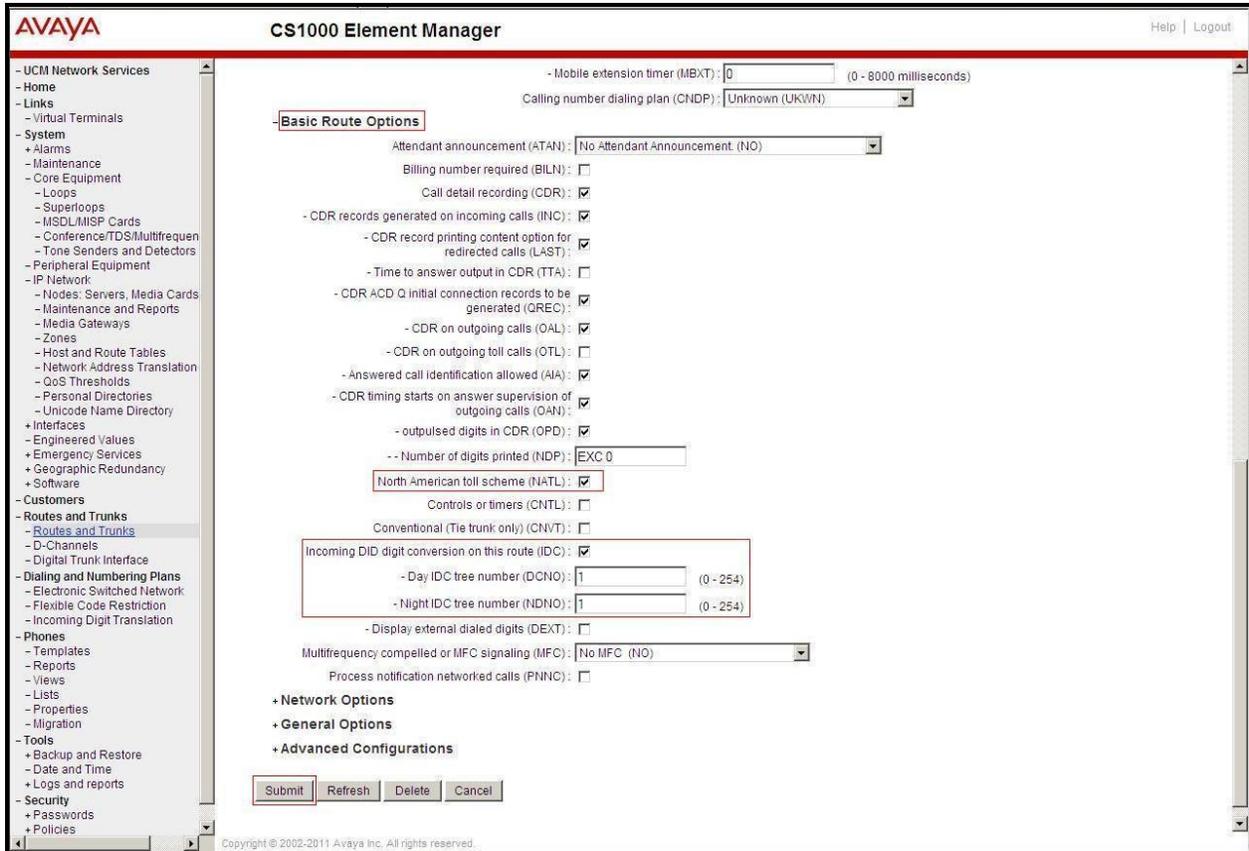


Figure 32 – Route Configuration 2

5.5.6. Administer Virtual Trunks

Select **Routes and Trunks** → **Route and Trunks** (not shown). The Route list is now updated with the newly added routes. In the example, the Route 100 was being added. Click on the **Add trunk** button as shown in **Figure 33**.



Figure 33 – Routes and Trunks

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. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown in **Figure 34**.

Note: The Multiple trunk input number (MTINPUT) field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.

- **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:** Select **Immediate (IMM)**.
- **Start arrangement Outgoing:** Select **Immediate (IMM)**.
- **Trunk group access restriction:** Desired trunk group access restriction level.
- **Channel ID for this trunk:** An available starting channel ID.

The screenshot shows the AVAYA CS1000 Element Manager interface. The main title is "Customer 0, Route 100, Trunk 1 Property Configuration". The left sidebar contains a navigation menu with categories like "UCM Network Services", "Home", "Links", "System", "Maintenance", "Core Equipment", "Loops", "Superloops", "MSDL/MISP Cards", "Conference/TDS/Multifrequen", "Tone Senders and Detectors", "Peripheral Equipment", "IP Network", "Nodes: Servers, Media Cards", "Maintenance and Reports", "Media Gateways", "Zones", "Host and Route Tables", "Network Address Translation", "QoS Thresholds", "Personal Directories", "Unicode Name Directory", "Interfaces", "Engineered Values", "Emergency Services", "Geographic Redundancy", "Software", "Customers", "Routes and Trunks", "Routes and Trunks", "D-Channels", "Digital Trunk Interface", and "Dialing and Numbering Plans". The main content area is titled "Basic Configuration" and contains the following fields:

- 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:

At the bottom of the "Basic Configuration" section, there is a "Class of Service:" label followed by an "Edit" button. Below this, there is an "Advanced Trunk Configurations" section which is currently empty. At the bottom right of the form, there are three buttons: "Save", "Delete", and "Cancel".

Figure 34 – New Trunk Configuration

For **Media Security**, select **Media Security Never (MSNV)**. Enter the values for the specified fields as shown in **Figure 35**. Scroll down to the bottom of the screen and click **Return Class of Service** and click on the **Save** button (shown in **Figure 34**).

The screenshot displays the 'Class of Service' configuration page in the AVAYA CS1000 Element Manager. The interface includes a left-hand navigation menu with categories such as 'UCM Network Services', 'System', 'Interfaces', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', and 'Tools'. The main content area is titled '- Class of Service' and contains a table with two columns: 'Input Description' and 'Input Value'. The table lists various service parameters, each with a corresponding dropdown menu. The 'Media Security' parameter is highlighted with a red box, and its value is 'Media Security Never (MSNV)'. Other parameters include 'ACD Priority' (ACD Priority not required (APN)), 'Analog Semi-Permanent Connections' (Analog Semi-Permanent Connections Denied (SPCD)), 'Centrex Switchhook Flash' (Centrex Switchhook Flash Denied (THFD)), and 'Transmission Class of Service' (Non-Transmission Compensated (NTC)). At the bottom of the page, there are two buttons: 'Return Class of Service' and 'Cancel'. The footer of the page reads 'Copyright © 2002-2011 Avaya Inc. All rights reserved.'

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

Figure 35 – Class of Service Configuration

5.5.7. Administer Calling Line Identification Entries

Select **Customers** on the left pane, then select **00 → ISDN and ESN Networking** (Not shown). Click on **Calling Line Identification Entries** as shown in **Figure 36**.

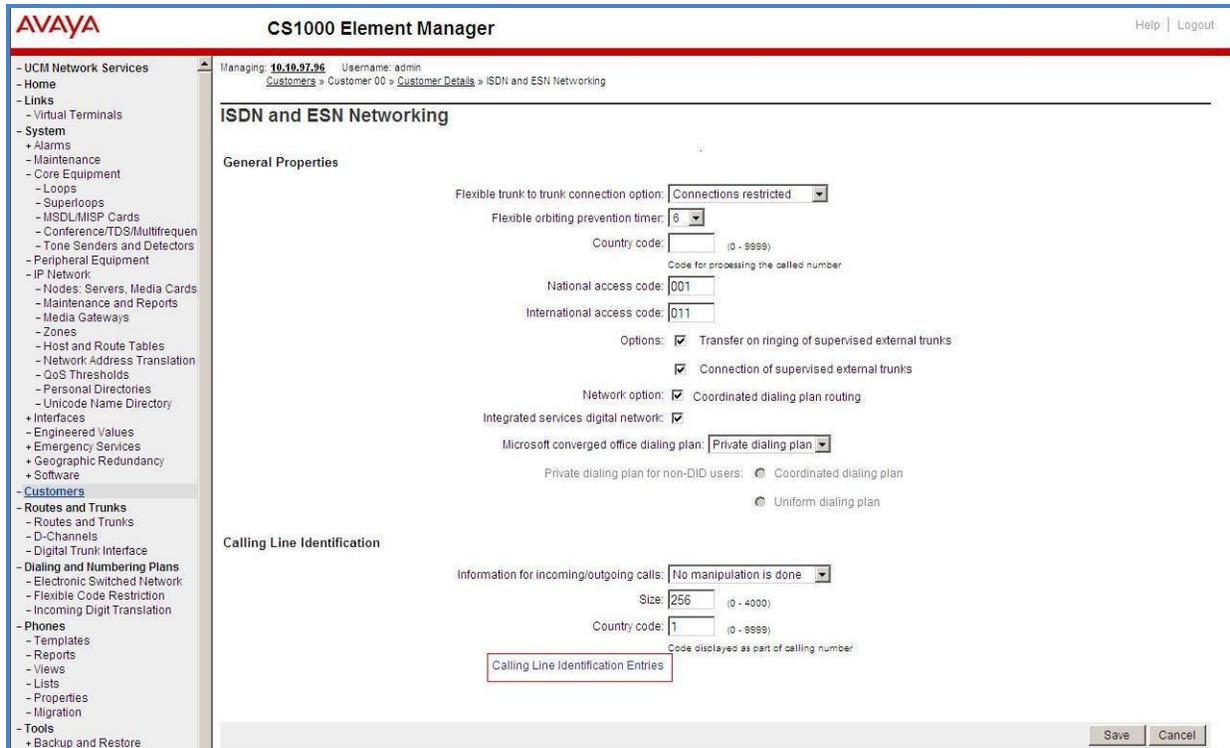


Figure 36 – ISDN and ESN Networking

Click on **Add** as shown in **Figure 37**.

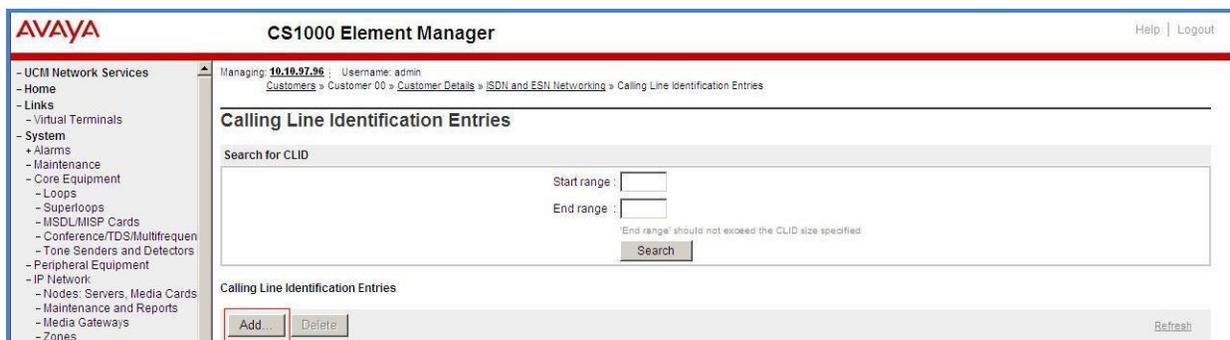


Figure 37 – Calling Line Identification Entries

The add entry **0** screen is displayed. Enter or select the following values for the specified fields and retain the default values for the remaining fields. The **Edit Calling Line Identification** of the existing entry **0** is displayed as shown in **Figure 38**.

- **National Code:** Leave it blank.
- **Local Code:** Input prefix digits assigned by Virgin Media SIP Trunk Service, in this case 7 digits – **011XXX7**. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code:** Input the prefix digits assigned by Virgin Media SIP Trunk Service, in this case 7 digits – **011XXX7**. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code:** Input prefix digits assigned by Virgin Media SIP Trunk Service, in this case 7 digits – **011XXX7**. This **Local Steering Code** 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 on the **Save** button as shown in **Figure 38**.

The screenshot shows the 'Edit Calling Line Identification 0' configuration page in the AVAYA CS1000 Element Manager. The page is divided into several sections:

- General Properties:**
 - National Code: (empty)
 - Local Code: 011XXX7 (1-12 digits)
 - Home Location Code: 011XXX7 (1-7 digits)
 - Local Steering Code: 011XXX7 (1-7 digits)
 - Use DN as DID: YES
- Emergency Services Access:**
 - Emergency Local Code: (empty)
 - 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: (empty)
 - Expected Length: 7
 - Display Format: First name, Last name

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

Figure 38 – Edit Calling Line Identification 0

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 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): 33600126  USED U P: 8345621 954062  TOT: 45579868
DISK SPACE NEEDED: 1722 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 as shown in **Figure 39**.

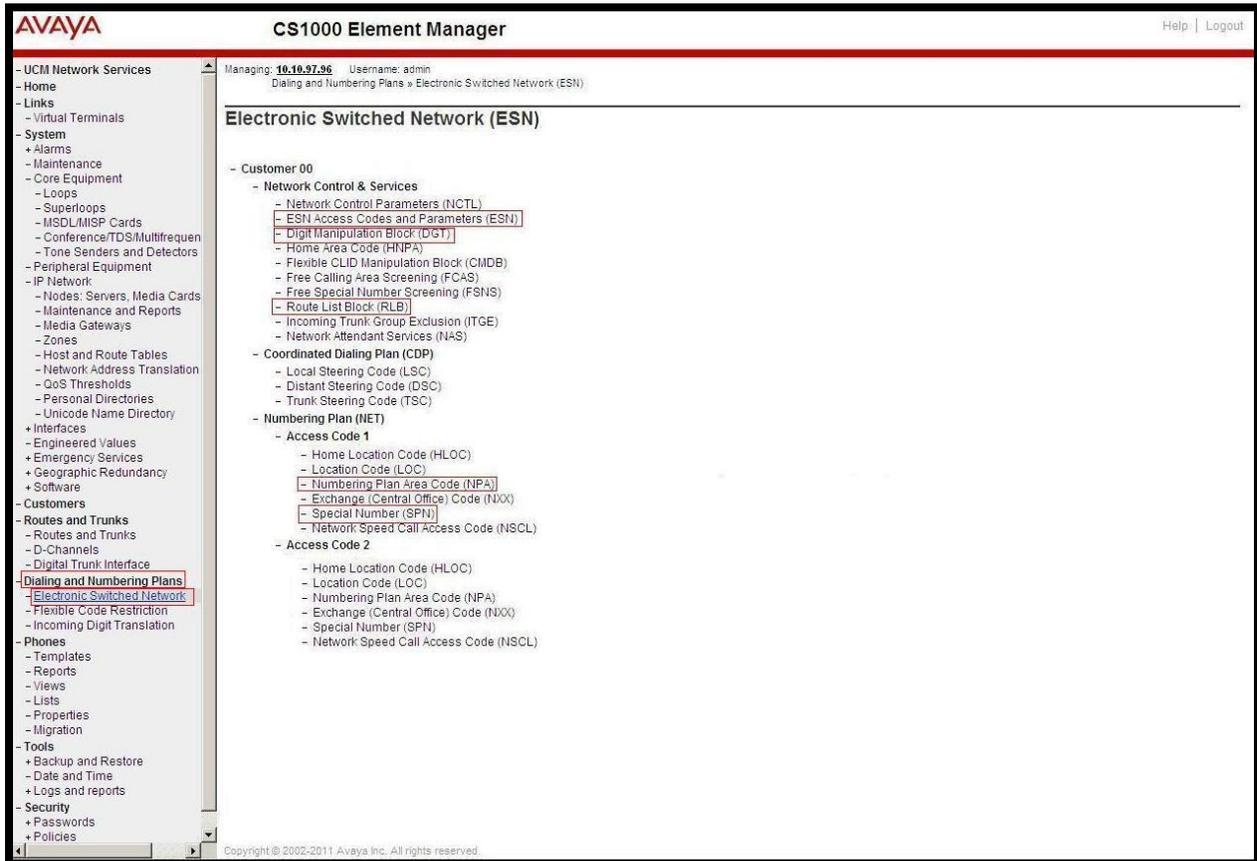


Figure 39 –ESN Configuration

On **Electronic Switched Network (ESN)** screen, select **ESN Access Codes and Parameters** to define **NARS/BARS Access Code 1** as shown in **Figure 40**.

