.

Application Notes for Configuring TDC Business 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 6.3 – Issue 1.0

Abstract

These Application Notes describe the procedure for configuration of the TDC Business 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 6.3.

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.

TDC Business Trunk Service provides PSTN access via SIP trunks between the enterprise and the TDC Business 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

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 6.3 with TDC Business Trunk Service. TDC Business Trunk Service provides PSTN access via SIP Trunks between the enterprise and the TDC Business 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 over the enterprise internal IP network. Avaya SBCE was connected to TDC Business Trunk Service's network via SIP trunks over the public Internet. Various call types were made from CS1000 to TDC Business 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 TDC Business Trunk Service, including the following:
  - Codec/ptime: G.711 a-law/20ms, G.729 a-law/20ms, G.711 mu-law/20ms, no Voice Activity Detection (VAD).
  - Calling Line Identification Display (CLID).
  - Ring-back tone.
  - Speech (audio) path.
- Incoming PSTN calls to various phone types including UNISTim, 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 UNISTim, 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.
- Various call types including: long distance, international, outbound toll-free, 11414, 1177, 118118 and 112 services.
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference). Call redirection was performed from both ends. Note: TDC Business Trunk Service supports Diversion Header for off-net call forwarding.
- Response to SIP OPTIONS queries.

- Response to incomplete call attempts and trunk errors.
- Fax using T.38.
- Inbound and outbound long-hold call stability.
- Inbound and outbound long-duration 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.
- Additional TDC Mobile Extension (MEX) call testing. With TDC Business Trunk, MEX calls from MEX enabled mobile phones are tromboned in the Avaya PBX and returned as normal Business Trunk calls. The MEX implementation relies on IN triggers on the PSTN side which prefixes the called number with a routing number used for routing the call towards the Avaya PBX.

The following are items not supported:

- Inbound toll free - TDC Business Trunk setup is not available at the compliance testing.
- CS1000 Mobile-X feature - In the TDC network, the PSTN number or mobile number should be known to be twinned to make it work. This test can only be done with mobile phones that are part of the MEX solution (i.e. the SIM cards with numbers in Sweden). If they were, tests could be executed using ANG signaling (it is added by TDC) and prefix (+46394980) added by Avaya PBX. The testing of TDC Mobile Extension (MEX) was documented in **Appendix B, Section 13**.

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 in compliance with 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 and audio path as well as 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 hold and resumed 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 successfully. However, the following observations were noted during the compliance testing:

- **TDC-sourced SIP OPTIONS included Max-Forward = 0, and Avaya responded with “483 Too Many Hops”** - The OPTIONS request is simply a keep-alive message. As long as TDC received a legitimate reply, TDC treated the connection to be alive. Of course the value of Max-Forward could be increased but since it did not cause any problem during compliance testing, TDC would like to keep the existing configuration.
- **TDC responded to Avaya-sourced SIP OPTIONS with "404 Called User Unknown"** - As long as Avaya received a legitimate reply, Avaya treated the connection to be alive.
- **Anonymous outbound call from Avaya PBX to PSTN failed** - In this call scenario, Avaya set Privacy header as “id” and sent FROM header with “anonymous” for user’s Name and ID number. TDC would reject the call because the system needed a Privacy header with “id” as well as a valid ID number instead of an anonymous ID number to trust with 3GPP specifications. In order to fix this, TDC has a workaround to replace the anonymous string with the fixed pilot user identity. Consequently, charging for these calls cannot be done on individual basis.
- **If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed**. This is a CS1000 known limitation.
- **Due to the SIP UPDATE problem, the off-net blind transfer did not work properly -** For PSTN-originated inbound calls to an Avaya Communication Server 1000 phone, the caller could not press the transfer button on Avaya Communication Server 1000 phone to complete blind transfer. In this particular scenario, SIP UPDATE support was required on the Communication Server 1000 for blind transfer, but SIP UPDATE did not work properly on the TDC PSTN-to-SIP gateway used for this interop test. In order to resolve this problem, 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). However, with this fix, when the user pressed the transfer button on the Avaya Communication Server 1000 to complete blind transfer, the original PSTN calling phone could not hear ring-back tones while the call was being transferred. In order to resolve this, the Avaya SBCE was configured to translate the SIP 183 with SDP to SIP 180 without SDP (see **Section 7.2.1** and **Section 7.3.1**), so that the original PSTN calling phone could receive the local ring-back tones. However, this translation on the Avaya SBCE removed support for early media. Customers of the TDC Business Trunk Service should be aware of this limitation before implementing this specific translation on the Avaya SBCE.
- **When the Avaya 1140E SIP telephone hosted a conference call, but dropped out of the conference first, the entire conference call was terminated** –This is a known CS1000 SIP telephone limitation.

- **Call from Mobile Extension (MEX) mobile A to any MEX Fixed network numbers or to any MEX Fixed extension numbers, the MEX Fixed number was always displayed in full length number instead of extension number** - This is the configuration of SIP manipulation on Avaya SBCE to replace the MEX mobile extension number by MEX fixed number.

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 TDC Business Trunk system, please use the support link at http://www.tdc.se/, or call the customer support number at 020-832 832.

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance test between CS1000 and TDC Business 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.

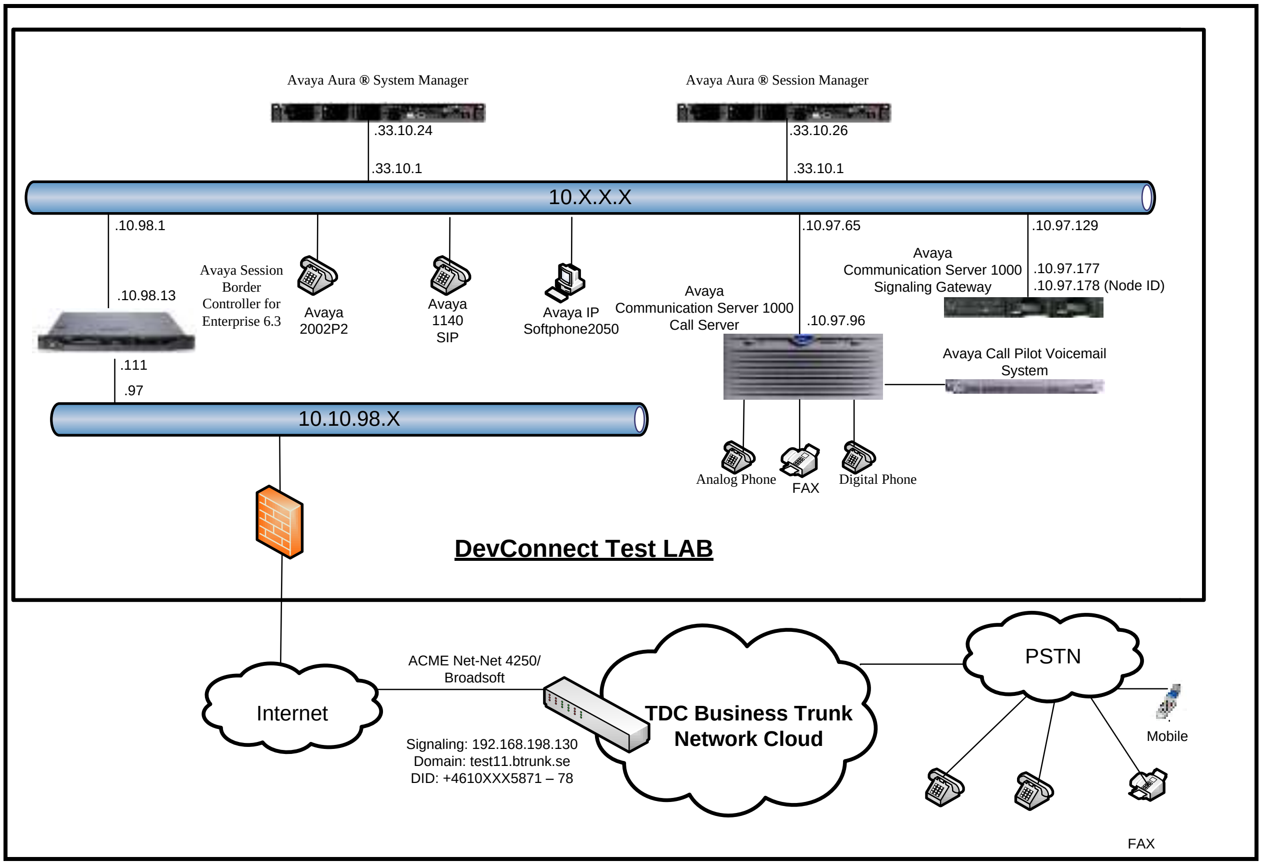

Avaya Aura ® System Manager
Avaya Aura ® Session Manager
.33.10.24
.33.10.26
.33.10.1
.33.10.1
10.X.X.X
.10.98.1
.10.97.65
.10.97.129
Avaya Session Border Controller for Enterprise 6.3
.10.98.13
Avaya 2002P2
Avaya 1140 SIP
Avaya IP Softphone2050
Avaya Communication Server 1000 Call Server
.10.97.96
Avaya Communication Server 1000 Signaling Gateway
.10.97.177
.10.97.178 (Node ID)
Avaya Call Pilot Voicemail System
.111
.97
10.10.98.X
Analog Phone
FAX
Digital Phone
DevConnect Test LAB
ACME Net-Net 4250/ Broadsoft
Internet
Signaling: 192.168.198.130
Domain: test11.btrunk.se
DID: +4610XXX5871 – 78
TDC Business Trunk Network Cloud
PSTN
Mobile
FAX

Figure 1 - Network diagram for Avaya and TDC Business Trunk Service

4. Equipment and Software Validated

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

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 Aura® Session Manager running on Avaya S8800 Server	6.3.13 (6.3.13.631303)
Avaya Aura® System Manager running on Avaya S8800 Server	6.3.13 (Build No 6.3.0.8.5682 – Patch 6.3.8.5108 Software Update Revision No: 6.3.13.10.3336)
Avaya Session Border Controller for Enterprise	6.3.2-08-5478
Avaya Phones: 2002 p2 (UNIStim) 1140E SIP	 0604DCO 04.04.18.00
Avaya 3904 Digital Phone	Core: 2.4 – Flash: 9.4 PO L1.8
Avaya IP Softphone 2050	4.04.0067
Analog Symphony 2000	N/A
HP Office jet 4500 Fax	N/A

TDC Business Trunk Service systems:

System	**Software**
ACME Net-Net 4250	Firmware SC6.1.0 MR-9 Patch 3 (Build 967)
Broadsoft	R20SP1

The following assumptions were made for the compliance tested configuration:

- CS1000 R7.6 software with latest patches.
- TDC Business Trunk Service provides support to set up, configure and troubleshoot on the TDC network side during test execution.

Additional patch lineup for the configuration is listed as follows:

Call Server: 7.65 P+ GA plus latest DEPLIST – CPM_7.6_6.zip (X2107.65P)
Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_6.ntl (7.65.16.00)
CS1000 Signaling Server patch list:

```
    [admin@car3-cores ~]$ pstat
    Product Release: 7.65.16.00
    In system patches: 5
    PATCH#   NAME      IN_SERVICE   DATE     SPECINS  TYPE   RPM
```

```
38    p31484_1   Yes        20/02/14  NO      FRU    cs1000-shared-general-7.65.16-00.i386
47    p33125_1   Yes        23/12/14  NO      FRU    cs1000-OS-1.00.00.00-00.noarch
48    p33274_1   Yes        23/12/14  YES     FRU    initscripts-8.45.25-1.el5.i386
49    p33331_1   Yes        23/12/14  YES     FRU    cs1000-OS-1.00.00.00-00.noarch
50    p33384_1   Yes        23/12/14  NO      FRU    cs1000-OS-1.00.00.00-00.noarch

In System service updates: 31
PATCH#  IN_SERVICE   DATE      SPECINS   REMOVABLE   NAME
0      Yes        23/12/14  YES      YES        cs1000-linuxbase-7.65.16.23-3.i386.000
1      Yes        23/12/14  NO       YES        cs1000-Jboss-Quantum-7.65.16.23-3.i386.000
2      Yes        23/12/14  YES      YES        cs1000-patchWeb-7.65.16.22-4.i386.000
3      Yes        23/12/14  YES      YES        cs1000-dmWeb-7.65.16.23-1.i386.000
4      Yes        23/12/14  YES      YES        cs1000-csoneksvrmgr-7.65.16.22-5.i386.000
5      Yes        23/12/14  YES      YES        cs1000-baseWeb-7.65.16.22-4.i386.000
6      Yes        23/12/14  YES      YES        cs1000-oam-logging-7.65.16.22-4.i386.000
7      Yes        23/12/14  YES      YES        cs1000-csv-7.65.16.22-2.i386.000
8      Yes        23/12/14  YES      YES        cs1000-mscTone-7.65.16.22-2.i386.000
9      Yes        23/12/14  YES      YES        cs1000-mscMusc-7.65.16.22-4.i386.000
10      Yes        23/12/14   YES      YES        cs1000-mscConf-7.65.16.22-2.i386.000
11      Yes        23/12/14   YES      YES        cs1000-mscAnnc-7.65.16.22-2.i386.000
12      Yes        23/12/14   YES      YES        cs1000-mscAttn-7.65.16.22-2.i386.000
13      Yes        23/12/14   NO      YES        cs1000-gk-7.65.16.22-1.i386.000
14      Yes        23/12/14   YES      YES        cs1000-shared-pbx-7.65.16.22-3.i386.000
15      Yes        20/02/14   NO      YES        cs1000-pd-7.65.16.21-00.i386.000
16      Yes        20/02/14   NO      YES        cs1000-shared-carrdtct-7.65.16.21-01.i386.000
17      Yes        20/02/14   NO      YES        cs1000-shared-tpselect-7.65.16.21-01.i386.000
18      Yes        20/02/14   NO      yes       cs1000-dbcom-7.65.16.21-00.i386.000
26      Yes        20/02/14   NO      YES        cs1000-snmp-7.65.16.21-00.i686.000
31      Yes        20/02/14   NO      YES        cs1000-shared-omm-7.65.16.21-2.i386.000
34      Yes        20/02/14   YES      YES        cs1000-ipsec-7.65.16.22-1.i386.000
36      Yes        20/02/14   NO      YES        cs1000-cppmUtil-7.65.16.22-1.i686.000
39      Yes        23/12/14   YES      YES        cs1000-shared-xmsg-7.65.16.22-1.i386.000
40      Yes        23/12/14   NO      YES        cs1000-sps-7.65.16.23-1.i386.000
41      Yes        23/12/14   YES      YES        jdk-1.6.0_81-fcs.i586.000
42      Yes        23/12/14   YES      YES        cs1000-cs-7.65.P.100-03.i386.000
43      Yes        23/12/14   NO      YES        bash-3.2-33.el5_11.4.i386.000
44      Yes        23/12/14   NO      YES        tzdata-2014g-1.el5.i386.000
45      Yes        23/12/14   YES      YES        cs1000-tps-7.65.16.23-7.i386.000
46      Yes        23/12/14   YES      YES        cs1000-vtrk-7.65.16.23-24.i386.000
```

5. Configure Avaya Communication Server 1000

The configuration documented by these Application Notes uses the Incoming Digit Translation feature to receive calls, the Numbering Plan Area Code (NPA), and the Special Number (SPN) features to route calls from the CS1000 to the PSTN via SIP trunks to the TDC Business 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**.

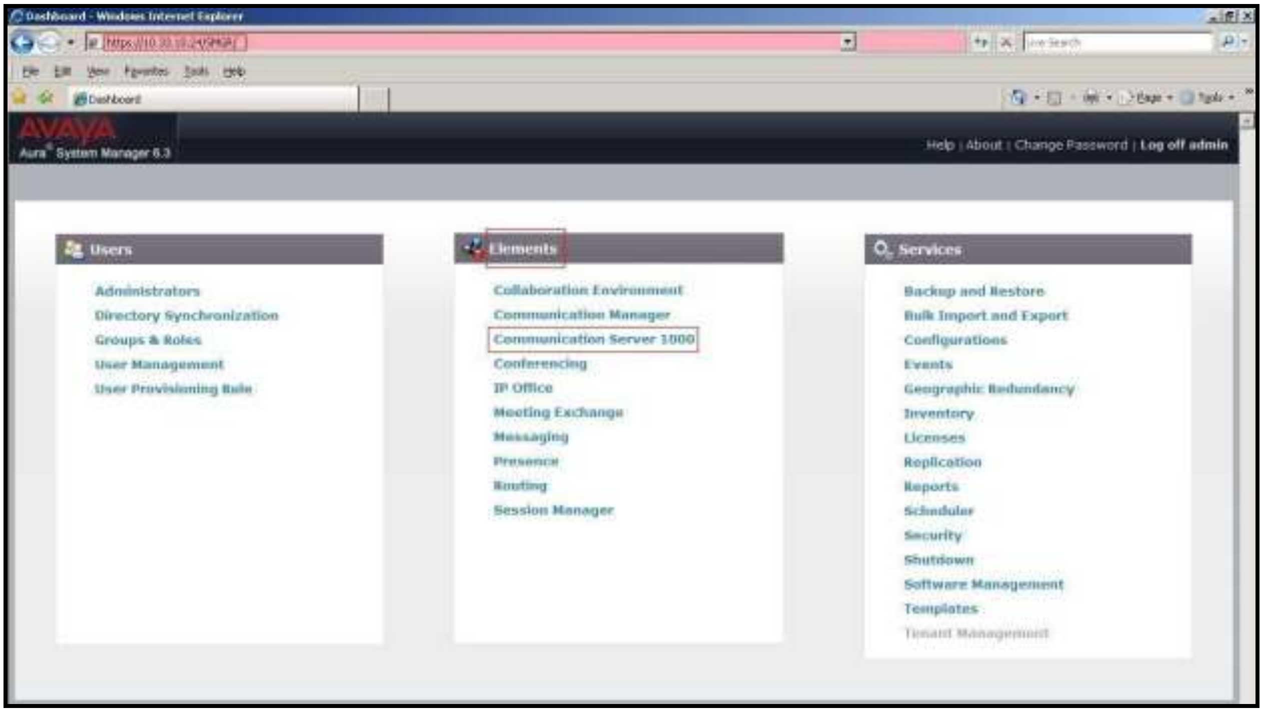
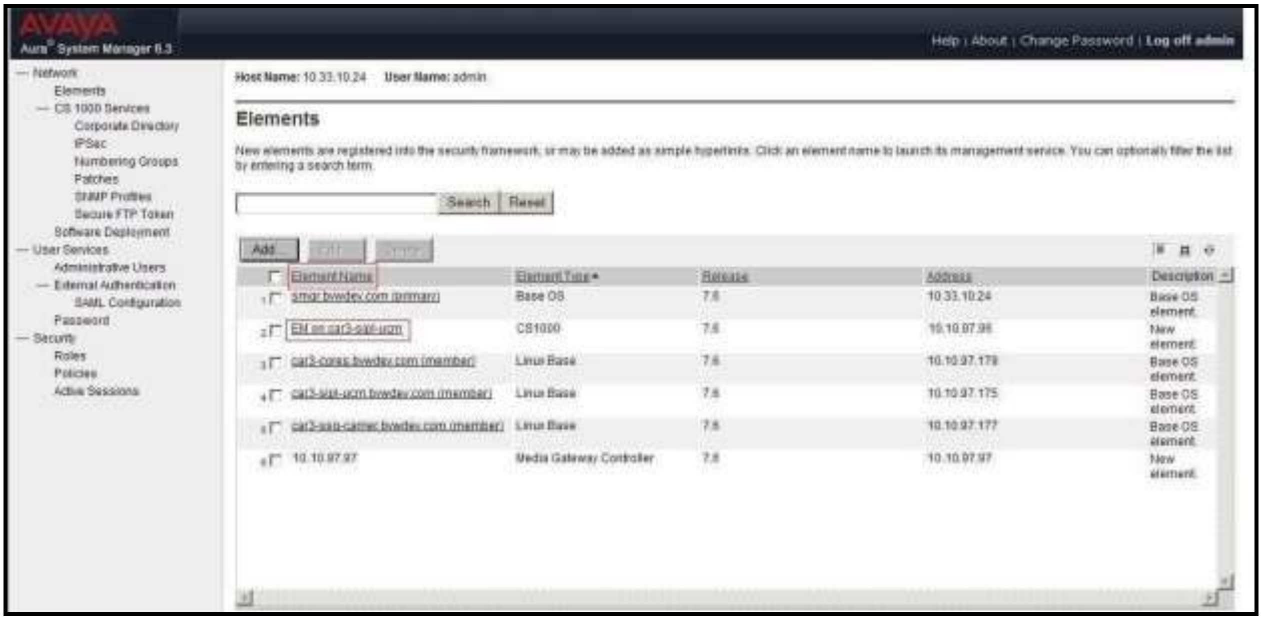


Figure 2 – System Manager Home Screen

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



Host Name: 10.33.10.24 **User Name:** admin

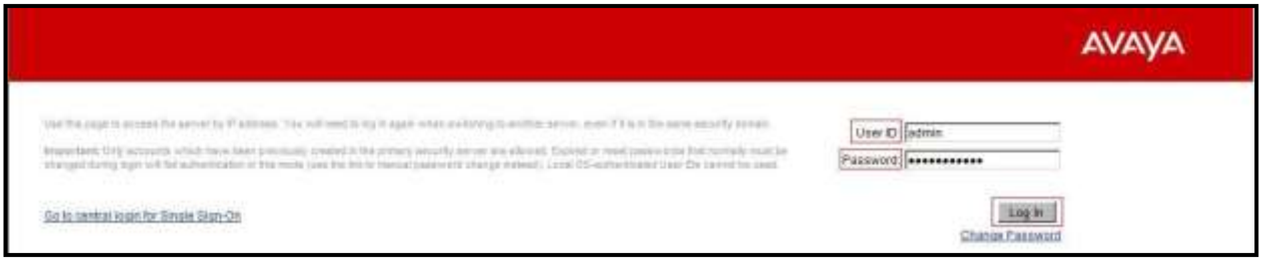
Elements

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

	Element Name	Element Type ▲	Release	Address	Description
1 □	smgr.bvwdev.com (primary)	Base OS	7.6	10.33.10.24	Base OS element
2 □	EM on car3-sipl-ucm	CS1000	7.6	10.10.97.98	New element
3 □	car3-coras.bvwdev.com (member)	Linux Base	7.6	10.10.97.179	Base OS element
4 □	car3-sipl-ucm.bvwdev.com (member)	Linux Base	7.6	10.10.97.175	Base OS element
5 □	car3-ssg-carrier.bvwdev.com (member)	Linux Base	7.6	10.10.97.177	Base OS element
6 □	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**.



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

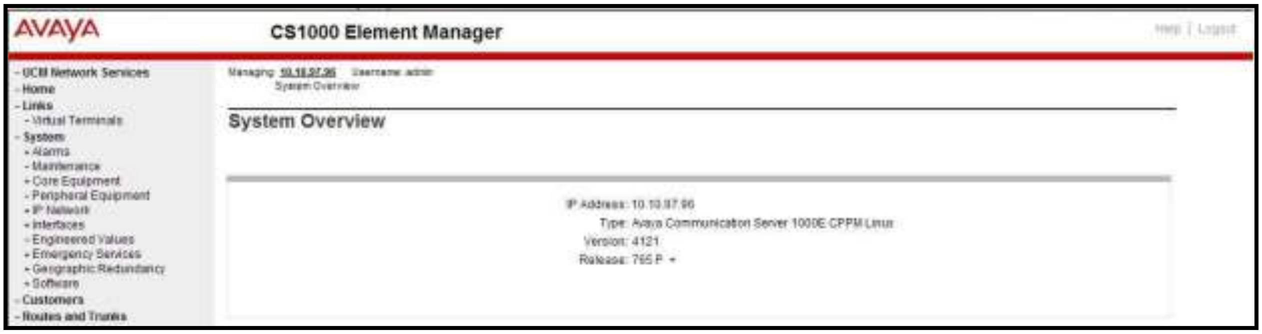
Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during sign in will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot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

User ID: admin
Password: ●●●●●●●●●●●●

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 +



Managing: 10.10.97.96 Username: admin
System Overview

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@10.10.97.178's password: ← Enter the password
Last login: Mon Aug 24 07:20:18 2015 from 10.10.98.78
[admin@car3-cores ~]$ 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 24/8/2015
```

```
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.

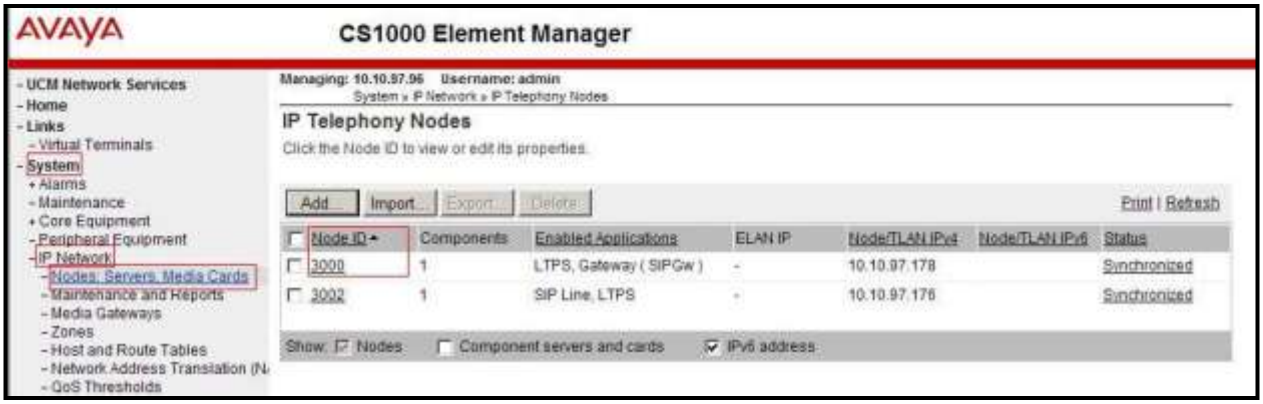
5.2. Administer IP Telephony Node

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 TDC Business 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**.



Managing: 10.10.97.96 Username: admin

System » IP Network » IP Telephony Nodes

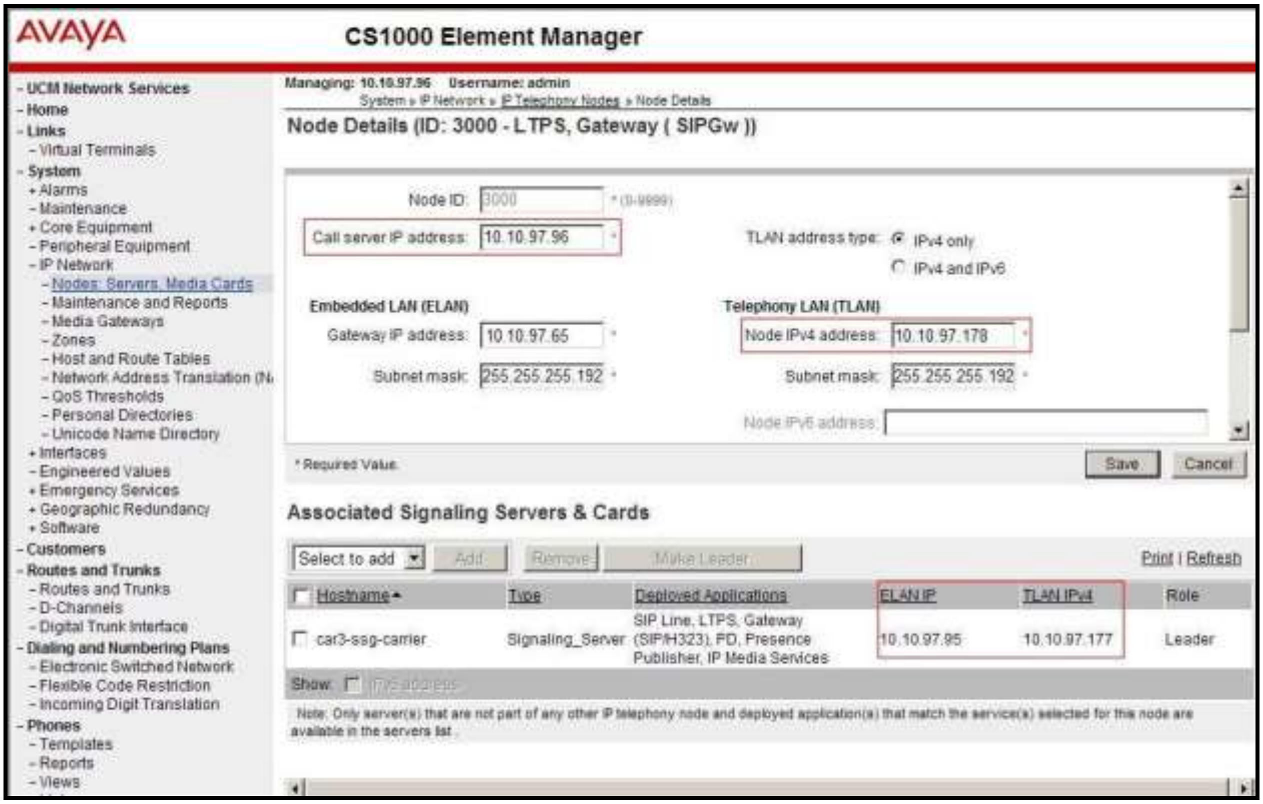
IP Telephony Nodes

Click the Node ID to view or edit its properties.

□	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 Node

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** for **Telophony LAN (TLAN)** 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.



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

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

Node ID: 3000 * (0-9999)

Call server IP address: 10.10.97.96 *

TLAN address type: ● IPv4 only ○ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 10.10.97.65 *

Subnet mask: 255.255.255.192 *

Telephony LAN (TLAN)

Node IPv4 address: 10.10.97.178 *

Subnet mask: 255.255.255.192 *

Node IPv6 address:

* Required Value.

Associated Signaling Servers & Cards

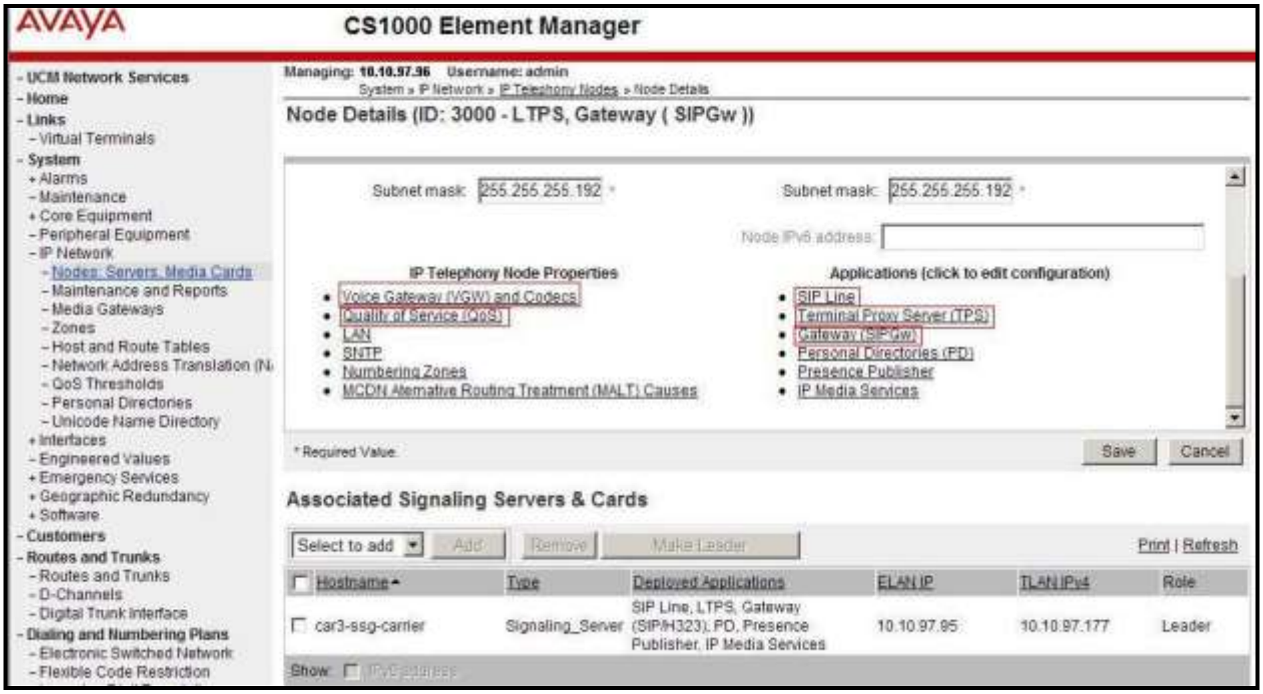
□ Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
□ car3-ssg-carrier	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

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

Scrolling down, the **Node Details** screen displays the **IP Telephony Node Properties** and **Applications** sections as shown in **Figure 8** with.



Managing: 10.10.97.96 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

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

Subnet mask: 255.255.255.192 *

Subnet mask: 255.255.255.192 *

Node IPv6 address:

IP Telephony Node Properties

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

Applications (click to edit configuration)

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

* Required Value.

Associated Signaling Servers & Cards

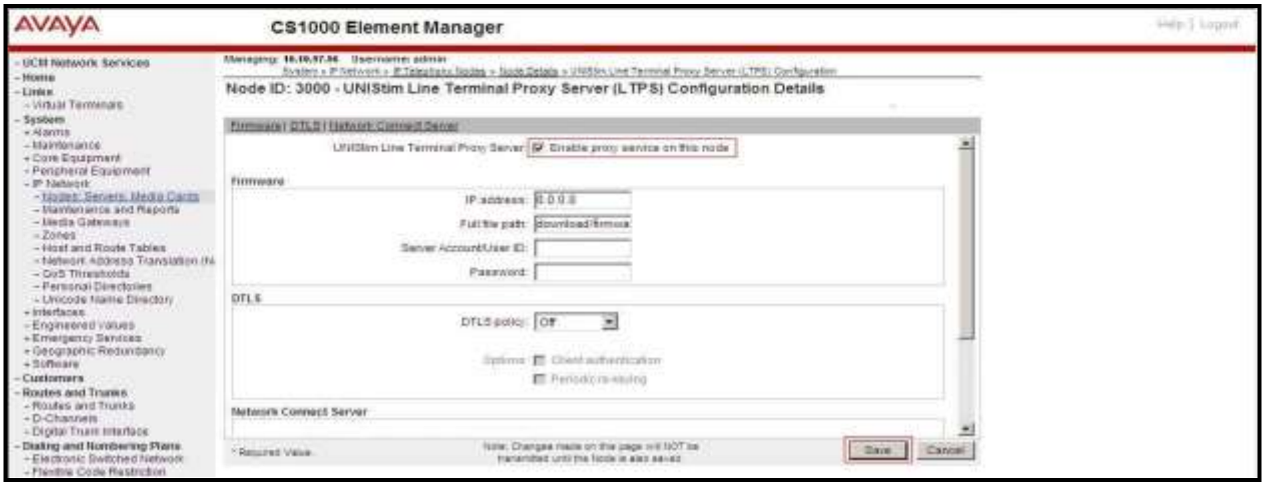
Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
☐ car3-ssg-carrier	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: ☐ IPv6 address

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 **UNIStim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click the **Save** button as shown in **Figure 9**.



Managing: 10.10.97.96 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » UNIStim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 3000 - UNIStim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware | DTLS | Network Connect Server

UNIStim Line Terminal Proxy Server: ☑ Enable proxy service on this node

Firmware

IP address: 0.0.0.0

Full file path: download/firmwa

Server Account/User ID:

Password:

DTLS

DTLS policy: Off

Options: ☐ Client authentication

☐ Periodic re-keying

Network Connect Server

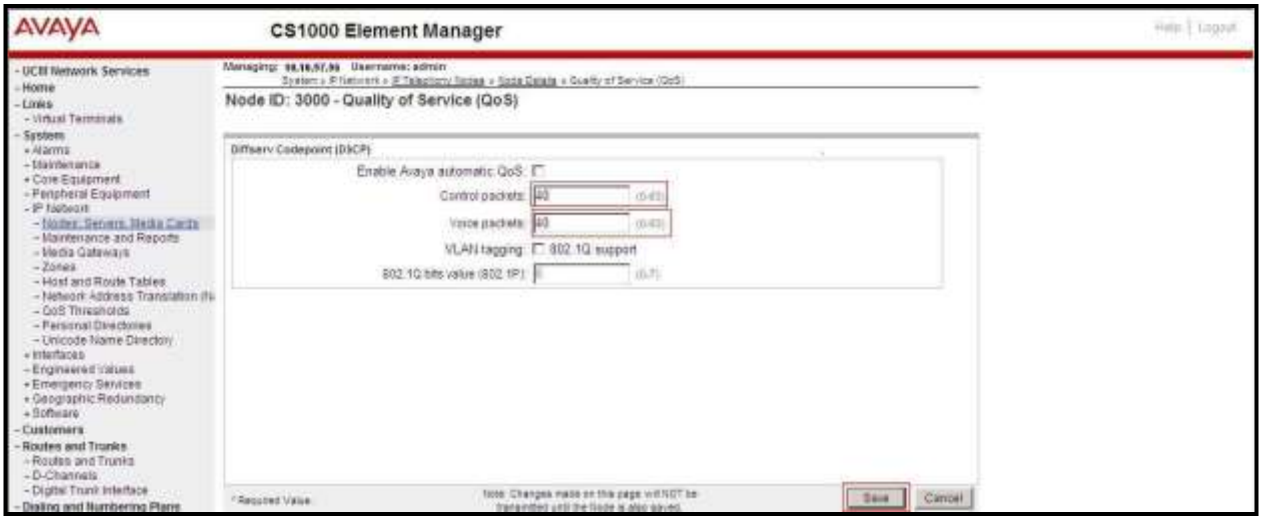
* Required Value.

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

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 shown in **Figure 10**. Click on the **Save** button.



Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Quality of Service (QoS)

Node ID: 3000 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: □
Control packets: 40 (0-63)
Voice packets: 40 (0-63)
VLAN tagging: □ 802.1Q support
802.1Q bits value (802.1P): (0-7)

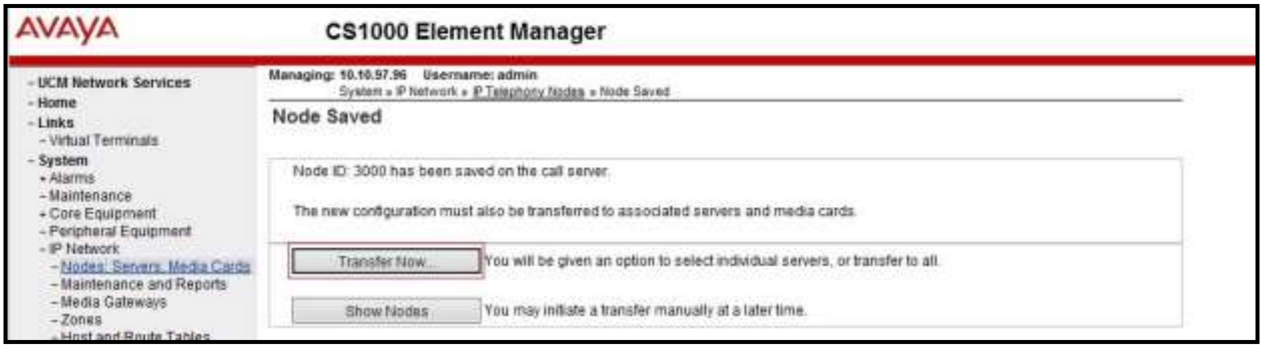
* Required Value.

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

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**.



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

Node Saved

Node ID: 3000 has been saved on the call server.

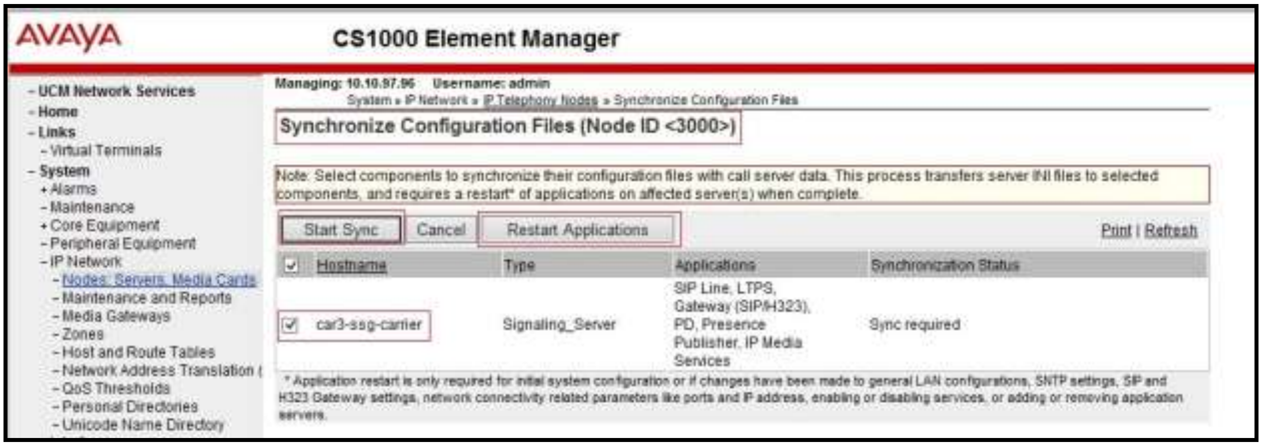
The new configuration must also be transferred to associated servers and media cards.

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

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

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.

☑	Hostname	Type	Applications	Synchronization Status
☑	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.

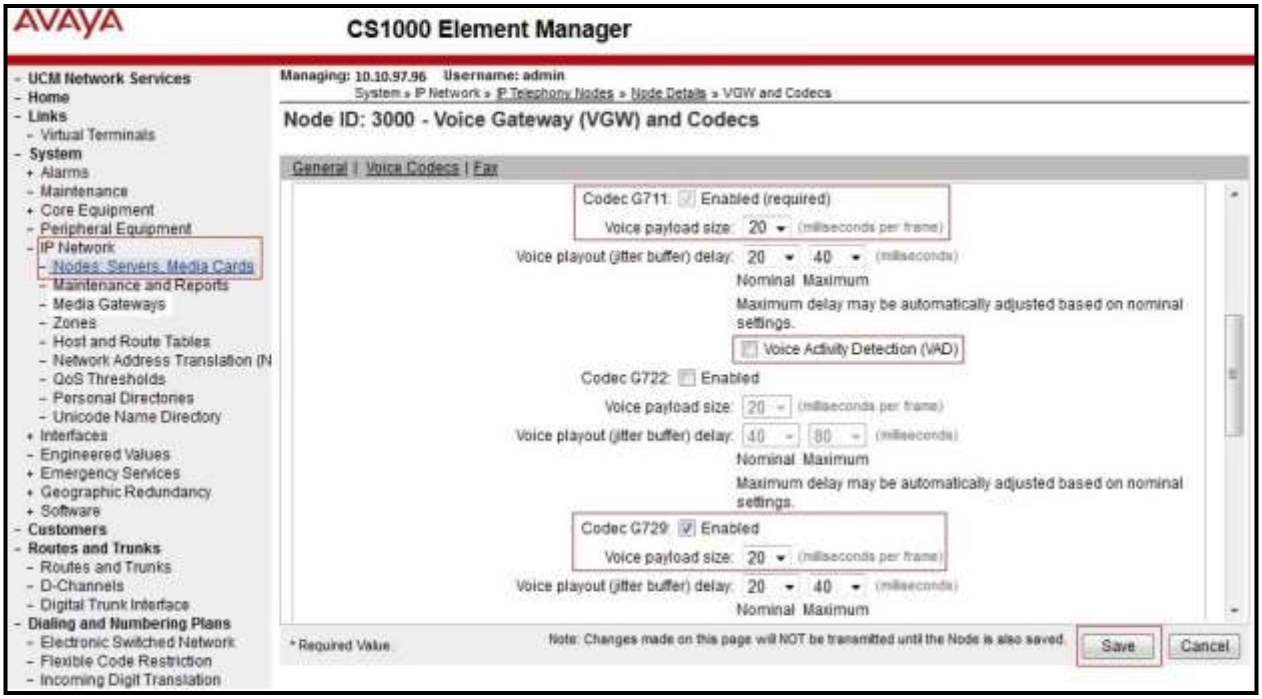
Figure 12 – Node Synchronized Screen

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G.711A-law, G.729A, G.711MU-law

Select **System → 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**.

TDC Business Trunk Service supports **G.711 a-law, G.729 a-law, G.711 mu-law** with **Voice payload size 20 milliseconds per frame.** Uncheck **Voice Activity Detection (VAD)** checkbox. Click on the **Save** button.



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

Node ID: 3000 - Voice Gateway (VGW) and Codecs

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

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

Codec G729: ☑ Enabled
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 20 40 (milliseconds)
Nominal Maximum

* Required Value

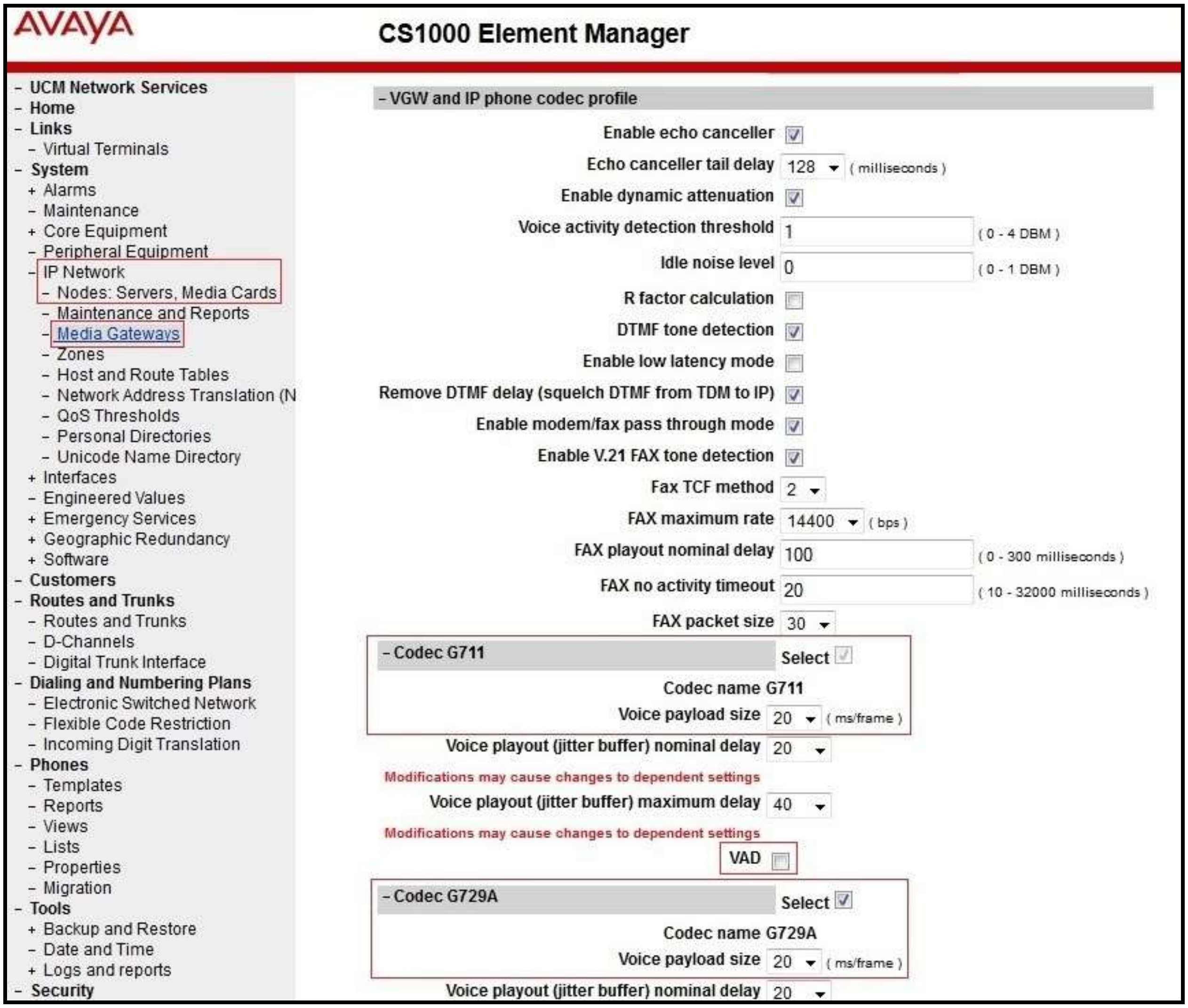
Note: Changes made on this page will NOT be transmitted until the Node is also saved.

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 **System → 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 **G.729A** with **Voice payload size 20 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).



- VGW and IP phone codec profile

Enable echo canceller ☑

Echo canceller tail delay 128 (milliseconds)

Enable dynamic attenuation ☑

Voice activity detection threshold 1 (0 - 4 DBM)

Idle noise level 0 (0 - 1 DBM)

R factor calculation ☐

DTMF tone detection ☑

Enable low latency mode ☐

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

Enable modem/fax pass through mode ☑

Enable V.21 FAX tone detection ☑

Fax TCF method 2

FAX maximum rate 14400 (bps)

FAX playout nominal delay 100 (0 - 300 milliseconds)

FAX no activity timeout 20 (10 - 32000 milliseconds)

FAX packet size 30

- Codec G711 Select ☑

Codec name G711

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 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 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 20

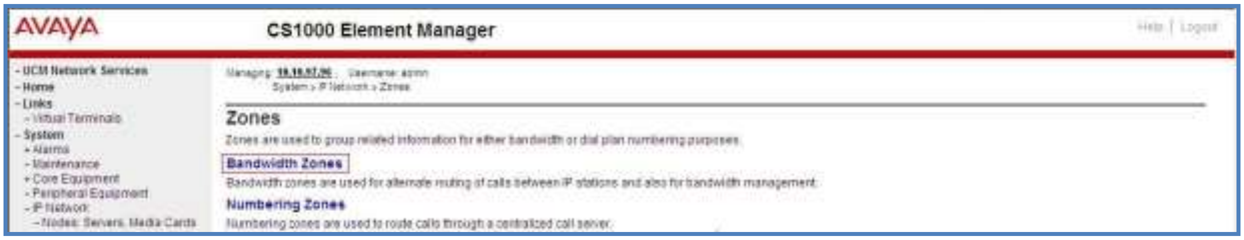
Figure 14 – Media Gateways Configuration Details

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



Zones

Zones are used to group related information for either bandwidth or dial plan numbering purposes.

Bandwidth Zones

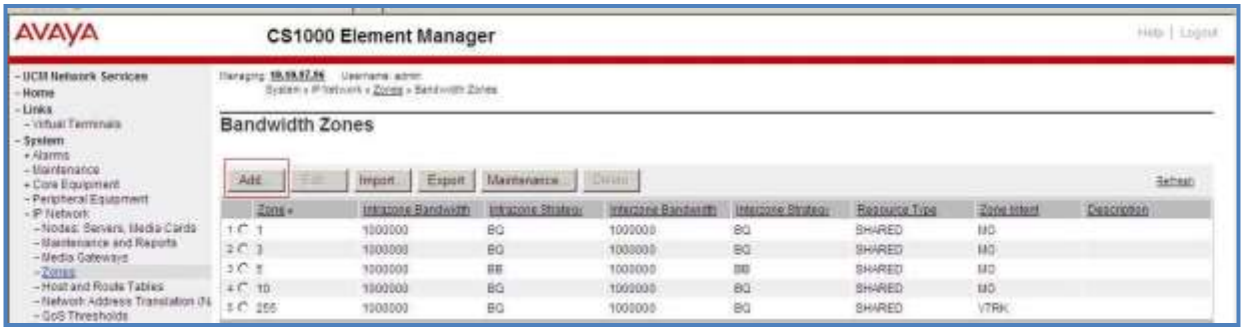
Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.

Numbering Zones

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.



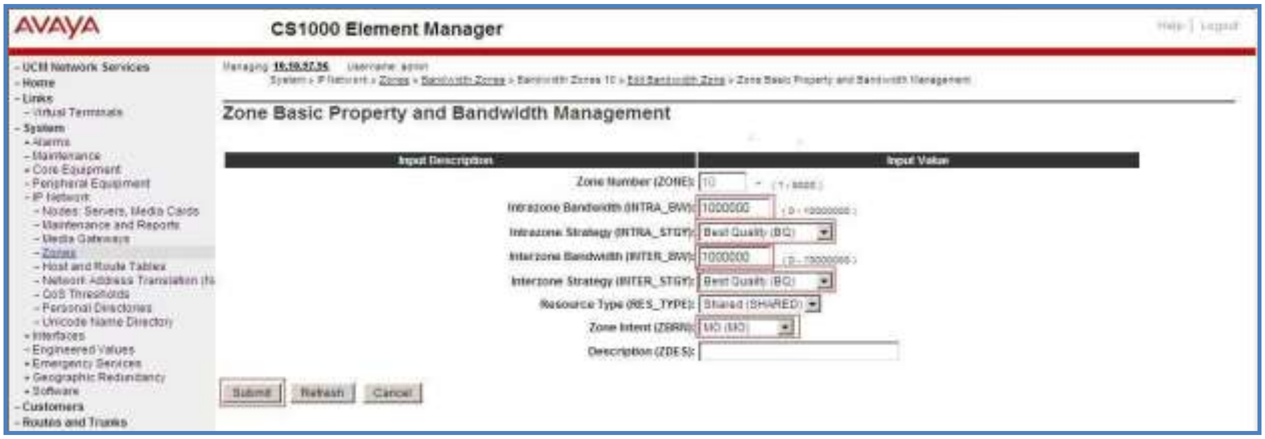
Bandwidth Zones

	Zone ▲	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1 ○	1	1000000	BQ	1000000	BQ	SHARED	MO	
2 ○	3	1000000	BQ	1000000	BQ	SHARED	MO	
3 ○	5	1000000	BB	1000000	BB	SHARED	MO	
4 ○	10	1000000	BQ	1000000	BQ	SHARED	MO	
5 ○	255	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.



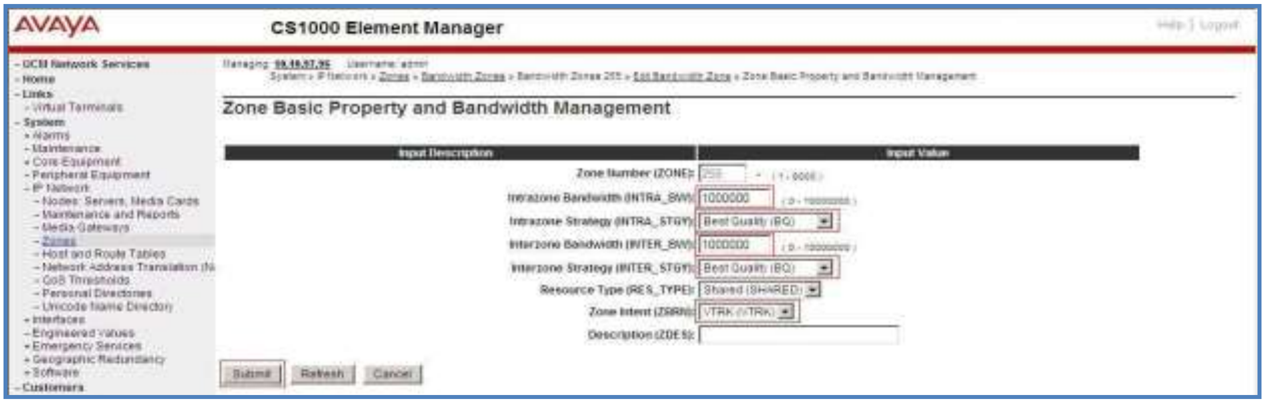
Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	10 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

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(VTRK)** for virtual trunk as shown in **Figure 18** and then click on the **Submit** button.



Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	

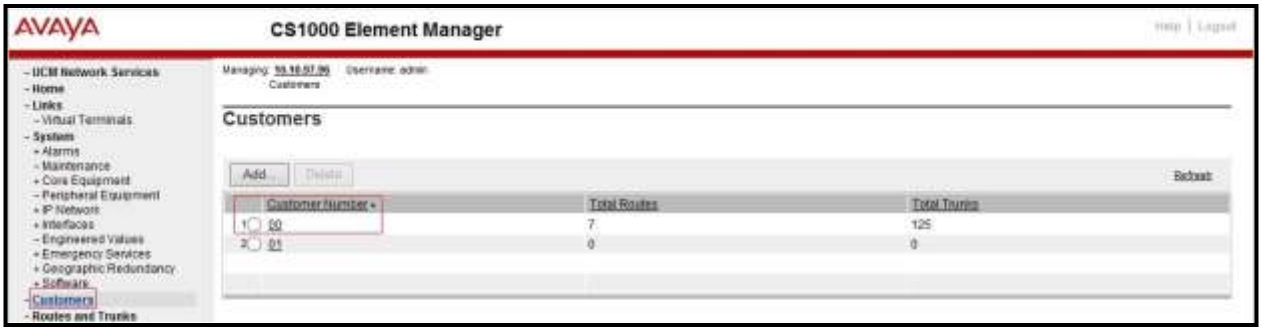
Figure 18 – Bandwidth Management Configuration Details – Virtual SIP trunk

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**.



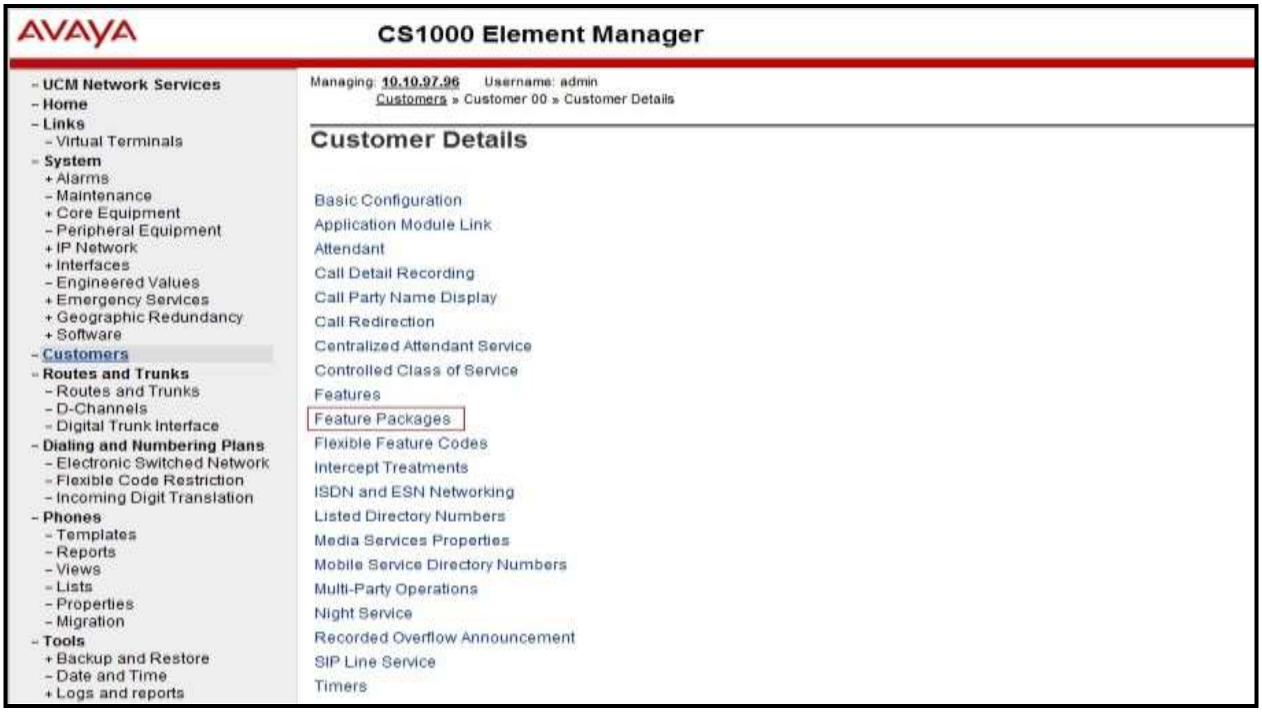
Managing: 10.10.97.96 Username: admin
Customers

Customers

	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.

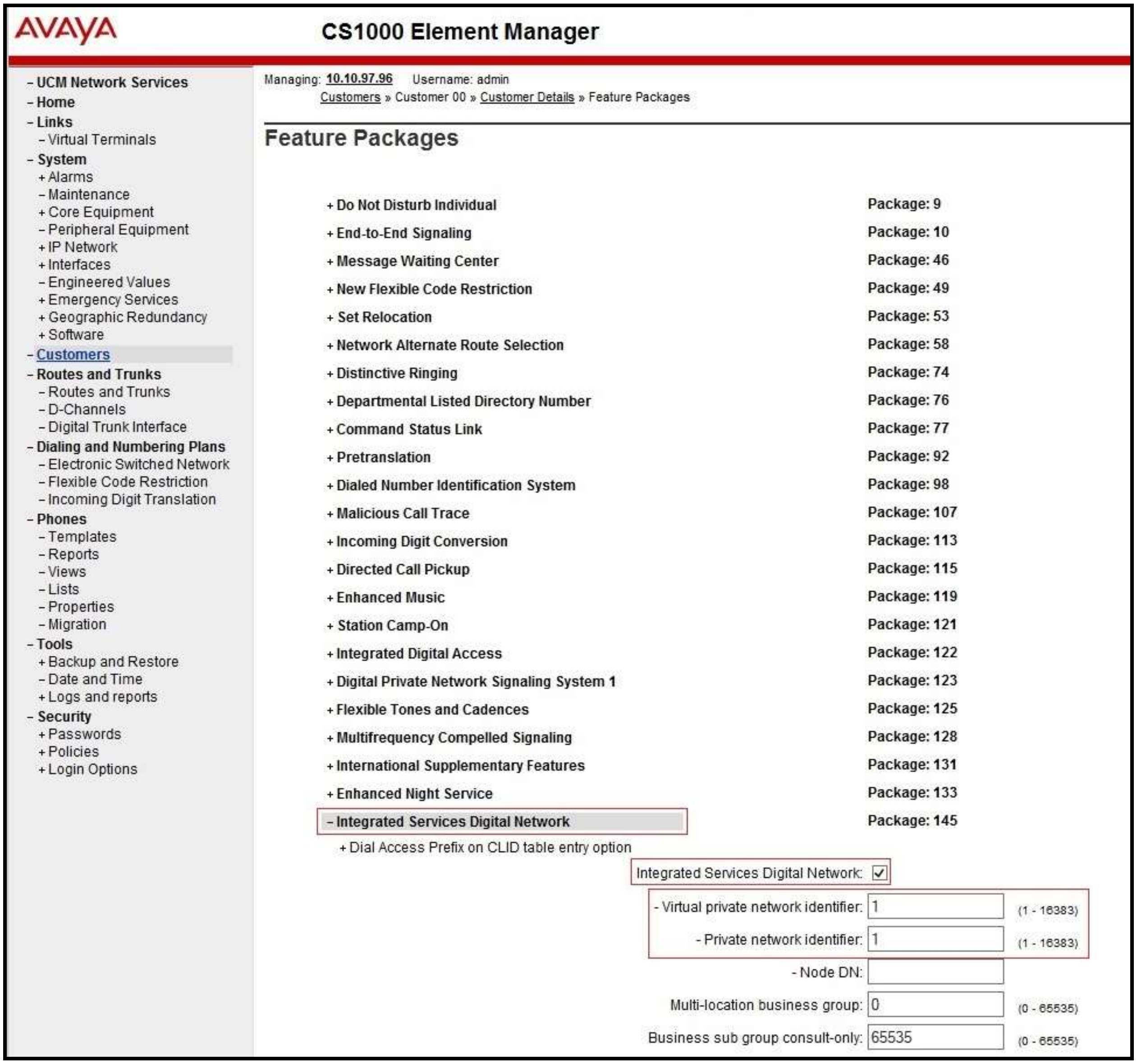


Managing: 10.10.97.96 Username: admin
Customers » Customer 00 » Customer Details

Customer Details

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).



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 (1 - 16383)

- Private network identifier: 1 (1 - 16383)

- Node DN:

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

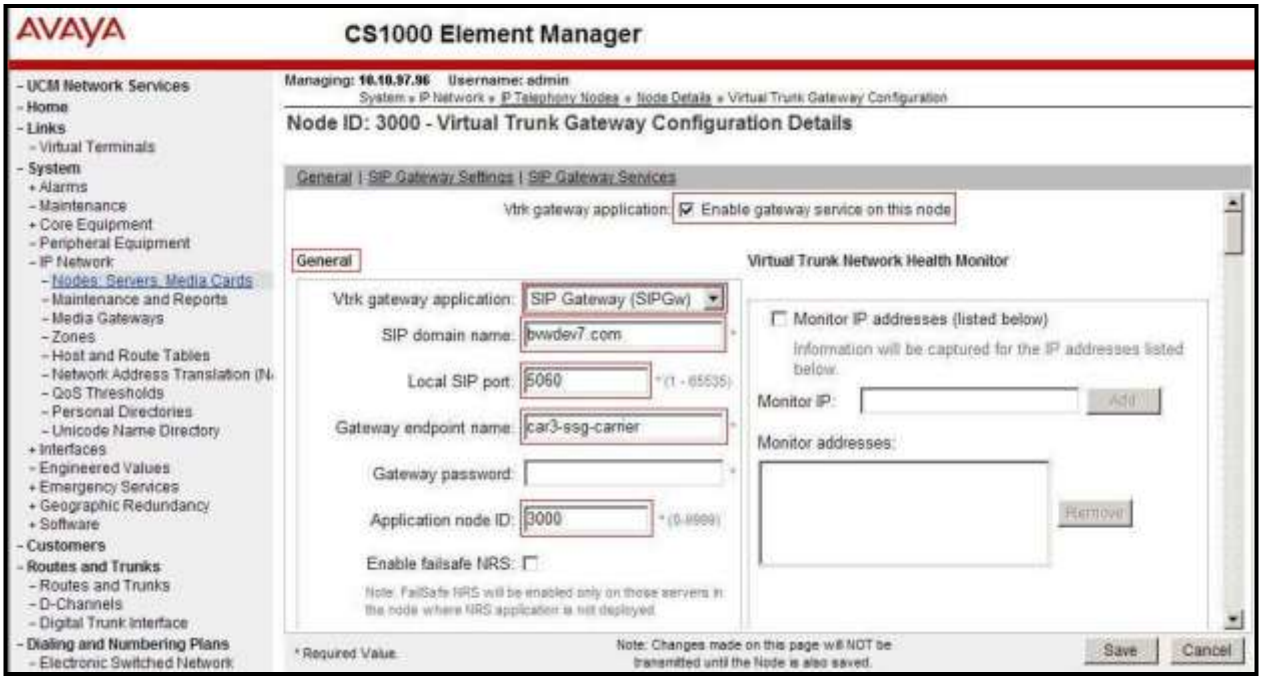
Business sub group consult-only: 65535 (0 - 65535)

Figure 21 – Customer – ISDN Configuration 3

5.5.2. Administer SIP Trunk Gateway to Avaya Communication Server 1000

Select **System → 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 Session Manager (in **Section 6.2**, and **6.6**).



Managing: 10.10.97.96 Username: admin

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

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

Vtrk gateway application: ☑ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: bvwdev7.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: car3-ssg-carrier *

Gateway password: *

Application node ID: 3000 * (0-9999)

Enable failsafe NRS: □

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

Virtual Trunk Network Health Monitor

□ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

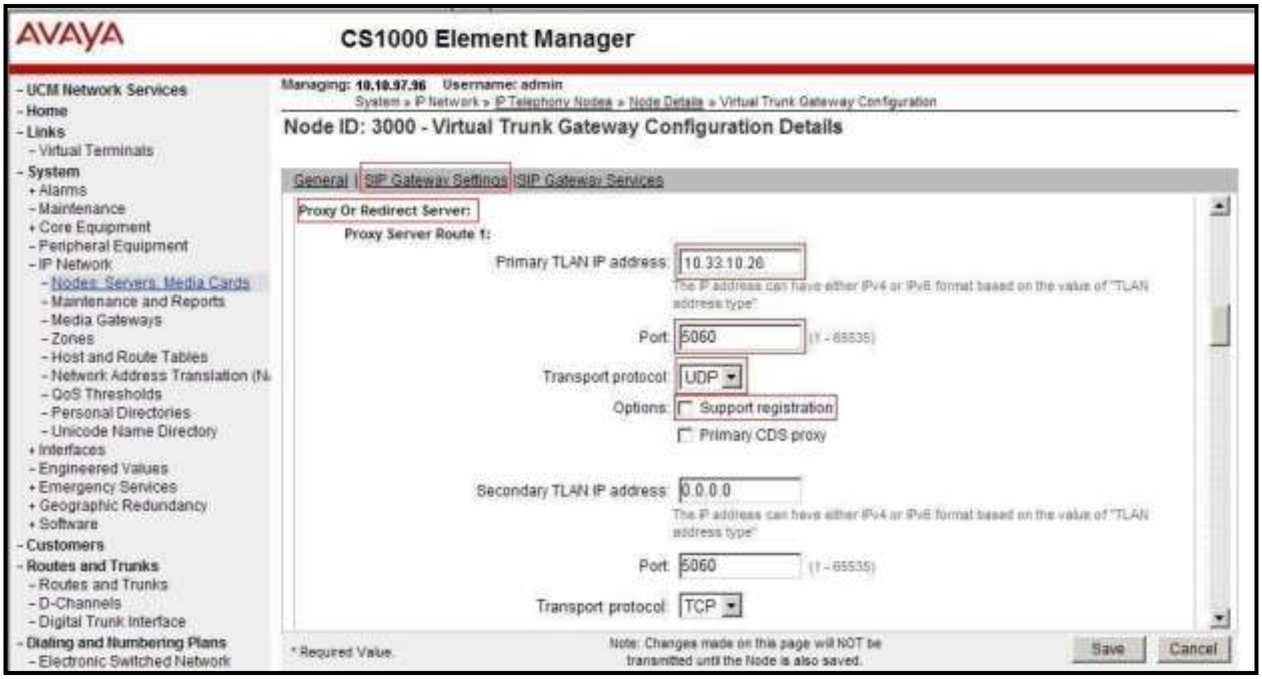
Monitor addresses:

* Required Value.

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

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 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 in **Section 6.5.1**). Uncheck the **Support registration** checkbox.



Managing: 10.10.97.96 Username: admin

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

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.33.10.26

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

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: □ Support registration

□ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0

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

Port: 5060 (1 - 65535)

Transport protocol: TCP

* Required Value.

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

Figure 23 – Virtual Trunk Gateway Configuration Details

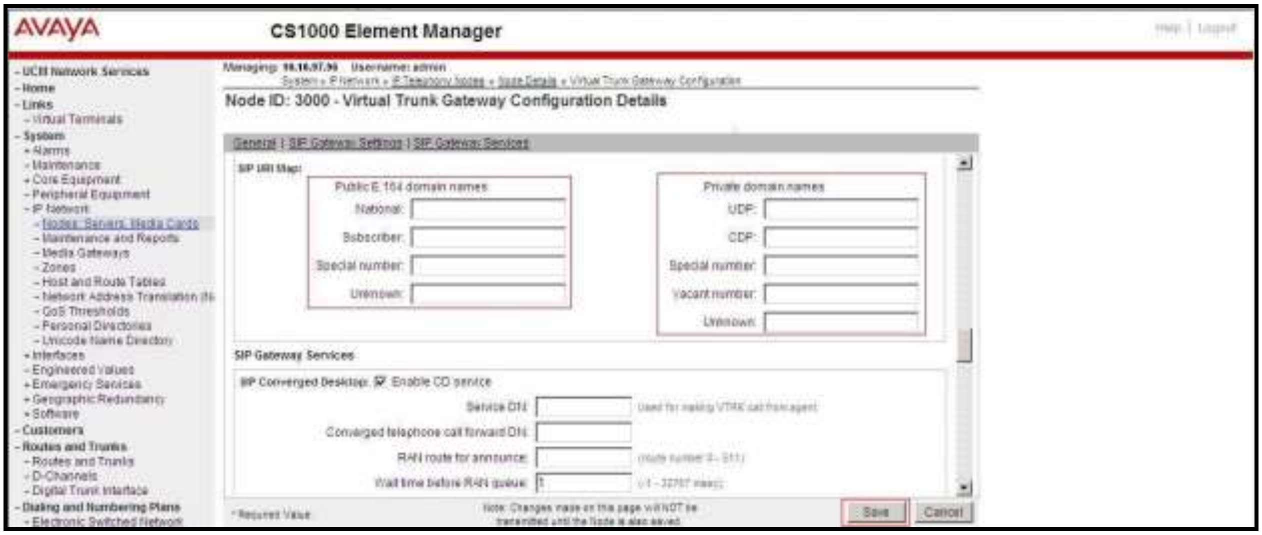
On the same page as shown in **Figure 23**, scroll down to the **SIP URI Map** section. Under **Public E.164 domain names**, enter the following:

- **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.