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The main title is "CS1000 Element Manager" with "Help | Logout" in the top right. The left navigation menu includes: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System (with sub-items: + Alarms, - Maintenance and Reports, + Core Equipment, - Peripheral Equipment, - IP Network, - Nodes: Servers, Media Cards, - Maintenance and Reports, - Media Gateways, - Zones, - Host and Route Tables, - Network Address Translation (N), - QoS Thresholds, - Personal Directories, - Unicode Name Directory), + Interfaces (with sub-items: - Engineered Values, + Emergency Services, + Geographic Redundancy), + Software, - Customers, and - Routes and Trunks. The main content area is titled "ESN Access Codes and Basic Parameters" and shows "General Properties" for "NARS/BARS Access Code 1". The configuration includes: NARS/BARS Access Code 1: 6, NARS Access Code 2: 9, 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: 1000 (1-64000), Number of digits in CDP DN (DSC + DN or LSC + DN): 10 (3-10), Routing Controls: , and Check for Trunk Group Access Restrictions: .

Figure 40 – ESN Access Codes and Parameters

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**.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600086  USED U P: 8325631 954152  TOT: 44879869
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 Index (DMI)

The following steps show how to add DMI for the outbound call. There is an index, which was added to the Digit Manipulation Block List (14).

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 41**. In the **Please choose the** field, select an available **Digit Manipulation Block Index** from the drop-down list, and click on the **to Add** button.



Figure 41 – Add a DMI

The DMI_14 screen will open. In this testing, no leading digits are to be deleted, therefore, enter **0** for **Number of leading digits to be deleted** and select **NPA (NPA)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button as shown in **Figure 42**.

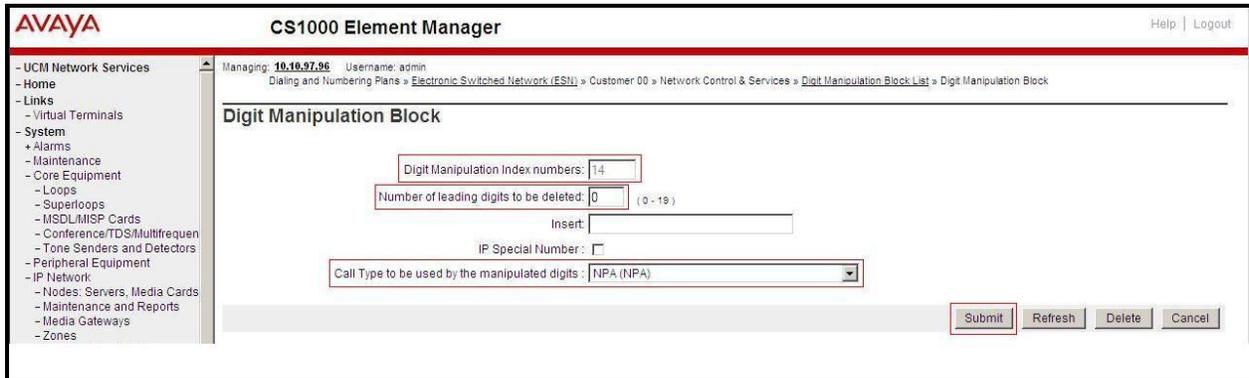


Figure 42 – DMI_14 Configuration

5.6.4. Route List Block (RLB) (RLB 14)

This session shows how to add a RLB associated with the DMI created in **Section 5.6.3**. Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39**. Select **Route List Block (RLB)**.

Enter an available value in the textbox for the **Please enter a route list index** (in this case **14**) and click on the **to Add** button as shown in **Figure 43**. The screen shown in **Figure 44** will open.



Figure 43 – Add a Route List Block

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 44**. Scroll down to the bottom of the screen, and click on the **Submit** button (not shown).

- **Digit Manipulation Index: 14** (created in **Section 5.6.3**).
- **Incoming CLID Table: 0** (created in **Section 5.5.7**).
- **Route number: 100** (created in **Section 5.5.5**).

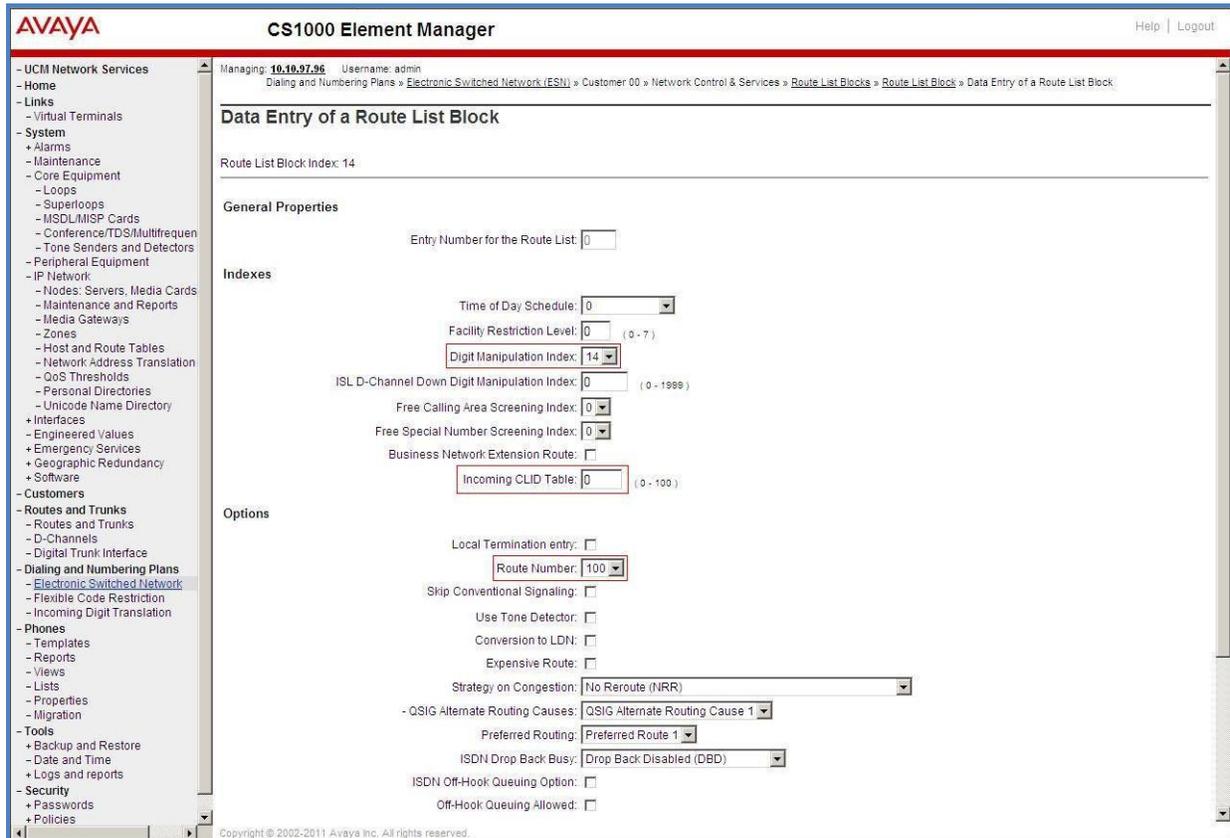


Figure 44 – RLB_14 Route List Block Configuration

5.6.5. Inbound Call – Incoming Digit Translation Configuration

This section describes the configuration steps required in order to receive calls from the PSTN via the Virgin Media SIP Trunk Service.

Select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown in **Figure 45**.

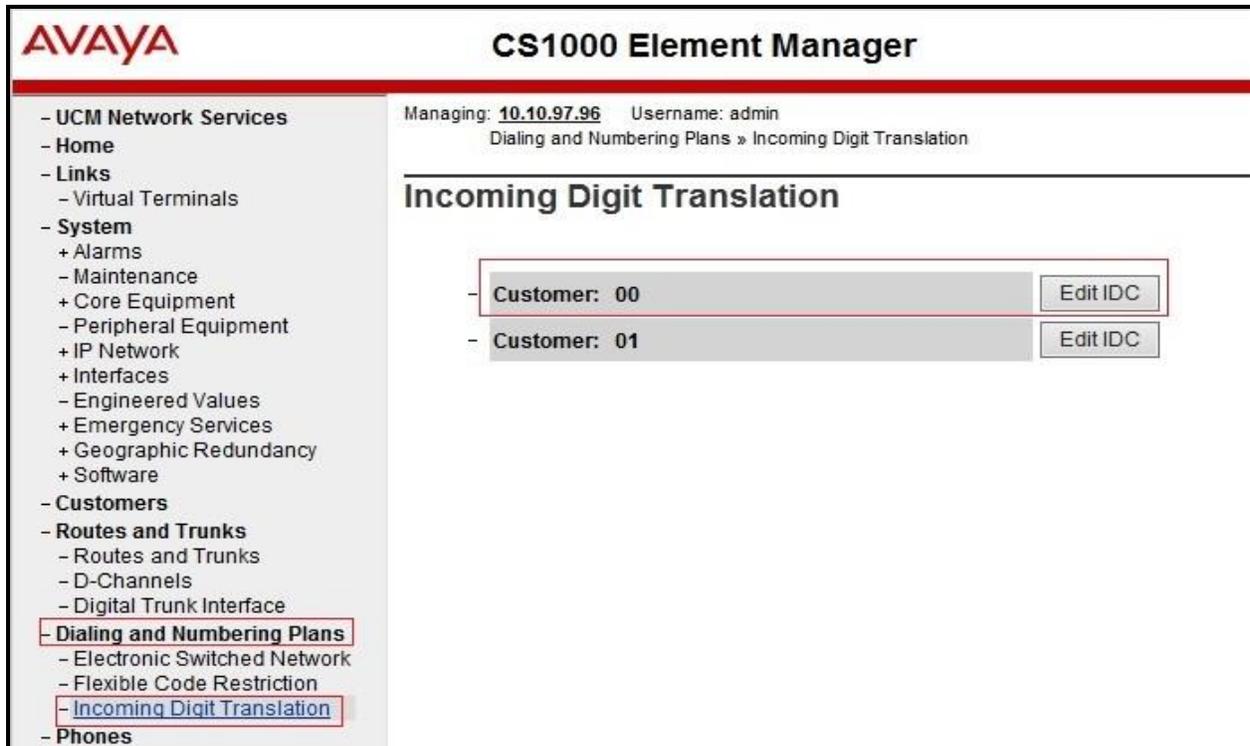


Figure 45 – Incoming Digit Translation

Click on the **New DCNO** to create the digit translation mapping. In this example, **Digit Conversion Tree Number 1** has been previously created as shown in **Figure 46**.



Figure 46 – Incoming Digit Conversion Property

Detailed configuration of the Digit Conversion Tree Configuration is shown in **Figure 47**. The **Incoming Digits** can be added to map to the Converted Digits which would be the associated CS1000 system phone DN. This **DCNO** has been assigned to route 100 as shown in **Figure 32**.

In the following configuration, the incoming call from the PSTN to DID with prefix **011XXX7** will be translated to the associated DN with 4 digits. DID number **011XXX74149** is translated to **1700** for voicemail testing and DID number **011XXX74146** is translated to **4146** for Mobile Service Access DN number.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans > Incoming Digit Translation > Customer 00 > Digit Conversion Tree 1 Configuration

Digit Conversion Tree 1 Configuration

Regular IDC tree
Send calling party DID disabled

Buttons: Add..., Delete IDC, Delete IDC tree, Refresh

	Incoming Digits	Converted Digits	CPND Name	CPND language
1	011XXX74140	4140	,	Roman characters
2	011XXX74141	4141	,	Roman characters
3	011XXX74142	4142	,	Roman characters
4	011XXX74143	4143	,	Roman characters
5	011XXX74144	4144	,	Roman characters
6	011XXX74145	4145	,	Roman characters
7	011XXX74146	4146	,	Roman characters
8	011XXX74147	4147	,	Roman characters
9	011XXX74148	4148	,	Roman characters
10	011XXX74149	1700	,	Roman characters

Figure 47 – Digit Conversion Tree

5.6.6. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 112, 1800, 999 and so on.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as show in **Figure 39**. Select **Special Number (SPN)**. Enter a SPN number and then click on the **to Add** button. **Figure 48** shows all the special numbers used for this testing.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top navigation bar includes the AVAYA logo, the title "CS1000 Element Manager", and "Help | Logout" links. The left sidebar contains a tree view of system components, with "Dialing and Numbering Plans" and "Electronic Switched Network" highlighted. The main content area shows the "Special Number List" page. At the top, it indicates the user is logged in as "admin" and provides the current navigation path: "Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Numbering Plan (NET) > Access Code 1 > Special Number List". Below this, there is a form to "Please enter a Special Number" with an input field and a "to Add" button. The list below contains four entries, each with an "Edit" button:

- Special Number -- 0**: Flexible length: 15, Inhibit time-out handler: NO, Type of call that is defined by the special number: NONE, Route list index: 14.
- Special Number -- 112**: Flexible length: 3, Inhibit time-out handler: NO, Type of call that is defined by the special number: NONE, Route list index: 14.
- Special Number -- 1800**: Flexible length: 14, Inhibit time-out handler: NO, Type of call that is defined by the special number: NONE, Route list index: 14.
- Special Number -- 999**: Flexible length: 3, Inhibit time-out handler: NO, Type of call that is defined by the special number: NONE, Route list index: 14.

Figure 48 – Add a SPN

5.7. Administer a Phone

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

5.7.1. Phone creation

Refer to **Section 5.5.4** to create a Virtual Superloop **96** used for IP phones. Refer to **Section 5.4.1** to create a bandwidth zone **10** for IP phones. Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail). Create an IP phone by using **ld 11** as shown below:

```
>ld 11
REQ: new
TYPE: 2002p2
TN 96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED
DES 2002P2 ← Describe information for IP Phone
TN 96 0 00 02 VIRTUAL ← Set Terminal Number for IP Phone
TYPE 2002P2
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010 ← Set bandwidth zone for IP phone
CUR_ZONE 00010
MRT
ERL 12345
ECL 0
FDN
TGAR 0
LDN NO
NCOS 7
SGRP 0
RNPG 0
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXA 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
FSDS 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 4140 0  MARP ← Set the position of DN 4140 to display on key 0 of the phone
  CPND
    CPND_LANG ROMAN
      NAME Virgin1 ← Set name to display
      XPLN 13
      DISPLAY_FMT FIRST, LAST
    01
<Text removed for brevity>

```

5.7.2. Enable Privacy for the Phone

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

To hide the display number, set **CLS** (Class of Service) to **DDGD**. CS1000 will include “Privacy:id” in the SIP message header before sending it to Virgin Media SIP Trunk Service.

```

>ld 11
REQ: chg
TYPE: 2002p2
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 Virgin Media SIP Trunk Service.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM CLS DDGA
...
```

5.7.3. Enable Call Forward for Phone

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

Select **Customer** → **00** → **Call Redirection**. The Call Redirection page is shown in **Figure 49**.

- **Total redirection count limit: 0** (unlimited).
- **Call Forward: Originating**.
- **Number of normal ring cycle for CFNA: 3**.
- Click **Save** to save the configuration.