Managing: 10.10.97.96 Username: admin

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

SIP URI Map:

Public E.164 domain names
National:
Subscriber:
Special number:
Unknown:

Private domain names
UDP:
CDP:
Special number:
Vacant number:
Unknown:

SIP Gateway Services

SIP Converged Desktop: ☑ Enable CD service
Service DN: (Used for making VTRK call from agent)
Converged telephone call forward DN:
RAN route for announce: (route number 0 - 511)
Wait time before RAN queue: 1 (1 - 32767 msec)

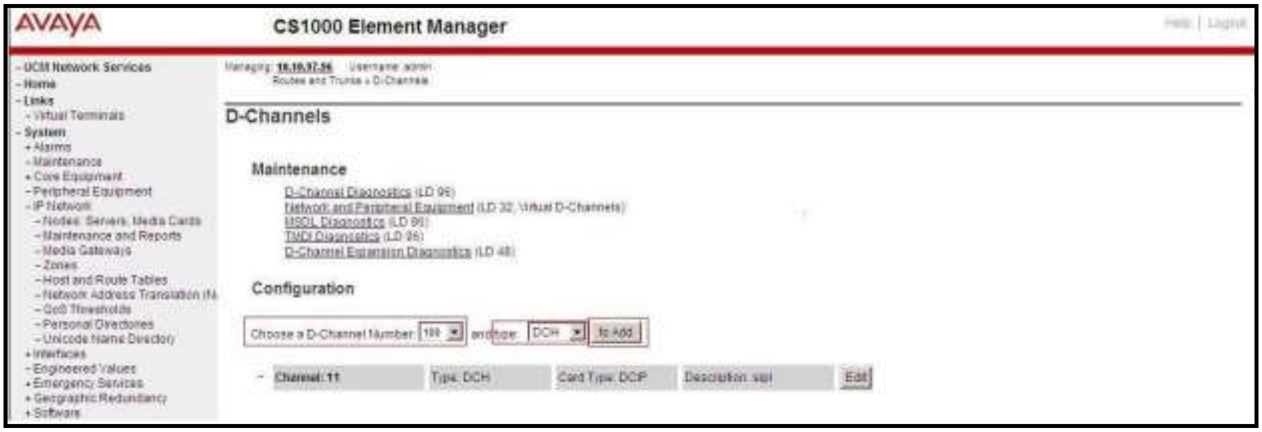
* Required Value
Note: Changes made on this page will NOT be transmitted until the Node is also saved.

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.



Managing: 10.10.97.96 Username: admin

D-Channels

Maintenance

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

Configuration

Choose a D-Channel Number: 100 and type: DCH

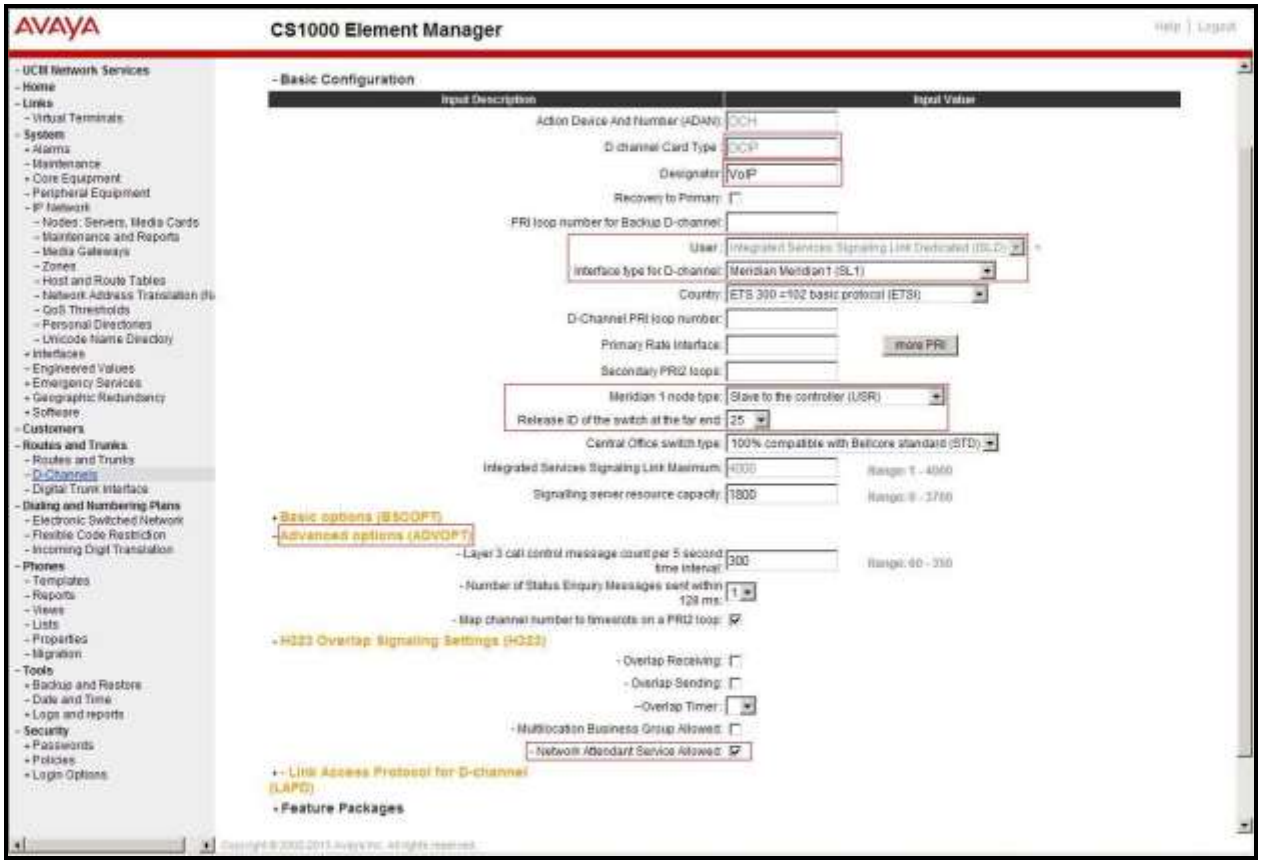
- Channel: 11 Type: DCH Card Type: DCIP Description: sip

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 under H323 Overlap Signaling Settings (H323) as shown in **Figure 26**. Other fields are left as default.



- Basic Configuration

Input Description	Input Value
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:	
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
Signaling 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:	☑

- H323 Overlap Signaling Settings (H323)

- Overlap Receiving:	□
- Overlap Sending:	□
--Overlap Timer :	
- Multilocation Business Group Allowed:	□
- Network Attendant Service Allowed:	☑

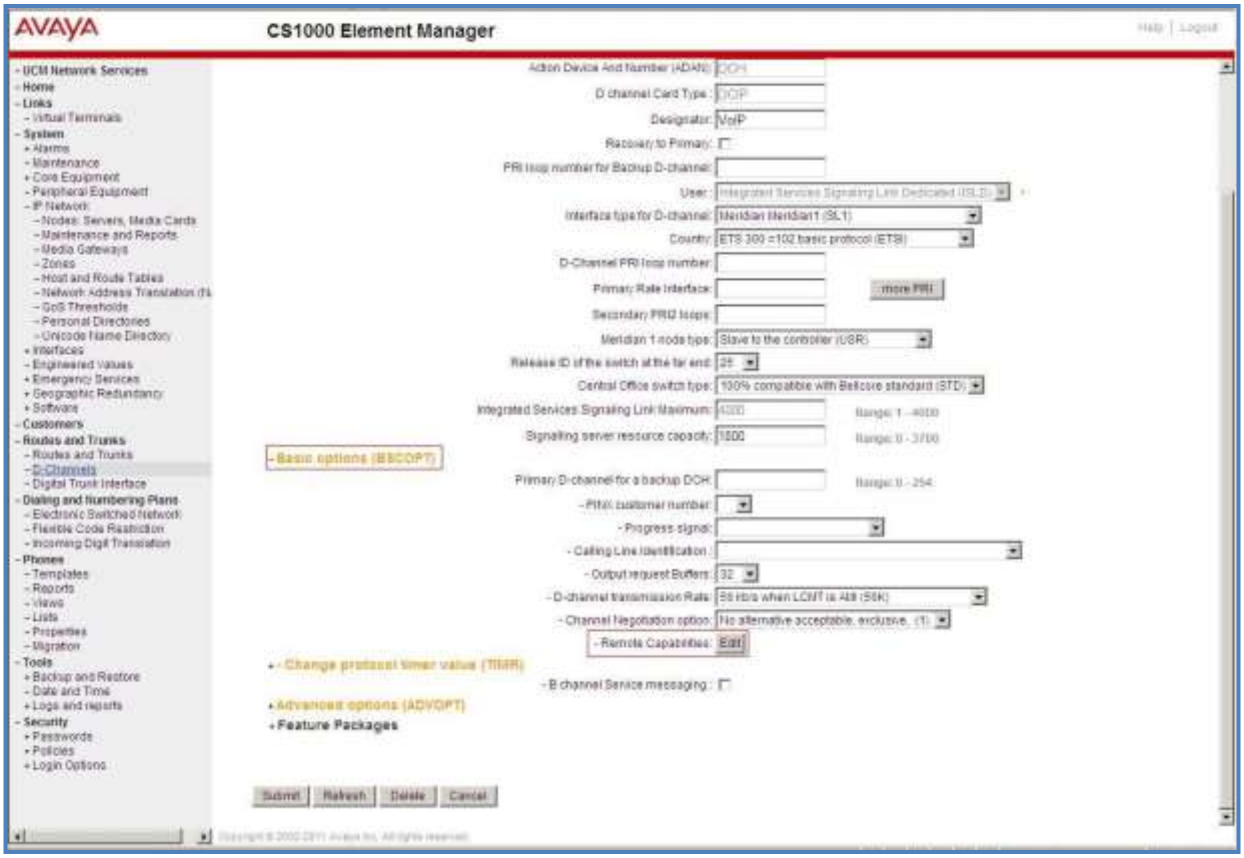
+ - Link Access Protocol for D-channel (LAPD)

+ Feature Packages

Copyright © 2002-2015 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**.



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:
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
Signaling server resource capacity: 1800 Range: 0 - 3700

- Basic options (BSCOPT)

Primary D-channel for a backup DCH: Range: 0 - 254
- PINX customer number:
- Progress signal:
- Calling Line Identification :
- Output request Buffers: 32
- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)
- Channel Negotiation option: No alternative acceptable, exclusive. (1)
- Remote Capabilities: Edit

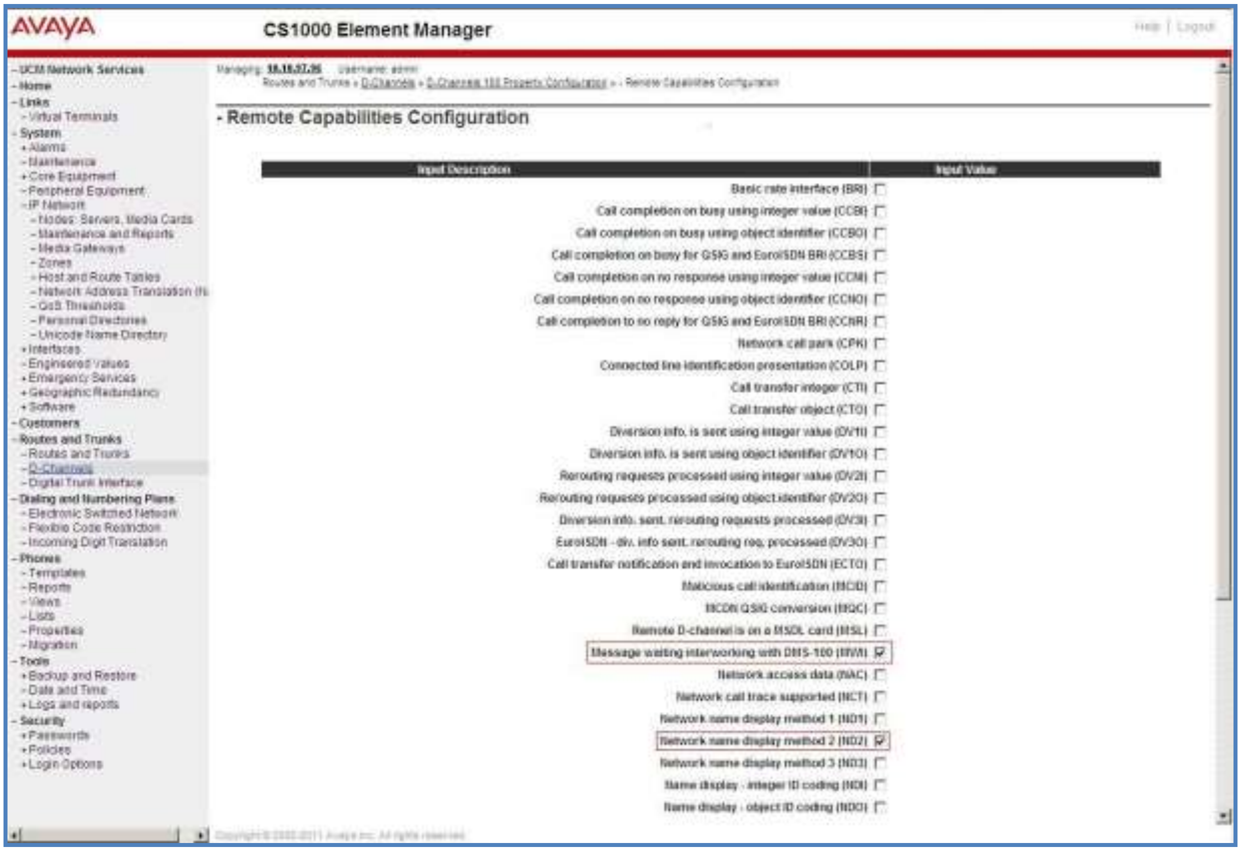
+ - Change protocol timer value (TIMR)

- B channel Service messaging : □

+ Advanced options (ADVOPT)
+ Feature Packages

Figure 27 – D-Channel Configuration

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



- Remote Capabilities Configuration

Input Description	Input Value
Basic rate interface (BRI)	□
Call completion on busy using integer value (CCBI)	□
Call completion on busy using object identifier (CCBO)	□
Call completion on busy for QSIG and EuroISDN BRI (CCBS)	□
Call completion on no response using integer value (CCNI)	□
Call completion on no response using object identifier (CCNO)	□
Call completion to no reply for QSIG and EuroISDN BRI (CCNR)	□
Network call park (CPK)	□
Connected line identification presentation (COLP)	□
Call transfer integer (CTI)	□
Call transfer object (CTO)	□
Diversion info. is sent using integer value (DV1I)	□
Diversion info. is sent using object identifier (DV1O)	□
Rerouting requests processed using integer value (DV2I)	□
Rerouting requests processed using object identifier (DV2O)	□
Diversion info. sent, rerouting requests processed (DV3I)	□
EuroISDN - div. info sent, rerouting req. processed (DV3O)	□
Call transfer notification and invocation to EuroISDN (ECTO)	□
Malicious call identification (MCID)	□
MCDN QSIG conversion (MQC)	□
Remote D-channel is on a MSDL card (MSL)	□
Message waiting interworking with DMS-100 (MWI)	☑
Network access data (NAC)	□
Network call trace supported (NCT)	□
Network name display method 1 (ND1)	□
Network name display method 2 (ND2)	☑
Network name display method 3 (ND3)	□
Name display - integer ID coding (NDI)	□
Name display - object ID coding (NDO)	□

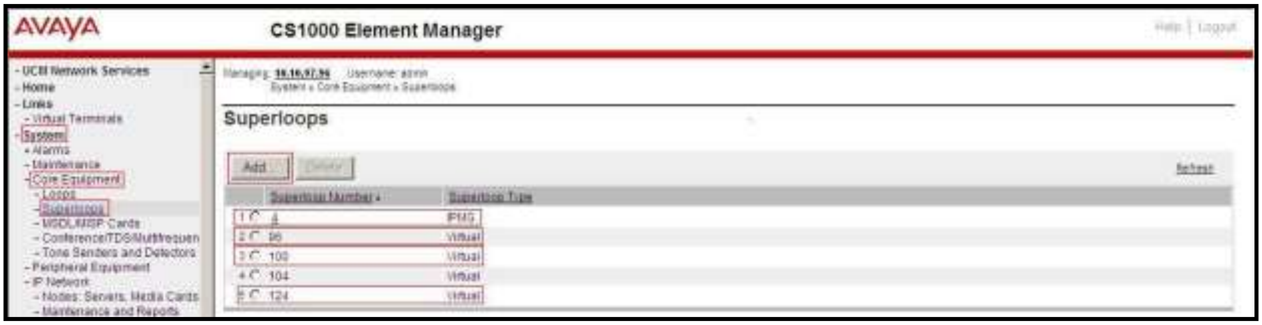
Figure 28 – Remote Capabilities Configuration

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, Superloops 4, 96, 100, and 124 have been added and are being used.



Managing: 10.10.97.96 Username: admin
System » Core Equipment » Superloops

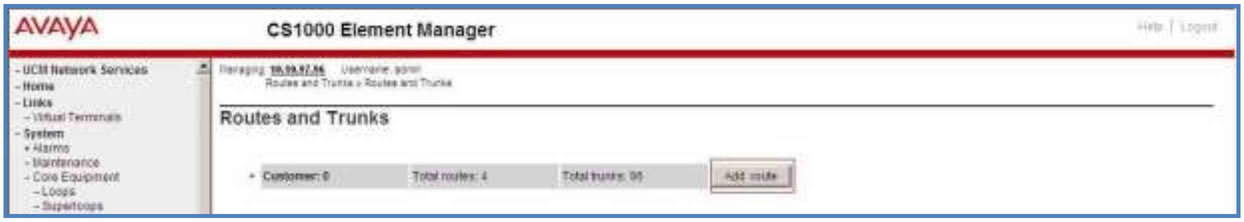
Superloops

	Superloop Number ▲	Superloop Type
1 ○	4	IPMG
2 ○	96	Virtual
3 ○	100	Virtual
4 ○	104	Virtual
5 ○	124	Virtual

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**.



Managing: 10.10.97.96 Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

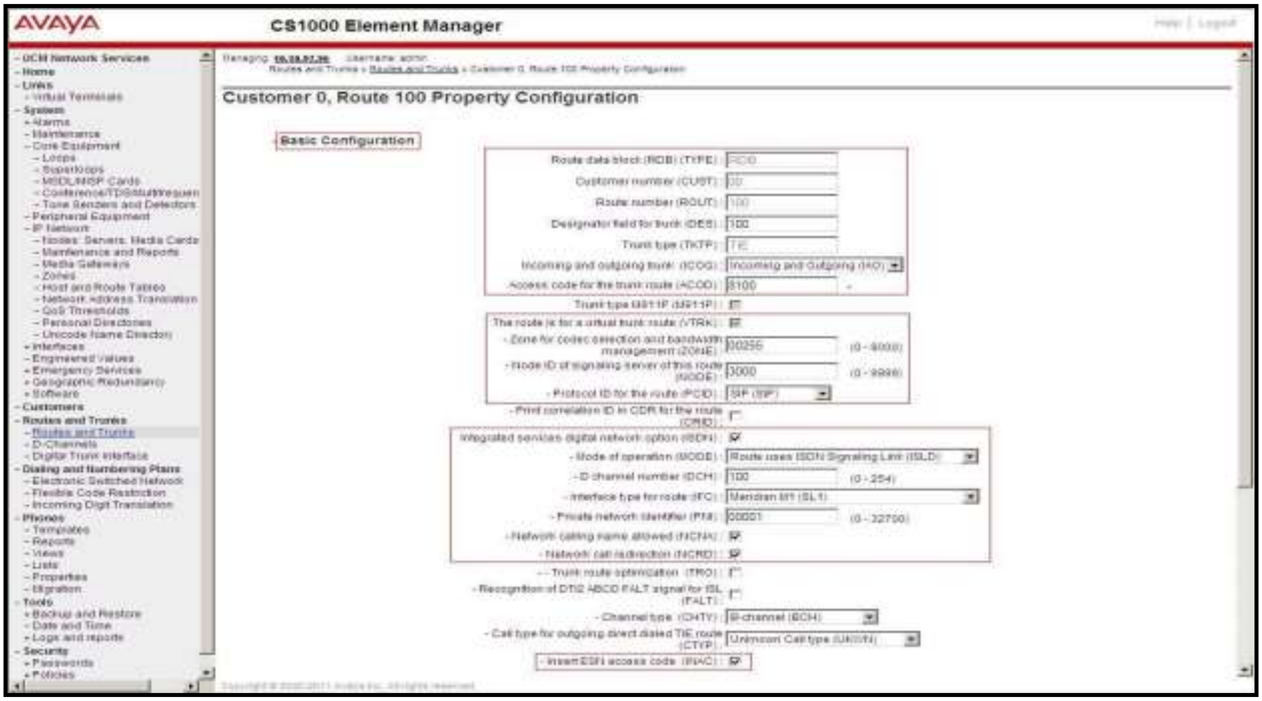
+ Customer: 0 | Total routes: 4 | Total trunks: 96

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 **Figure 31**.

- **Route data block (RDB) (TYPE)**: **RDB** as default.
- **Customer number (CUST)**: **0** as customer 0 is 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 Signalling 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**).



Managing: [illegible] Username: admin
Routes and Trunks » Routes and Trunks » Customer 0, Route 100 Property Configuration

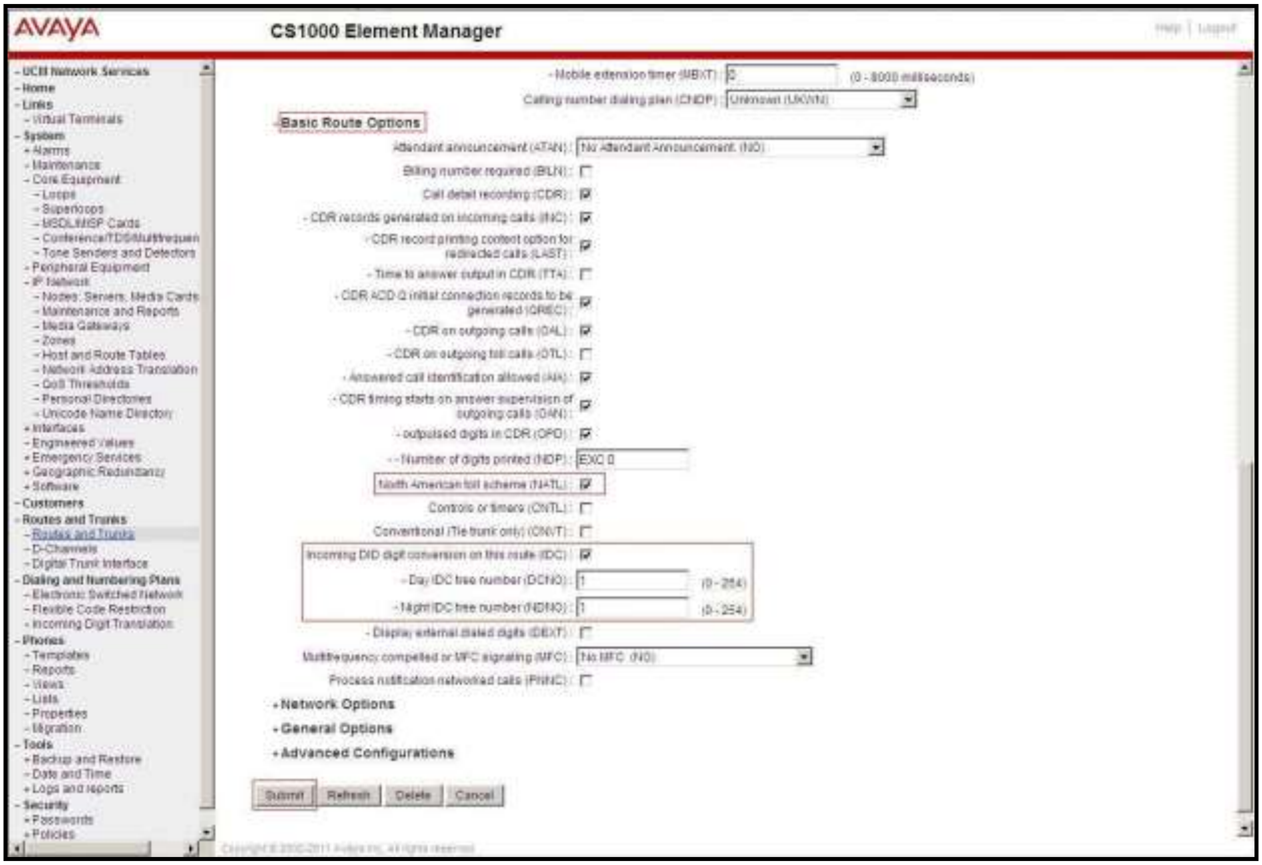
Customer 0, Route 100 Property Configuration

Route data block (RDB) (TYPE): RDB
Customer number (CUST): 00
Route number (ROUT): 100
Designator field for trunk (DES): 100
Trunk type (TKTP): TIE
Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD): 8100
Trunk type M911P (M911P): □
The route is for a virtual trunk route (VTRK): ☑
- Zone for codec selection and bandwidth management (ZONE): 00255 (0 - 8000)
- Node ID of signaling server of this route (NODE): 3000 (0 - 9999)
- Protocol ID for the route (PCID): SIP (SIP)
- Print correlation ID in CDR for the route (CRID): □
Integrated services digital network option (ISDN): ☑
- Mode of operation (MODE): Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH): 100 (0 - 254)
- Interface type for route (IFC): Meridian M1 (SL1)
- Private network identifier (PNI): 00001 (0 - 32700)
- Network calling name allowed (NCNA): ☑
- Network call redirection (NCRD): ☑
- - Trunk route optimization (TRO): □
- Recognition of DTI2 ABCD FALT signal for ISL (FALT): □
- Channel type (CHTY): B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP): Unknown Call type (UKWN)
- Insert ESN access code (INAC): ☑

Copyright © 2002-2011 Avaya Inc. All rights reserved.

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.



- Mobile extension timer (MBXT): 0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP): Unknown (UKWN)

- Basic Route Options

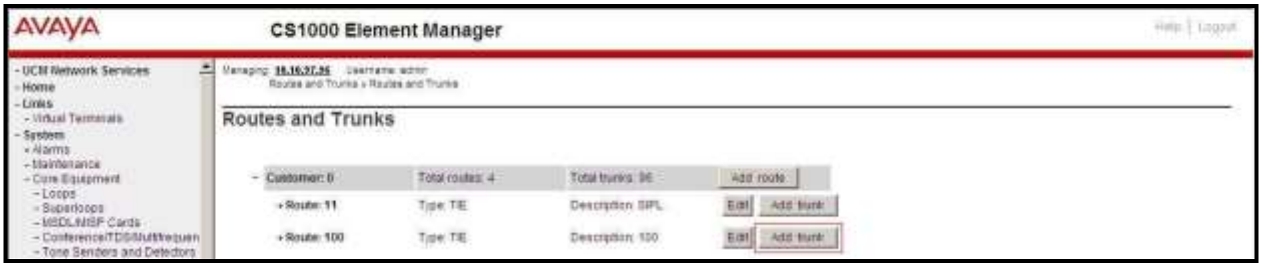
Attendant announcement (ATAN): No Attendant Announcement (NO)
Billing number required (BLN): □
Call detail recording (CDR): ☑
- CDR records generated on incoming calls (INC): ☑
- CDR record printing content option for redirected calls (LAST): ☑
- Time to answer output in CDR (TTA): □
- CDR ACD Q initial connection records to be generated (QREC): ☑
- CDR on outgoing calls (OAL): ☑
- CDR on outgoing toll calls (OTL): □
- Answered call identification allowed (AIA): ☑
- CDR timing starts on answer supervision of outgoing calls (OAN): ☑
- outpulsed digits in CDR (OPD): ☑
- - Number of digits printed (NDP): EXC 0
North American toll scheme (NATL): ☑
Controls or timers (CNTL): □
Conventional (Tie trunk only) (CNVT): □
Incoming DID digit conversion on this route (IDC): ☑
- Day IDC tree number (DCNO): 1 (0 - 254)
- Night IDC tree number (NDNO): 1 (0 - 254)
- Display external dialed digits (DEXT): □
Multifrequency compelled or MFC signaling (MFC): No MFC (NO)
Process notification networked calls (PNNC): □

+ Network Options
+ General Options
+ Advanced Configurations

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**.



Managing: 10.10.97.35 Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

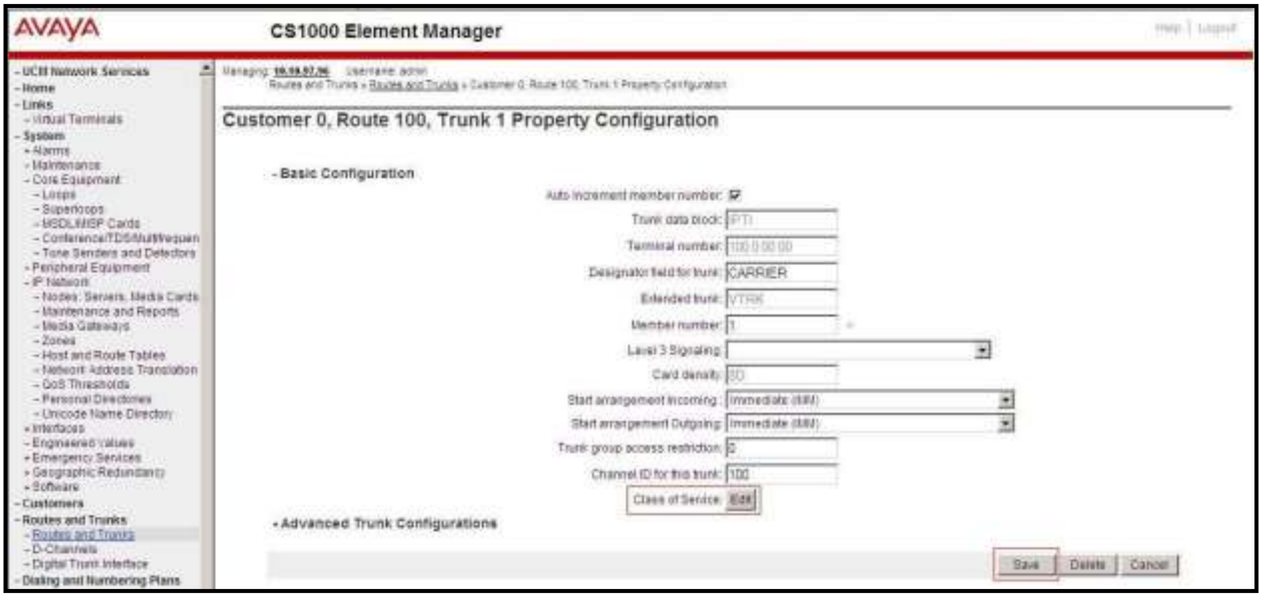
- Customer: 0 | Total routes: 4 | Total trunks: 96
+ Route: 11 | Type: TIE | Description: SIPL
+ Route: 100 | Type: TIE | Description: 100

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 (not shown) may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.

- **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.



Managing: 10.10.97.96 Username: admin
Routes and Trunks » Routes and Trunks » Customer 0, Route 100, Trunk 1 Property Configuration

Customer 0, Route 100, Trunk 1 Property Configuration

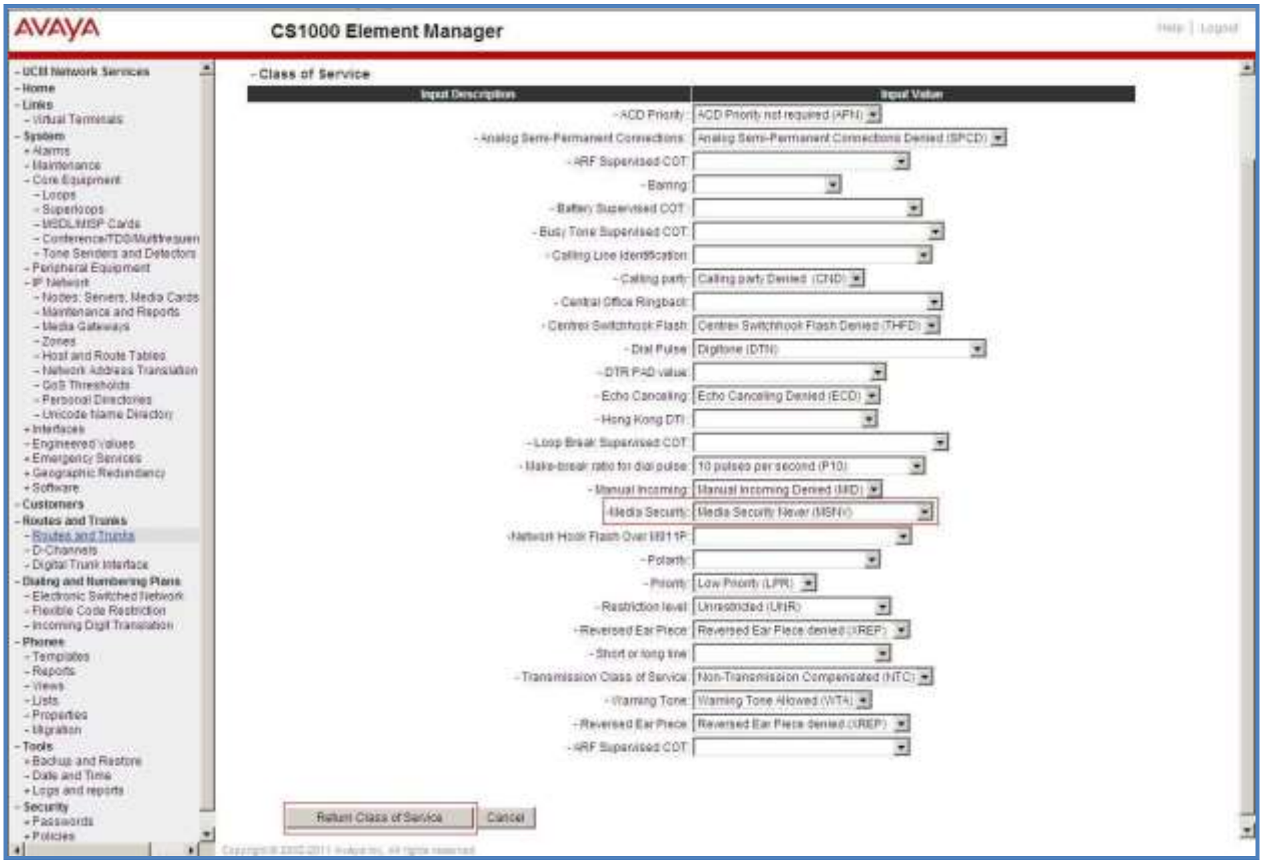
- Basic Configuration

Auto increment member number: ☑
Trunk data block: IPTI
Terminal number: 100 0 00 00
Designator field for trunk: CARRIER
Extended trunk: VTRK
Member number: 1
Level 3 Signaling:
Card density: 8D
Start arrangement Incoming: Immediate (IMM)
Start arrangement Outgoing: Immediate (IMM)
Trunk group access restriction: 2
Channel ID for this trunk: 100
Class of Service: Edit

- Advanced Trunk Configurations

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**).



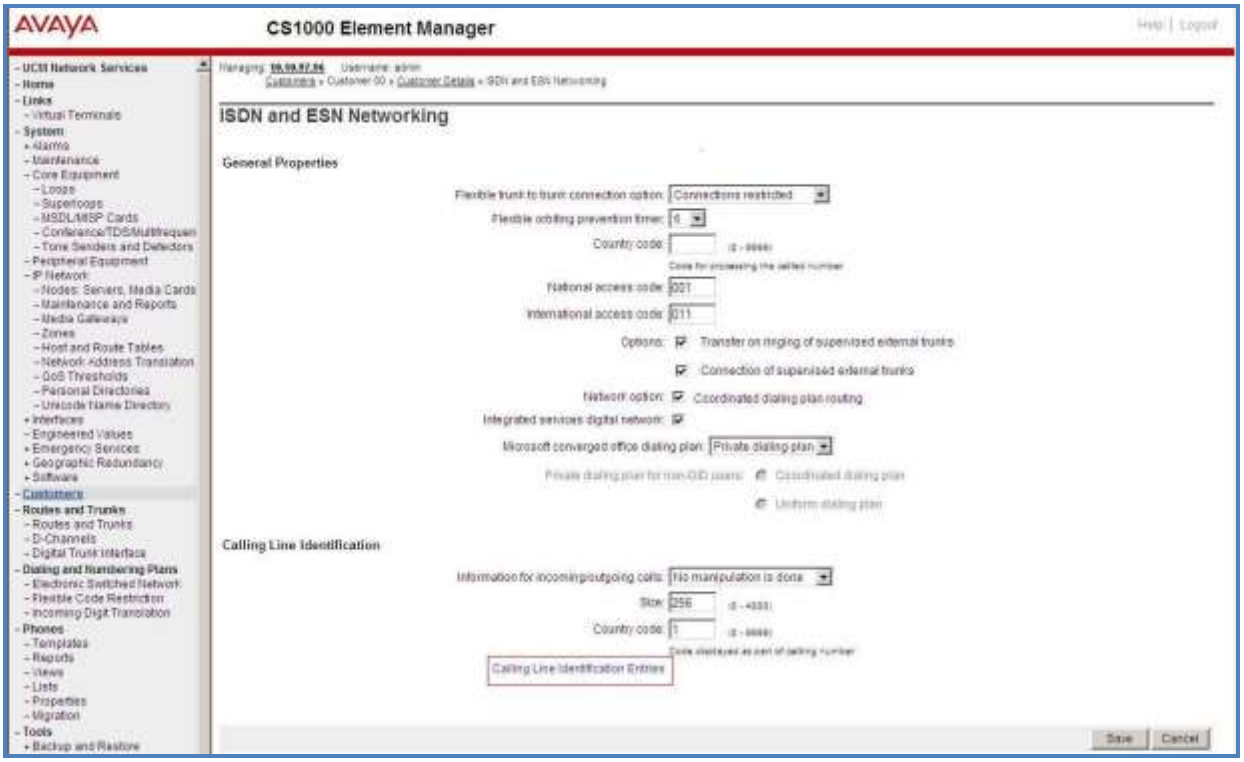
- Class of Service

Input Description	Input Value
- ACD Priority:	ACD Priority not required (APN)
- Analog Semi-Permanent Connections:	Analog Semi-Permanent Connections Denied (SPCD)
- ARF Supervised COT:	
- Barring:	
- Battery Supervised COT:	
- Busy Tone Supervised COT:	
- Calling 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 MG1 1P:	
- 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**.


AVAYA
CS1000 Element Manager
Help | Logout
Customers » Customer 00 » Customer Details » ISDN and ESN Networking
Save
Cancel

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option: Connections restricted

Flexible orbiting prevention timer: 6

Country code: (0 - 9999)

National access code: 001

International access code: 011

Options: ☑ Transfer on ringing of supervised external trunks

☑ Connection of supervised external trunks

Network option: ☑ Coordinated dialing plan routing

Integrated services digital network: ☑

Microsoft converged office dialing plan: Private dialing plan

Private dialing plan for non-DID users: ● Coordinated dialing plan ○ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls: No manipulation is done

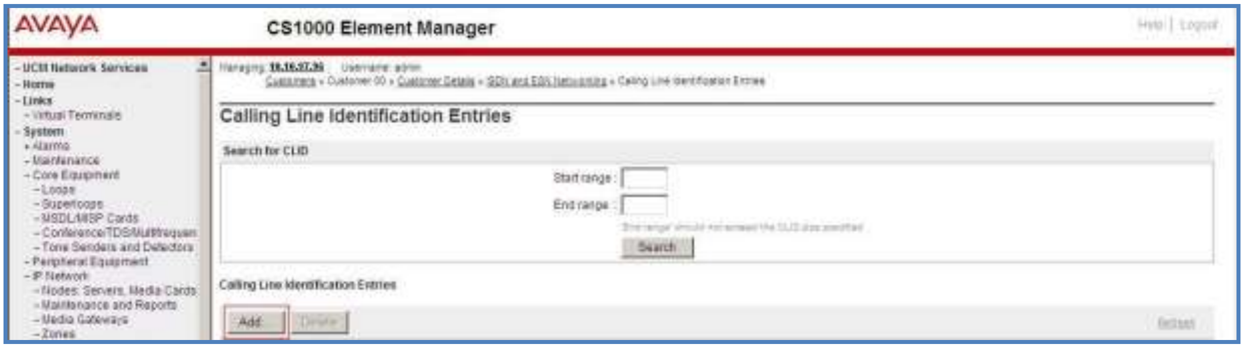
Size: 256 (0 - 4000)

Country code: 1 (0 - 9999)

Calling Line Identification Entries

Figure 36 – ISDN and ESN Networking

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


AVAYA
CS1000 Element Manager
Help | Logout
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries
Search
Add
Delete

Calling Line Identification Entries

Search for CLID

Start range :

End range :

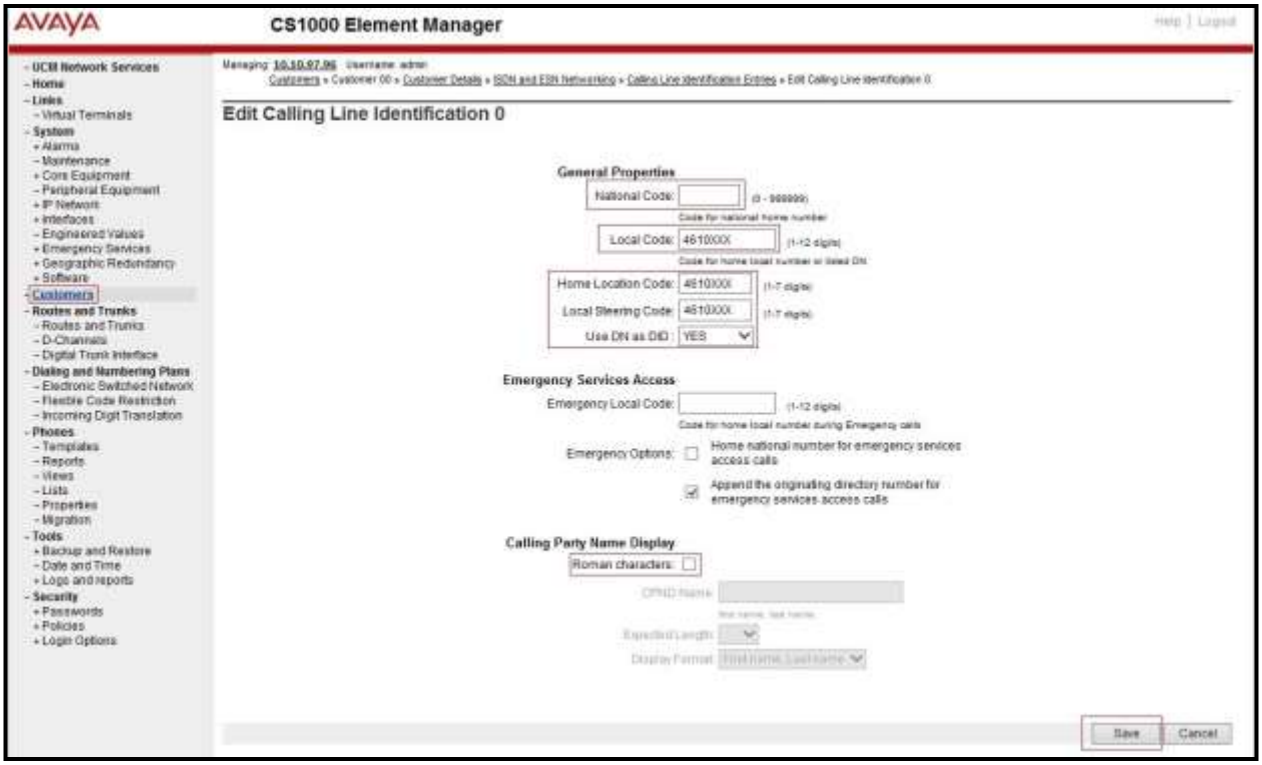
Calling Line Identification Entries

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** screen of the existing entry 0 is displayed as shown in **Figure 38**.

- **National Code**: Leave it blank.
- **Local Code**: Input prefix digits assigned by TDC Business Trunk Service, in this case 7 digits – **4610XXX**. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code**: Input the prefix digits assigned by TDC Business Trunk Service, in this case 7 digits – **4610XXX**. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code**: Input prefix digits assigned by TDC Business Trunk Service, in this case 7 digits – **4610XXX**. 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**.



Managing: 10.10.97.96 Username: admin
Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 0

Edit Calling Line Identification 0

General Properties

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

Local Code: 4610XXX (1-12 digits)
Code for home local number or listed DN

Home Location Code: 4610XXX (1-7 digits)

Local Steering Code: 4610XXX (1-7 digits)

Use DN as DID: YES

Emergency Services Access

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

Emergency Options: ☐ Home national number for emergency services access calls

☑ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☐

DPNSS Name:
first name, last name

Expected Length:

Display Format: First name, Last name

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**.

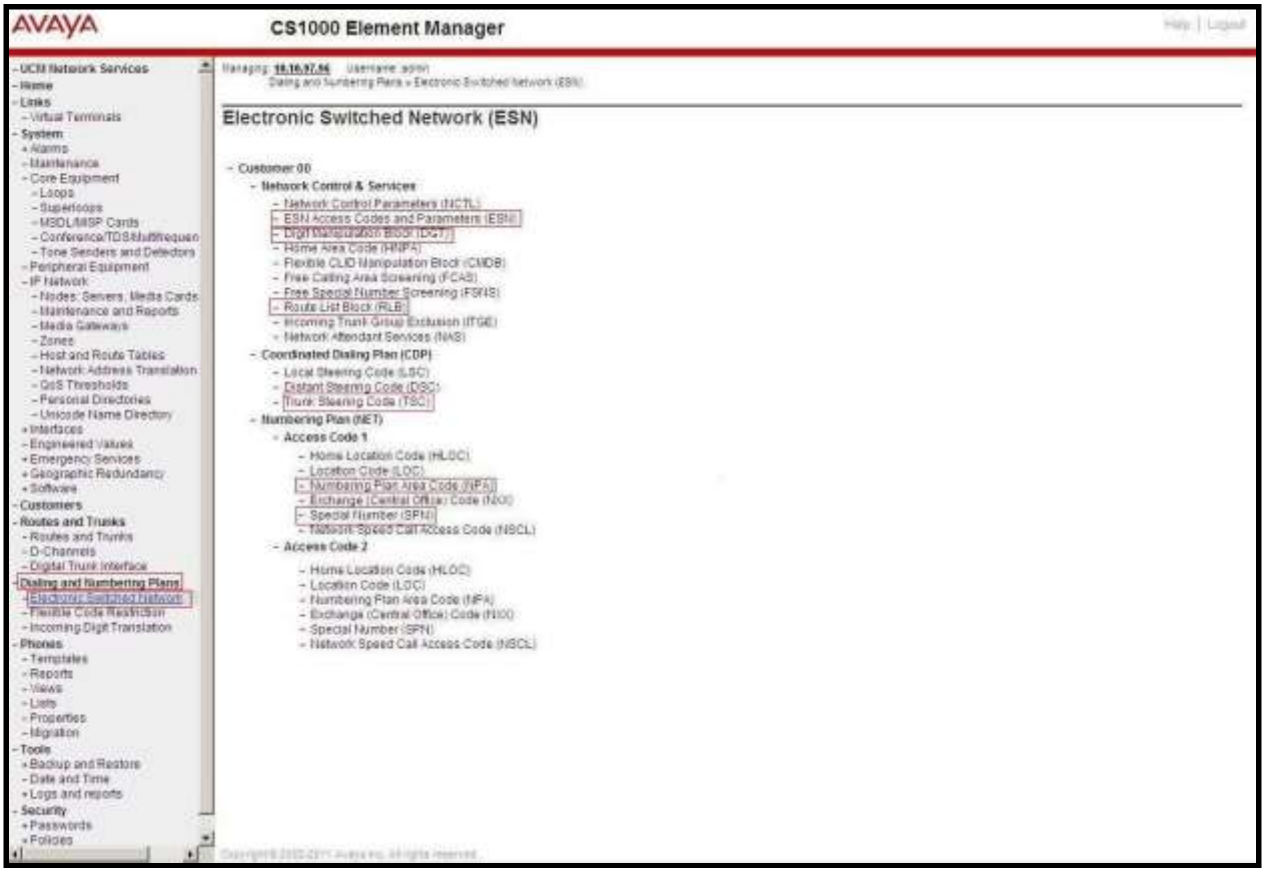
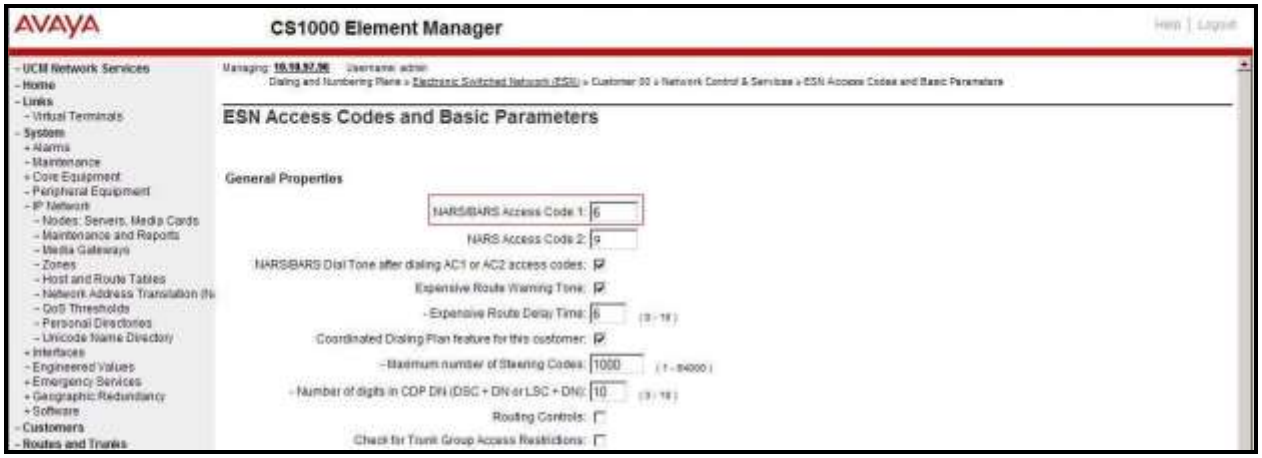

AVAYA
CS1000 Element Manager
Help | Logout
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDL/MISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
- IP Network
- Nodes: Servers, 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
- 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
Managing: 10.10.97.56 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN)
Electronic Switched Network (ESN)
- Customer 00
- Network Control & Services
- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)
- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)
- Numbering Plan (NET)
- Access Code 1
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
- Access Code 2
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
Copyright © 2002-2011 Avaya Inc. All rights reserved.

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).



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » ESN Access Codes and Basic Parameters

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 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 (3 - 18)
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 - 18)
Routing Controls: ☐
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
…
```

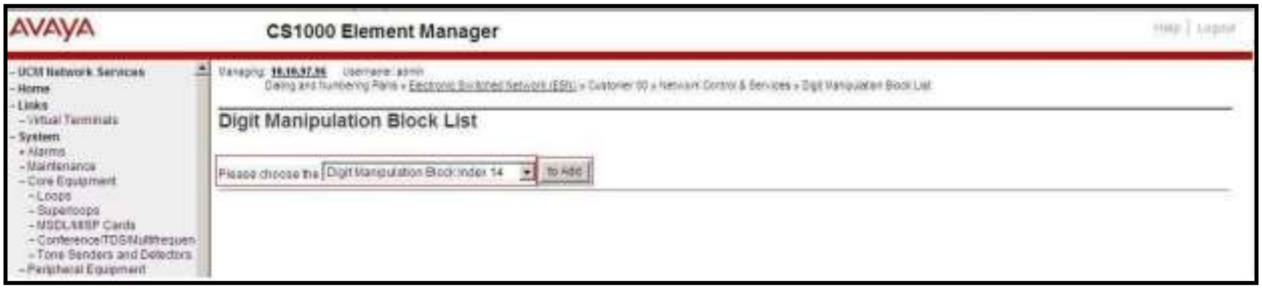
Verify Customer Net Data block by using **ld 21**.

```
>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 Index (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.



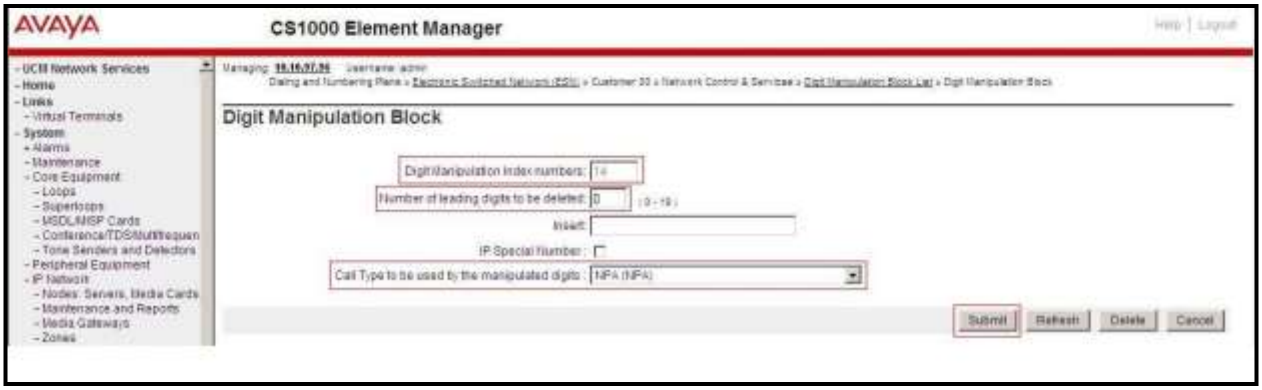
Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List

Digit Manipulation Block List

Please choose the Digit Manipulation Block Index 14

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**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block

Digit Manipulation Block

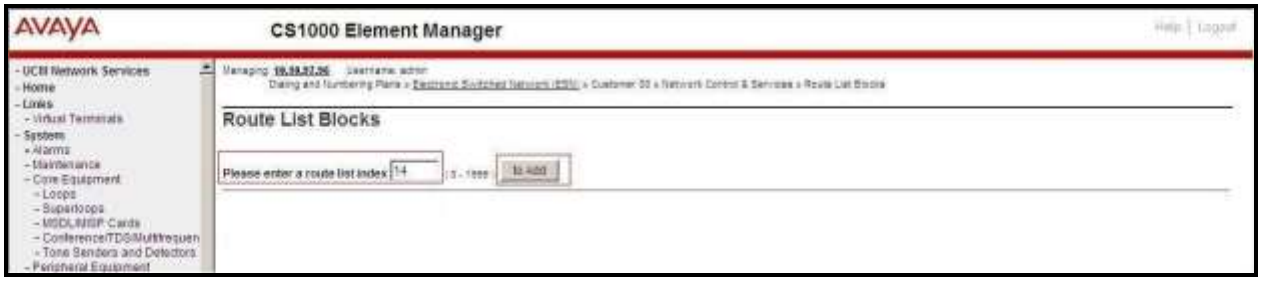
Digit Manipulation index numbers: 14
Number of leading digits to be deleted: 0 (0 - 19)
Insert:
IP Special Number: □
Call Type to be used by the manipulated digits: NPA (NPA)

Figure 42 – DMI 14 Configuration

5.6.4. Route List Block Index (RLI 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**.

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.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

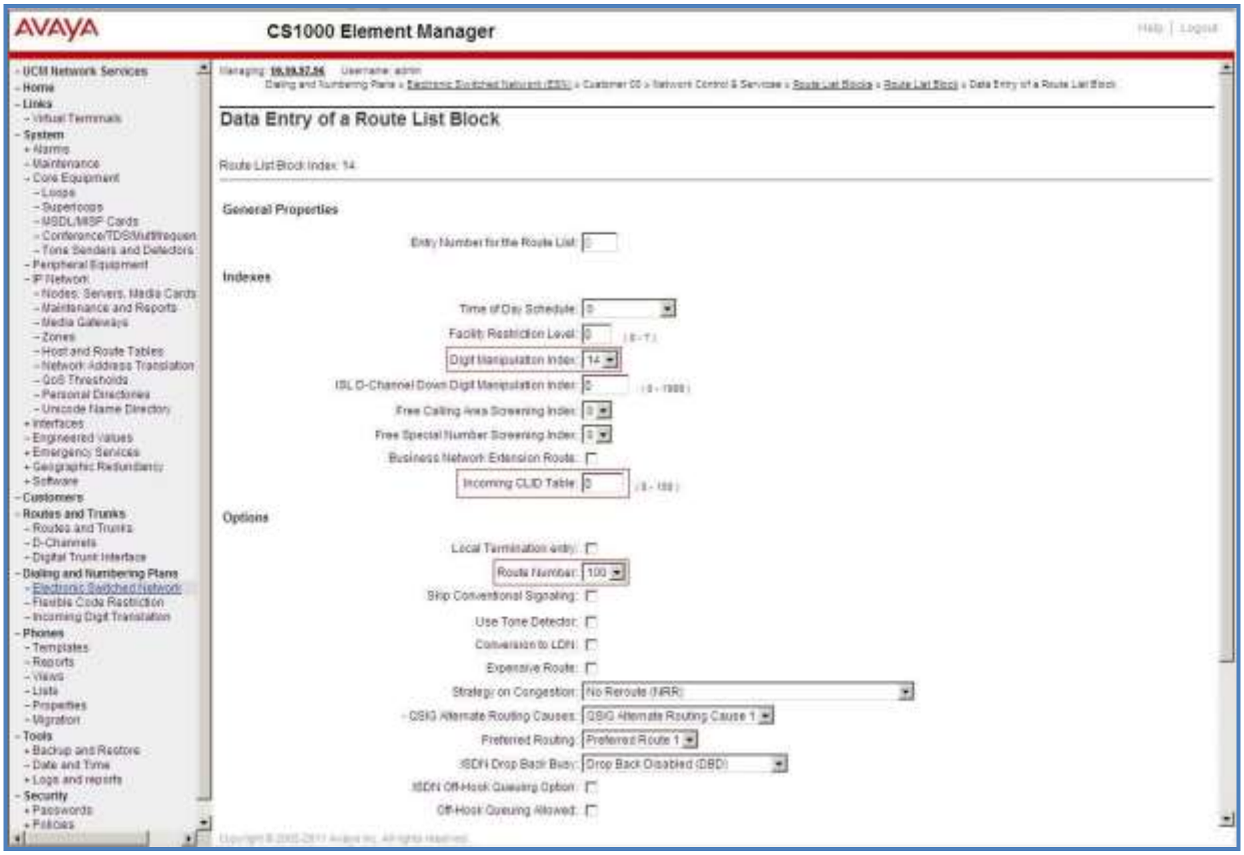
Route List Blocks

Please enter a route list index: 14 (0 - 1999)

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**).



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks » Route List Block » Data Entry of a Route List Block

Data Entry of a Route List Block

Route List Block Index: 14

General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0
Facility Restriction Level: 0 (0 - 7)
Digit Manipulation Index: 14
ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: □
Incoming CLID Table: 0 (0 - 100)

Options

Local Termination entry: □
Route Number: 100
Skip Conventional Signaling: □
Use Tone Detector: □
Conversion to LDN: □
Expensive Route: □
Strategy on Congestion: No Reroute (NRR)
- QSIG Alternate Routing Causes: QSIG Alternate Routing Cause 1
Preferred Routing: Preferred Route 1
ISDN Drop Back Busy: Drop Back Disabled (DBD)
ISDN Off-Hook Queuing Option: □
Off-Hook Queuing Allowed: □

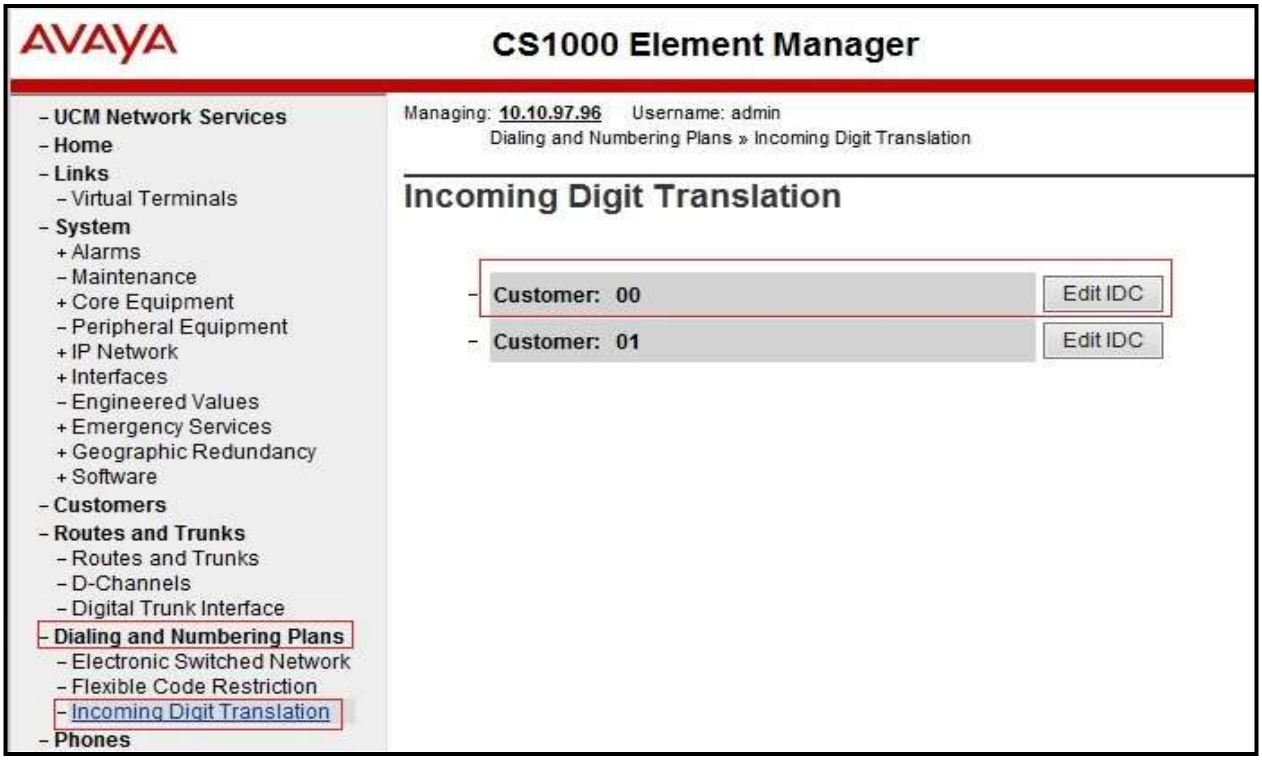
Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 44 – RLI 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 TDC Business 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**.



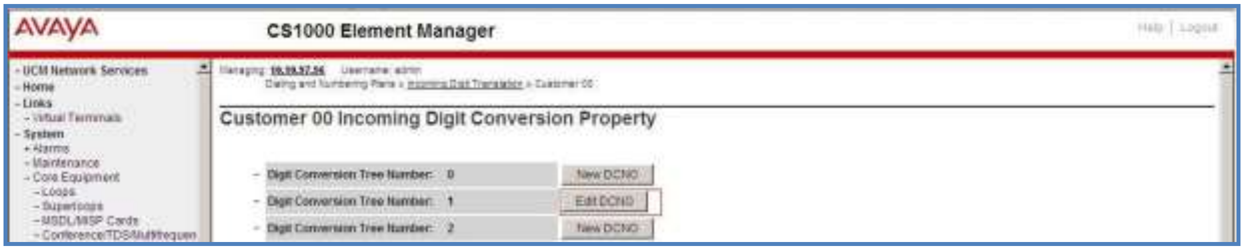
Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation

Incoming Digit Translation

- Customer: 00
- Customer: 01

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 and its **Edit DCNO** button is shown in **Figure 46**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00

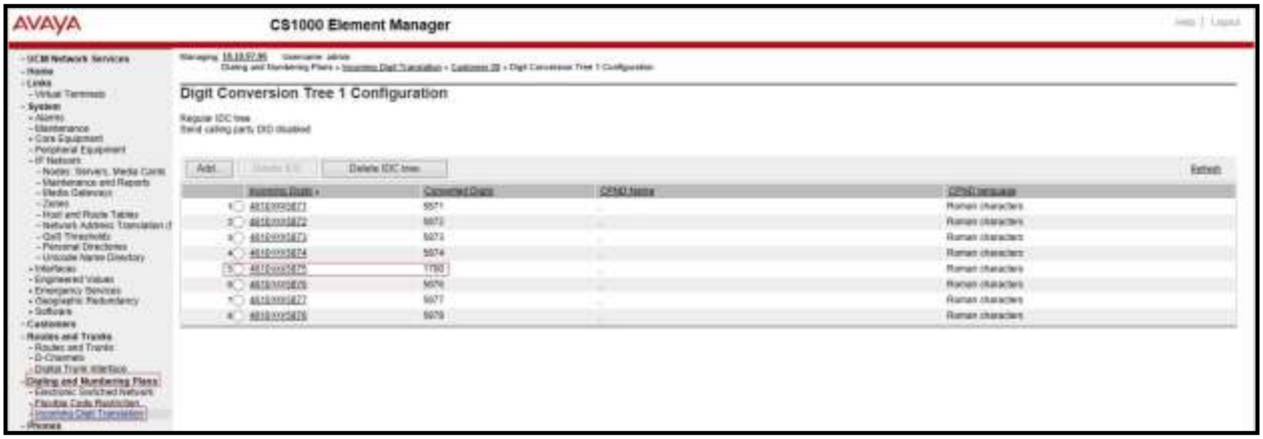
Customer 00 Incoming Digit Conversion Property

- Digit Conversion Tree Number: 0
- Digit Conversion Tree Number: 1
- Digit Conversion Tree Number: 2

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 configured on route 100 as shown in **Figure 32**.

In the following configuration, the incoming call from the PSTN to DID with prefix **4610XXX** will be translated to the associated DN with 4 digits. For testing purposes, DID number **4610XXX5875** is translated to **1700** for voicemail testing.



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

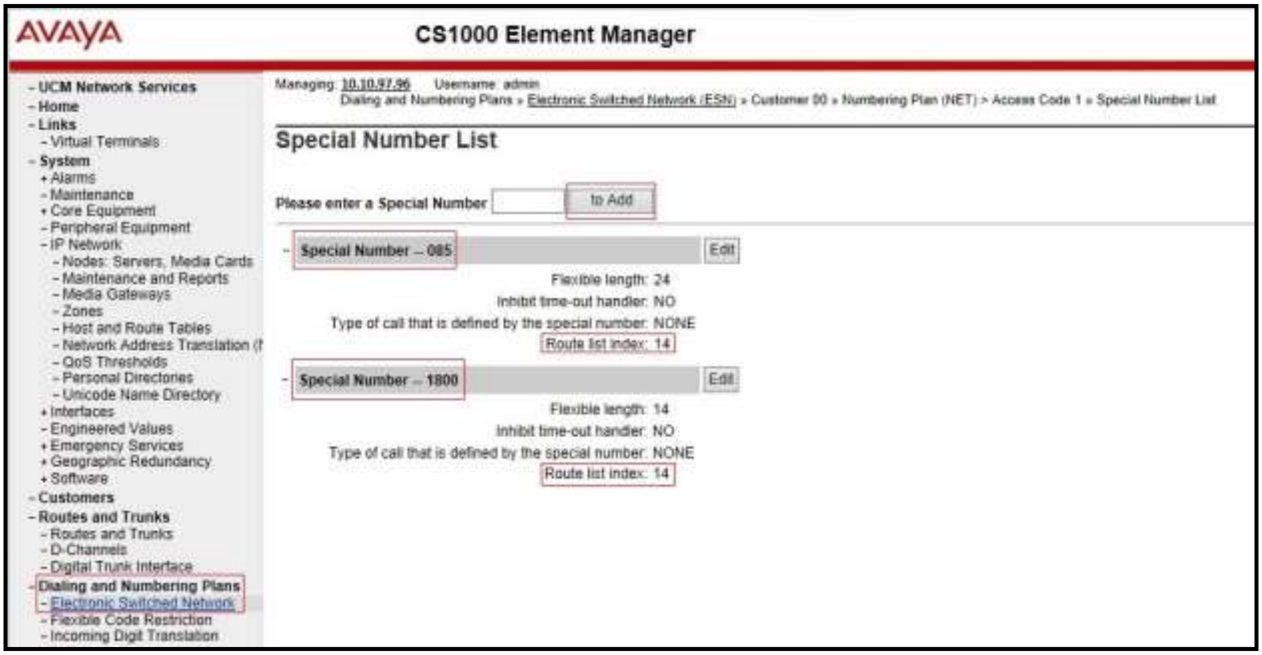
	Incoming Digits	Converted Digits	CPND Name	CPND language
1 ○	4610XXX5871	5871	-	Roman characters
2 ○	4610XXX5872	5872	-	Roman characters
3 ○	4610XXX5873	5873	-	Roman characters
4 ○	4610XXX5874	5874	-	Roman characters
5 ○	4610XXX5875	1700	-	Roman characters
6 ○	4610XXX5876	5876	-	Roman characters
7 ○	4610XXX5877	5877	-	Roman characters
8 ○	4610XXX5878	5878	-	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: 085, 1800, and so on. These special numbers were associated to **Route list index 14** created in **Section 5.6.4**.

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



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) > Access Code 1 » Special Number List

Special Number List

Please enter a Special Number [ ] to Add

- Special Number – 085 Edit

Flexible length: 24
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

- Special Number – 1800 Edit

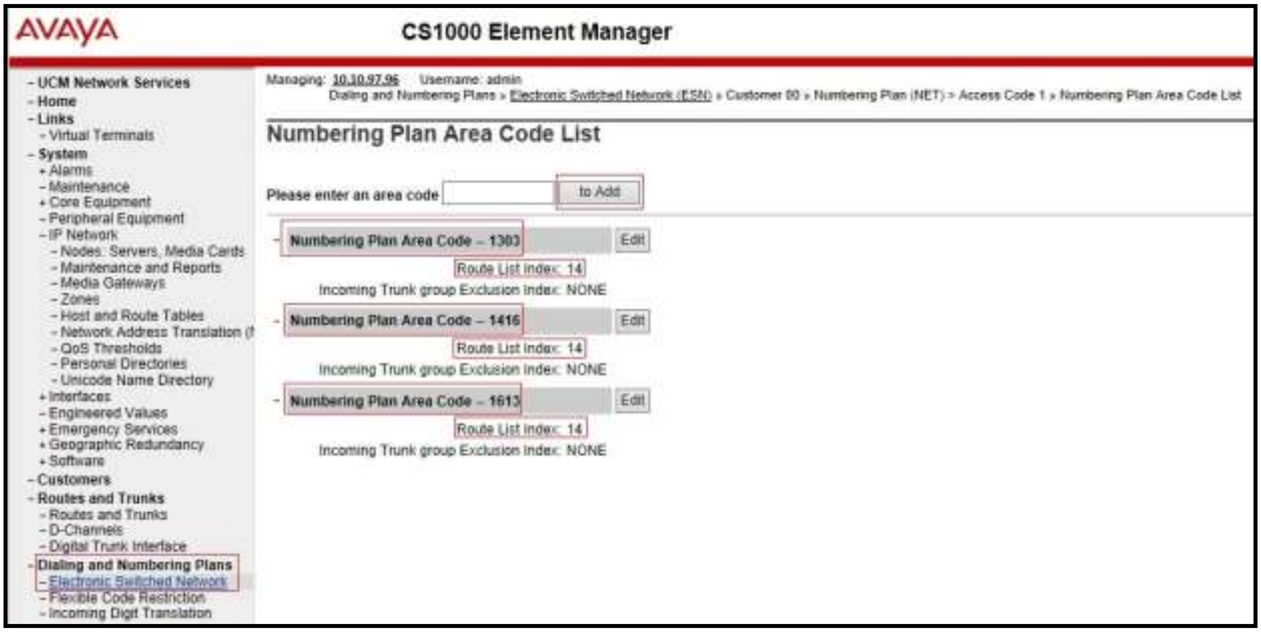
Flexible length: 14
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

Figure 48 – SPN numbers

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown). Select **Numbering Plan Area Code (NPA)** as shown in **Figure 39**. Enter the area code desired in the textbox and click on the **to Add** button. The 1303, 1416, and 1613 area codes were used in this configuration as shown in **Figure 49**. These area codes were associated to **Route List Index 14** created in **Section 5.6.4**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List

Numbering Plan Area Code List

Please enter an area code

Numbering Plan Area Code – 1303
Route List Index: 14
Incoming Trunk group Exclusion Index: NONE

Numbering Plan Area Code – 1416
Route List Index: 14
Incoming Trunk group Exclusion Index: NONE

Numbering Plan Area Code – 1613
Route List Index: 14
Incoming Trunk group Exclusion Index: NONE

Figure 49 – Numbering Plan Area List

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 FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
    MSNV FRA  PKCH MWTD DVLD CROD ELCD
CPND_LANG ENG
HUNT
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
```

```
KEY  00 SCR 5871 0     MARP ← Set the position of DN 5871 to display on key 0 of the phone
       CPND
         CPND_LANG ROMAN
           NAME TDC_01 ← 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 TDC Business 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 TDC Business Trunk Service.