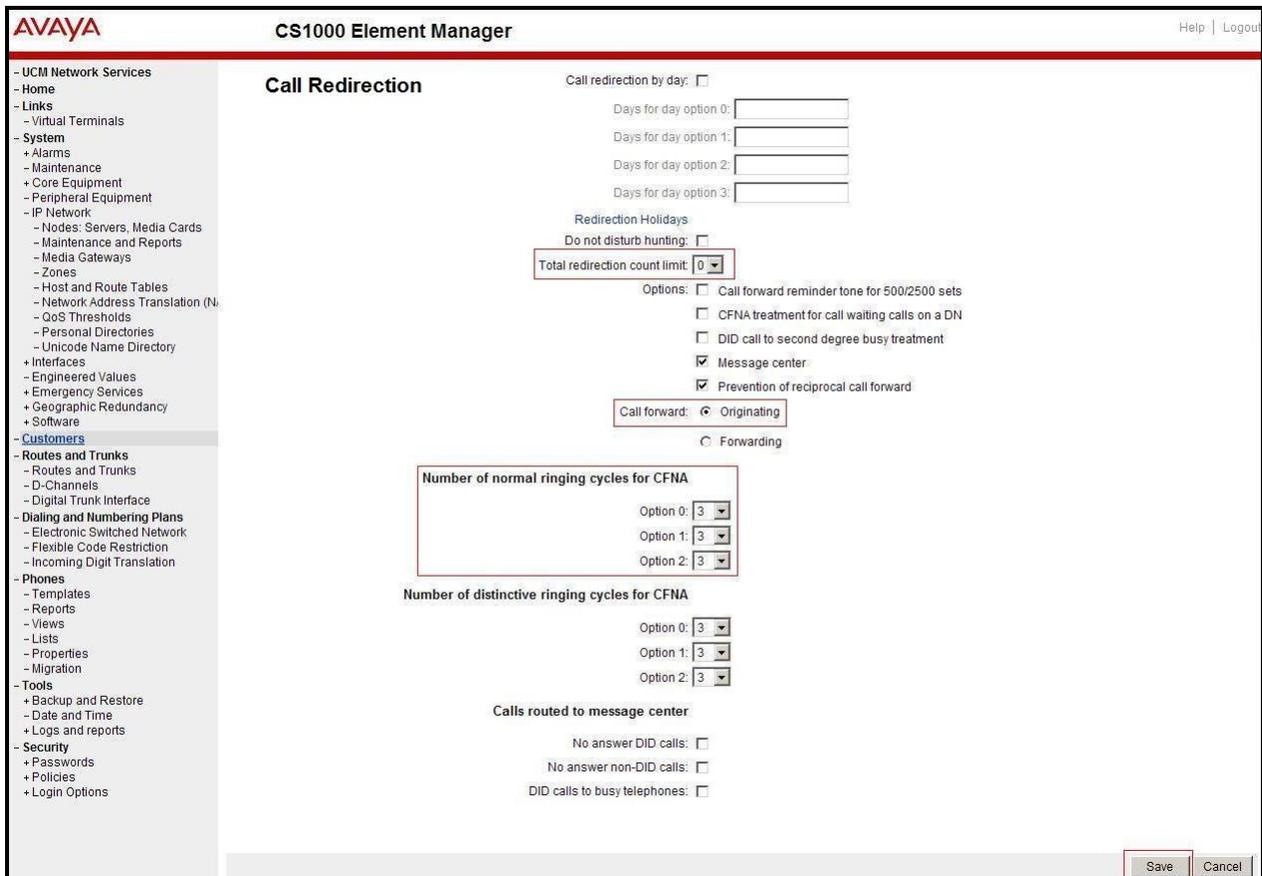


Figure 49 – Call Redirection

To enable Call Forward All Call (CFAC) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **CFXA**, and **SFA**, then program the forward number on the phone set. The following is the configuration of a phone that has CFAC enabled with forwarding number **6001613XXX5206**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2

ECHG yes
ITEM CLS CFXA SFA
ITEM key 19 CFW 16 6001613XXX5206
```

To enable Call Forward Busy (CFB) feature for phone over SIP trunk, use **ld 11**. Change its **CLS** to **FBA**, **HTA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone with CFB enabled to forwarding number **6001613XXX5206**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2
ECHG yes
ITEM CLS FBA HTA SFA
ITEM HUNT 6001613XXX5206
ITEM FDN 6001613XXX5206
```