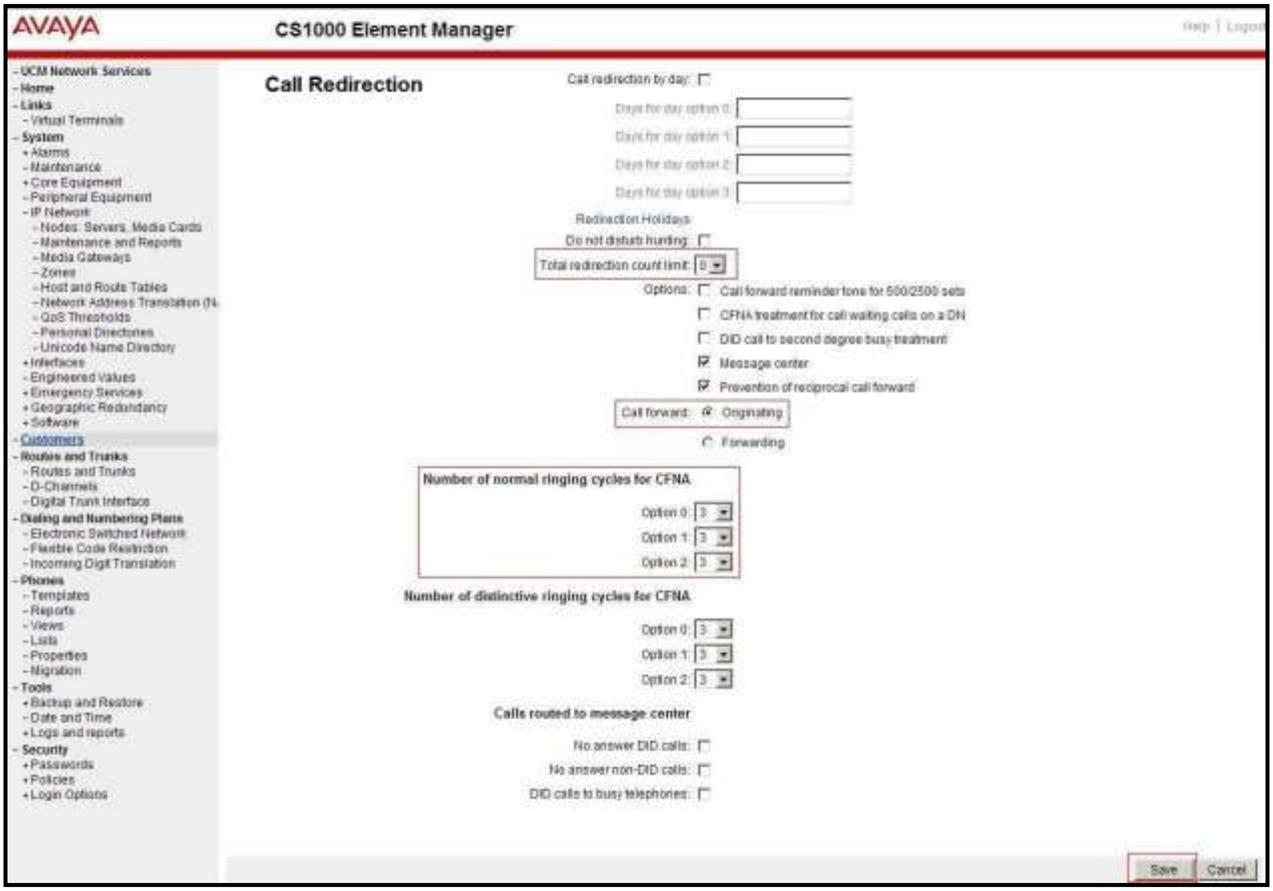
```
>ld 11
REQ: chg
TYPE: 2002p2
TN   96 0 0 2
ECHG yes
ITEM CLS DDGA
…
```

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 50**.

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



Call Redirection

Call redirection by day: □

Days for day option 0:

Days for day option 1:

Days for day option 2:

Days for day option 3:

Redirection Holidays

Do not disturb hunting: □

Total redirection count limit: 0

Options:
□ Call forward reminder tone for 500/2500 sets
□ CFNA treatment for call waiting calls on a DN
□ DID call to second degree busy treatment
☑ Message center
☑ Prevention of reciprocal call forward

Call forward: ● Originating ○ Forwarding

Number of normal ringing cycles for CFNA

Option 0: 3
Option 1: 3
Option 2: 3

Number of distinctive ringing cycles for CFNA

Option 0: 3
Option 1: 3
Option 2: 3

Calls routed to message center

No answer DID calls: □
No answer non-DID calls: □
DID calls to busy telephones: □

Figure 50 – 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 **61303XXX9045**.

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

ECHG yes
ITEM CLS CFXA SFA
ITEM key 19 CFW 16 61303XXX9045
```

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 **61303XXX9045**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN   96 0 0 2
ECHG yes
ITEM CLS FBA HTA SFA
ITEM HUNT 61303XXX9045
ITEM FDN 61303XXX9045
```