To enable Call Forward No Answer (CFNA) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **FNA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone that has CFNA enabled with forwarding number **6001613XXX5206**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2
ECHG yes
ITEM CLS FNA SFA
ITEM HUNT 6001613XXX5206
ITEM FDN 6001613XXX5206
```

6. Configure Avaya Aura[®] Session Manager

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

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to CS1000, Avaya SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.

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

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the **System Manager Log On** screen, enter an appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

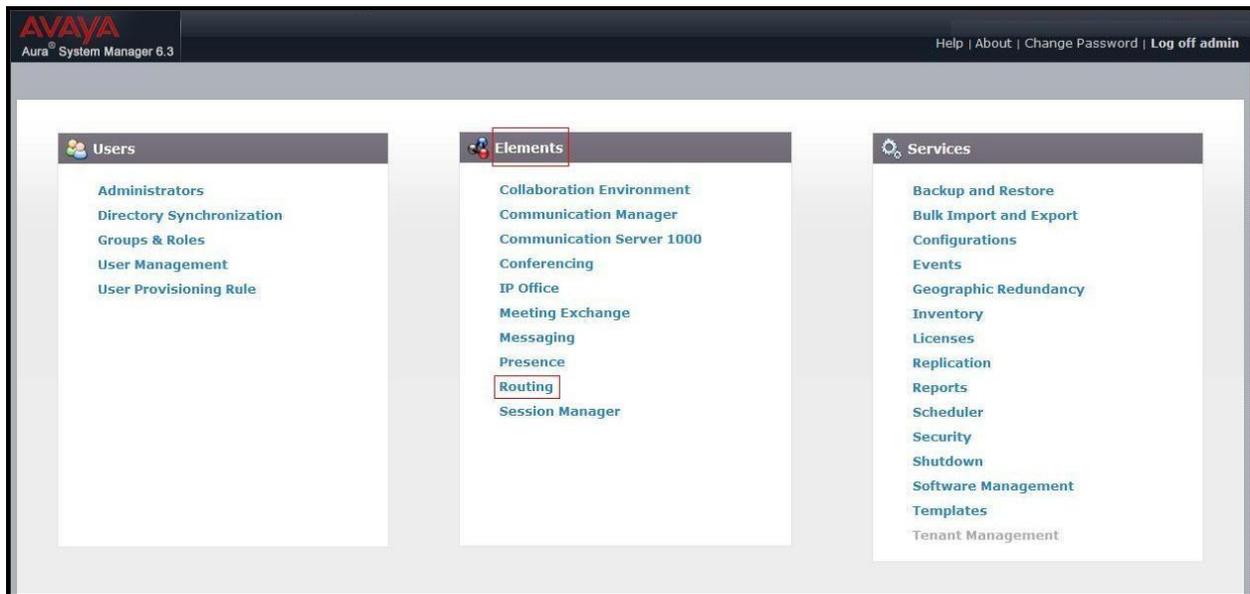


Figure 50 – System Manager Home Screen

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column 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.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The top header includes the Avaya logo, 'Aura System Manager 6.3', and navigation links for 'Help | About | Change Password | Log off admin'. The left navigation pane is expanded to show the 'Routing' section, which includes sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Introduction to Network Routing Policy' and contains the following text:

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.
The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 7: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 - (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 8: Create "Dial Patterns"
 - Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Figure 51 – Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev7.com**.

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

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

Click **Commit** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.

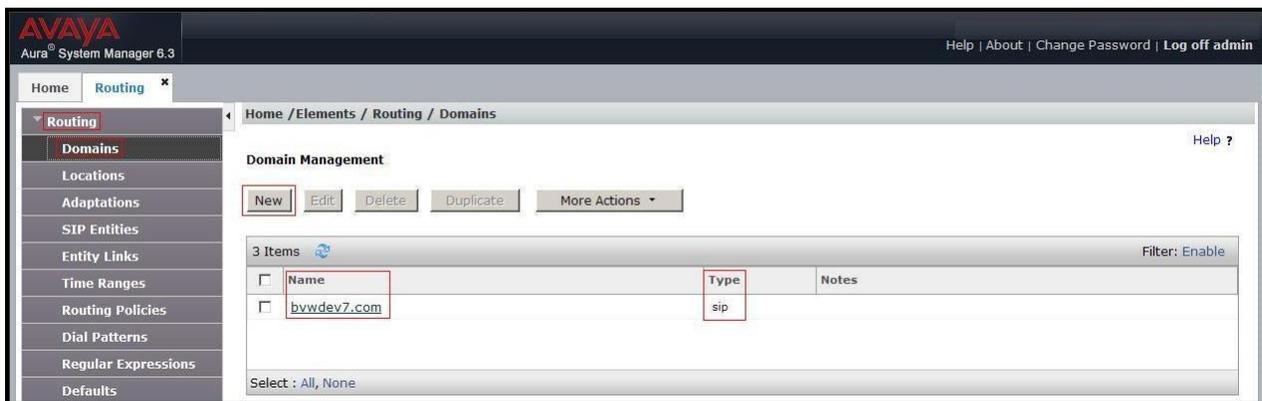


Figure 52 – Domain Management

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including CS1000, Session Manager and Avaya SBCE.

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

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

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

AVAYA
Aura® System Manager 6.3

Home Routing x

Home / Elements / Routing / Locations

Location Details Commit Cancel Help ?

General

* Name: Belleville

Notes: GSSCP Belleville

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

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

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

* Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth:

Figure 53 – Location Configuration

In the **Location Pattern** section, click **Add** to enter IP Address patterns. The following patterns were used in testing:

- **IP Address Pattern:** 10.33.*, 10.10.97.*, 10.10.98.*

Location Pattern

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.97.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.98.*	<input type="text"/>

Select : All, None

Commit Cancel

Figure 54 – IP Ranges Configuration

Click **Commit** to save.

Note that call bandwidth management parameters should be set per customer requirement.

6.4. Configure Adaptations

An Adaptation is configured to format the History Info on CS1000 to be compatible with other Avaya products. To add a new adaptation, select **Routing** → **Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the adaptation. Select **CS1000Adapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **fromto** and **Value** as **true**. Click the **Commit** button after changes are completed.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with 'Routing' selected. The main content area is titled 'Adaptation Details' and 'General'. The 'Adaptation Name' field is set to 'CS1K76_Adaptation'. The 'Module Name' dropdown is set to 'CS1000Adapter'. The 'Module Parameter Type' dropdown is set to 'Name-Value Parameter'. Below these fields are 'Add' and 'Remove' buttons. A table with two columns, 'Name' and 'Value', contains one row with 'fromto' and 'true'. Below the table is a 'Select : All, None' dropdown. At the bottom, there are fields for 'Egress URI Parameters' and 'Notes'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

Figure 55 - CS1000 Adaptation

An Adaptation is configured to convert the History Info to Diversion Header and to remove MIME. To add a new adaptation, select **Routing** → **Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the adaptation. Select **DiversionTypeAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **MIME** and **Value** as **no**. Click the **Commit** button after changes are completed.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with 'Routing' selected. The main content area is titled 'Adaptation Details' and 'General'. The 'Adaptation Name' field is set to 'Diversion-Type-Remove-MIME'. The 'Module Name' dropdown is set to 'DiversionTypeAdapter'. The 'Module Parameter Type' dropdown is set to 'Name-Value Parameter'. Below these fields are 'Add' and 'Remove' buttons. A table with two columns, 'Name' and 'Value', contains one row with 'MIME' and 'no'. Below the table is a 'Select : All, None' dropdown. At the bottom, there are fields for 'Egress URI Parameters' and 'Notes'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

Figure 56 – Diversion Header Adaptation

6.5. Add SIP Entities

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

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **Other** for CS1000 and Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate Adaptation module that will be applied to the SIP Entity being created.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville**.
- **Time Zone:** Select the time zone for the Location above.

In this configuration, there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager 1000 SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.5.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **SM63**. The IP address of Session Manager's signaling interface **10.33.10.26** is entered for **FQDN or IP Address**. The **Location** field is set to **Belleville**. Select **Time Zone** as **America/Toronto**.

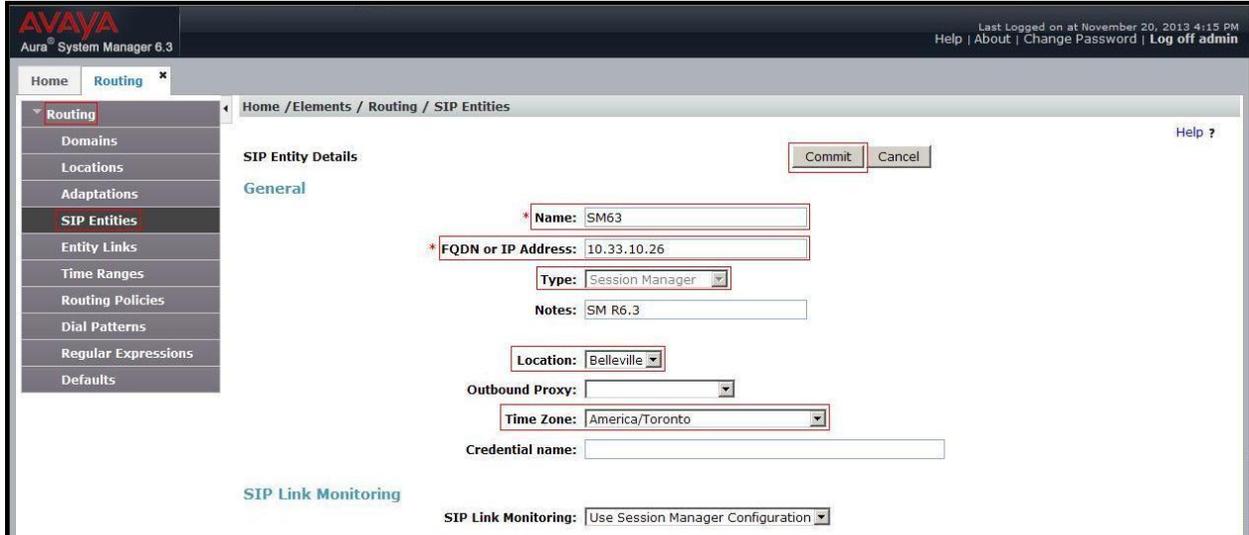


Figure 57 – Session Manager SIP Entity

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

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

- **Port:** Port number on which Session Manager listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

Defaults can be used for the remaining fields. Click the **Commit** button (not shown) to save.

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

Port

TCP Failover port:

TLS Failover port:

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	bvwdev7.com	<input type="text"/>

Select : All, None

Figure 58 – Session Manager SIP Entity Port

6.5.2. Configure Communication Server 1000 SIP Entity

The following screen shows the addition of the CS1000 SIP Entity named **car3-ssg-carrier**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to CS1000, it is necessary to create a separate SIP Entity for CS1000, in addition to the one created at Session Manager installation, for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of CS1000 signaling Node **10.10.97.178**. Select **Type** as **Other**. Select **Adaptation** as **CS1K76_Adaptation** (created in **Section 6.4**). The **Location** field is set to **Belleville** which is the location that includes the subnet where CS1000 resides. Select **Time Zone** as **America/Toronto**.

AVAYA
Aura System Manager 6.3 Last Logged on at October 21, 2014 4:04 AM

Home Routing

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details

General

* Name: car3-ssg-carrier

* FQDN or IP Address: 10.10.97.178

Type: Other

Notes:

Adaptation: CS1K76_Adaptation

Location: Belleville

Time Zone: America/Toronto

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Figure 59– Communication Server 1000 SIP Entity

6.5.3. Configure Avaya SBCE SIP Entity

The following screen shows the SIP Entities for the Avaya SBCE. Two SIP Entities were used for the two interfaces established so that routing could take place to both the Virgin Media SBC A and Virgin Media SBC B. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE's private network interfaces. Select **Type** as **Other**. Select **Adaptation** as **Diversion-Type-Remove-MIME** (created in **Section 6.4**). The **Location** field is set to **Belleville** which includes the subnet where Avaya SBCE resides. Select **Time Zone** as **America/Toronto**.

The following screenshot shows the SIP Entity for Avaya SBCE - Virgin Media SBC A.

The screenshot displays the Avaya Aura System Manager 6.3 interface. The breadcrumb navigation shows 'Home / Elements / Routing / SIP Entities'. The left-hand navigation menu includes 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible: Name: SBCE_Virgin_A; FQDN or IP Address: 10.10.98.13; Type: Other; Notes: (empty); Adaptation: Diversion-Type-Remove-MIME; Location: Belleville; Time Zone: America/Toronto; SIP Timer B/F (in seconds): 4; Credential name: (empty); Call Detail Recording: none; and CommProfile Type Preference: (empty).

Figure 60 – Avaya SBCE SIP Entity – Virgin Media SBC A

The following screenshot shows the SIP Entity for Avaya SBCE - Virgin Media SBC B.

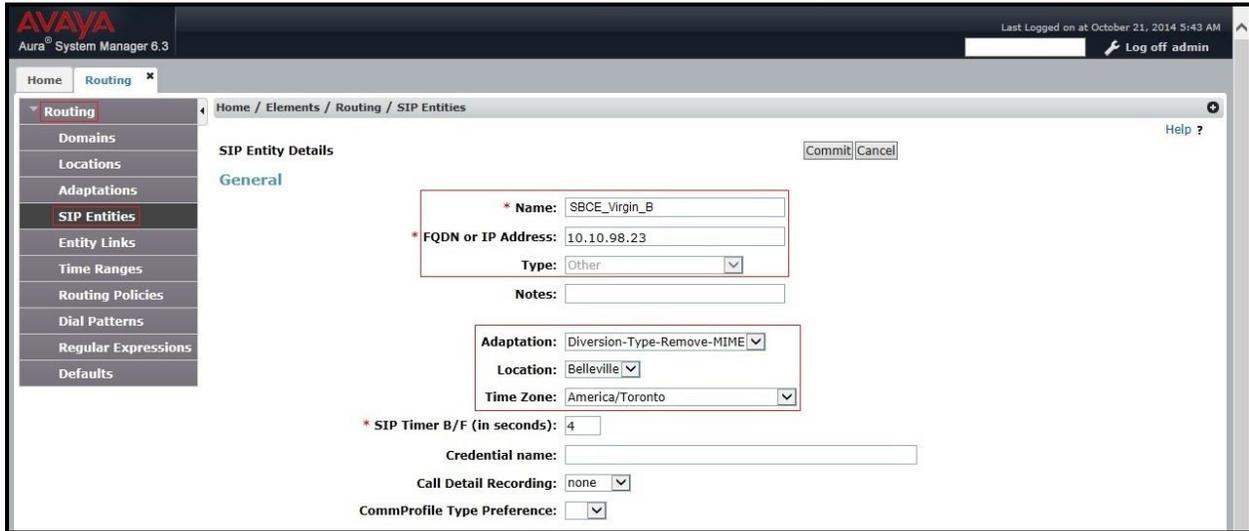


Figure 61 – Avaya SBCE SIP Entity - Virgin Media SBC B

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Three Entity Links were created: one to CS1000 and two to Avaya SBCE.

To add an Entity Link, navigate to **Routing** → **Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Connection Policy:** Select **trusted**. Note: If this box is not selected as trusted, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save.

The following screen illustrates the Entity Link to the CS1000. The protocol and ports defined here must match the values used for the CS1000 signaling in **Section 5.5.2**.

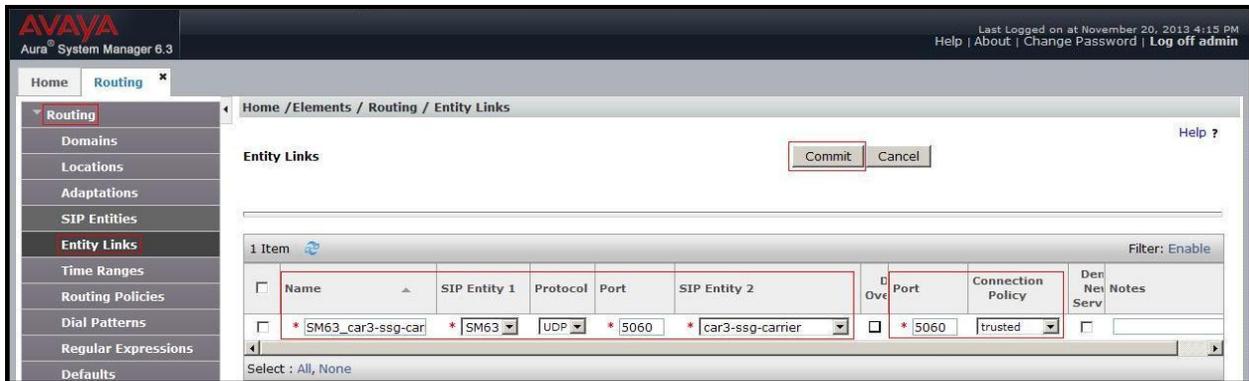


Figure 62 – Communication Server 1000 Entity Link

The following screen illustrates the Entity Links to Avaya SBCE - Virgin Media SBC A. The protocol and ports defined here must match the values used for Avaya SBCE mentioned in **Section 7.2.8**, later in this document.

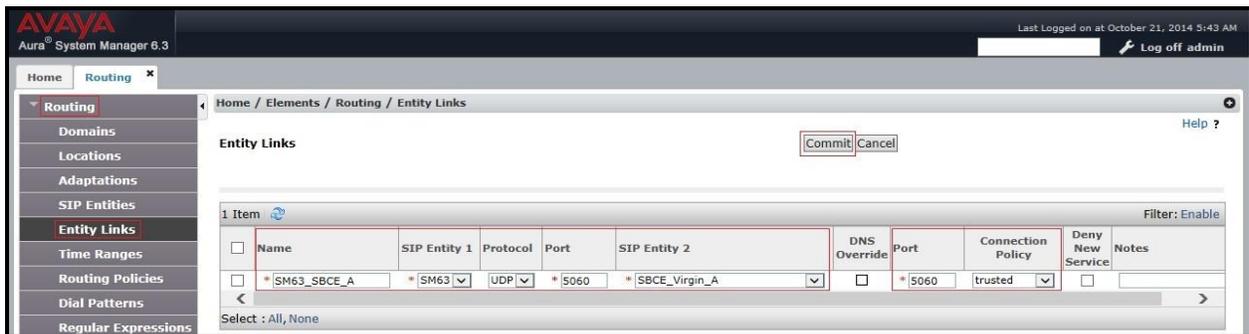


Figure 63 – Avaya SBCE - Virgin Media SBC A Entity Link

The following screen illustrates the Entity Links to Avaya SBCE - Virgin Media SBC B. The protocol and ports defined here must match the values used for Avaya SBCE mentioned in **Section 7.2.9**, later in this document.

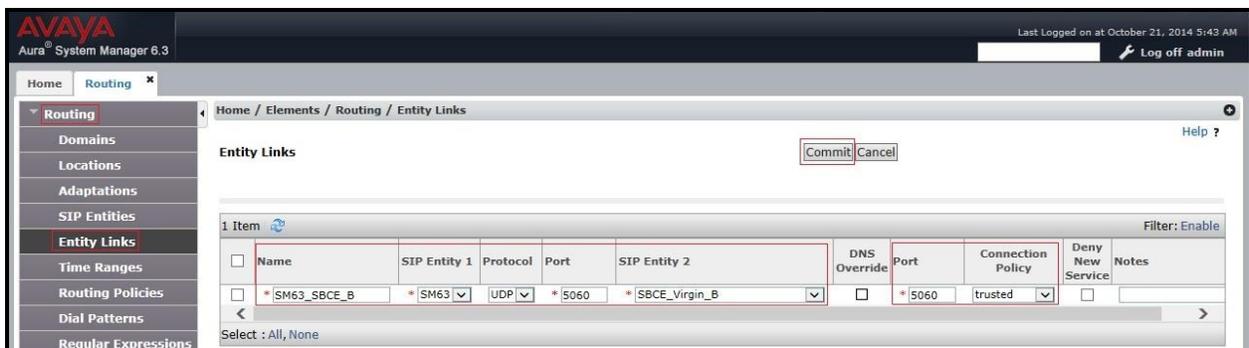


Figure 64 – Avaya SBCE - Virgin Media SBC B Entity Link

6.7. Configure Time Ranges

Time Ranges are configured for time-based routing. In order to add Time Ranges, select **Routing** → **Time Ranges** in the left-hand navigation pane and then click **New** button in the right pane. The Routing Policies shown subsequently will use the **24/7** range since time-based routing was not the focus of these Application Notes.

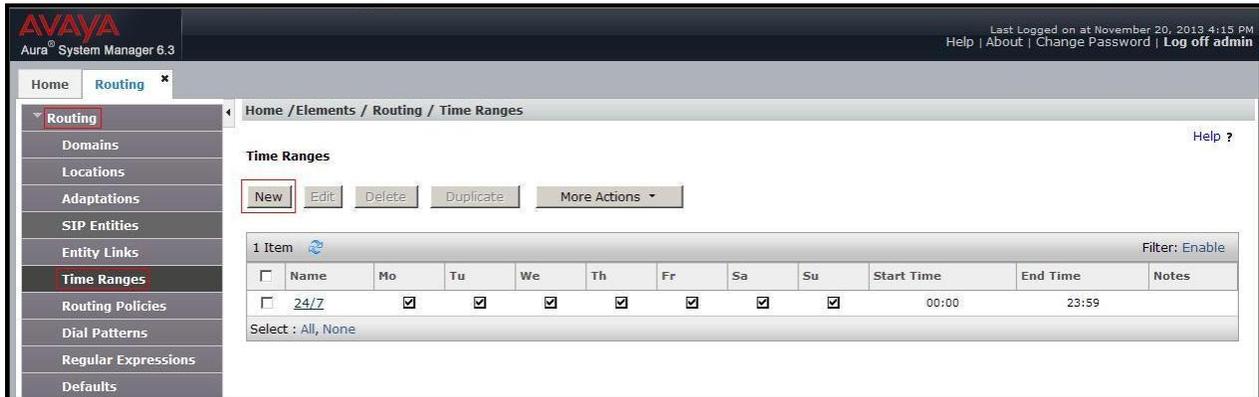


Figure 65 – Time Ranges

6.8. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Three Routing Policies must be added: one for the CS1000 and two for Avaya SBCE. To add a Routing Policy, navigate to **Routing** → **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

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

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

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

The following screen shows the **Routing Policy Details** for the policy named **Virgin_Inbound_To_CS1K76** associated with incoming PSTN calls from Virgin Media SIP Trunk Service to the CS1000. Observe the **SIP Entity as Destination** is the entity named **car3-ssg-carrier**.

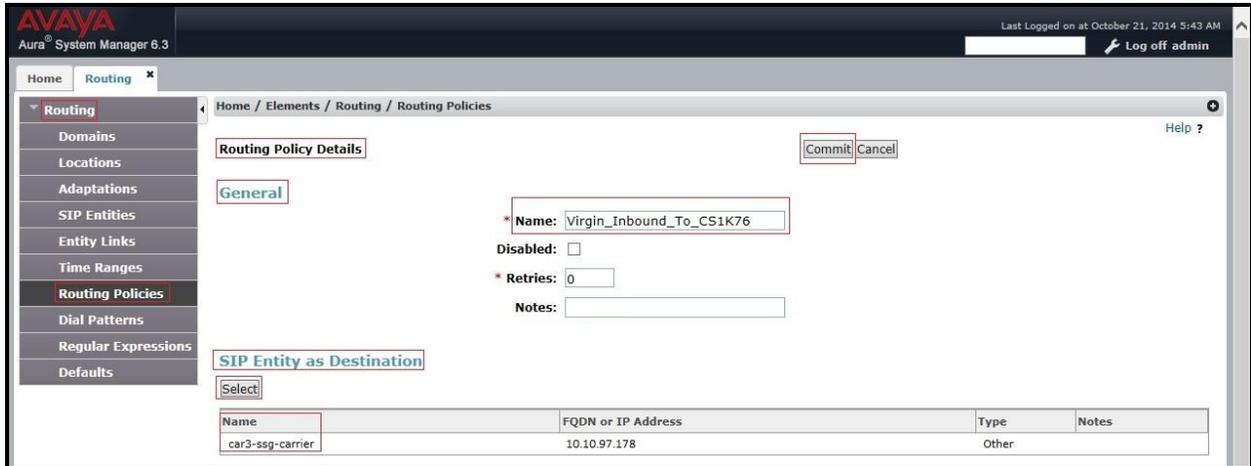


Figure 66 – Routing to Communication Server 1000