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 **61303XXX9045**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN   96 0 0 2
ECHG yes
ITEM CLS FNA SFA
ITEM HUNT 61303XXX9045
ITEM FDN 61303XXX9045
```

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.

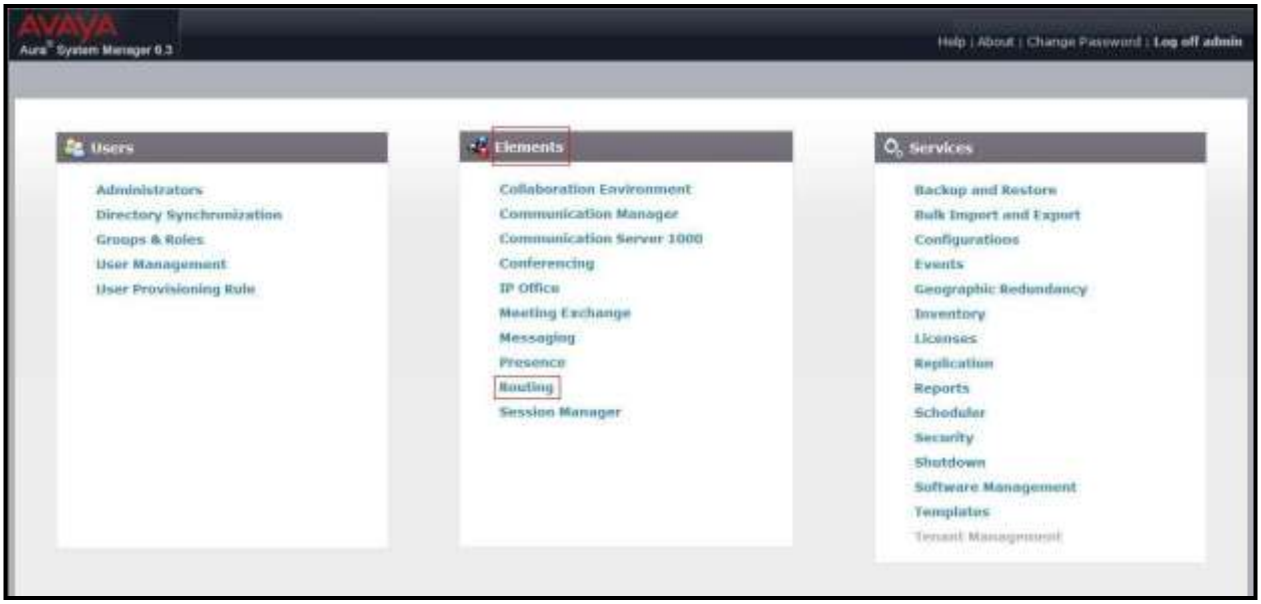
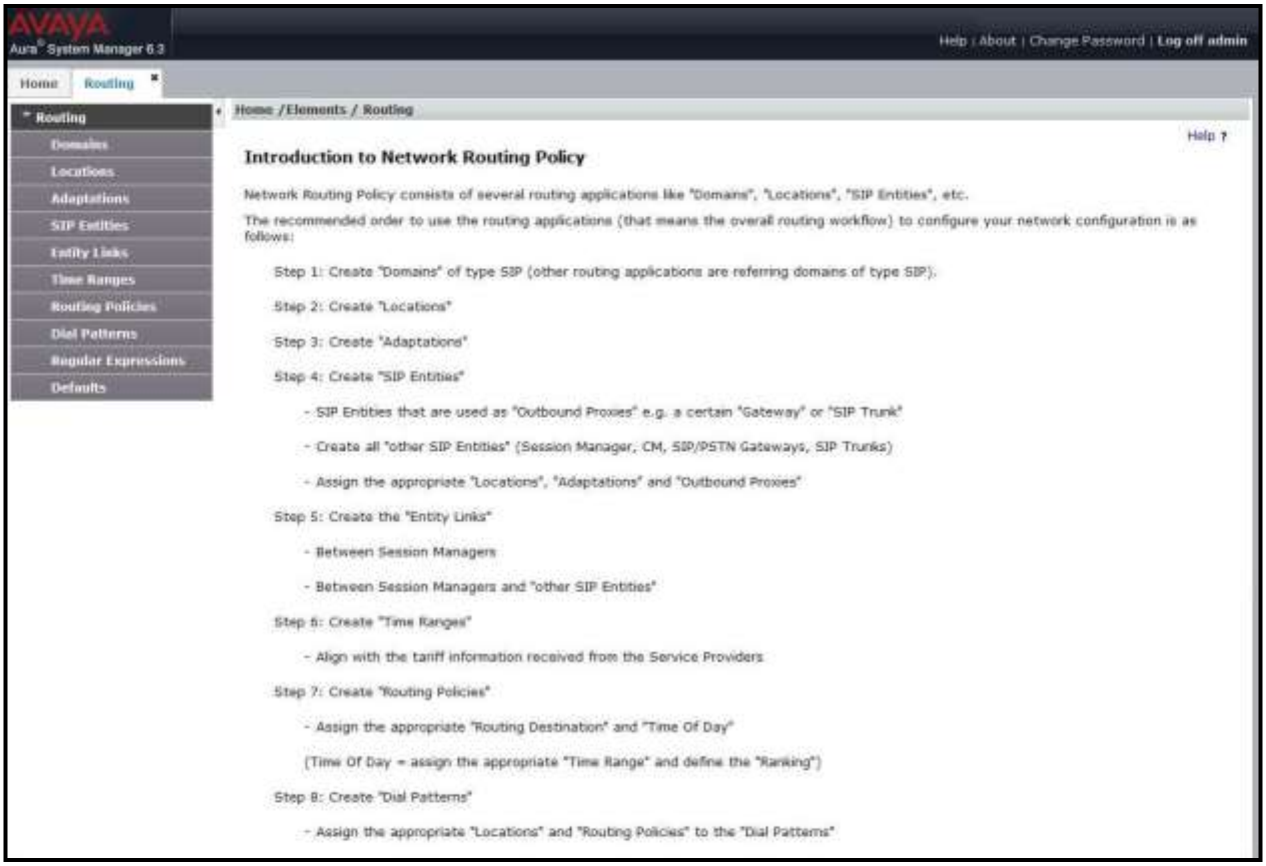


Figure 51 – System Manager Home Screen

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.



Introduction to Network Routing Policy

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 52 – Network Routing Policy

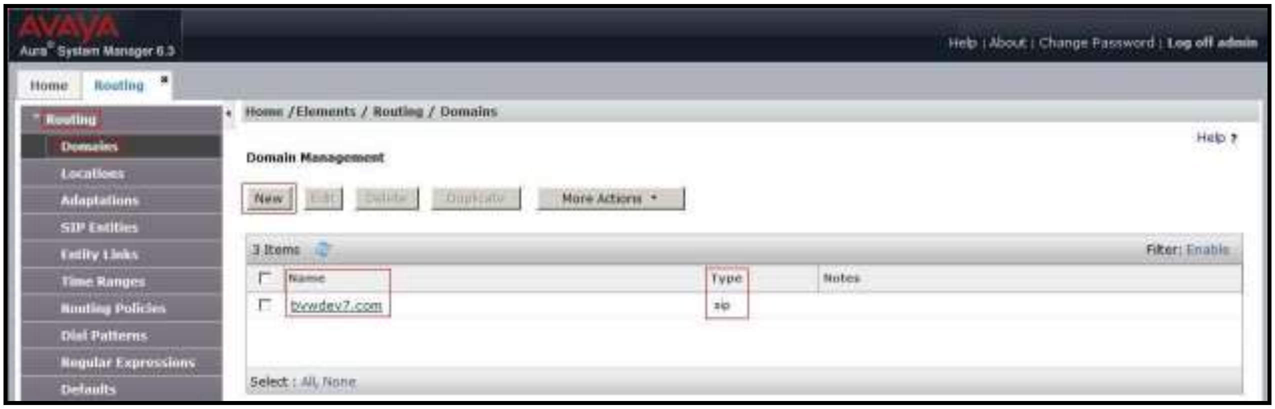
6.2. Specify SIP Domain

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 (refer to **Section 5.5.2**).
- **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 configured entry for the enterprise domain.



Domain Management

3 Items

	Name	Type	Notes
□	bvwdev7.com	sip	

Figure 53 – Domain Management

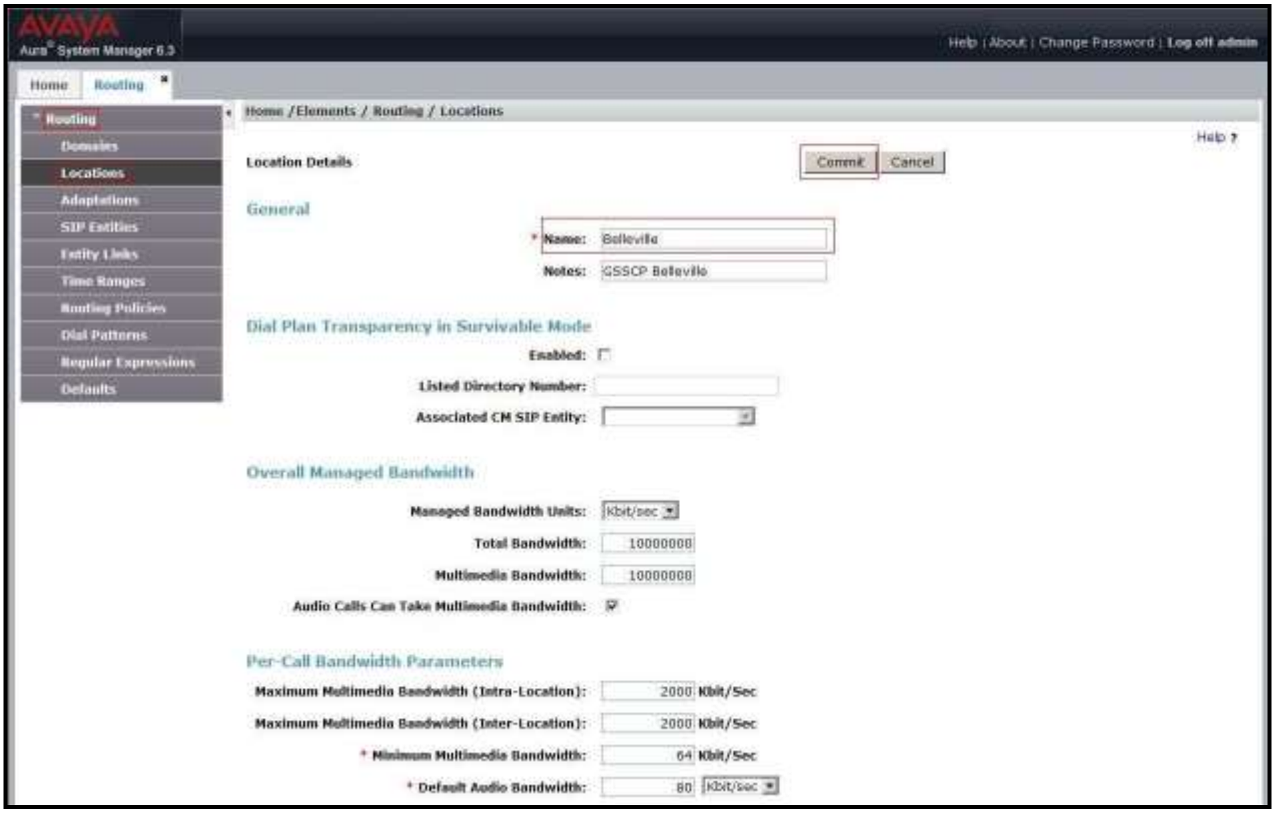
6.3. Add Location

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).



Location Details

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: Kbit/sec

Total Bandwidth: 10000000

Multimedia Bandwidth: 10000000

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

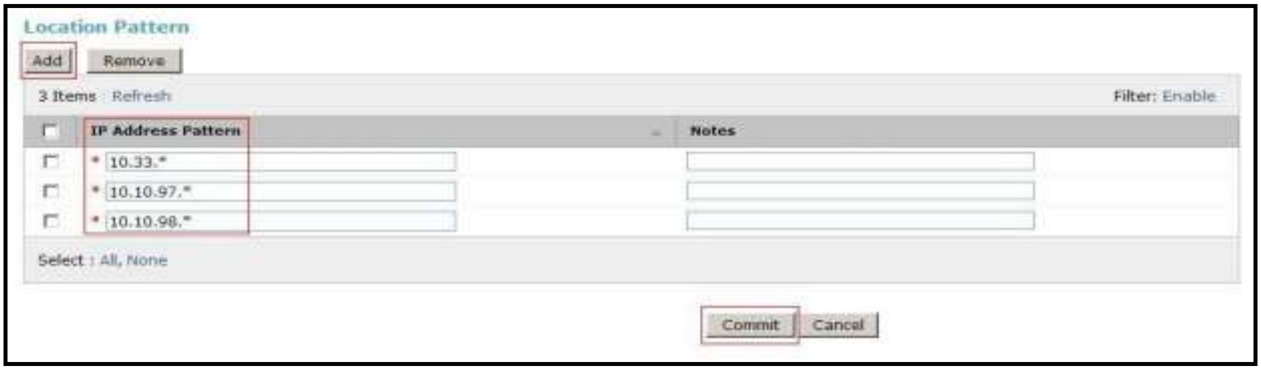
* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Figure 54 – 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.*



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

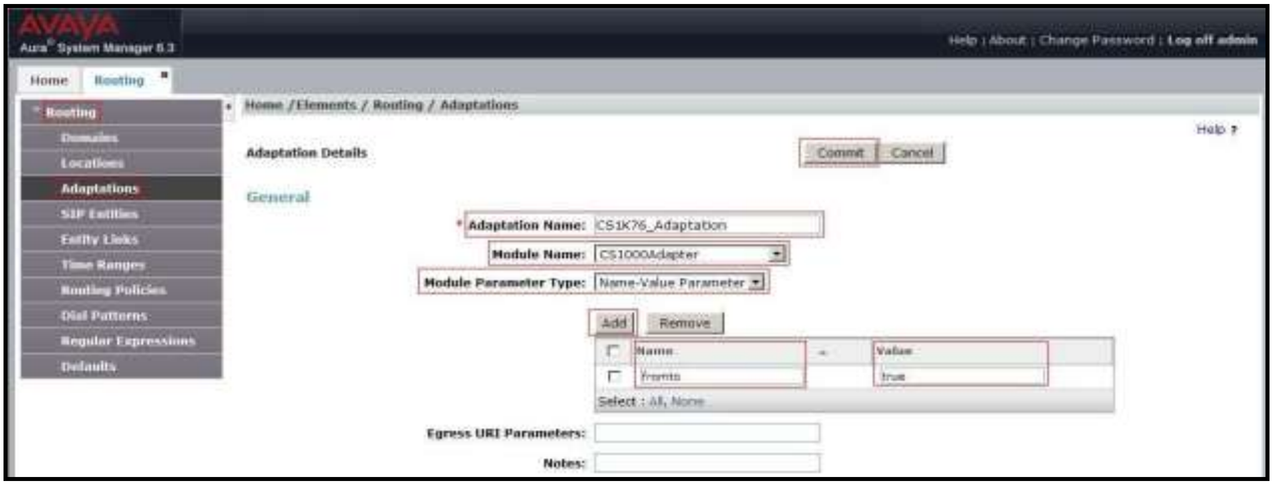
Figure 55 – IP Ranges Configuration

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.



Adaptation Details

General

* Adaptation Name: CS1K76_Adaptation

Module Name: CS1000Adapter

Module Parameter Type: Name-Value Parameter

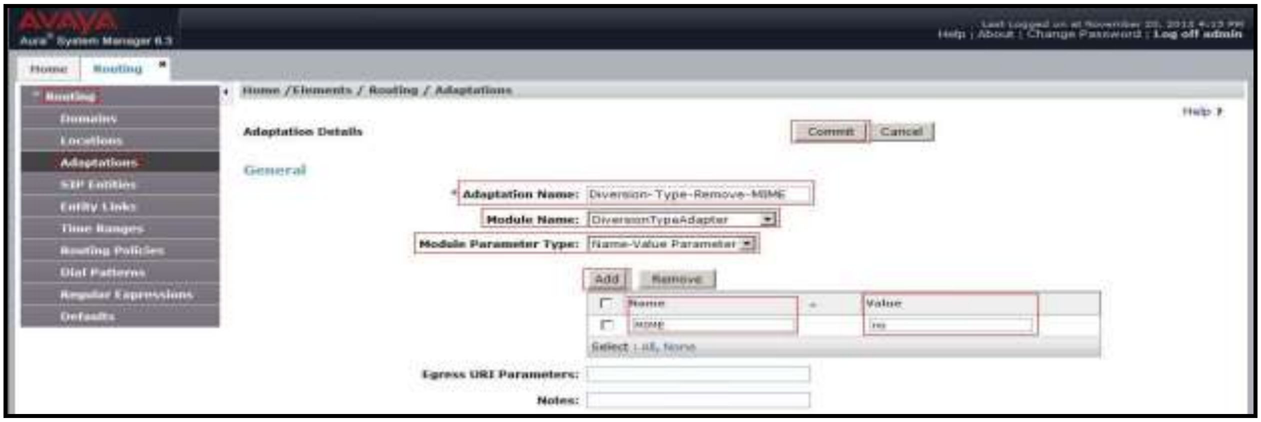
	Name	=	Value
□	fromto		true

Egress URI Parameters:

Notes:

Figure 56 - 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.



Adaptation Details

General

* Adaptation Name: Diversion-Type-Remove-MIME

Module Name: DiversionTypeAdapter

Module Parameter Type: Name-Value Parameter

	Name	=	Value
□	MIME		no

Egress URI Parameters:

Notes:

Figure 57 – 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.

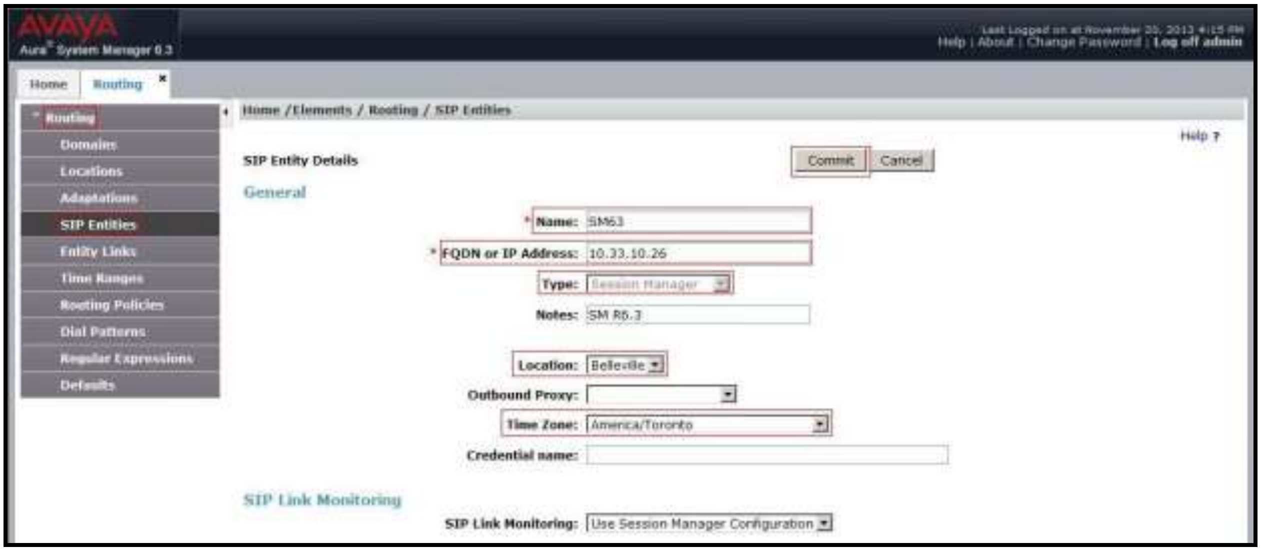
- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **Other** for CS1000 and Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not 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 user will need to select the specific values for the **Location** and **Time Zone**.



SIP Entity Details

General

* Name: SM63

* FQDN or IP Address: 10.33.10.26

Type: Session Manager

Notes: SM R6.3

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Figure 58 – Session Manager SIP Entity

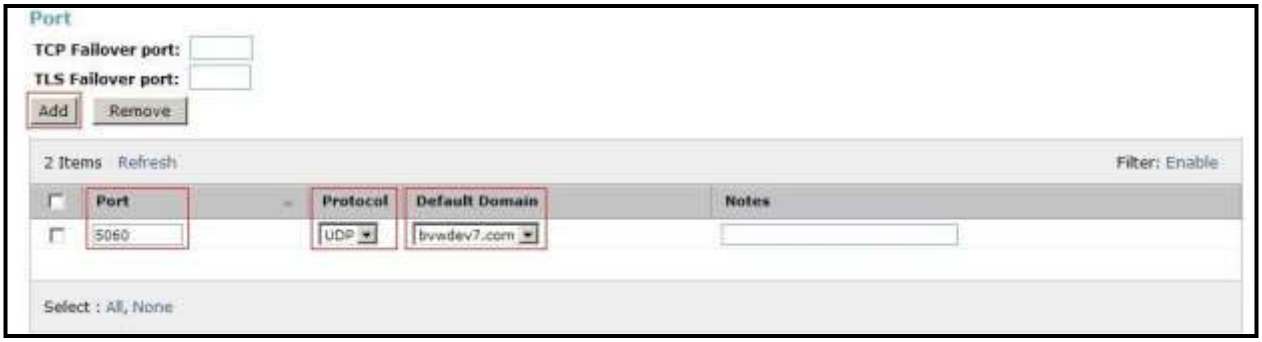
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

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.



TCP Failover port:

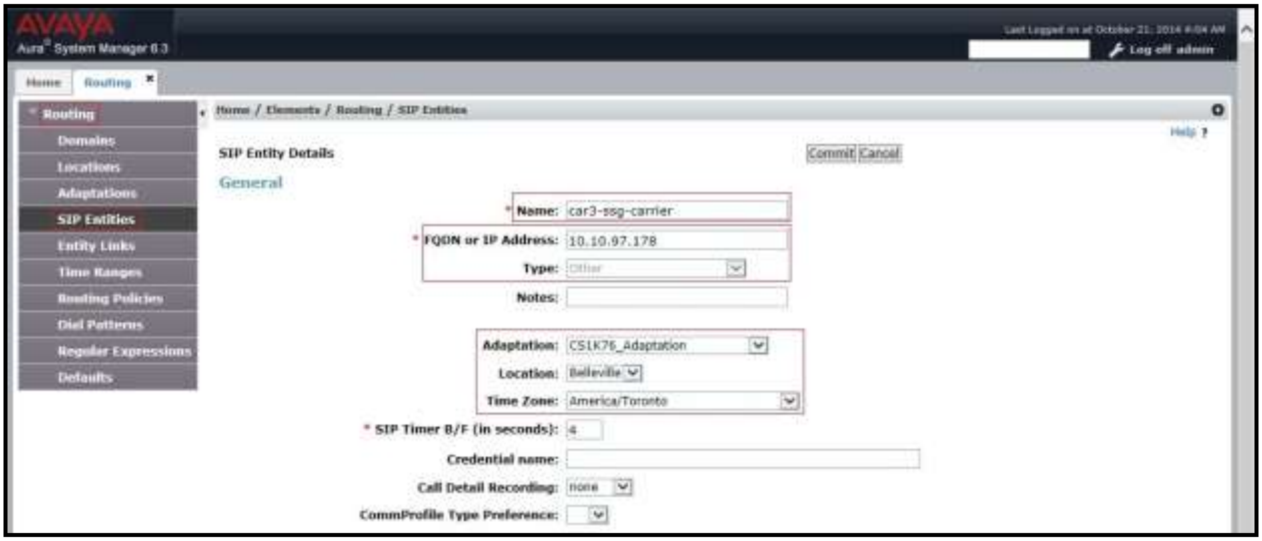
TLS Failover port:

	Port	Protocol	Default Domain	Notes
□	5060	UDP	bvwdev7.com	

Figure 59 – 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 user will need to select the specific values for the **Location** and **Time Zone**.



SIP Entity Details

General

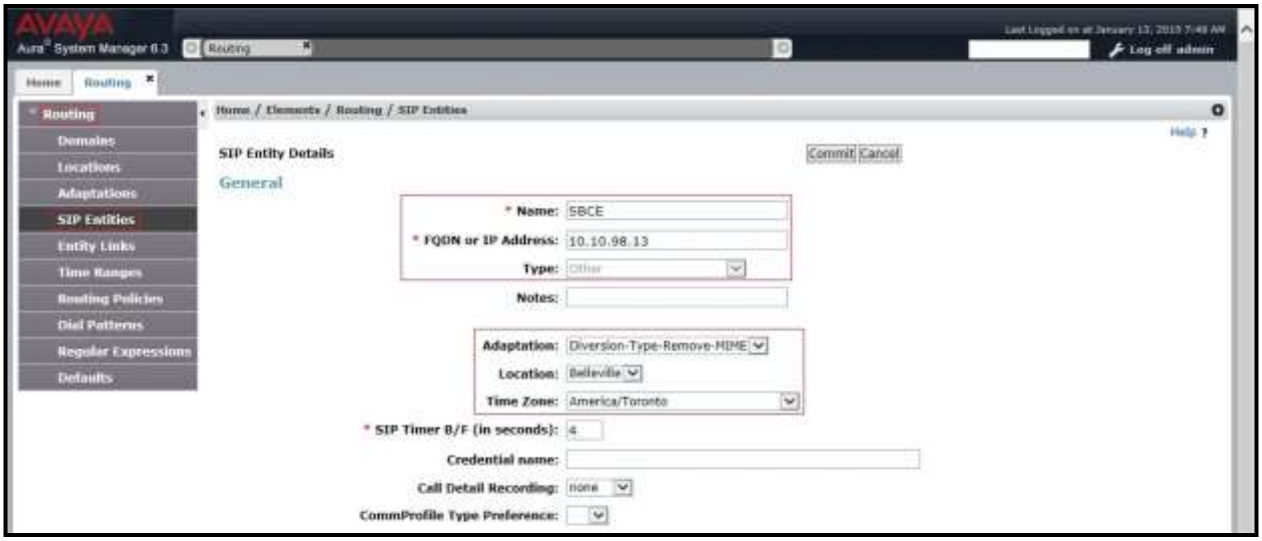
* Name:	car3-ssg-carrier
* FQDN or IP Address:	10.10.97.178
Type:	Other
Notes:	
Adaptation:	CS1K76_Adaptation
Location:	Belleville
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none
CommProfile Type Preference:	

Figure 60 – Communication Server 1000 SIP Entity

6.5.3. Configure Avaya SBCE SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE named **SBCE**. 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 user will need to select the specific values for the **Location** and **Time Zone**.

The following screenshot shows the SIP Entity for Avaya SBCE.



SIP Entity Details

General

* Name: SBCE

* FQDN or IP Address: 10.10.98.13

Type: Other

Notes:

Adaptation: Diversion-Type-Remove-MIME

Location: Belleville

Time Zone: America/Toronto

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Figure 61 – Avaya SBCE SIP Entity

6.6. Add Entity Links

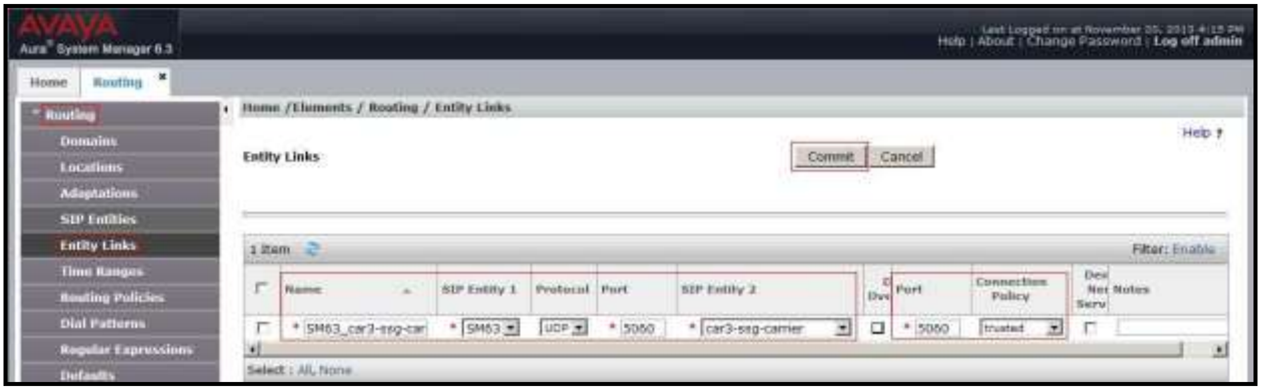
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to CS1000 and one to Avaya SBCE.

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**.



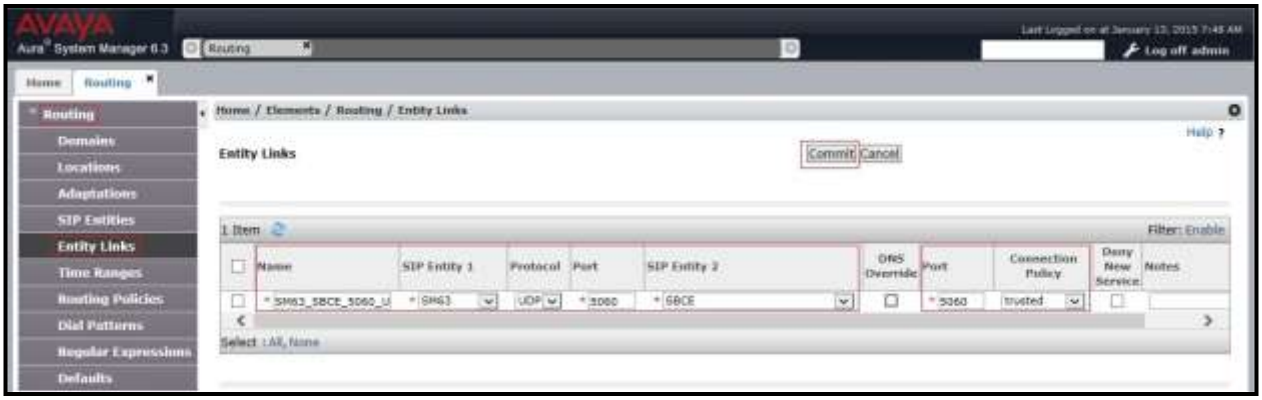
Entity Links

1 Item

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	D Dw	Port	Connection Policy	Der Ner Serv	Notes
☐	* SM63_car3-ssg-car	* SM63	UDP	* 5060	* car3-ssg-carrier	☐	* 5060	trusted	☐	

Figure 62 – Communication Server 1000 Entity Link

The following screen illustrates the Entity Link to Avaya SBCE. The protocol and ports defined here must match the values used for Avaya SBCE mentioned in **Section 7.2.4**, later in this document.



Entity Links

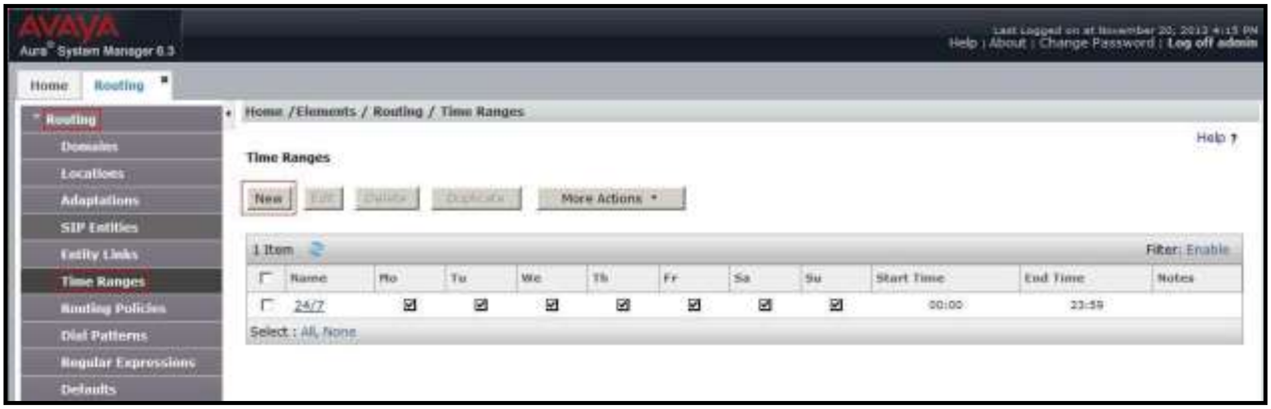
1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
□	* SM63_SBCE_5060_U	* SM63	UDP	* 5060	* SBCE	□	* 5060	trusted	□	

Figure 63 – Avaya SBCE 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.



Time Ranges

□	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
□	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	

Figure 64 – Time Ranges

6.8. Add Routing Policies

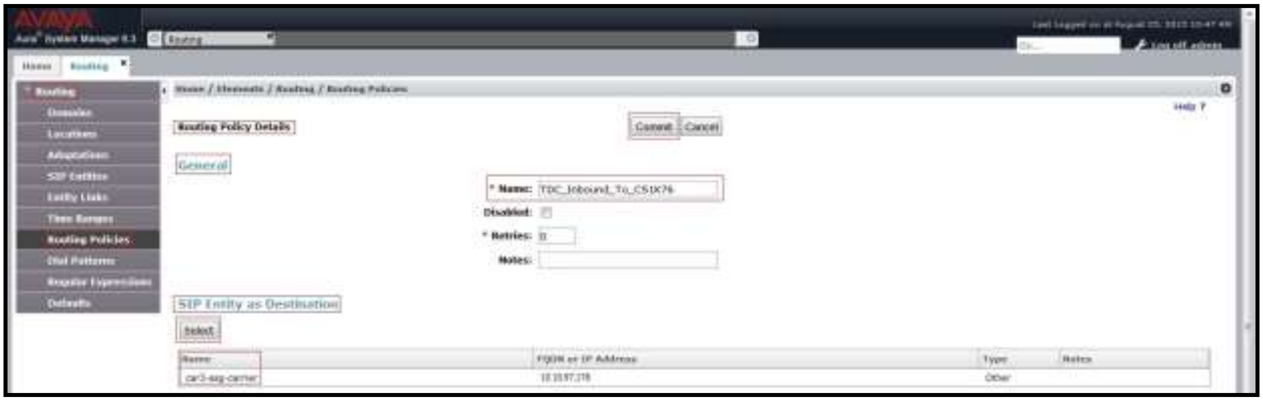
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for the CS1000 and one for Avaya SBCE. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane 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 **TDC_Inbound_To_CS1K76** associated with incoming PSTN calls from the TDC Business Trunk Service to the CS1000. Observe the **SIP Entity as Destination** is the entity named **car3-ssg-carrier**.



Routing Policy Details

General

* Name: TDC_Inbound_To_CS1K76

Disabled: □

* Retries: 0

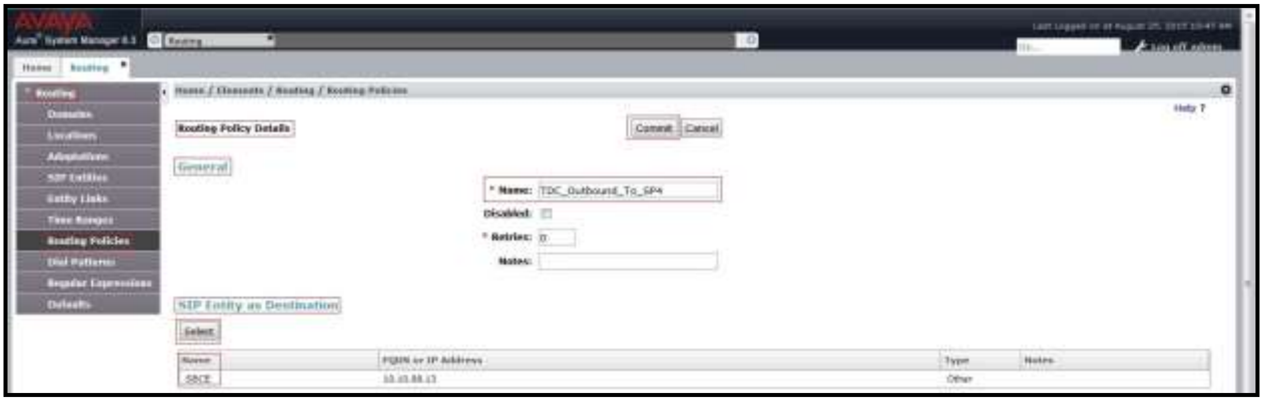
Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
car3-ssg-carrier	10.10.97.178	Other	

Figure 65 – Routing to Communication Server 1000

The following screen shows the **Routing Policy Details** for the policy named **TDC_Outbound_To_SP4**. This is associated with outgoing calls from the CS1000 to the PSTN via the TDC Business Trunk Service, through Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.



Routing Policy Details

General

* Name: TDC_Outbound_To_SP4

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBCE	10.10.88.13	Other	

Figure 66 – Routing to Avaya SBCE

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 the TDC Business 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:

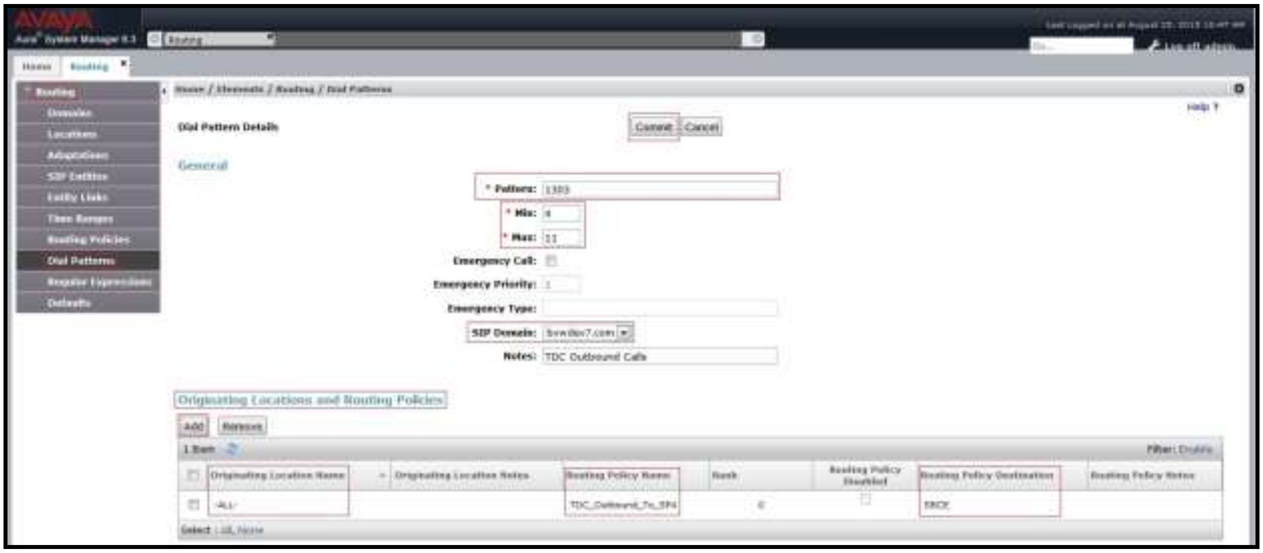
In the **General** section, enter the following values. Use default values for all remaining fields.

- **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., 1800, 08, etc.) were similarly defined.

The following screen shows that outbound dialed numbers with a maximum of 11 digits that begin with **1303** and have a destination SIP Domain of **bvwdev7.com** use the Routing Policy Names **TDC_Outbound_To_SP4** as defined in **Section 6.8**.



Dial Pattern Details

General

* Pattern: 1303
* Min: 4
* Max: 11
Emergency Call: □
Emergency Priority: 1
Emergency Type:
SIP Domain: bvwdev7.com
Notes: TDC Outbound Calls

Originating Locations and Routing Policies

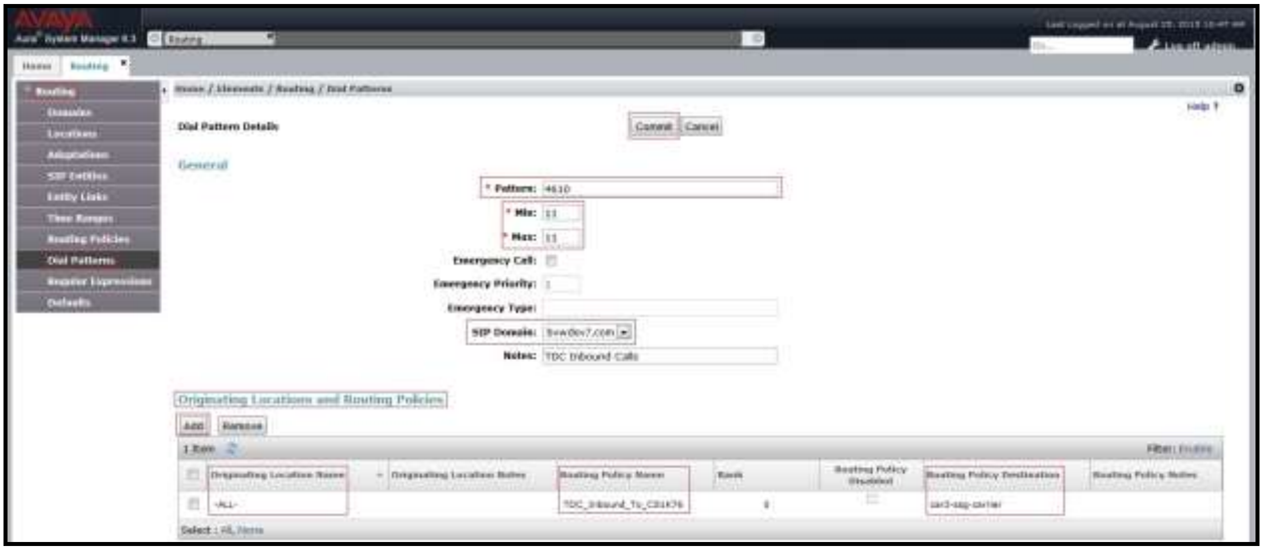
1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Outbound_To_SP4	0	□	SBCE	

Figure 67 – Dial Pattern 1303

Note that with the above Dial Pattern, the TDC Business Trunk did not restrict outbound calls to this specific US area code. In real deployments, appropriate restriction can be exercised per customer business policies.

The following screen shows that inbound 11-digit numbers that start with **4610** use Routing Policy Name **TDC_Inbound_To_CS1K76** as defined in **Section 6.8**. This Dial Pattern matches the DID numbers assigned to the enterprise by TDC Business Trunk Service.



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 4610

* Min: 11

* Max: 11

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: TDC Inbound Calls

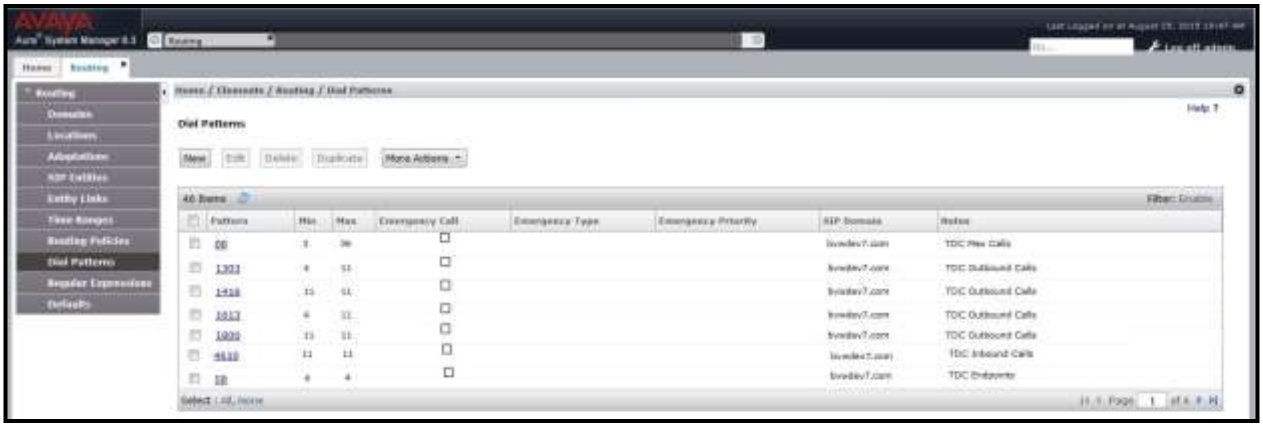
Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Inbound_To_CS1K76	0	□	[illegible]	

Figure 68 – Dial Pattern 4610

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



Home / Elements / Routing / Dial Patterns

Dial Patterns

46 Items

□	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
□	00	3	36	□			bvwdev7.com	TDC Misc Calls
□	1303	4	11	□			bvwdev7.com	TDC Outbound Calls
□	1410	11	11	□			bvwdev7.com	TDC Outbound Calls
□	1813	4	11	□			bvwdev7.com	TDC Outbound Calls
□	1900	11	11	□			bvwdev7.com	TDC Outbound Calls
□	4610	11	11	□			bvwdev7.com	TDC Inbound Calls
□	58	4	4	□			bvwdev7.com	TDC Endpoints

Page 1

Figure 69 – Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and the TDC Business Trunk system.

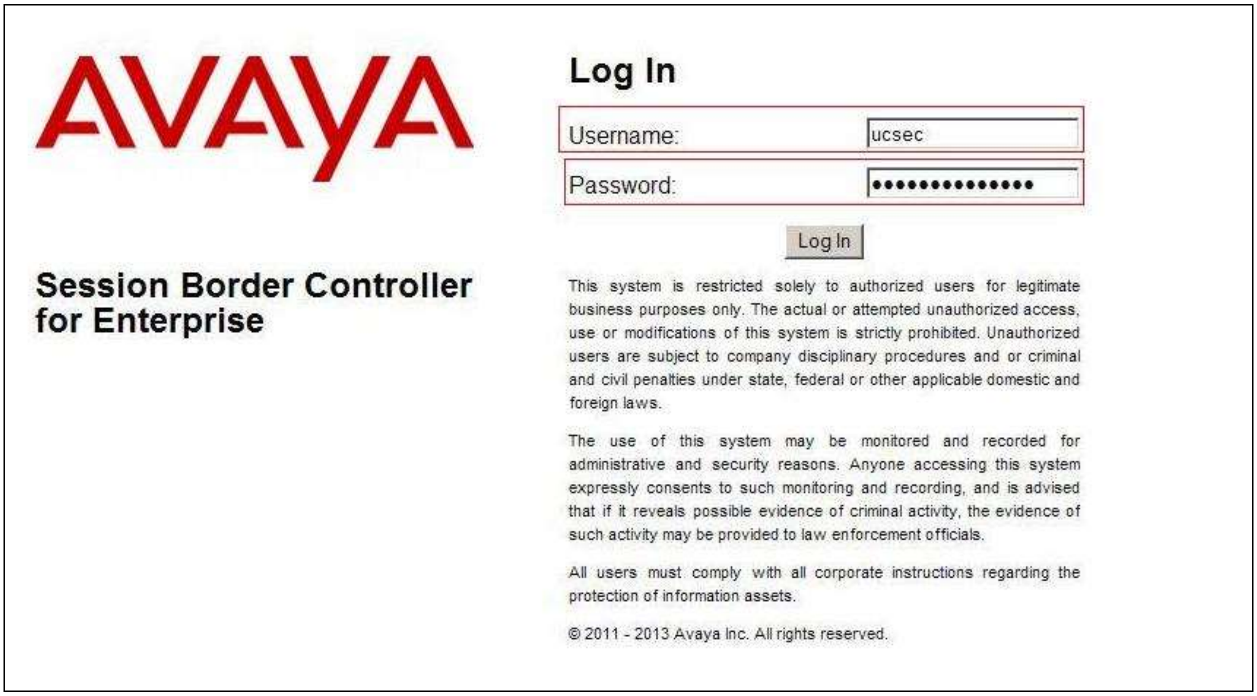
In this test configuration as shown in **Figure 1**, the Avaya elements reside on the Private side and the TDC Business Trunk system resides on the Public side of the network.

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

7.1. Log in Avaya Session Border Controller for Enterprise

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: ucsec

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.

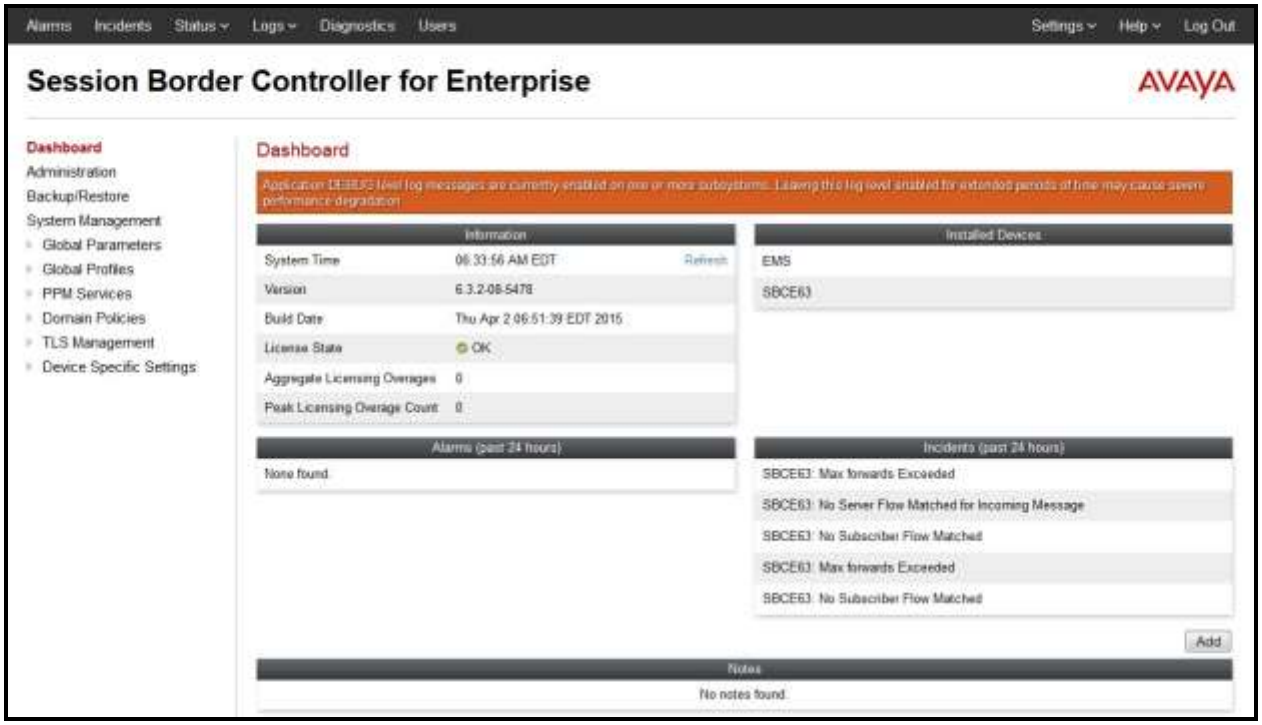
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

Figure 70 - Avaya SBCE Login

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



Dashboard

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation

Information	
System Time	06:33:56 AM EDT
Version	6.3.2-08-5478
Build Date	Thu Apr 2 06:51:39 EDT 2015
License State	● OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0

Installed Devices
EMS
SBCE63

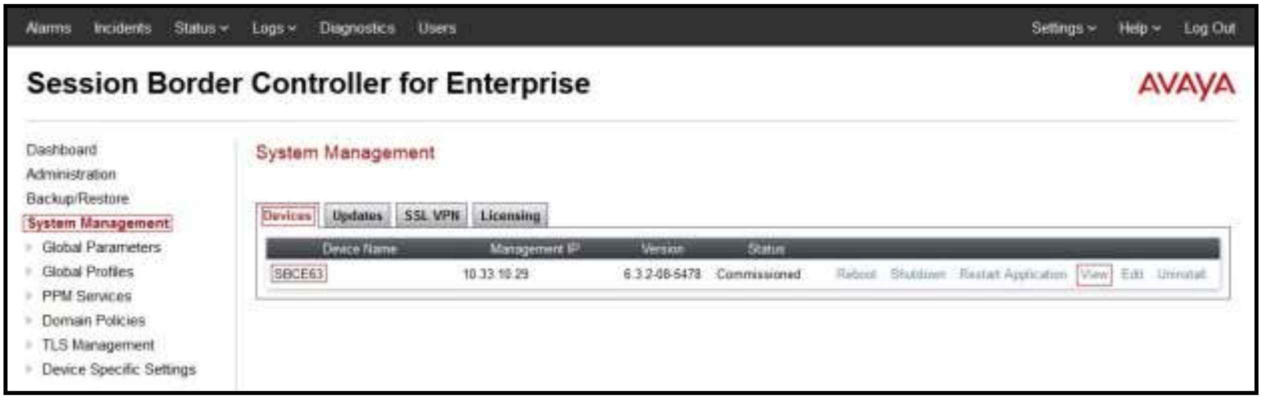
Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE63: Max forwards Exceeded
SBCE63: No Server Flow Matched for Incoming Message
SBCE63: No Subscriber Flow Matched
SBCE63: Max forwards Exceeded
SBCE63: No Subscriber Flow Matched

Notes
No notes found.

Figure 71 - Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance test, a single Device Name **SBCE63** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.

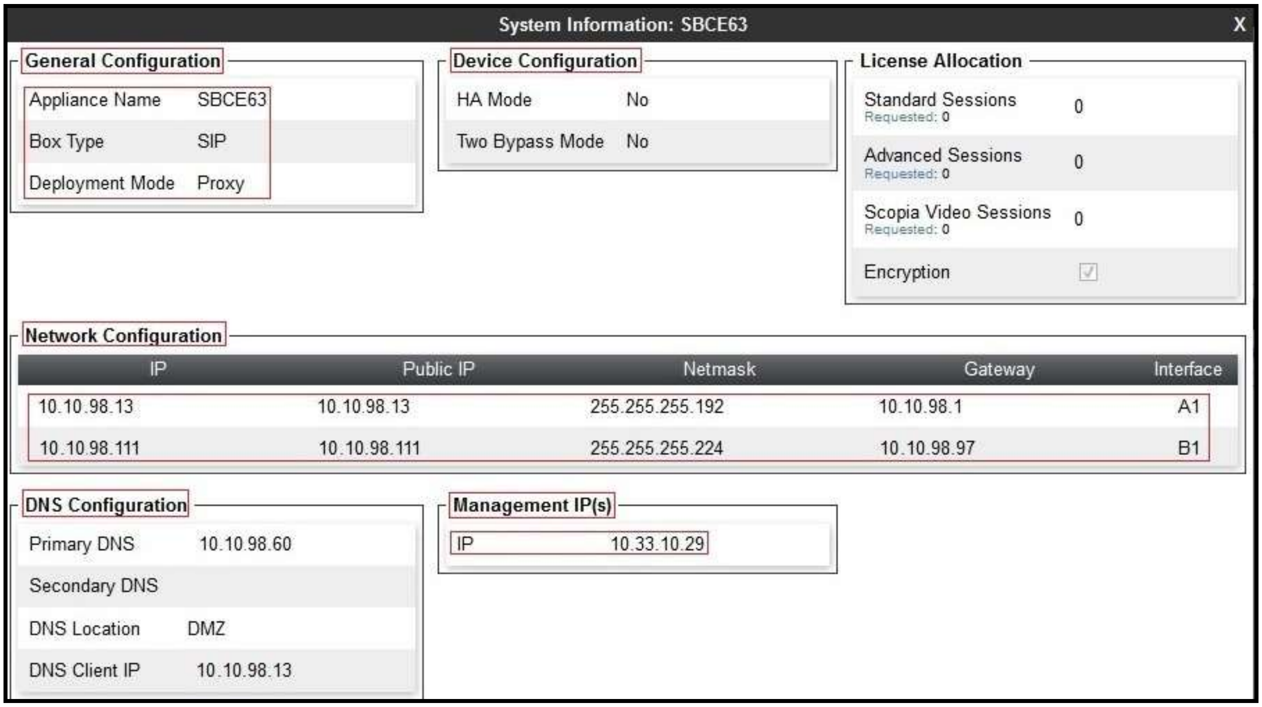


System Management

Device Name	Management IP	Version	Status	
SBCE63	10.33.10.29	6.3.2-08-5478	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Figure 72 - Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.



System Information: SBCE63

General Configuration

Appliance Name	SBCE63
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 0	0
Advanced Sessions Requested: 0	0
Scopia Video Sessions Requested: 0	0
Encryption	☑

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.98.13	10.10.98.13	255.255.255.192	10.10.98.1	A1
10.10.98.111	10.10.98.111	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.98.13

Management IP(s)

IP	10.33.10.29

Figure 73 - Avaya SBCE System Information

7.2. Global Profiles

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

7.2.1. Configure Server Interworking Profile - Avaya Session Manager

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

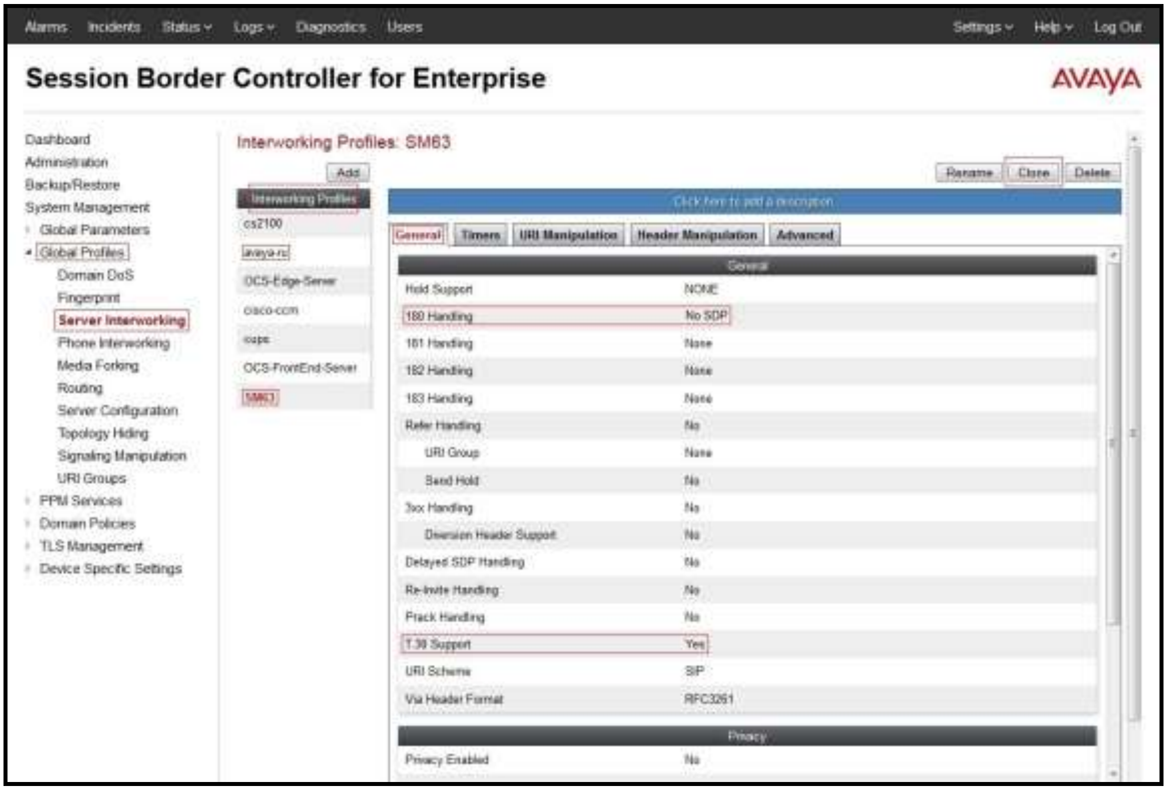
From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- 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, Check **180 Handling** as **No SDP** and set **T.38 Support** to **Yes** (TDC Business Trunk supports T.38 Fax). Click **Next** button (not shown) to leave other options at default. Click **Finish** (not shown).

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



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

Figure 74 - Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – TDC Business Trunk

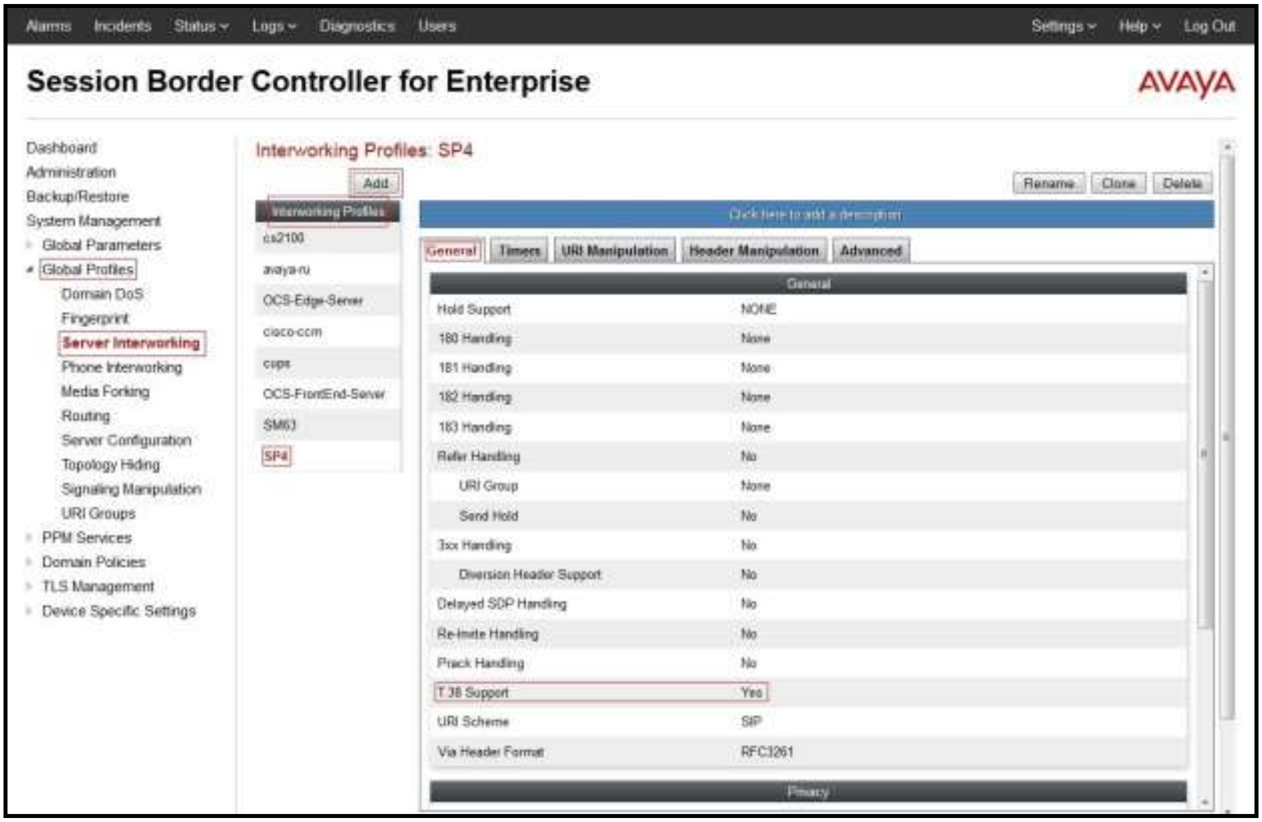
From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter **Profile Name**: **SP4** (not shown).
- Click **Next** button to leave all options at default. Click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **SP4** to edit.

- On the **General** tab, click on **Edit** button (not shown) and set **T.38 Support** to **Yes** (TDC Business Trunk supports T.38 Fax). Click **Next** button (not shown) to leave other options at default.
- Click **Finish** (not shown).

The following screen shows that TDC Business Trunk server interworking profile (named: **SP4**) was added.

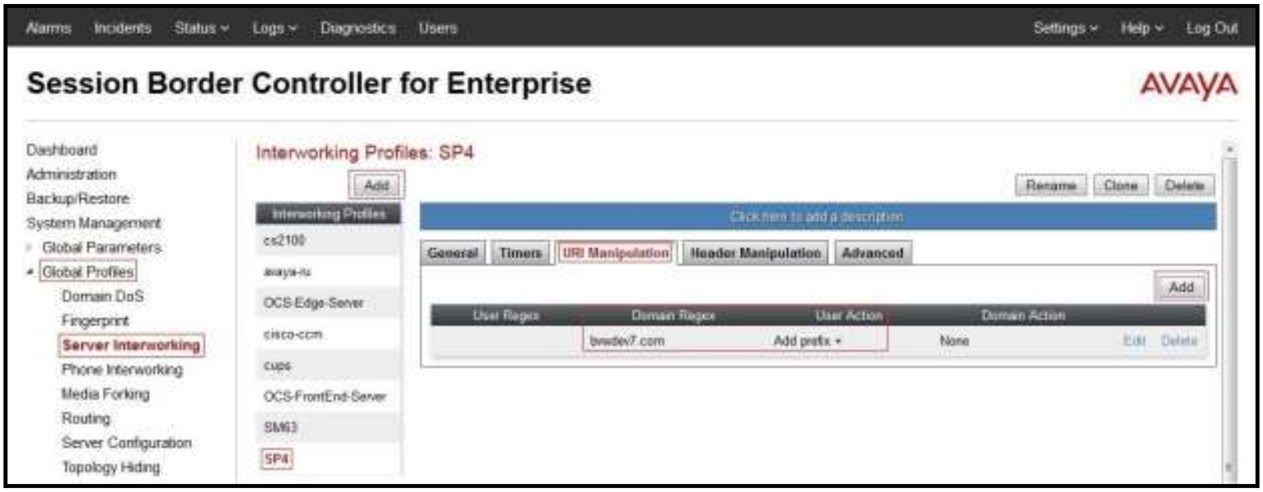


General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format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

Figure 75 - Server Interworking – TDC Business Trunk site

- On the **URI Manipulation** tab, click **Add** button to create the URI manipulation to add the prefix “**+**” sign in front of user number for any outbound calls. When a URI [user@domain] matches the following: **Domain Regex** as **bvwdev7.com**, do this with the user section: **User Action → Add prefix[Value]**, enter **User Values 1**: **+** (Not shown).

Note: TDC Business Trunk requires numbers to be given in E.164 with leading plus for all fields. This applies for Request-URI, To- and From- headers as well as the Diversion header.



User Regex	Domain Regex	User Action	Domain Action	
	bvwdev7.com	Add prefix +	None	Edit Delete

Figure 76 - Server Interworking – TDC Business Trunk site - URI Manipulation

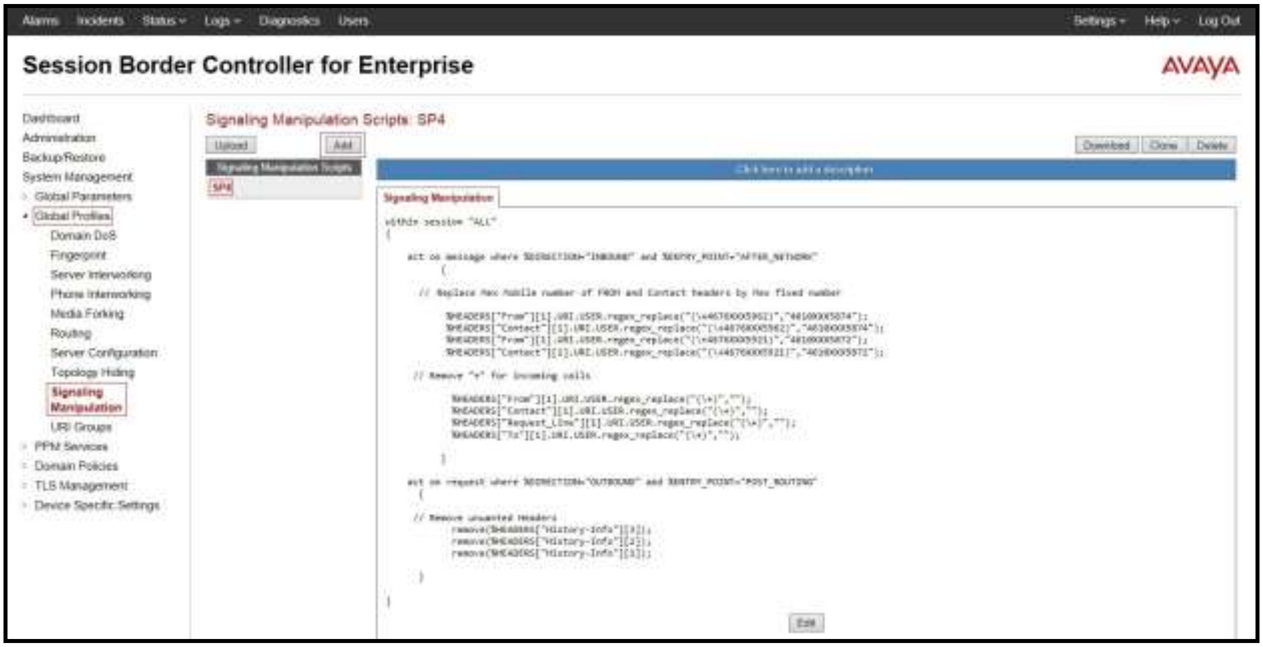
7.2.3. Configure Signaling Manipulation

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.

From the menu on the left-hand side, select **Global Profiles → Signaling Manipulation → Add**.

- Enter script **Title**: **SP4**. In the script editing window, enter the text exactly as shown in the screenshot below to perform the following:
  - Replace MEX enabled mobile number on From and Contact headers by MEX fixed number for incoming calls.
  - Remove “+” on SIP headers for incoming calls.
  - Remove unwanted SIP headers for outgoing calls.
  - Click **Save** (not shown).

Note: See **Appendix A** in **Section 12** for the reference of this sigma script.