The following screen shows the **Routing Policy Details** for the policy named **Virgin_A_Outbound**. This is associated with outgoing calls from the CS1000 to the PSTN via Virgin Media SIP Trunk Service, through Avaya SBCE - Virgin Media SBC A. Observe the **SIP Entity as Destination** is the entity named **SBCE_Virgin_A**.

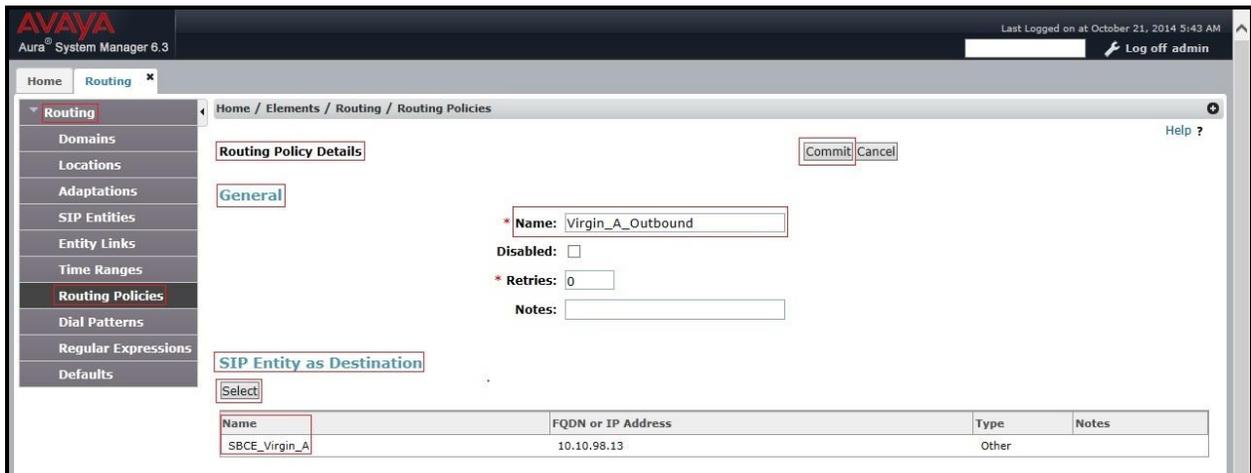


Figure 67 – Routing to Avaya SBCE - Virgin Media SBC A

The following screen shows the **Routing Policy Details** for the policy named **Virgin_B_Outbound**. This is associated with outgoing calls from the CS1000 to the PSTN via Virgin Media SIP Trunk Service, through Avaya SBCE - Virgin Media SBC B. Observe the **SIP Entity as Destination** is the entity named **SBCE_Virgin_B**.

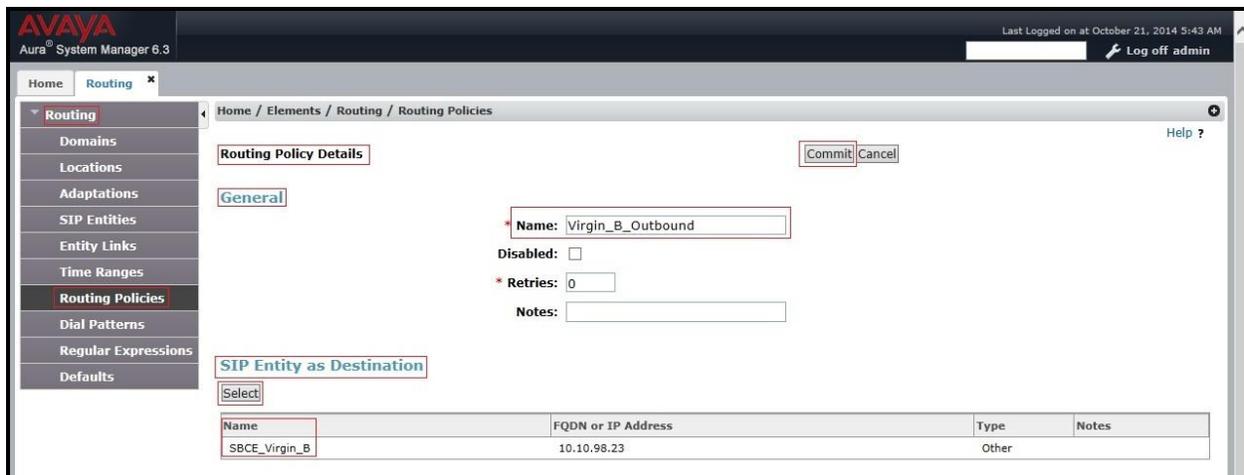


Figure 68 – Routing to Avaya SBCE - Virgin Media SBC B

6.9. Add Dial Patterns

Dial Patterns are used to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from the CS1000 to Virgin Media SIP Trunk Service and vice versa. Dial Patterns define which Route Policy will be selected as route destination 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-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

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

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

Default values can be used for the remaining fields. Click **Commit** to save. Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns (e.g., 18000, 999, etc.) were similarly defined.

In the Virgin Media network, two network SBCs are provided as the interface to the enterprise equipment. These are Sandbox SBCs and for the purposes of this document they have been designated as Virgin Media SBC A and Virgin Media SBC B. The routing and fallback for these two SBCs is configured on the Session Manager (See **Section 6.8**), with two server flows configured on the Avaya SBCE for routing to each network SBC (See **Section 7.4.4.2**). There is an interface configured on the Avaya SBCE for each of these server flows (See **Section 7.4.3**), and a corresponding SIP Entity, Entity Link and Routing Policy is required on the Session Manager for each of these interfaces.

A full description of the configuration of the interfaces and server flows on the Avaya SBCE is provided in **Sections 7.4.2, 7.4.3, 7.4.4.1, and 7.4.4.2**.

The following screen shows that outbound dialed numbers with a maximum of 15 digits that begin with **0** and have a destination SIP Domain of **bwvdev7.com** use the Routing Policy Names **Virgin_A_Outbound** and **Virgin_B_Outbound** as defined in **Section 6.8**.

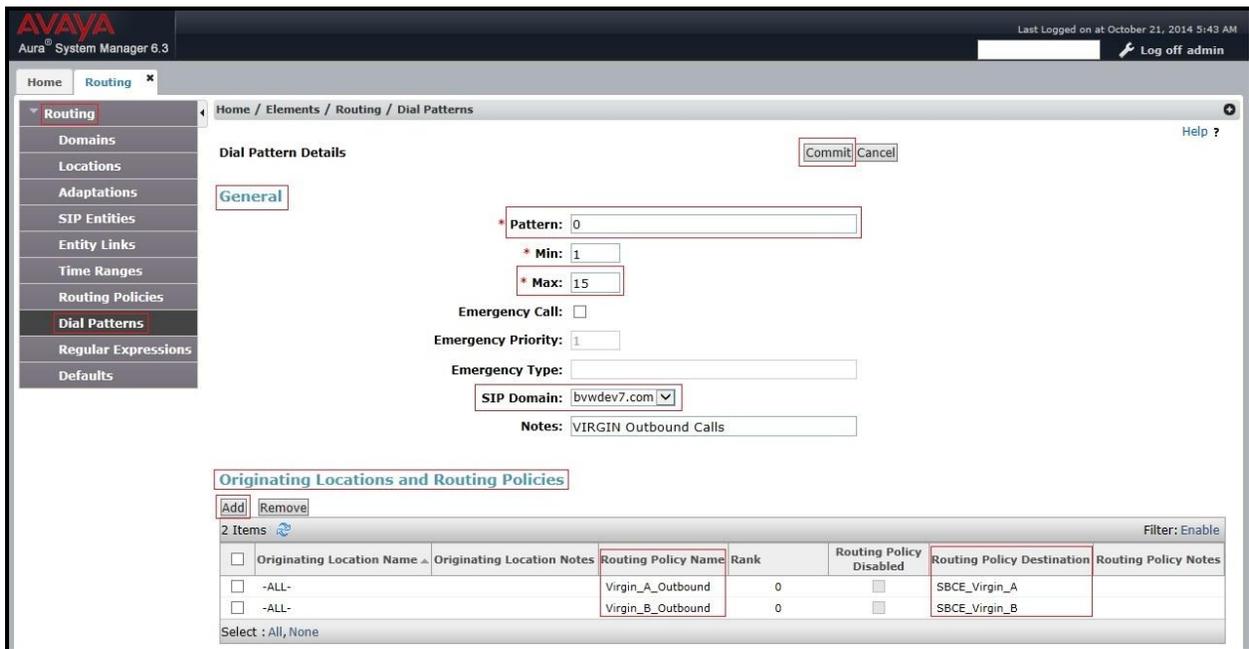


Figure 69 – Dial Pattern 0

Note that the above Dial Pattern did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

The following screen shows that inbound 11-digit numbers that start with **011XX** use Routing Policy Name **Virgin_Inbound_To_CS1K76** as defined in **Section 6.8**. This Dial Pattern matches the DID numbers assigned to the enterprise by Virgin Media SIP Trunk Service.

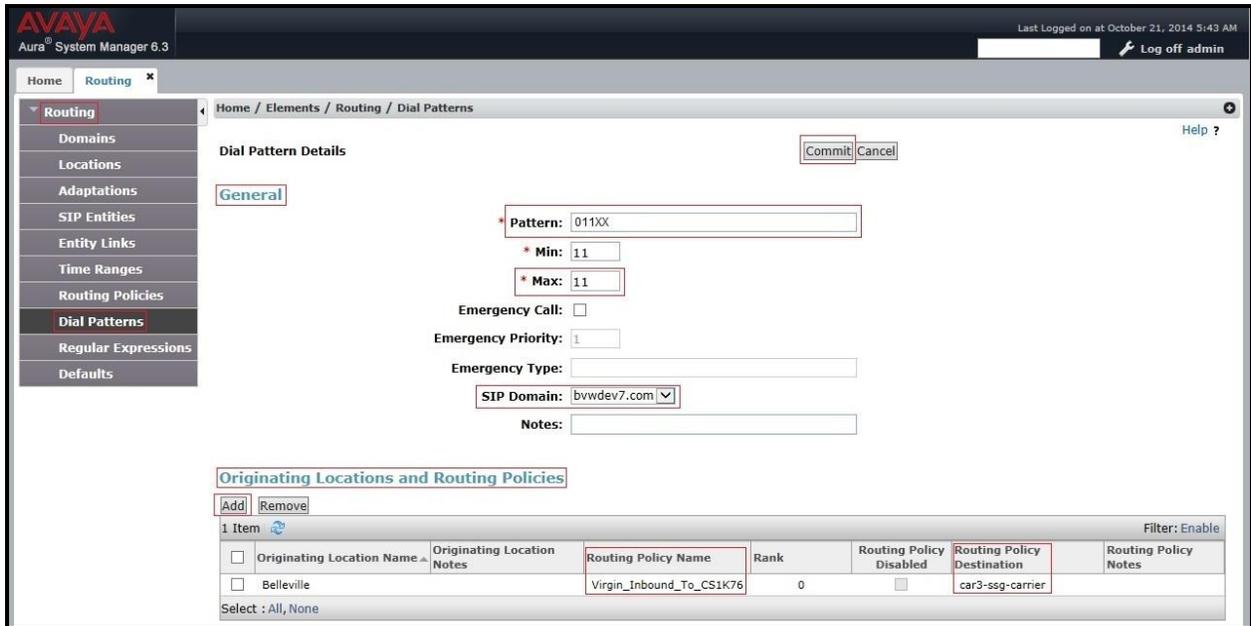


Figure 70 – Dial Pattern_011XX

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.



Figure 71 – Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the Session Manager and Virgin Media SIP Trunk Service.

Avaya elements reside on the Private side and the Virgin Media SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

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 relevant product documentation references in **Section 11** of these Application Notes.

7.1. Log into the SBCE

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

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



AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

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

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

Figure 72 – Avaya SBCE Login

7.2. Global Profiles

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

7.2.1. Configure Server Interworking - Avaya Site

Server Interworking allows to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in Interworking Profiles.
- Click **Clone**.
- Enter **Clone Name: SM63** and Click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **SM63** to edit.

- On the **General** tab, set **180 Handling** as **No SDP** (Note: This configuration is optional and this is a workaround to resolve the ring-back-tone issue on blind transfer call. Due to the configuration on the trunk site, the 183 with SDP was converted to 180 with No SDP (See **Section 7.3.1**), this configuration will let Avaya site to interwork with 180 without SDP) and set **T.38 Support** as **Yes** (if using Fax T.38) or **No** (if using Fax G.711 pass-through). Other options can be left at default.
- On the **Timers, URI Manipulation, Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SM63**) was added.

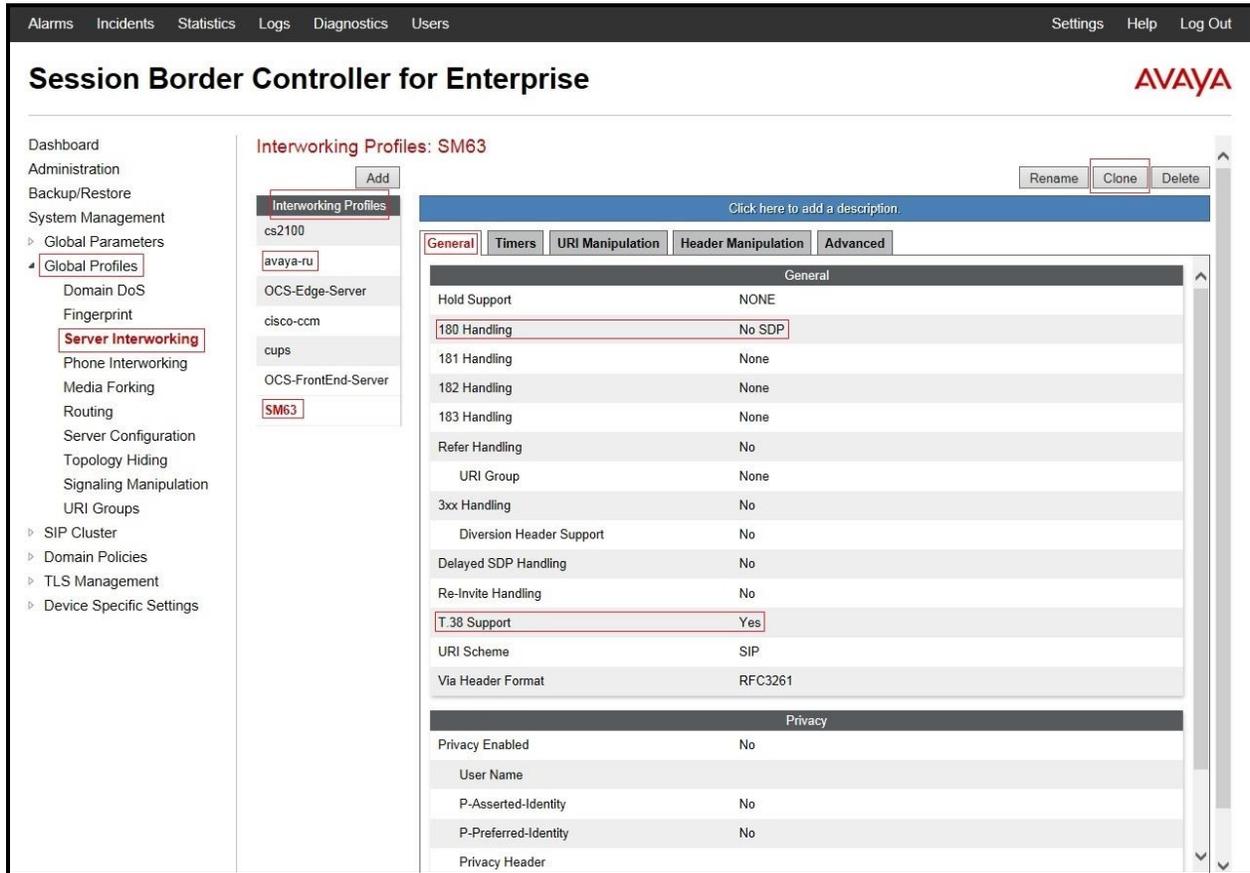


Figure 73 - Server Interworking – Avaya site

7.2.2. Configure Server Interworking – Virgin Media Site

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** and click **Add** as highlighted below.

- Enter **Profile Name: SP4**.
- On the **General** tab, set **T.38 Support** as **Yes** (if using Fax T.38) or **No** (if using Fax G.711 pass-through). Other options can be left at default.
- On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that the Virgin Media SIP Trunk Service interworking profile (named **SP4**) was added.

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

The left sidebar contains a navigation menu with categories like 'Dashboard', 'Administration', 'System Management', 'Global Profiles', 'SIP Cluster', 'Domain Policies', 'TLS Management', and 'Device Specific Settings'. Under 'Global Profiles', 'Server Interworking' is highlighted.

The main content area is titled 'Interworking Profiles: SP4'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a list of interworking profiles: 'cs2100', 'avaya-ru', 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'OCS-FrontEnd-Server', 'SM63', and 'SP4' (which is selected and highlighted with a red box).

The configuration for the selected profile 'SP4' is shown in a tabbed interface with tabs for 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced'. The 'General' tab is active, displaying 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	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

Figure 74 - Server Interworking – Virgin Media site

7.2.3. Configure URI Groups

The URI Group feature allows administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in the particular domain or group.

The following URI Group configuration is used for the compliance test in a lab environment where equipment is for shared use. The URI-Group named **SP4** was used to match the “From” and “To” headers in a SIP call dialog received from both Enterprise and Virgin Media SIP Trunk Service. If there is a match, the Avaya SBCE will apply the appropriate Routing Profiles (see **Section 7.2.4, 7.2.5**), Server Flows (see **Section 7.4.4**), and Session Flow (see **Section 7.4.5**) to route incoming and outgoing calls to the right destinations. In the production environment, there is not a requirement to define this URI Group.

From the menu on the left-hand side, select **Global Profiles → URI Groups**. Select **Add** as highlighted below.

- Enter **Group Name: SP4**.
- Edit the **URI Type: Regular Expression** (not shown).
- **Add URI: .*10\10\98\111** (Avaya SBCE public interface IP address), **.*10\10\98\13** (Avaya SBCE internal interface IP address), **.*10\10\98\23** (Avaya SBCE internal interface IP address), **.*192\168\171\234** (Virgin Media SBC B), **.*192\168\222\186** (Virgin Media SBC A), **.*anonymous\invalid** (Anonymous URI), **.*bvwdev7\com** (Enterprise domain).
- Click **Finish** (not shown).

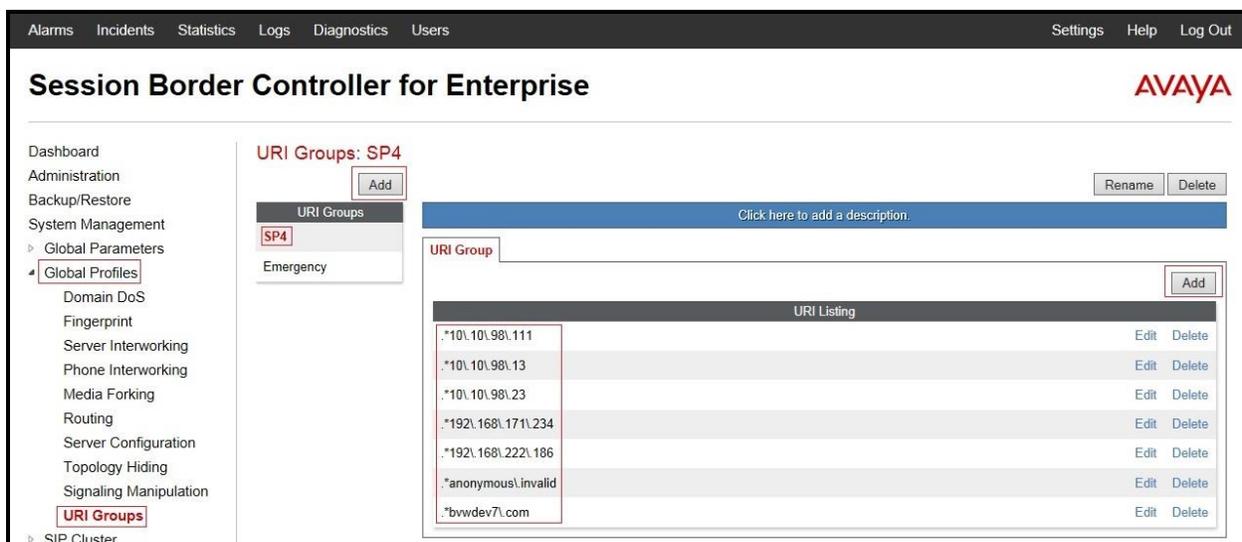


Figure 75 - URI Group

7.2.4. Configure Routing – Avaya Site

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.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SP4_To_SM63**.

- **URI Group: SP4** (Refer to **Section 7.2.3**).
- **Next Hop Server 1: 10.33.10.26:5060** (Session Manager IP address).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the AVAYA logo. A left-hand navigation menu lists various system management options, with "Global Profiles" and "Routing" highlighted. The main content area is titled "Routing Profiles: SP4_To_SM63" and features an "Add" button. Below this, a table lists existing routing profiles. The table has columns for Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. One profile is listed with Priority 1, URI Group SP4, and Next Hop Server 1 10.33.10.26:5060. There are "View" and "Edit" buttons for this profile. An "Add" button is also present at the end of the table.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	SP4	10.33.10.26:5060	---	View Edit

Figure 76 - Routing to Avaya

7.2.5. Configure Routing – Virgin Media Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SM63_To_SP4_SBCa**.

- **URI Group: SP4** (Refer to **Section 7.2.3**).
- **Next Hop Server 1: 192.168.222.186:5060** (Virgin Media SBC A).
- **Next Hop Server 2: 192.168.171.234:5060** (Virgin Media SBC B).

Note: When the heartbeat (See **Section 7.2.8** and **7.2.9**) is setup to send from Avaya SBCE to both Virgin Media SBC A and Virgin Media SBC B, the call will be routed to the Next Hop Server 1 unless this server 1 doesn't respond to the heartbeat (OPTIONS). If the heartbeat on server 1 is down, the call will be routed to the Next Hop Server 2.

- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown).

The following screen shows the Routing Profile to Virgin Media SBC A.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Routing' highlighted. The main content area is titled 'Routing Profiles: SM63_To_SP4_SBCa' and features an 'Add' button. Below this, a table lists the configured routing profiles:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	SP4	192.168.222.186:5060	192.168.171.234:5060	View Edit

Figure 77 - Routing to Virgin Media SBC A

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SM63_To_SP4_SBCb**.

- **URI Group: SP4** (Refer to **Section 7.2.3**).
- **Next Hop Server 1: 192.168.171.234:5060** (Virgin Media SBC B).
- **Next Hop Server 2: 192.168.222.186:5060** (Virgin Media SBC A).

Note: When the heartbeat (See **Section 7.2.8** and **7.2.9**) is setup to send from Avaya SBCE to both Virgin Media SBC A and Virgin Media SBC B, the call will be routed to the Next Hop Server 1 unless this server 1 doesn't respond to the heartbeat (OPTIONS). If the heartbeat on server 1 is down, the call will be routed to the Next Hop Server 2.

- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown).

The following screen shows the Routing Profile to Virgin Media SBC B.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Global Profiles' expanded to show 'Routing' highlighted. The main content area is titled 'Routing Profiles: SM63_To_SP4_SBCb' and features an 'Add' button. Below this, a table lists existing routing profiles: 'default', 'SP4_To_SM63', 'SM63_To_SP4_SBCa', and 'SM63_To_SP4_SBCb' (highlighted). To the right, a configuration form for the selected profile is shown, including a description field and a table for Next Hop Servers.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	SP4	192.168.171.234:5060	192.168.222.186:5060	View Edit

Figure 78 - Routing to Virgin Media SBC B

7.2.6. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

- Select **Global Profiles** from the menu on the left-hand side.
- Select the **Signaling Manipulation**.
- Select **Add**. Enter **Script Title: SP4**. In the script editing window, enter the text exactly as shown in the screenshot below to remove unwanted SIP Headers from outgoing calls. (See Appendix 12).
- Click **Save** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various configuration areas, with 'Signaling Manipulation' highlighted. The main content area is titled 'Signaling Manipulation Scripts: SP4' and contains a list of scripts: 'Signaling Manipulation Scripts', 'Rogers', 'OutboundChgContact', and 'SP4'. The 'SP4' script is selected, and its configuration is shown in a text editor. The script content is as follows:

```
within session "All"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    // Remove unwanted Headers

    remove(%HEADERS["History-Info"][2]);
    remove(%HEADERS["History-Info"][1]);
    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["x-nt-e164-clid"][1]);
    remove(%HEADERS["P-AV-Message-Id"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["Av-Global-Session-ID"][1]);
    remove(%HEADERS["Remote-Party-ID"][1]);
    remove(%HEADERS["Remote-Address"][1]);
    remove(%HEADERS["P-Location"][1]);
  }
}
```

Figure 79 – Signaling Manipulation

7.2.7. Configure Server – Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** and click **Add** as highlighted below.

Enter **Profile Name: SM63**.

On **General** tab, enter the following:

- **Server Type:** Select **Call Server**.
- **IP Address/FQDNs:** **10.33.10.26** (Session Manager IP Address).
- **Supported Transports:** **UDP**.
- **UDP Port:** **5060**.
- Click **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left-hand navigation menu lists various system management options, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: SM63' and features an 'Add' button. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a configuration table with the following data:

Server Type	Call Server
IP Addresses / FQDNs	10.33.10.26
Supported Transports	UDP
UDP Port	5060

An 'Edit' button is located at the bottom right of the configuration table. The left-hand menu also shows 'Global Profiles' expanded, with 'SM63' listed under it.

Figure 80 – Session Manager - General Server Configuration

On the **Advanced** tab:

- Check on **Enable Grooming**.
- Select **SM63** for **Interworking Profile**.
- Click **Finish** (not shown).

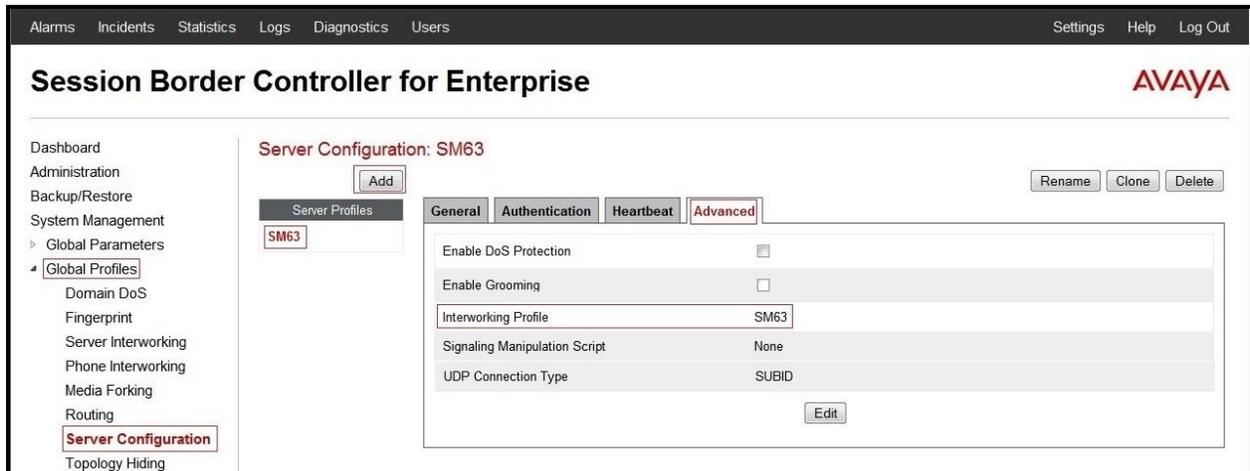


Figure 81 – Session Manager - Advanced Server Configuration

7.2.8. Configure Server – Virgin Media SBC A

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** and click **Add** as highlighted below.

Enter **Profile Name: SP4_SBCa**.

On **General** tab, enter the following:

- **Server Type:** Select **Trunk Server**.
- **IP Address:** **192.168.222.186** (Virgin Media SBC A).
- **Supported Transports:** **UDP**.
- **UDP Port:** **5060**.
- Click **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: SP4_SBCa' and features an 'Add' button. Below this, a 'Server Profiles' list shows 'SM63' and 'SP4_SBCa'. The 'General' tab is active, displaying a configuration table with the following details:

Field	Value
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.222.186
Supported Transports	UDP
UDP Port	5060

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

Figure 82 – Virgin Media SBC A - General Server Configuration

On the **Authentication** tab, edit the following:

- Check **Enable Authentication**.
- Enter **User Name: virginpbx01_011XXX74140** (Virgin Media provided this information).
- Leave **Realm** as blank.
- Enter **Password: XXXXX** (Virgin Media provided this information).
- Enter **Confirm Password: XXXXX** (Virgin Media provided this information).
- Click **Finish**.

The screenshot shows a configuration window titled "Edit Server Configuration Profile - Authentication". At the top, there is a checkbox labeled "Enable Authentication" which is checked. Below this, there are four input fields: "User Name" containing "virginpbx01_011XXX741", "Realm" (empty), "Password" (masked with four dots), and "Confirm Password" (masked with four dots). A "Finish" button is located at the bottom center of the form area.

Figure 83 – Virgin Media SBC A - Authentication Server Configuration

On the **Heartbeat** tab, enter the following:

- Check **Enable Heartbeat**.
- Select **Method: OPTIONS**.
- Enter **Frequency: 60 seconds**.
- Enter **From URI: virginpbx01_011XXX74140@10.10.98.111**.
- Enter **To URI: virginpbx01_011XXX74140@192.168.222.186**.
- Click **Finish** (not shown).

Heartbeat Configuration	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	virginpbx01_011XXX74140@10.10.98.111
To URI	virginpbx01_011XXX74140@192.168.222.186

Figure 84 – Virgin Media SBC A - Heartbeat Server Configuration

On the **Advanced** tab, enter the following:

- **Interworking Profile:** Select **SP4** (Refer to **Section 7.2.2**).
- **Signaling Manipulation Script:** Select **SP4** (Refer to **Section 7.2.6**).
- Click **Finish** (not shown).

General	Authentication	Heartbeat	Advanced
Enable DoS Protection			<input type="checkbox"/>
Enable Grooming			<input type="checkbox"/>
Interworking Profile			SP4
Signaling Manipulation Script			SP4
UDP Connection Type			SUBID

Figure 85 - Virgin Media SBC A - Advanced Server Configuration

7.2.9. Configure Server – Virgin Media SBC B

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** and click **Add** as highlighted below.

Enter **Profile Name: SP4_SBCb**.

On **General** tab, enter the following:

- **Server Type:** Select **Trunk Server**.
- **IP Address:** **192.168.171.234** (Virgin Media SBC B).
- **Supported Transports:** **UDP**.
- **UDP Port:** **5060**.
- Click **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Server Configuration' highlighted in red. The main content area is titled 'Server Configuration: SP4_SBCb' and features an 'Add' button. Below this, a list of server profiles includes 'SM63', 'SP4_SBCa', and 'SP4_SBCb' (highlighted in red). The 'General' tab is active, showing a configuration table with the following details:

Field	Value
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.171.234
Supported Transports	UDP
UDP Port	5060

An 'Edit' button is located at the bottom right of the configuration table. Additional buttons for 'Rename', 'Clone', and 'Delete' are visible at the top right of the configuration area.

Figure 86 – Virgin Media SBC B - General Server Configuration

On the **Authentication** tab, edit the following:

- Check **Enable Authentication**.
- Enter **User Name: virginpbx01_011XXX74140** (Virgin Media provided this information).
- Enter **Realm** as blank.
- Enter **Password: XXXXX** (Virgin Media provided this information).
- Enter **Confirm Password: XXXXX** (Virgin Media provided this information).
- Click **Finish**.

The screenshot shows a configuration window titled "Edit Server Configuration Profile - Authentication". At the top, there is a checkbox labeled "Enable Authentication" which is checked. Below this, there are four input fields: "User Name" containing "virginpbx01_011XXX741", "Realm" (empty), "Password" (masked with four dots), and "Confirm Password" (masked with four dots). A "Finish" button is located at the bottom center of the form area.

Figure 87 – Virgin Media SBC B - Authentication Server Configuration

On the **Heartbeat** tab, enter the following:

- Check **Enable Heartbeat**.
- Select **Method: OPTIONS**.
- Enter **Frequency: 60 seconds**.
- Enter **From URI: virginpbx01_011XXX74140@10.10.98.111**.
- Enter **To URI: virginpbx01_011XXX74140@192.168.171.234**.
- Click **Finish** (not shown).

Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	virginpbx01_011XXX74140@10.10.98.111
To URI	virginpbx01_011XXX74140@192.168.171.234

Figure 88 – Virgin Media SBC B - Heartbeat Server Configuration

On the **Advanced** tab, enter the following:

- **Interworking Profile:** select **SP4** (Refer to **Section 7.2.2**).
- **Signaling Manipulation Script:** select **SP4** (Refer to **Section 7.2.6**).
- Click **Finish** (not shown).

General	Authentication	Heartbeat	Advanced
Enable DoS Protection			<input type="checkbox"/>
Enable Grooming			<input type="checkbox"/>
Interworking Profile			SP4
Signaling Manipulation Script			SP4
UDP Connection Type			SUBID

Figure 89 - Virgin Media SBC B - Advanced Server Configuration

7.2.10. Configure Topology Hiding – Avaya Site

The Topology Hiding screen allows one to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name: SP4_To_SM63**. Click **Finish** (not shown).

Select **SP4_To_SM63** under **Topology Hiding Profiles**, and click **Edit**.

- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**.
 - In the **Replace Action** column select: **Overwrite**.
 - In the **Overwrite Value** column: **bwvdev7.com**.
- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**.
 - In the **Replace Action** column select: **Overwrite**.
 - In the **Overwrite Value** column: **bwvdev7.com**.
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**.
 - In the **Replace Action** column select: **Overwrite**.
 - In the **Overwrite Value** column: **bwvdev7.com**.

Click **Finish** (not shown).

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bwvdev7.com
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	bwvdev7.com
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Overwrite	bwvdev7.com
SDP	IP/Domain	Auto	---

Figure 90 - Topology Hiding Session Manager

7.2.11. Configure Topology Hiding – Virgin Media Site

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name: SM63_To_SP4**. Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a navigation menu lists various configuration areas, with "Global Profiles" expanded to show "Topology Hiding" selected. The main content area is titled "Topology Hiding Profiles: SM63_To_SP4" and features an "Add" button. Below this, a list of profiles includes "default", "SP4_To_SM63", and "SM63_To_SP4". The "SM63_To_SP4" profile is selected, and its configuration is shown in a table with columns for Header, Criteria, Replace Action, and Overwrite Value. The table lists headers such as Refer-To, Via, Request-Line, Record-Route, From, Referred-By, To, and SDP, all with a criteria of "IP/Domain" and a replace action of "Auto". An "Edit" button is located at the bottom of the table.

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

Figure 91 - Topology Hiding Virgin Media

7.3. Domain Policies

The Domain Policies feature allows one to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or one can create a custom domain policy.

7.3.1. Create Signaling Rules

Signaling Rules allow one to 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 UC-Sec, 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.

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter **Clone Name: SP4**.
 - Click **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left-hand navigation menu lists various management options, with "Domain Policies" and "Signaling Rules" highlighted. The main content area is titled "Signaling Rules: SP4" and features a list of rules with "SP4" selected. Below the list, there are tabs for "General", "Requests", "Responses", "Request Headers", "Response Headers", "Signaling QoS", and "UCID". The "Requests" tab is active, showing a table of inbound and outbound request types and their actions. The "Responses" tab is also active, showing a table of response types and their actions. The "Content-Type Policy" section includes a checkbox for "Enable Content-Type Checks" (checked) and a table for "Action" (Allow, Multipart Action, Allow) and "Exception List".

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy	
Enable Content-Type Checks	<input checked="" type="checkbox"/>
Action	Allow
Multipart Action	Allow
Exception List	Exception List

Figure 92 – Virgin Media Signaling Rule 1

The following configuration on the Virgin Media Signaling Rule converts 183 with SDP to 180 with no SDP. Note: The following configuration is optional and this is a workaround to resolve the ring-back-tone issue on blind transfer call.

Form the list of **Signaling Rules**, select **SP4** to edit:

- Select the **Response Headers** tab.
- Select **Add In Header Control**.
 - **Header Name: Contact.**
 - **Response Code: 183.**
 - **Method Name: INVITE.**
 - **Header Criteria: Forbidden.**
 - **Presence Action: Change response to 180 Ringing.**
 - **Direction: IN.**
- Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise interface. The left sidebar contains navigation options like Dashboard, Administration, and Signaling Rules. The main area displays the configuration for 'Signaling Rules: SP4'. The 'Response Headers' tab is selected, and an 'Add In Header Control' rule is visible in the table below.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Contact	183	INVITE	Forbidden	Change response to "180 Ringing"	No	IN	Edit Delete

Figure 93 - Virgin Media Signaling Rule 2

7.3.2. Create End Point Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SM63_SP4_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: default.**
 - **Time of Day: default.**
- Select **Finish** (not shown).

The screenshot displays the Avaya Session Manager web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo. The left-hand navigation menu is expanded to 'Domain Policies', with 'End Point Policy Groups' selected. The main content area shows the configuration for 'Policy Groups: SM63_SP4_PolicyG'. It includes an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this is a table of policy rules with the following data:

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

Figure 94 – Session Manager - End Point Policy Group

From the menu on the left-hand side, select **Domain Policies** → **End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SP4_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: SP4 (See Section 7.3.1).**
 - **Time of Day: default.**
- Select **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various configuration areas, with 'Domain Policies' and 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: SP4_PolicyG' and features an 'Add' button, a 'Filter By Device...' dropdown, and 'Rename', 'Clone', and 'Delete' buttons. Below this, there are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.'. A 'Policy Group' section contains a 'Summary' button and an 'Add' button. A table lists the policy group's configuration:

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	default	default	default-low-med	default-med	SP4	default	Edit Clone

Figure 95 - Virgin Media - End Point Policy Group

7.3.3. Create Session Policy

Session Policies allow users to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

From the menu on the left-hand side, select **Domain Policies** → **Session Policies**.

- Select the **default** policy.
- Select **Clone** button.
 - Enter **Clone Name: SP4**.
 - Click **Finish** (not shown).

From the list of **Session Policies**, select **SP4**.

- On **Codec Prioritization** tab, click **Edit**.
 - Check **Codec Prioritization**.
 - Select **Preferred Codec#1: PCMA (8)**.
 - Select **Preferred Codec#2: G729 (18)**.
 - Select **Preferred Codec#3: PCMU (0)**.
 - Select **Preferred Codec#4: Dynamic (101)**.
 - Select **Finish** (not shown).

Note: The purpose of this setting was used for codec priority testing only.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo. A left-hand navigation menu lists various system management options, with 'Domain Policies' and 'Session Policies' highlighted. The main content area is titled 'Session Policies: SP4' and features a list of policies with 'default' and 'SP4' visible. The 'SP4' policy is selected, and the 'Codec Prioritization' tab is active. The configuration shows 'Codec Prioritization' checked under the 'Audio Codec' section. Below this, there is a table of preferred codecs:

Preferred Codec #	Codec Name (Priority)
Preferred Codec #1	PCMA (8)
Preferred Codec #2	G729 (18)
Preferred Codec #3	PCMU (0)
Preferred Codec #4	Dynamic (101)

The 'Video Codec' section below shows 'Codec Prioritization' unchecked. An 'Edit' button is visible at the bottom of the configuration area.

Figure 96 - Virgin Media - Session Policy – Codec Prioritization

- On **Media** tab, click Edit.
 - Check **Media Anchoring**.
 - Select **Finish** (not shown).

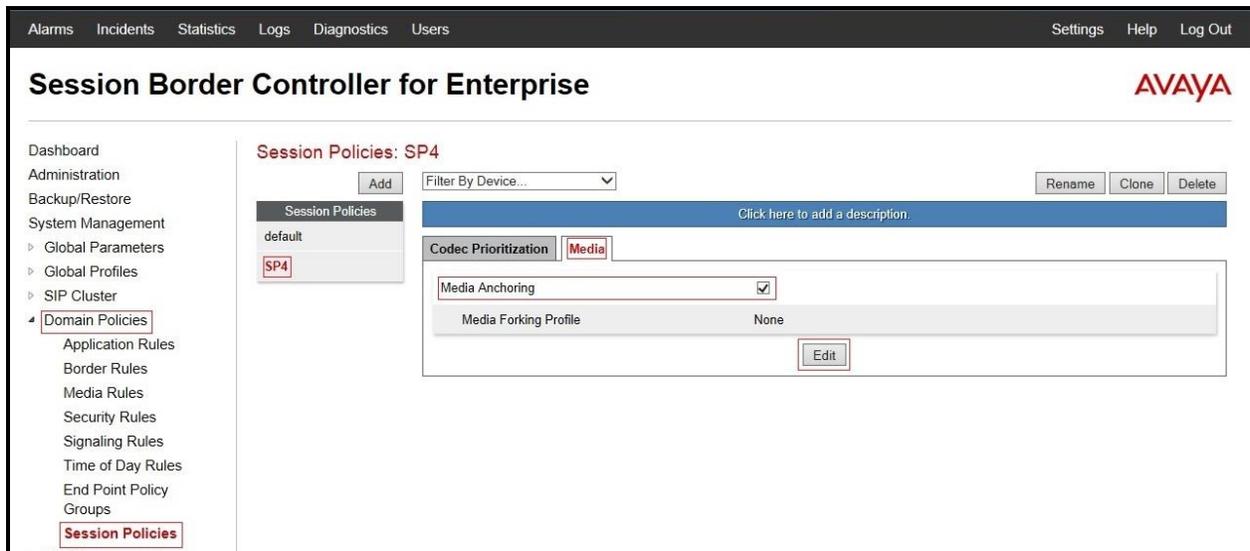


Figure 97 - Virgin Media - Session Policy – Anchoring Media

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, one has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
 - **IP Address** for Inside interface: **10.10.98.13**; **Gateway: 10.10.98.1**.
 - **IP Address** for Inside interface: **10.10.98.23**; **Gateway: 10.10.98.1**.
 - **IP Address** for Outside interface: **10.10.98.111**; **Gateway: 10.10.98.97**.

Note: In the test configuration, two IP addresses were used on the inside interface so that different server flows could be assigned depending on which interface address the SIP messages were received on. These server flows were used to direct traffic to the two Virgin Media SBCs separately.

- Select the physical interface used in the Interface column:
 - **Inside Interface: A1.**
 - **Outside Interface: B1.**

The screenshot displays the 'Network Management: SBCE62' interface. It features a navigation menu on the left with 'Device Specific Settings' expanded to 'Network Management'. The main content area has two tabs: 'Network Configuration' and 'Interface Configuration'. A warning banner at the top states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, a blue bar indicates 'Changes will not take effect until the interface is updated.' The configuration section includes fields for 'A1 Netmask' (255.255.255.192), 'A2 Netmask', 'B1 Netmask' (255.255.255.224), and 'B2 Netmask'. An 'Add' button is present. A table below lists configurations for three entries:

IP Address	Public IP	Gateway	Interface	Delete
10.10.98.13		10.10.98.1	A1	Delete
10.10.98.111		10.10.98.97	B1	Delete
10.10.98.23		10.10.98.1	A1	Delete

Figure 98 - Network Management

- Select the **Interface Configuration** tab.
- Toggle the state of the physical interfaces being used to **Enabled**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. At the top, there is a navigation bar with links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu includes options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The "Device Specific Settings" menu is expanded, showing "Network Management" and "Media Interface".

The main content area is titled "Network Management: SBCE62". It features two tabs: "Network Configuration" and "Interface Configuration". The "Interface Configuration" tab is active, displaying a table with the following data:

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

Figure 99 - Network Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya can be used for both inside and outside ports.

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

- Select **Add**.
 - **Name: InsideMedia1.**
 - **Media IP: 10.10.98.13** (Internal IP Address toward Session Manager – Virgin Media SBC A).
 - **Port Range: 35000 – 40000.**
 - Click **Finish** (not shown).
- Select **Add**
 - **Name: InsideMedia2.**
 - **Media IP: 10.10.98.23** (Internal IP Address toward Session Manager – Virgin Media SBC B).
 - **Port Range: 35000 – 40000.**
 - Click **Finish** (not shown).
- Select **Add**.
 - **Name: OutsideMedia.**
 - **Media IP: 10.10.98.111** (External IP Address toward Virgin Media SIP Trunk Service).
 - **Port Range: 35000 – 40000.**
 - Click **Finish** (not shown).

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ **Device Specific Settings**
‣ Network Management
‣ **Media Interface**

Media Interface: SBCE62

Devices
SBCE62

Media Interface

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

Name	Media IP	Port Range	Edit	Delete
InsideMedia1	10.10.98.13	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.111	35000 - 40000	Edit	Delete
InsideMedia2	10.10.98.23	35000 - 40000	Edit	Delete

Add

Figure 100 - Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add**.
 - **Name: InsideUDP1.**
 - **Media IP: 10.10.98.13** (Internal IP Address toward Session Manager – Virgin Media SBC A).
 - **UDP Port: 5060.**
 - Click **Finish** (not shown).
- Select **Add**.
 - **Name: InsideUDP2.**
 - **Media IP: 10.10.98.23** (Internal IP Address toward Session Manager – Virgin Media SBC B).
 - **UDP Port: 5060.**
 - Click **Finish** (not shown).
- Select **Add**.
 - **Name: OutsideUDP.**
 - **Media IP: 10.10.98.111** (External IP Address toward Virgin Media SIP Trunk Service).
 - **UDP Port: 5060.**
 - Click **Finish** (not shown).

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
‣ Network Management
‣ Media Interface
‣ **Signaling Interface**

Devices
SBCE62

Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideUDP1	10.10.98.13	---	5060	---	None	Edit Delete
OutsideUDP	10.10.98.111	---	5060	---	None	Edit Delete
InsideUDP2	10.10.98.23	---	5060	---	None	Edit Delete

Add

Figure 101 - Signaling Interface

7.4.4. Configuration End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the 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 policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Session Manager and the Virgin Media SIP Trunk Service.

Two server flows are required for outgoing traffic and two are required for incoming. This is so that traffic can be routed to both the network SBCs and can also be received from both network SBCs. As mentioned previously, the network SBCs have been designated as Virgin Media SBC A and Virgin Media SBC B for the purposes of the testing and documentation.

7.4.4.1 Create End Point Flows – Session Manager Flows

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name: SP4_TrunkA**.
 - **Server Configuration: SP4_SBCa** (refer to **Section 7.2.8**).
 - **URI Group: SP4** (refer to **Section 7.2.3**).
 - **Transport: ***.
 - **Remote Subnet: ***.
 - **Received Interface: InsideUDP1** (refer to **Section 7.4.3**).
 - **Signaling Interface: OutsideUDP** (refer to **Section 7.4.3**).
 - **Media Interface: OutsideMedia** (refer to **Section 7.4.2**).
 - **End Point Policy Group: SP4_PolicyG** (refer to **Section 7.3.2**).
 - **Routing Profile: SP4_To_SM63** (refer to **Section 7.2.4**).
 - **Topology Hiding Profile: SM63_To_SP4** (refer to **Section 7.2.11**).
 - Click **Finish**.

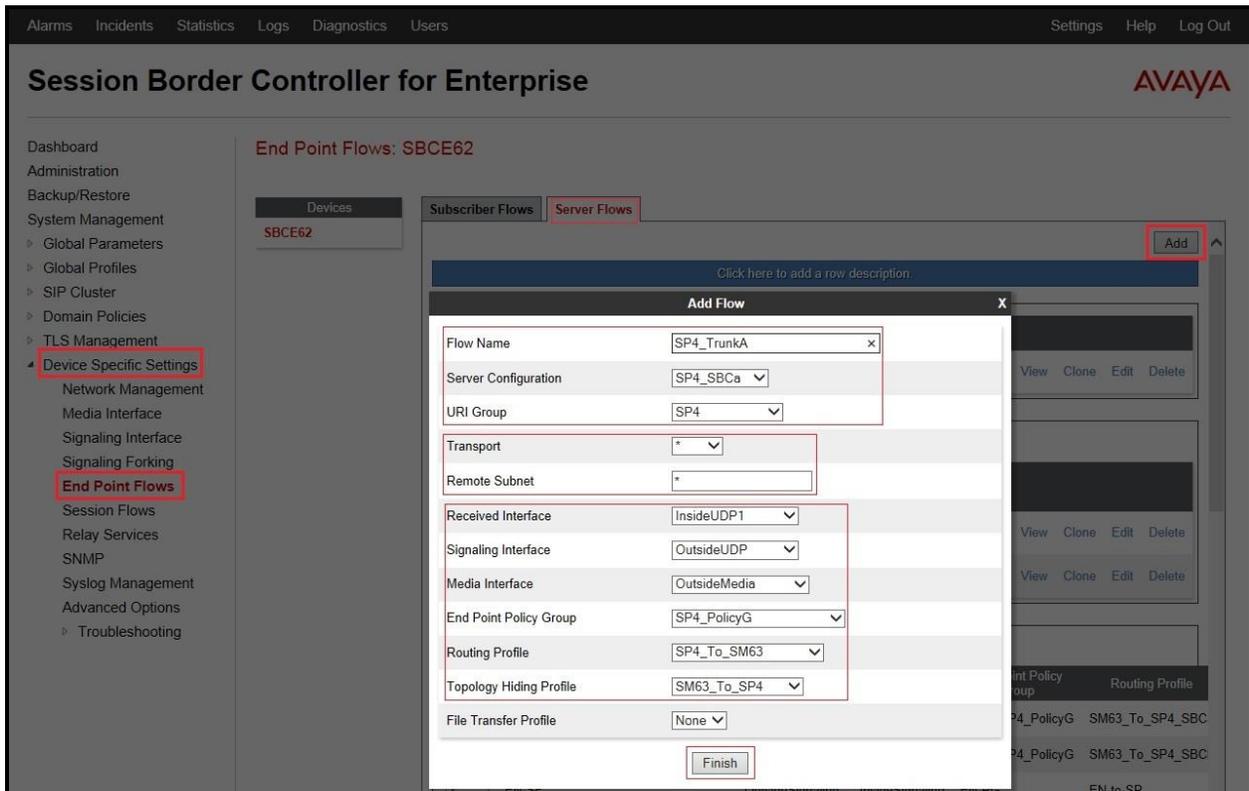


Figure 102 - End Point Flows 1

- Select the **Server Flows** tab
- Select **Add**, enter **Flow Name: SP4_TrunkB**.
 - **Server Configuration: SP4_SBCb** (refer to **Section 7.2.9**).
 - **URI Group: SP4** (refer to **Section 7.2.3**).
 - **Transport: ***.
 - **Remote Subnet: ***.
 - **Received Interface: InsideUDP2** (refer to **Section 7.4.3**).
 - **Signaling Interface: OutsideUDP** (refer to **Section 7.4.3**).
 - **Media Interface: OutsideMedia** (refer to **Section 7.4.2**).
 - **End Point Policy Group: SP4_PolicyG** (refer to **Section 7.3.2**).
 - **Routing Profile: SP4_To_SM63** (refer to **Section 7.2.4**).
 - **Topology Hiding Profile: SM63_To_SP4** (refer to **Section 7.2.11**).
 - Click **Finish**.

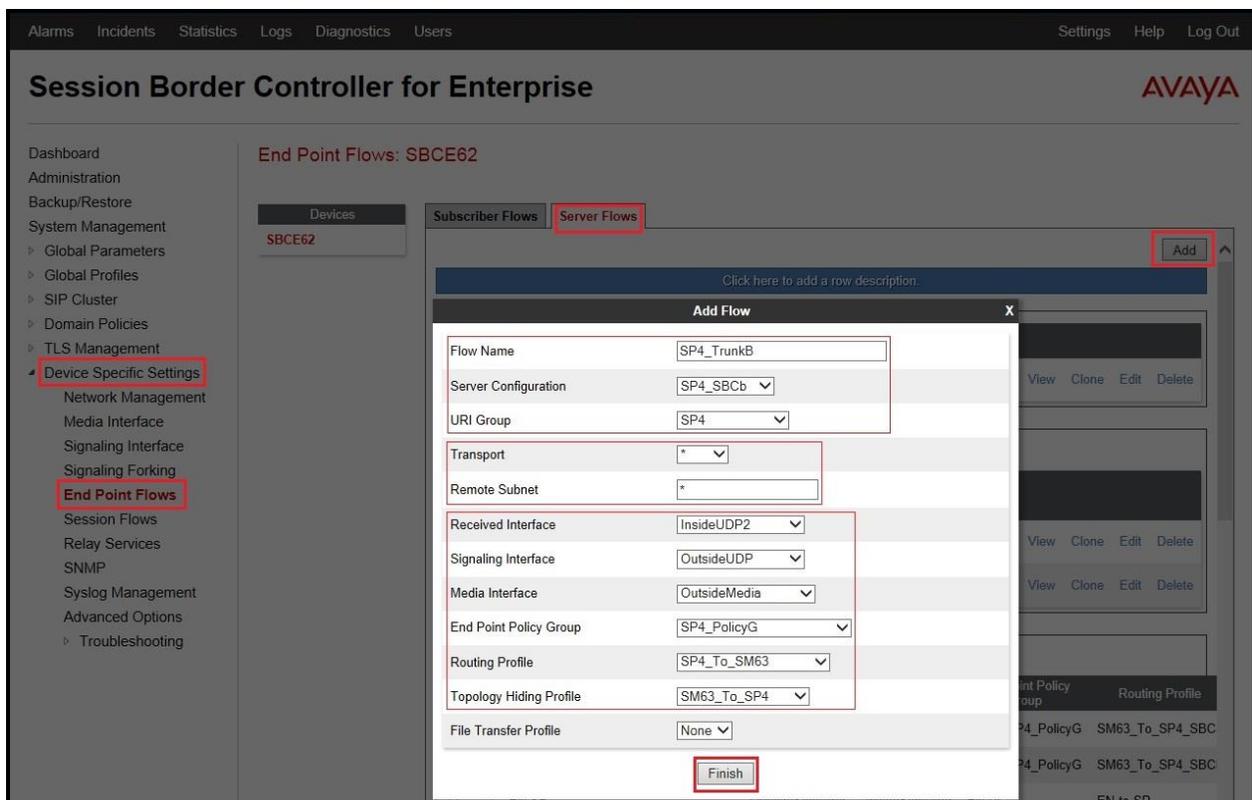


Figure 103 - End Point Flows 2

7.4.4.2 Create End Point Flows – Trunk Flows

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name: SP4_SBCa**.
 - **Server Configuration: SM63** (Refer to **Section 7.2.7**).
 - **URI Group: SP4** (Refer to **Section 7.2.3**).
 - **Transport: ***.
 - **Remote Subnet: ***.
 - **Received Interface: OutsideUDP** (refer to **Section 7.4.3**).
 - **Signaling Interface: InsideUDP1** (refer to **Section 7.4.3**).
 - **Media Interface: InsideMedia1** (refer to **Section 7.4.2**).
 - **End Point Policy Group: SM63_SP4_PolicyG** (refer to **Section 7.3.2**).
 - **Routing Profile: SM63_To_SP4_SBCa** (refer to **Section 7.2.5**).
 - **Topology Hiding Profile: SP4_To_SM63** (refer to **Section 7.2.10**).
 - Click **Finish**.

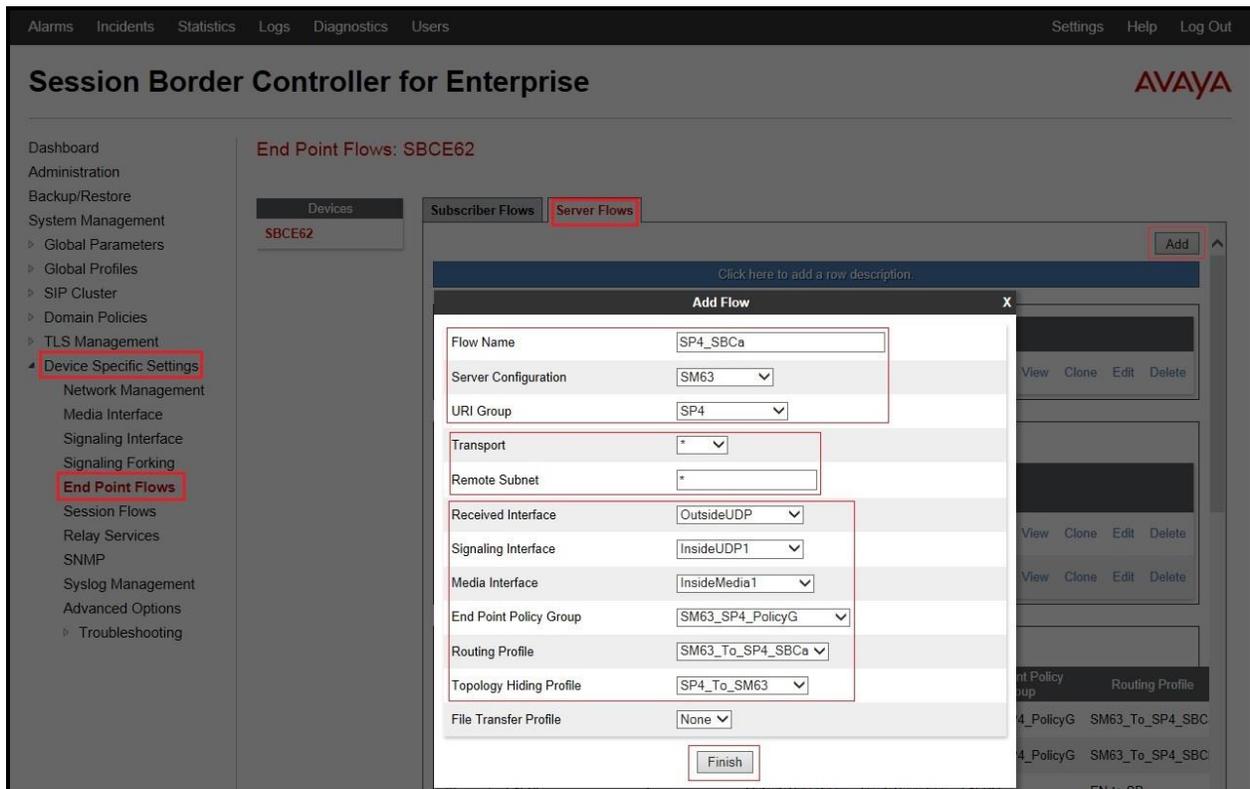


Figure 104 - End Point Flows 3

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name: SP4_SBCb**.
 - **Server Configuration: SM63** (Refer to **Section 7.2.7**).
 - **URI Group: SP4** (Refer to **Section 7.2.3**).
 - **Transport: ***.
 - **Remote Subnet: ***.
 - **Received Interface: OutsideUDP** (refer to **Section 7.4.3**).
 - **Signaling Interface: InsideUDP2** (refer to **Section 7.4.3**).
 - **Media Interface: InsideMedia2** (refer to **Section 7.4.2**).
 - **End Point Policy Group: SM63_SP4_PolicyG** (refer to **Section 7.3.2**).
 - **Routing Profile: SM63_To_SP4_SBCb** (refer to **Section 7.2.5**).
 - **Topology Hiding Profile: SP4_To_SM63** (refer to **Section 7.2.10**).
 - Click **Finish**.

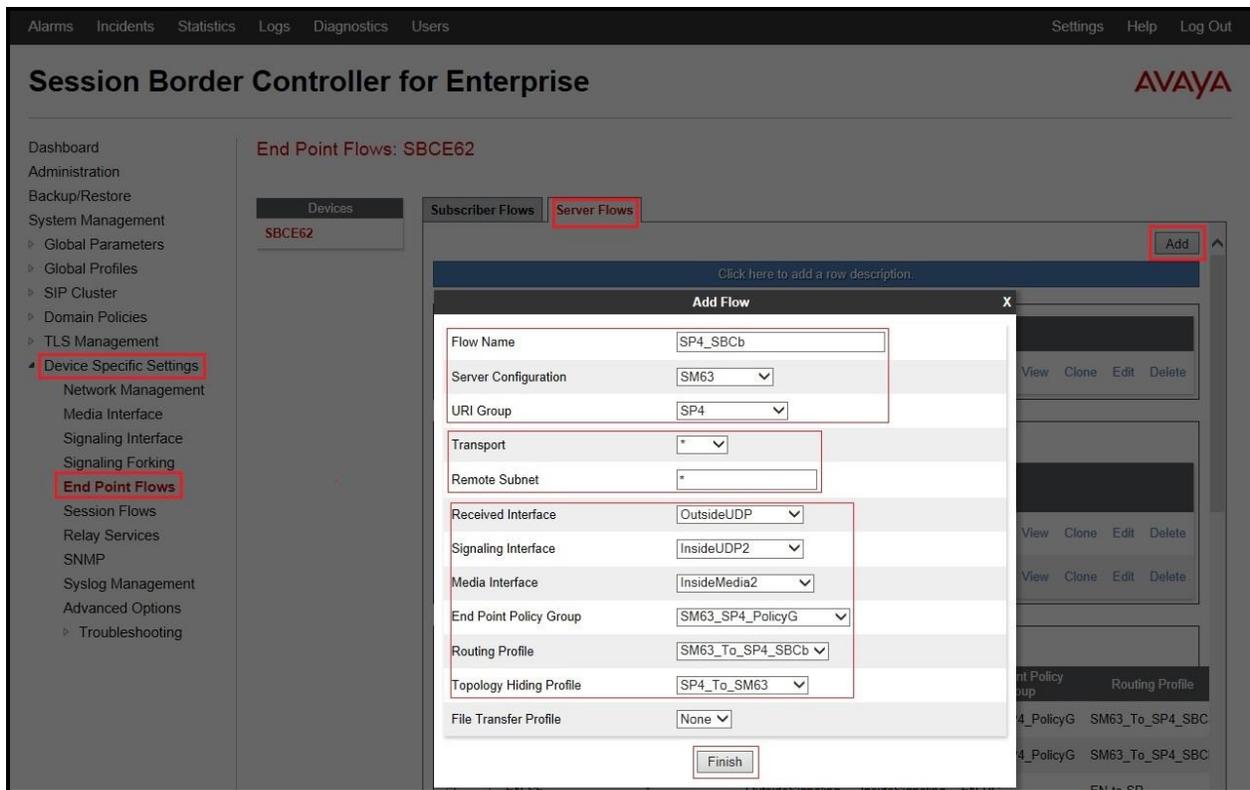


Figure 105 - End Point Flows 4

7.4.5. Create Session Flows

Session Flow determines the media (audio/video) sessions in order to apply the appropriate session policy.

- Select **Device Specific Settings** from the menu on the left-hand side.
- Select the **Session Flows**.
- Select **Add**.
- Enter **Flow Name: SP4**.
 - **URI Group#1: SP4** (refer to **Section 7.2.3**).
 - **URI Group#2: SP4** (refer to **Section 7.2.3**).
 - **Session Policy: SP4** (refer to **Section 7.3.3**).
- Select **Finish** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left-hand navigation menu lists various system management options, with "Device Specific Settings" expanded to show "Session Flows". The main content area is titled "Session Flows: SBCE62" and features a table with the following data:

Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy	
1	SP4	SP4	SP4	*	*	SP4	Clone Edit Delete

Additional interface elements include "Update" and "Add" buttons, a "Devices" dropdown menu showing "SBCE62", and a tooltip instruction: "Hover over a row to see its description."

Figure 106 – Session Flows

8. Virgin Media SIP Trunk Service Configuration

Virgin Media is responsible for the network configuration of the Virgin Media SIP Trunk Service. Virgin Media SIP Trunk Service will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. Virgin Media SIP Trunk Service will provide the IP addresses of Virgin Media's SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for CS1000, Session Manager, and Avaya SBCE discussed in the previous sections.

The configuration between Virgin Media SIP Trunk Service and the enterprise is a static configuration. There is an authentication of the SIP trunk from enterprise users to the Virgin Media's network.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

Place an inbound call from a PSTN phone to an internal Avaya phone, 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 Communication Server 1000

Active Call Trace (Id 80)

The following is an example of one of the commands available on the CS1000 to trace the DN for which the call is in progress or idle (4140). The call scenario involved PSTN phone number 1613XXX5206 calling 011XXX74140 (which is translated to phone 4140).

- Login into CS1000 Signaling Server 10.10.97.177 with admin 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 **Id 80** and then **trace 0 4140**.
- After the call is released, issue command **trac 0 4140** again to see if the DN is released back to idle state.

Below is the actual output of the CS1000 Call Server Command Line mode when the **4140** is in call state:

```
>Id 80
TRA000
.trac 0 4140

ACTIVE VTN 096 0 00 02

ORIG VTN 100 0 01 00 VTRK IPTI RMBR 101 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.98.13
FAR-END MEDIA ENDPOINT IP: 10.10.98.13 PORT: 35942
FAR-END VendorID: AVAYA-SM-6.3.7.0.637008
TERM VTN 096 0 00 02 KEY 0 SCR MARP CUST 0 DN 4140 TYPE 2002P2
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.33.5.31 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 10 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 4140
MAIN_PM ESTD
TALKSLOT ORIG 6 TERM 11
EES_DATA:
NONE
QUEU NONE
CALL ID 501 49

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 385
BEARER CAP = VOICE
HLC =
```

```
CALL STATE = 10  ACTIVE
CALLING NO = 1613XXX5206 NUM_PLAN:UNKNOWN  TON:UNKNOWN  ESN:UNKNOWN
CALLED NO = 011XXX74140 NUM_PLAN:UNKNOWN  TON:UNKNOWN  ESN:UNKNOWN
```

And this is the example after the call to 4140 is finished.

```
>ld 80
TRA000
.trac 0 4140
IDLE VTN 96 0 00 02  MARP
```

SIP Trunk monitoring (ld 32)

Place a call inbound from PSTN (1613XXX5206) to an internal device (011XXX74140). Then check the SIP trunk status by using ld 32, one trunk is BUSY.

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

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

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

9.3. Protocol Trace

Below is a wireshark trace of the same call scenario described in Section 9.2.

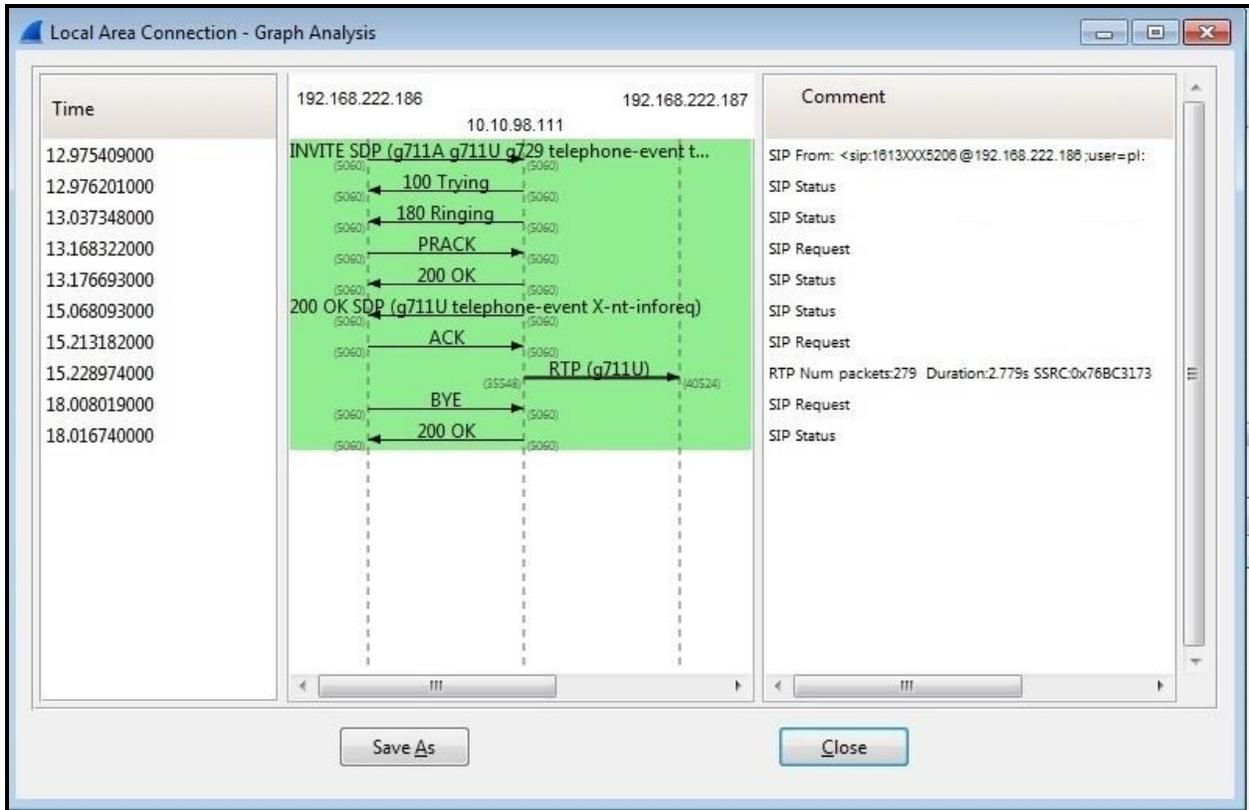


Figure 107 – SIP Call Trace

10. Conclusion

All of the test cases have been executed. Despite observations seen during the testing, as noted in **Section 2.2**, the test met the objectives outlined in **Section 2.1**. The Virgin Media SIP Trunk 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 6.2.1 Q18.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya products, including the following, is available at:
<http://support.avaya.com/>

Avaya Communication Server 1000

- [1] *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013
- [2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013
- [3] *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013
- [4] *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013
- [5] *Dialing Plans Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.
- [6] *Product Compatibility Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013

Avaya Aura[®] Session Manager/System Manager

- [7] *Administering Avaya Aura[®] Session Manager*, Release 6.3, Issue 2, June 2013
- [8] *Maintaining and Troubleshooting Avaya Aura[®] Session Manager*, Release 6.3, Issue 2, May 2013
- [9] *Administering Avaya Aura[®] System Manager*, Release 6.3, Issue 2, May 2013

Avaya Session Border Controller for Enterprise

- [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Issue 2, December 2013
- [11] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014

Product documentation for Virgin Media SIP Trunk may be found at:
<http://www.virginmediabusiness.co.uk/Products-and-solutions/Telephony-Solutions/SIP-Trunking/>

12. Appendix A: SigMa Script

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

```
within session "All"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    // Remove unwanted Headers

    remove(%HEADERS["History-Info"][2]);
    remove(%HEADERS["History-Info"][1]);
    remove(%HEADERS["Alert-Info"][1]);
    remove(%HEADERS["x-nt-e164-clid"][1]);
    remove(%HEADERS["P-AV-Message-Id"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["Av-Global-Session-ID"][1]);
    remove(%HEADERS["Remote-Party-ID"][1]);
    remove(%HEADERS["Remote-Address"][1]);
    remove(%HEADERS["P-Location"][1]);

  }
}
```

©2014 Avaya Inc. All Rights Reserved.

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

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