```
within session "ALL"
{

    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
          {

      // Replace Hex mobile number of FROM and Contact headers by Hex fixed number

             %HEADERS["From"][1].URI.USER.regex_replace("(\+46768XXX5962)","46100XXX5874");
             %HEADERS["Contact"][1].URI.USER.regex_replace("(\+46768XXX5962)","46100XXX5874");
             %HEADERS["From"][1].URI.USER.regex_replace("(\+46768XXX5921)","46100XXX5872");
             %HEADERS["Contact"][1].URI.USER.regex_replace("(\+46768XXX5921)","46100XXX5872");

     // Remove "+" for incoming calls

              %HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
              %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
              %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\+)","");
              %HEADERS["To"][1].URI.USER.regex_replace("(\+)","");

          }

    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
      {

     // Remove unwanted Headers
              remove(%HEADERS["History-Info"][3]);
              remove(%HEADERS["History-Info"][2]);
              remove(%HEADERS["History-Info"][1]);

      }

}
```

Figure 77 - Signaling Manipulation

7.2.4. Configure Server – Avaya Session Manager

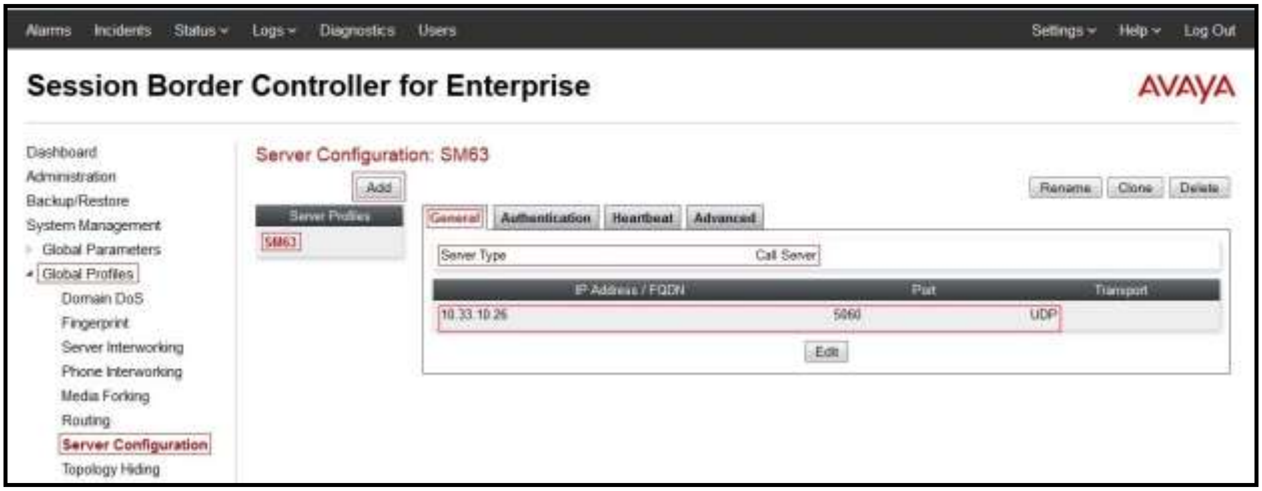
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and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

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**.

Enter **Profile Name**: **SM63**.

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

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



Server Configuration: SM63

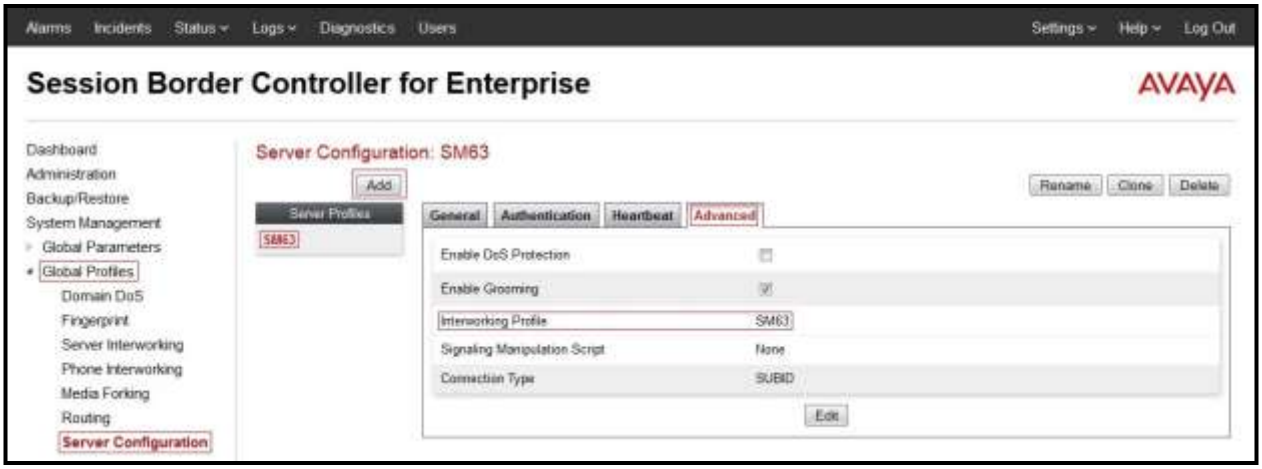
Server Type	Call Server

IP Address / FQDN	Port	Transport
10.33.10.26	5060	UDP

Figure 78 - Server Configuration – General - Avaya Session Manager

On the **Advanced** tab:

- Select **SM63** for **Interworking Profile** (see **Section 7.2.1**).
- Click **Finish** (not shown).



Server Configuration: SM63

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	SM63
Signaling Manipulation Script	None
Connection Type	SUBID

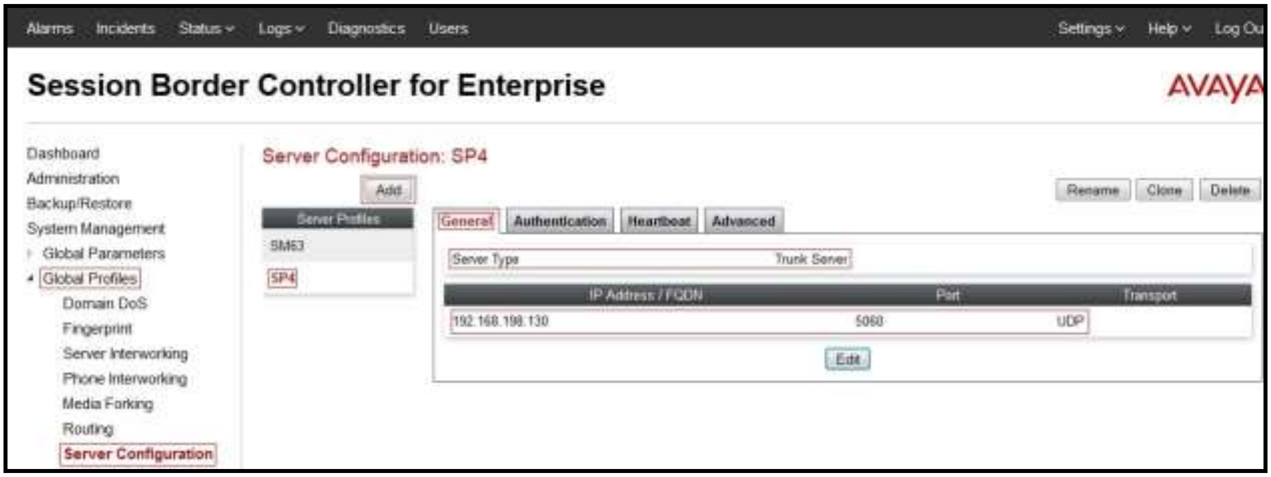
Figure 79 - Server Configuration – Advanced - Avaya site

7.2.5. Configure Server – TDC Business Trunk

From the menu on the left-hand side, select **Global Profiles → Server Configuration → Add**. Enter **Profile Name**: **SP4**.

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

- **Server Type**: Select **Trunk Server**.
- **IP Address/FQDN**: **192.168.198.130** (TDC Business Trunk Signaling Server IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).



Server Configuration: SP4

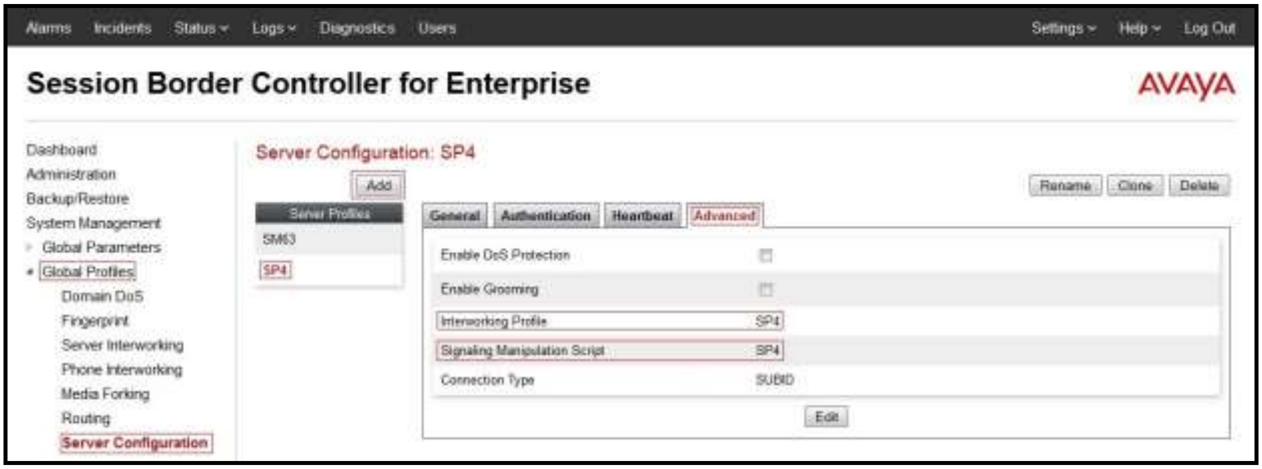
Server Type	Trunk Server

IP Address / FQDN	Port	Transport
192.168.198.130	5060	UDP

Figure 80 - Server Configuration – General - TDC site

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

- **Interworking Profile**: select **SP4** (see **Section 7.2.2**).
- **Signaling Manipulation Script**: select **SP4** (see **Section 7.2.3**)
- Click **Finish** (not shown).



Server Configuration: SP4

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	SP4
Signaling Manipulation Script	SP4
Connection Type	SUBID

Figure 81 - Server Configuration – Advanced - TDC site

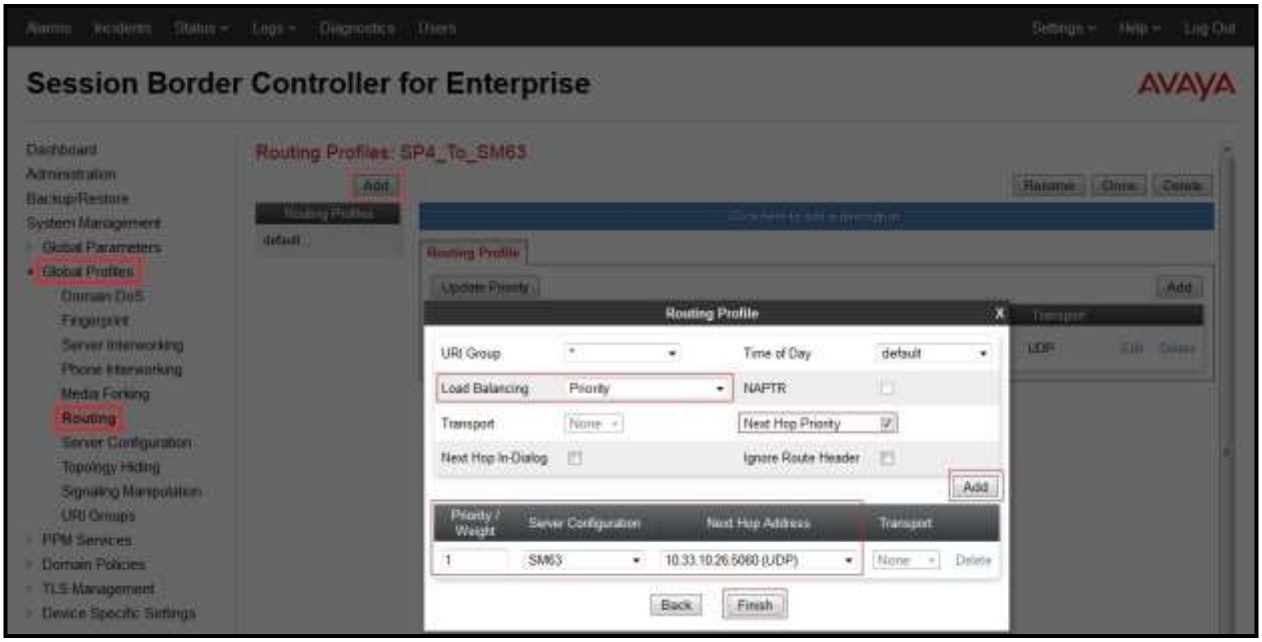
7.2.6. Configure Routing – Avaya Session Manager

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** (not shown).

- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **SM63** (see **Section 7.2.4**). This selection will automatically populate the **Next Hop Address** field.
- Click **Finish**.



Routing Profiles: SP4_To_SM63

Routing Profile

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

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	SM63	10.33.10.26:5060 (UDP)	None	Delete

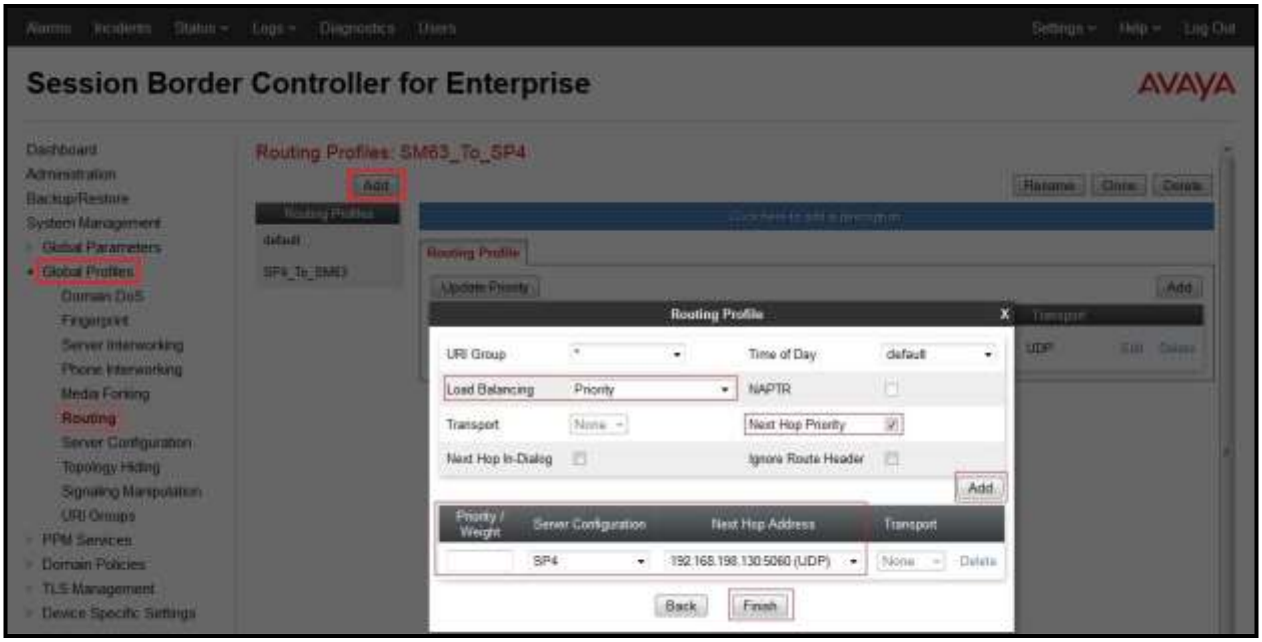
Figure 82 - Routing to Session Manager

7.2.7. Configure Routing – TDC Business Trunk

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

Enter **Profile Name**: **SM63_To_SP4** (not shown).

- **Load Balancing**: **Priority**.
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address.
- **Priority/Weight**: **1**.
- **Server Configuration**: **SP4** (see **Section 7.2.5**). This selection will automatically populate the **Next Hop Address** field.
- Click **Finish**.



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

Priority / Weight	Server Configuration	Next Hop Address	Transport
	SP4	192.168.198.130:5060 (UDP)	None

Figure 83 - Routing to TDC Business Trunk

7.2.8. Configure Topology Hiding – Avaya Session Manager

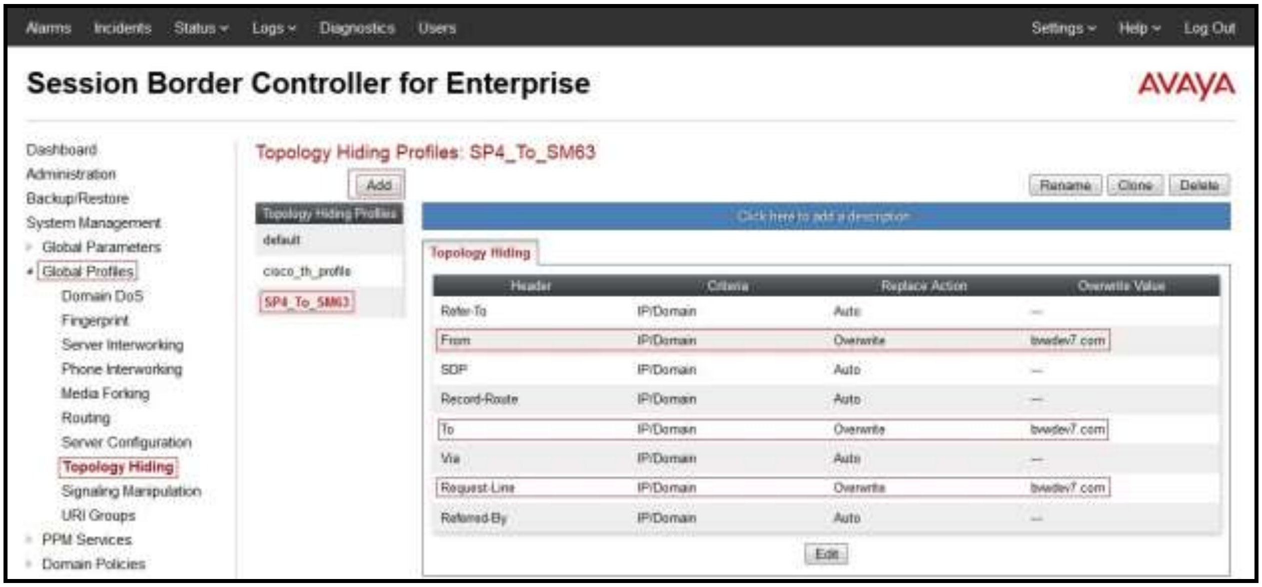
The **Topology Hiding** screen allows administrator to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

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

Select **Add** button to enter **Profile Name**: **SP4_To_SM63**.

- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
    In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **bvwdev7.com**

Click **Finish** (not shown).



Topology Hiding Profiles: SP4_To_SM63

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Overwrite	bvwdev7.com
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	bvwdev7.com
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bvwdev7.com
Referred-By	IP/Domain	Auto	---

Figure 84 - Topology Hiding Session Manager

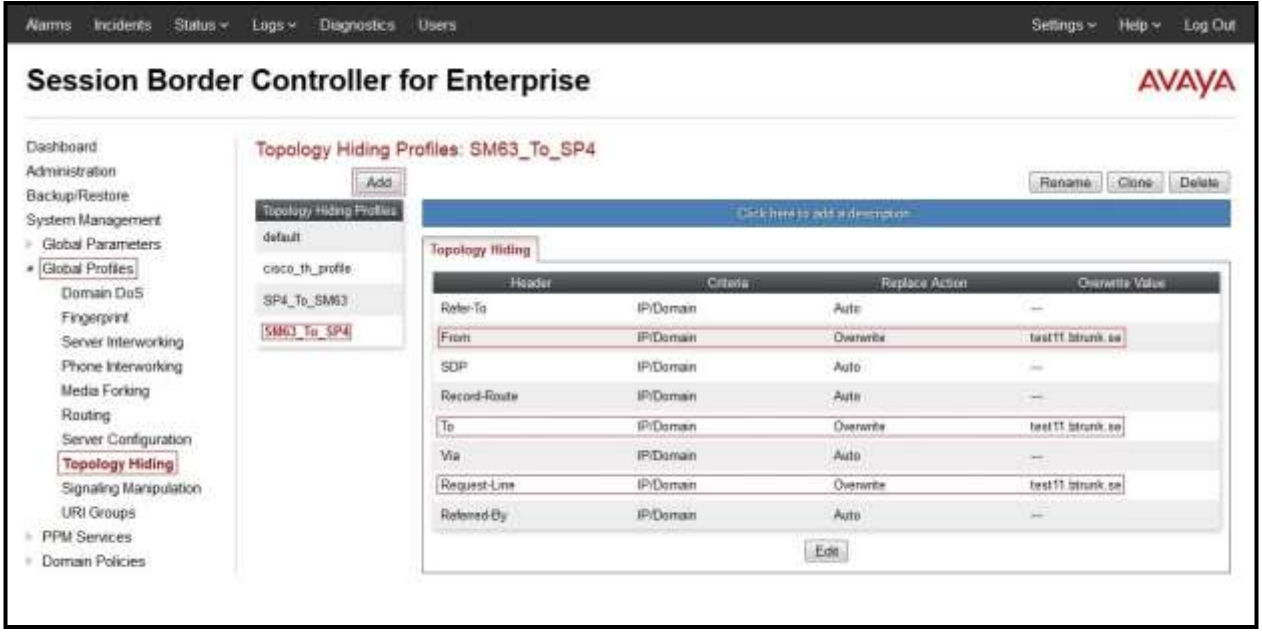
7.2.9. Configure Topology Hiding – TDC Business Trunk

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

Select **Add** button to enter **Profile Name**: **SM63_To_SP4**.

- For the Header **From,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **test11.btrunk.se**
- For the Header **To,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **test11.btrunk.se**
- For the Header **Request-Line,**
  - In the **Criteria** column select **IP/Domain**
  - In the **Replace Action** column select: **Overwrite**
  - In the **Overwrite Value** column: **test11.btrunk.se**

Click **Finish** (not shown).



Topology Hiding Profiles: SM63_To_SP4

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Auto	—
From	IP/Domain	Overwrite	test11.btrunk.se
SDP	IP/Domain	Auto	—
Record-Route	IP/Domain	Auto	—
To	IP/Domain	Overwrite	test11.btrunk.se
Via	IP/Domain	Auto	—
Request-Line	IP/Domain	Overwrite	test11.btrunk.se
Referred-By	IP/Domain	Auto	—

Figure 85 - Topology Hiding TDC Business Trunk

7.3. Domain Policies

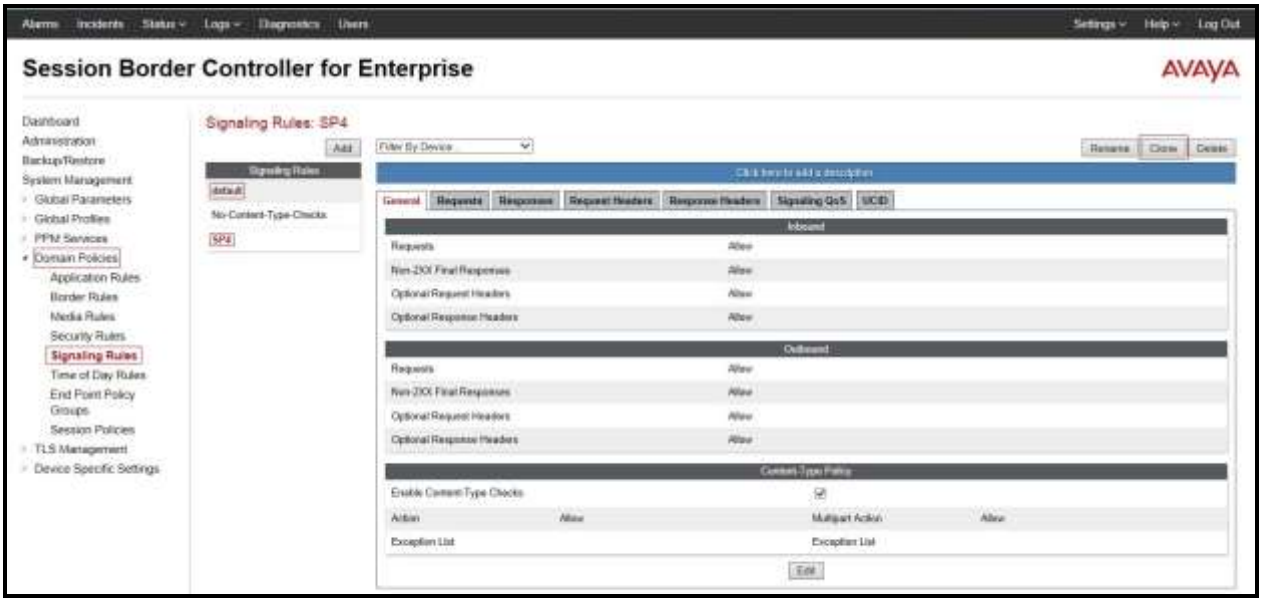
The Domain Policies feature allows one to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which 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).



Signaling Rules: SP4

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

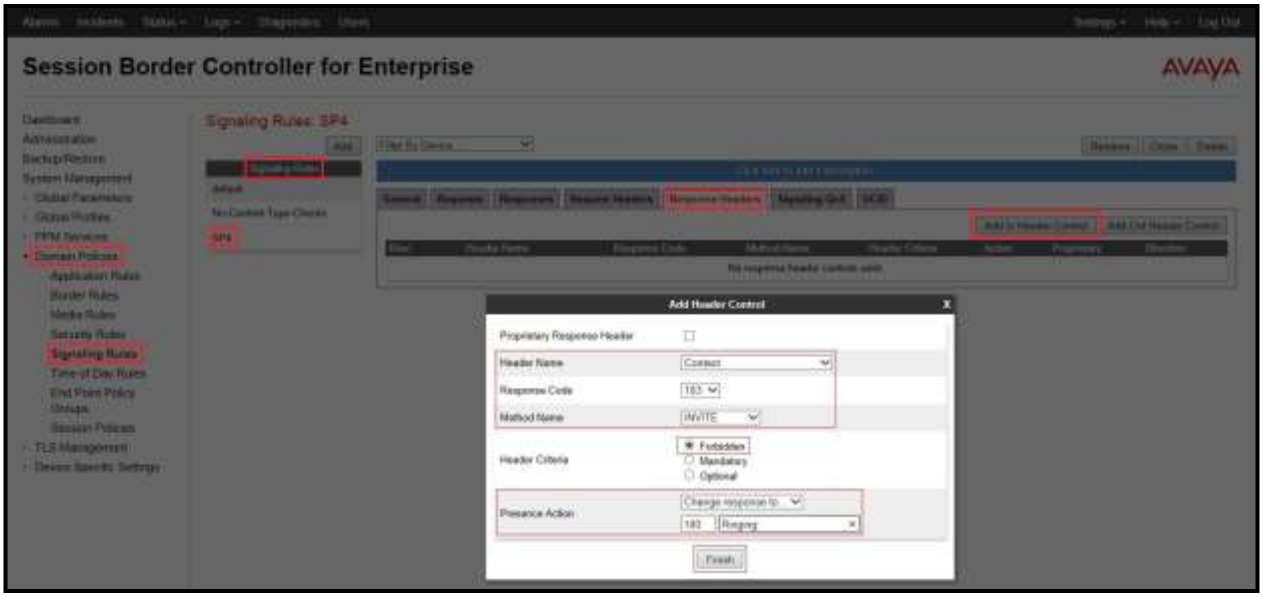
Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Figure 86 - Signaling Rule SP4

The following configuration on the SP4 Signaling Rule converts 183 with SDP to 180 without SDP.

From the list of **Signaling Rules**, click on **SP4**.

- On 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**.
- Click **Finish**.



Proprietary Response Header □

Header Name: Contact

Response Code: 183

Method Name: INVITE

Header Criteria: ● Forbidden ○ Mandatory ○ Optional

Presence Action: Change response to 180 Ringing

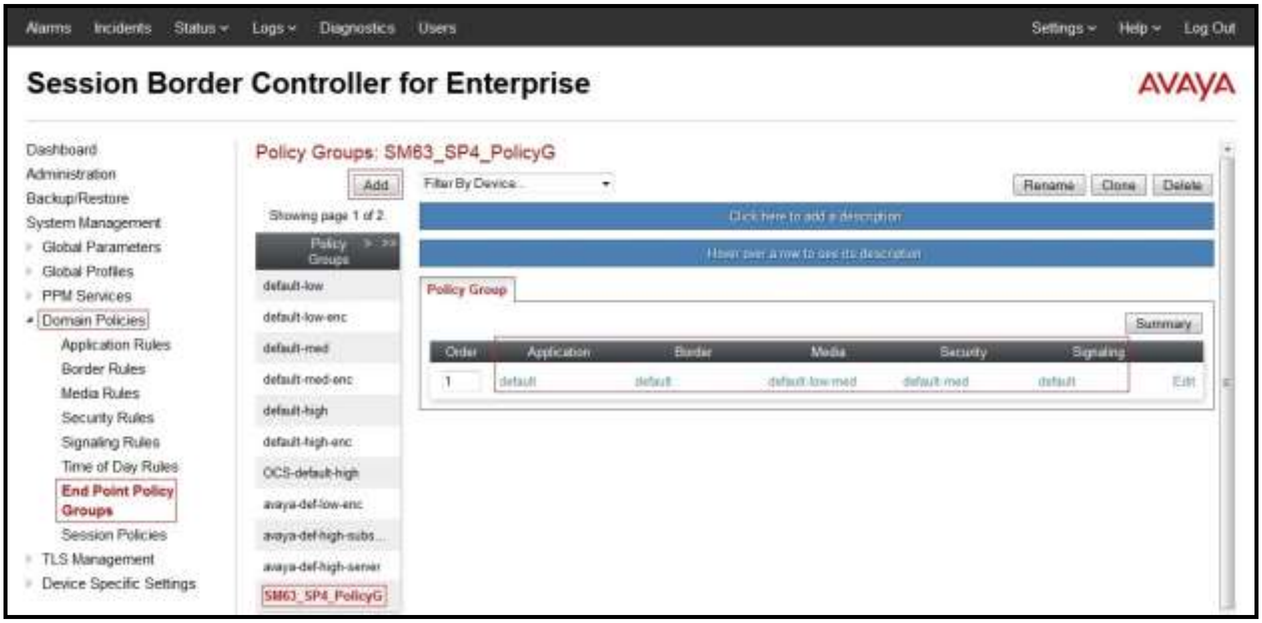
Figure 87 - Signaling Rule SP4 – Header Control

7.3.2. Create Endpoint 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 Avaya 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).



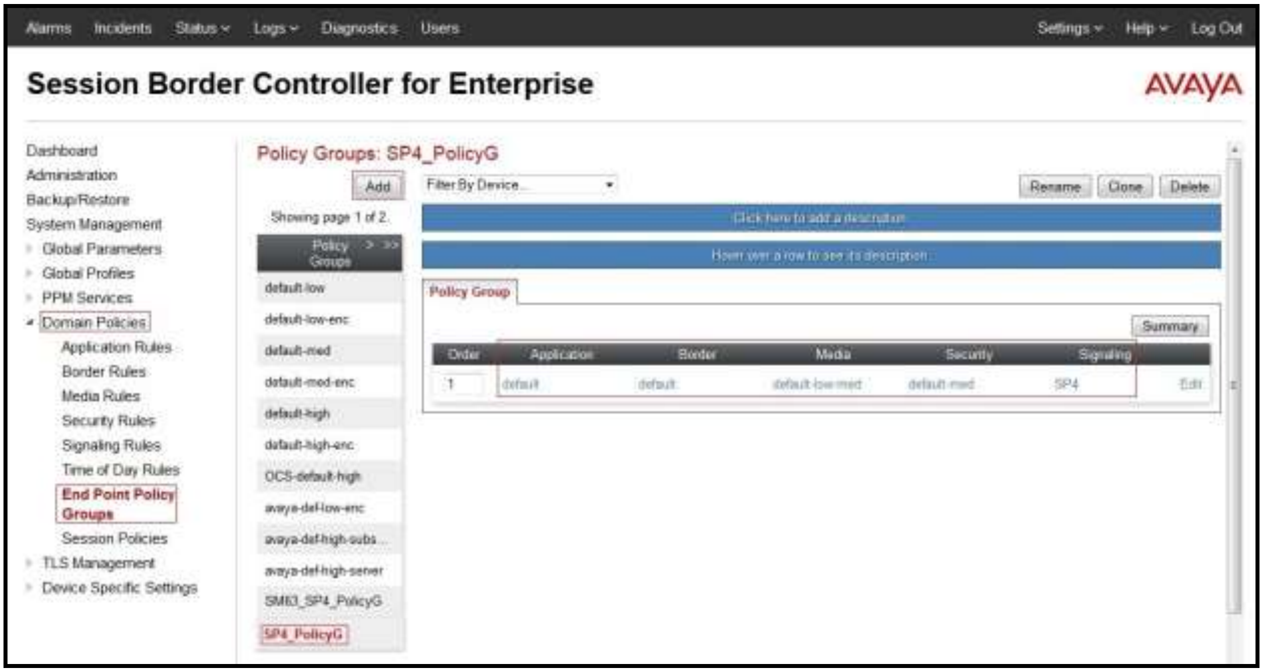
Policy Groups: SM63_SP4_PolicyG

Order	Application	Border	Media	Security	Signaling
1	default	default	default-low-med	default-med	default

Figure 88 - Endpoint Policy – Avaya site

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).



Policy Groups: SP4_PolicyG

Order	Application	Border	Media	Security	Signaling
1	default	default	default-low-med	default-med	SP4

Figure 89 - Endpoint Policy – TDC Business Trunk site

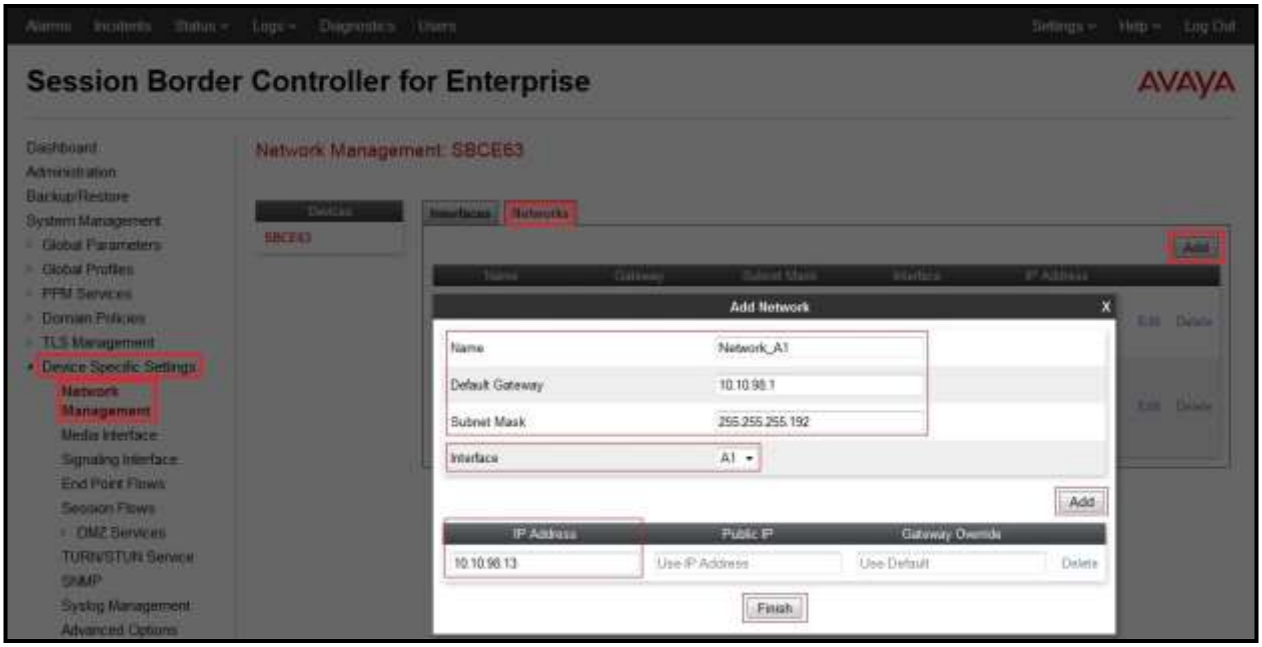
7.4. Device Specific Settings

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**.

- Select **Networks** tab and click **Add** button to add a network of inside interface as follows:
  - **Name**: **Network_A1**.
  - **Default Gateway**: **10.10.98.1**.
  - **Subnet Mask**: **255.255.255.192**.
  - **Interface**: **A1** (This is Avaya SBCE's inside interface).
  - Click **Add** button to add **IP Address** for inside interface: **10.10.98.13**.
  - Click **Finish** button to save the changes.



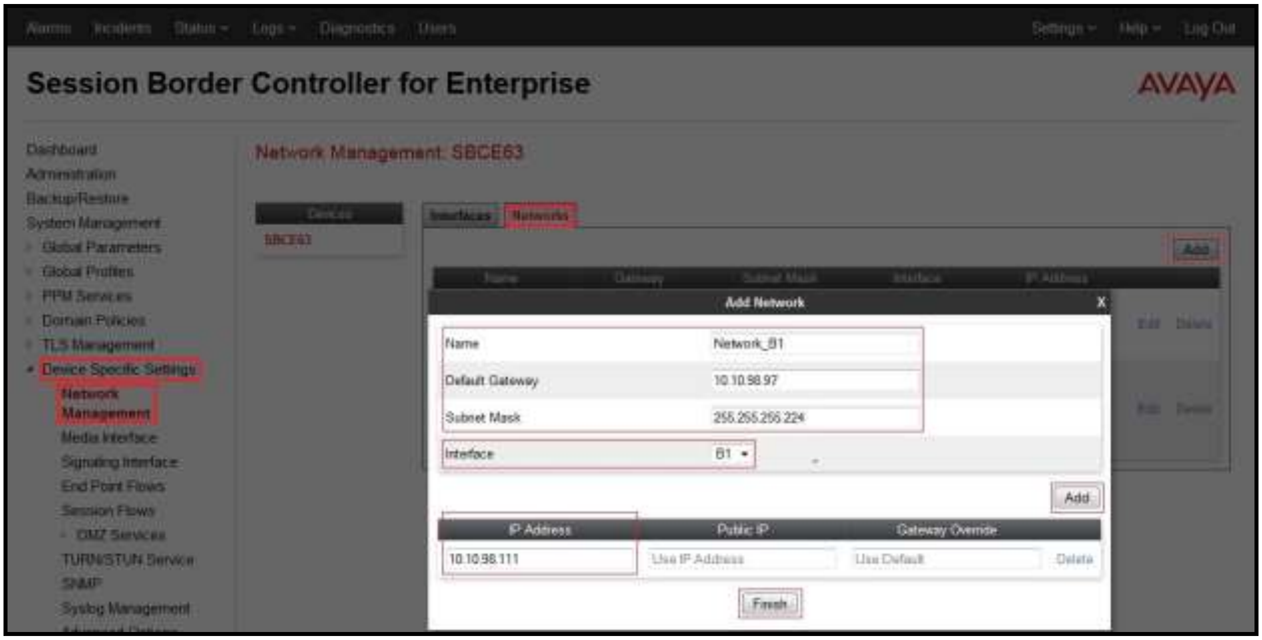
Name	Network_A1
Default Gateway	10.10.98.1
Subnet Mask	255.255.255.192
Interface	A1

IP Address	Public IP	Gateway Override	
10.10.98.13	Use IP Address	Use Default	Delete

Figure 90 - Network Management – Inside Interface

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

- Select **Networks** tab and click **Add** button to add a network of outside interface as followings:
  - **Name**: **Network_B1**.
  - **Default Gateway**: **10.10.98.97**.
  - **Subnet Mask**: **255.255.255.224**.
  - **Interface**: **B1** (This is Avaya SBCE outside interface).
  - Click **Add** button to add **IP Address** for outside interface: **10.10.98.111**.
  - Click **Finish** button to save the changes.



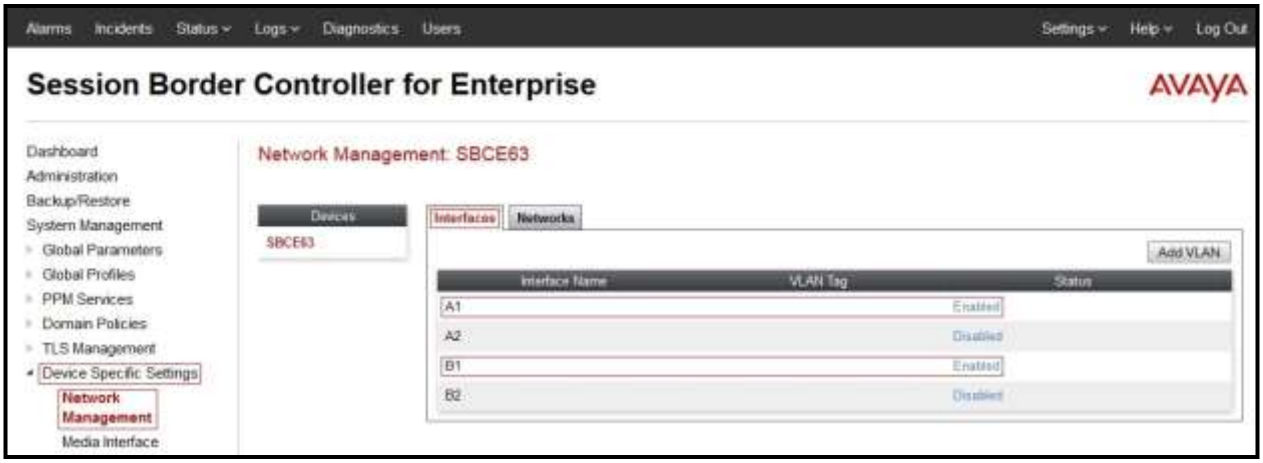
Name	Network_B1
Default Gateway	10.10.98.97
Subnet Mask	255.255.255.224
Interface	B1

IP Address	Public IP	Gateway Override
10.10.98.111	Use IP Address	Use Default

Figure 91 - Network Management – Outside Interface

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

- Select **Interfaces** tab.
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state.



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

Figure 92 - Network Management – Interface Status

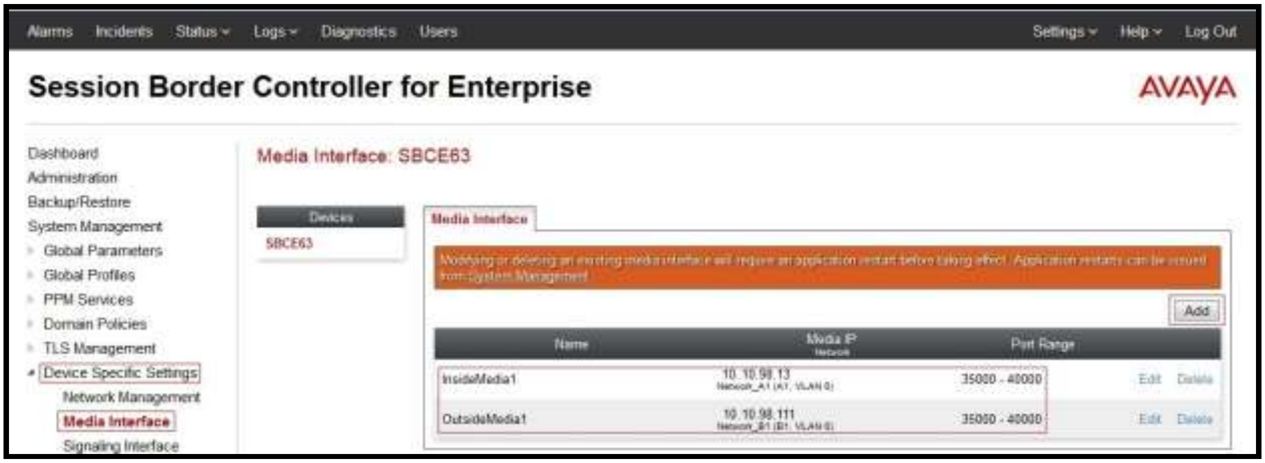
7.4.2. Create Media Interfaces

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, **Device Specific Settings** → **Media Interface**.

- Select **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideMedia1**.
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Session Manager).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).
- Select **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideMedia1**.
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward TDC Business SIP Trunk).
  - **Port Range**: **35000 – 40000**.
  - Click **Finish** (not shown).

The screen below shows the configured media interfaces:



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 Network	Port Range		
InsideMedia1	10.10.98.13 Network_A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
OutsideMedia1	10.10.98.111 Network_B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

Figure 93 - 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**.

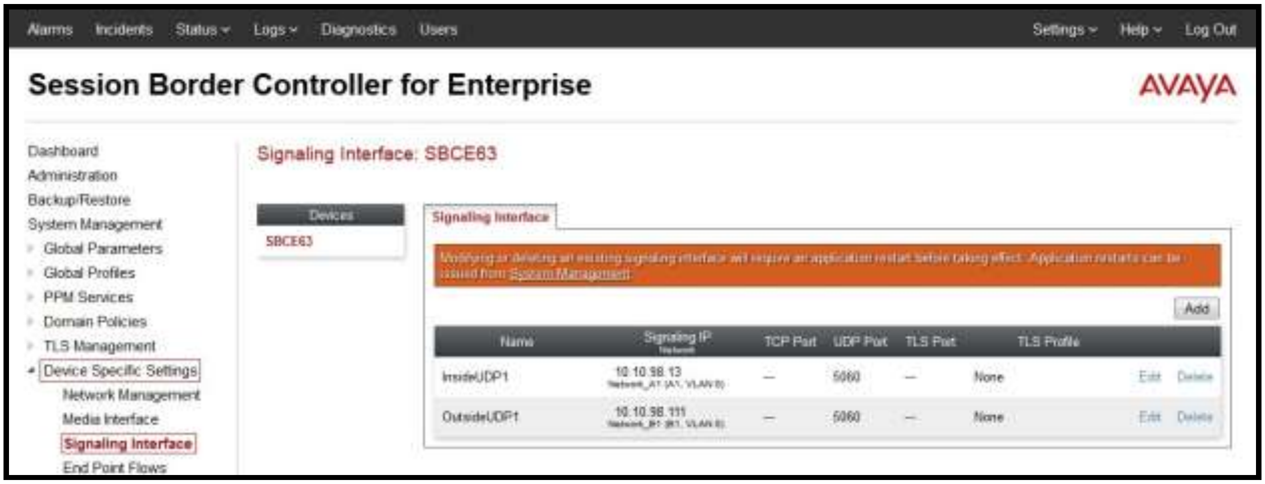
- Select **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **InsideUDP1**.
  - **IP Address**: Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Session Manager).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

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

- Select **Add** button and enter the following in the configuration window (not shown):
  - **Name**: **OutsideUDP1**.
  - **IP Address**: Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward TDC Business SIP trunk).
  - **UDP Port**: **5060**.
  - Click **Finish** (not shown).

Note: For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 as same by TDC Business Trunk.

The screen below shows the configured singnaling interfaces:



Signaling Interface: SBCE63

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

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
InsideUDP1	10.10.98.13 Network_A1 (A1, VLAN 0)	—	5060	—	None	Edit	Delete
OutsideUDP1	10.10.98.111 Network_B1 (B1, VLAN 0)	—	5060	—	None	Edit	Delete

Figure 94 - Signaling Interface

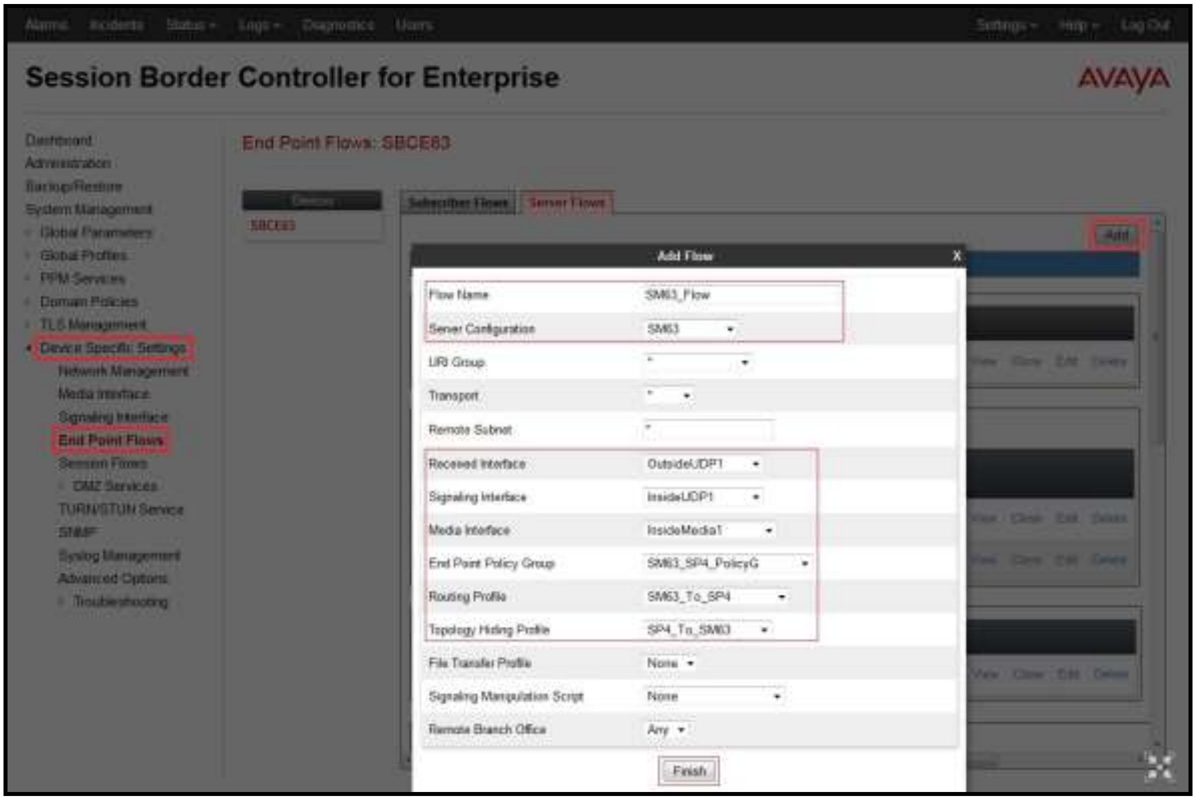
7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize signaling and apply various policies.

7.4.4.1 Create End Point Flows – Avaya Session Manager

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**: **SM63_Flow**.
  - **Server Configuration**: **SM63** (see **Section 7.2.4**).
  - **URI Group**: *****.
  - **Transport: ***.
  - **Remote Subnet: ***.
  - **Received Interface**: **OutsideUDP1** (see **Section 7.4.3**).
  - **Signaling Interface**: **InsideUDP1** (see **Section 7.4.3**).
  - **Media Interface**: **InsideMedia1** (see **Section 7.4.2**).
  - **End Point Policy Group**: **SM63_SP4_PolicyG** (see **Section 7.3.2**).
  - **Routing Profile**: **SM63_To_SP4** (see **Section 7.2.7**).
  - **Topology Hiding Profile**: **SP4_To_SM63** (see **Section 7.2.8**).
  - Click **Finish**.



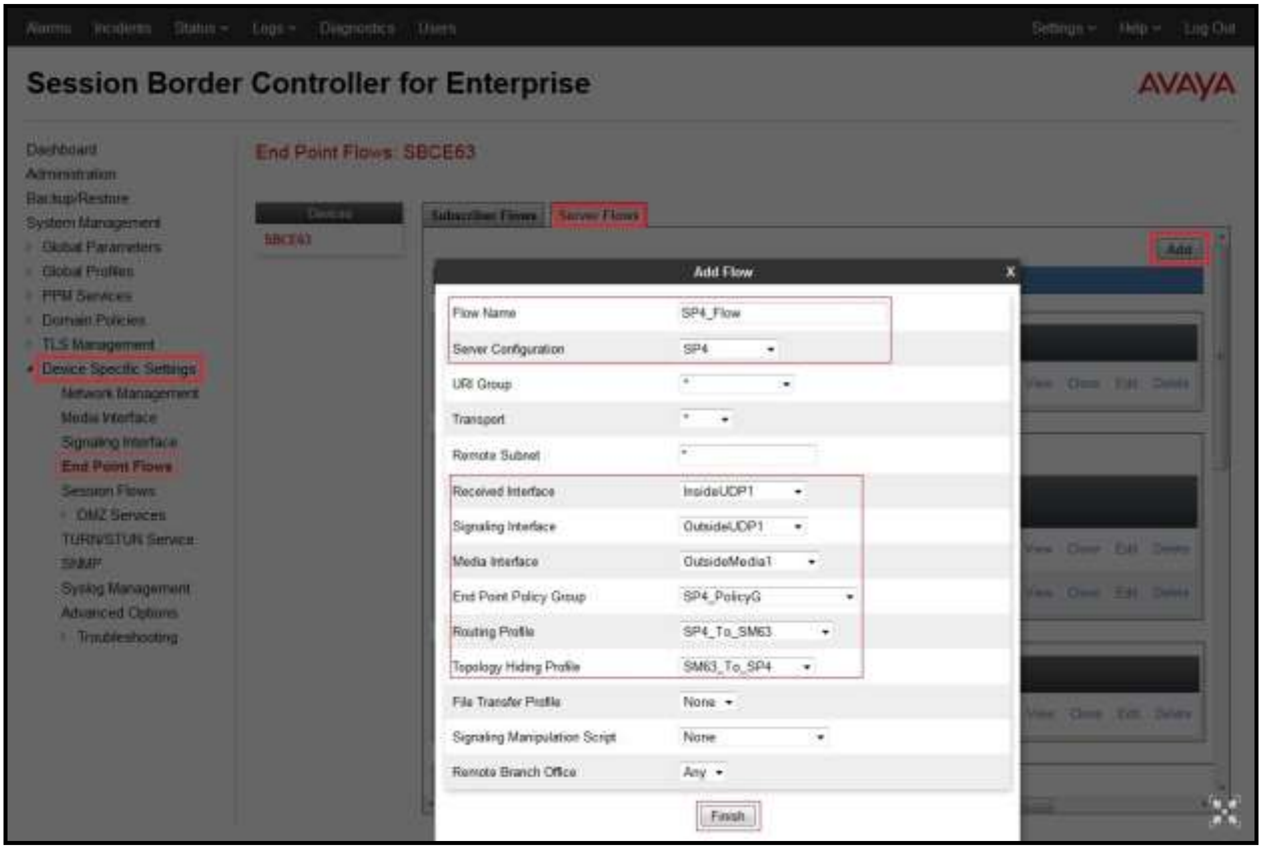
Flow Name	SM63_Flow
Server Configuration	SM63
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideUDP1
Signaling Interface	InsideUDP1
Media Interface	InsideMedia1
End Point Policy Group	SM63_SP4_PolicyG
Routing Profile	SM63_To_SP4
Topology Hiding Profile	SP4_To_SM63
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 95 - End Point Flow to TDC Business Trunk

7.4.4.2 Create End Point Flows – TDC Business Trunk

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_Flow**.
  - **Server Configuration**: **SP4** (see **Section 7.2.5**).
  - **URI Group**: *****.
  - **Transport: ***.
  - **Remote Subnet: ***.
  - **Received Interface**: **InsideUDP1** (see **Section 7.4.3**).
  - **Signaling Interface**: **OutsideUDP1** (see **Section 7.4.3**).
  - **Media Interface**: **OutsideMedia1** (see **Section 7.4.2**).
  - **End Point Policy Group**: **SP4_PolicyG** (see **Section 7.3.2**).
  - **Routing Profile**: **SP4_To_SM63** (see **Section 7.2.6**).
  - **Topology Hiding Profile**: **SM63_To_SP4** (see **Section 7.2.9**).
  - Click **Finish**.



Flow Name	SP4_Flow
Server Configuration	SP4
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideUDP1
Signaling Interface	OutsideUDP1
Media Interface	OutsideMedia1
End Point Policy Group	SP4_PolicyG
Routing Profile	SP4_To_SM63
Topology Hiding Profile	SM63_To_SP4
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 96 - End Point Flow from TDC Business Trunk

8. TDC Business Trunk Service Configuration

TDC Business Trunk is responsible for the network configuration of the TDC Business Trunk service. TDC Business Trunk will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. TDC Business Trunk will provide the IP address of the TDC Business Trunk SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. TDC Business Trunk also provides the TDC SIP Specification document for reference. This information is used to complete configurations for Avaya Communication Server 1000, , Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between TDC Business Trunk and the enterprise is a static IP configuration.

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 (ld 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 (5871). The call scenario involved PSTN phone number 1303XXX9042 calling 4610XXX5871 (which is translated to extension 5871).

- 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 **ld 80** and then **trace 0 5871**.
- After the call is released, issue command **trac 0 5871** 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 **5871** is in call state:

```
>ld 80
TRA000
.trace 0 5871

TRA100

.trac 0 5871

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: 35590
  FAR-END VendorID: AVAYA-SM-6.3.13.0.631304
TERM   VTN 096 0 00 02  KEY 0  SCR MARP  CUST 0  DN 5871  TYPE 2002P2
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 10.33.5.9  PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW  PAYLOAD 20 ms  VAD OFF
RFC2833:  RXPT  101   TXPT  101   DIAL DN 5871
MAIN_PM  ESTD
TALKSLOT  ORIG  18   TERM  23
EES_DATA:
NONE
QUEU  NONE
CALL ID 501 16
```

```
----  ISDN ISL CALL (ORIG) ----
CALL REF # =  385
BEARER CAP =  VOICE
HLC =
CALL STATE =  10     ACTIVE
CALLING NO =  1303XXX9042  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
CALLED NO  =  4610XXX5871  NUM_PLAN:UNKNOWN     TON:UNKNOWN   ESN:UNKNOWN
```

And this is the example after the call to 5871 is finished.

```
>ld 80
TRA000
.trac 0 5871
IDLE VTN 96 0 00 02   MARP
```

SIP Trunk monitoring (ld 32)

Place a call inbound from PSTN (1303XXX9042) to an internal Avaya phone (4610XXX5871). Then check the SIP trunk status by using ld 32, and verify one trunk is BUSY.

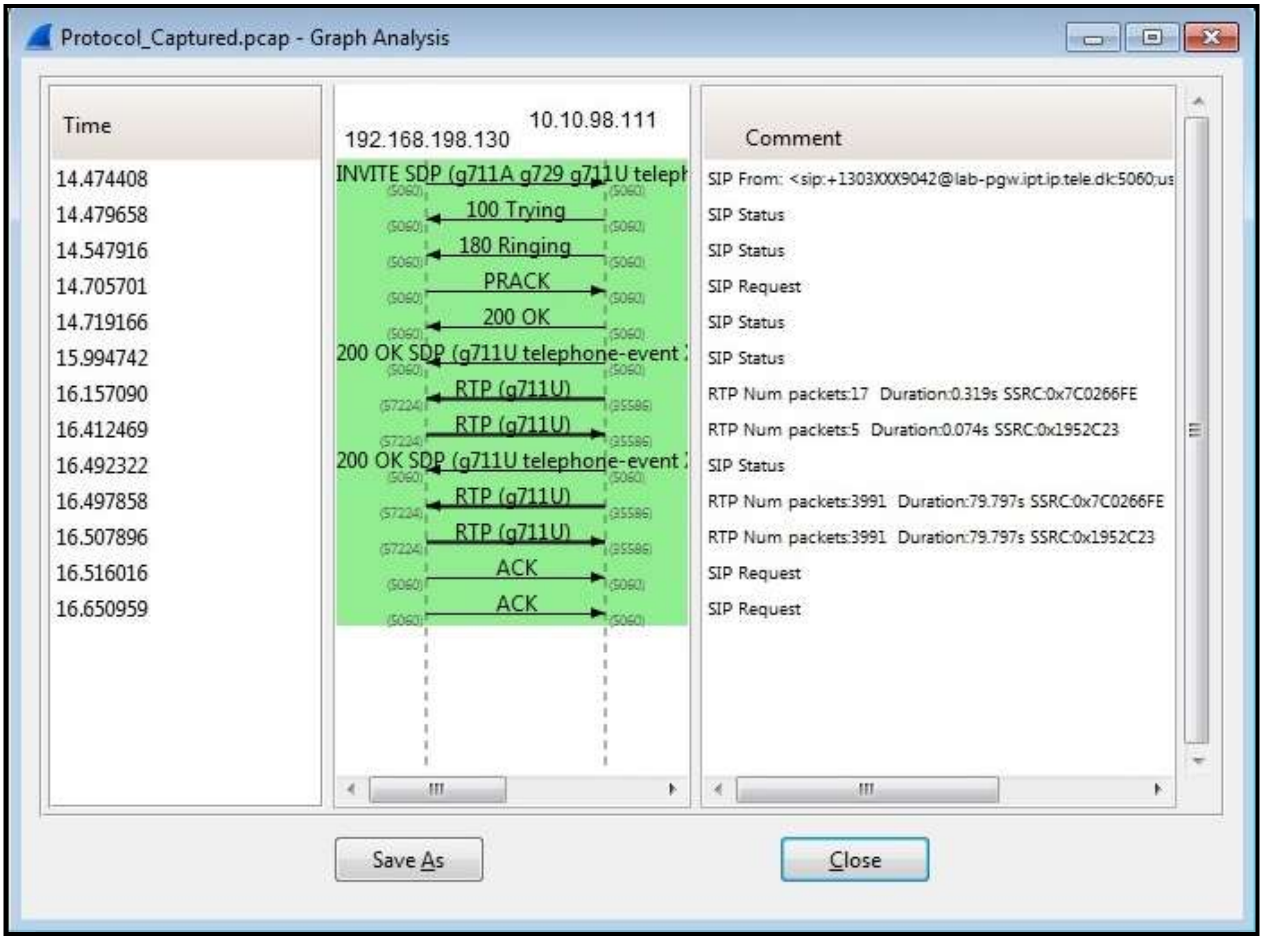
```
>ld 32
NPR000
.stat 100 0
091 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

After the call is released, check that SIP trunk status should change 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**.



Time	192.168.198.130		10.10.98.111	Comment
14.474408	(5060)	INVITE SDP (g711A g729 g711U teleph →	(5060)	SIP From: <sip:+1303XXX9042@lab-pgw.ipt.ip.tele.dk:5060;us
14.479658	(5060)	← 100 Trying	(5060)	SIP Status
14.547916	(5060)	← 180 Ringing	(5060)	SIP Status
14.705701	(5060)	PRACK →	(5060)	SIP Request
14.719166	(5060)	← 200 OK	(5060)	SIP Status
15.994742	(5060)	← 200 OK SDP (g711U telephone-event	(5060)	SIP Status
16.157090	(57224)	← RTP (g711U)	(35586)	RTP Num packets:17 Duration:0.319s SSRC:0x7C0266FE
16.412469	(57224)	RTP (g711U) →	(35586)	RTP Num packets:5 Duration:0.074s SSRC:0x1952C23
16.492322	(5060)	← 200 OK SDP (g711U telephone-event	(5060)	SIP Status
16.497858	(57224)	← RTP (g711U)	(35586)	RTP Num packets:3991 Duration:79.797s SSRC:0x7C0266FE
16.507896	(57224)	RTP (g711U) →	(35586)	RTP Num packets:3991 Duration:79.797s SSRC:0x1952C23
16.516016	(5060)	ACK →	(5060)	SIP Request
16.650959	(5060)	ACK →	(5060)	SIP Request

Figure 97 – SIP Call Trace

10. Conclusion

All of the test cases have been executed. Observations/limitations seen during the test was noted in **Section 2.2**. The test met the objectives outlined in **Section 2.1**. The TDC Business 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 6.3.

11. References

This section references 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

- *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013
- *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013
- *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013
- *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013
- *Dialing Plans Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.
- *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

- *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 7, Sep 2014
- *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3, Issue 7, Mar 2015
- *Administering Avaya Aura® System Manager for Release 6.3.13* , Release 6.3, Issue 8, Jul 2015

Avaya Session Border Controller for Enterprise

- *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014

12. Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE in **Section 7.2.3**:

```
within session "ALL"
{
        act on message where %DIRECTION="INBOUND" and
        %ENTRY_POINT="AFTER_NETWORK"
    {

     // Replace Mex Mobile number of FROM and Contact headers by Mex fixed number

        %HEADERS["From"][1].URI.USER.regex_replace("(\+4676XXX5962)","4610XX
        X5874");

        %HEADERS["Contact"][1].URI.USER.regex_replace("(\+4676XXX5962)","4610
        XXX5874");

        %HEADERS["From"][1].URI.USER.regex_replace("(\+4676XXX5921)","4610XX
        X5872");

        %HEADERS["Contact"][1].URI.USER.regex_replace("(\+4676XXX5921)","4610
        XXX5872");

    // Remove "+" for incoming calls

        %HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
        %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
        %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\+)","");
        %HEADERS["To"][1].URI.USER.regex_replace("(\+)","");

       }

        act on request where %DIRECTION="OUTBOUND" and
        %ENTRY_POINT="POST_ROUTING"
       {

    // Remove unwanted Headers
        remove(%HEADERS["History-Info"][3]);
        remove(%HEADERS["History-Info"][2]);
        remove(%HEADERS["History-Info"][1]);
    }

}
```

13. Appendix B: MEX Testing

In this compliance test, the below test extensions can only be used in Sweden to be able to trigger IN services.

MEX 1 fixed number = +46104925874 (MEX1 enabled mobile= +46767225962) extension 5874.
MEX 2 fixed number = +46104925872 (MEX2 enabled mobile= +46767225921) extension 5872.

R1 number: +222 and Prefix: +46394980.

13.1. Inbound Call To MEX Fixed Number

This section explains inbound Calls to a MEX fixed number, which is routed to the enterprise: its corresponding MEX enabled mobile number.
After receiving the SIP Invite from TDC, the PBX should send a SIP re-Invite against the SIP trunk with the To-header user part containing a concatenation of PREFIX +46394980 and the MEX enabled mobile number in international format. The From-header user part is the original calling number generated by the PBX (the number to display on the MEX enabled mobile).

Example 1:
Assuming a call from +46767892721 to the MEX1 fixed number (+46104925874) associated with MEX1 enabled mobile +46767225962.

Firstly, TDC sent SIP Invite message to Avaya with the To and From headers :
To: <sip:+2220104925874@test11.btrunk.se>
From: <sip:+46767892721@test11.btrunk.se>

Then, Avaya PBX sent SIP re-Invite to TDC with the To and From headers:
To: <sip:+4639498046767225962@test11.btrunk.se>
From: <sip:+46104925872@test11.btrunk.se>

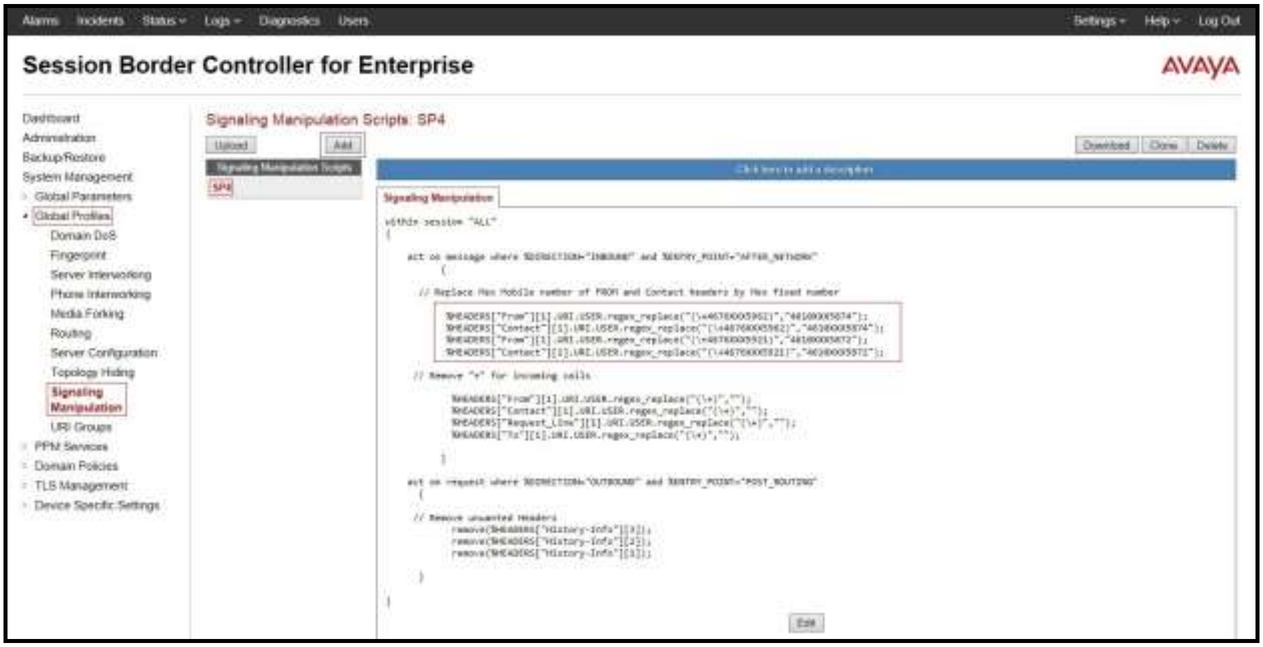
Example 2:
Assuming a call from MEX1 enabled mobile +46767225962 to a MEX2 fixed extension number (5872) associated with MEX2 enabled mobile +46767225921.

Firstly, TDC sent SIP Invite message to Avaya with the To- and From-headers might look like:
To: <sip:+2225872@test11.btrunk.se>
From: <sip:+46767225962@test11.btrunk.se>

Then, Avaya PBX sent SIP re-Invite to TDC with the To- and From-headers might look like:
To: <sip:+4639498046767225921@test11.btrunk.se>
From: <sip:+46104925874@test11.btrunk.se>

13.1.1. Configure Signaling Manipulation on Avaya SBCE

The information below is defined in **Section 7.2.3**. This script implements the manipulation to replace MEX enabled mobile number on From and Contact headers by MEX fixed number for incoming calls.

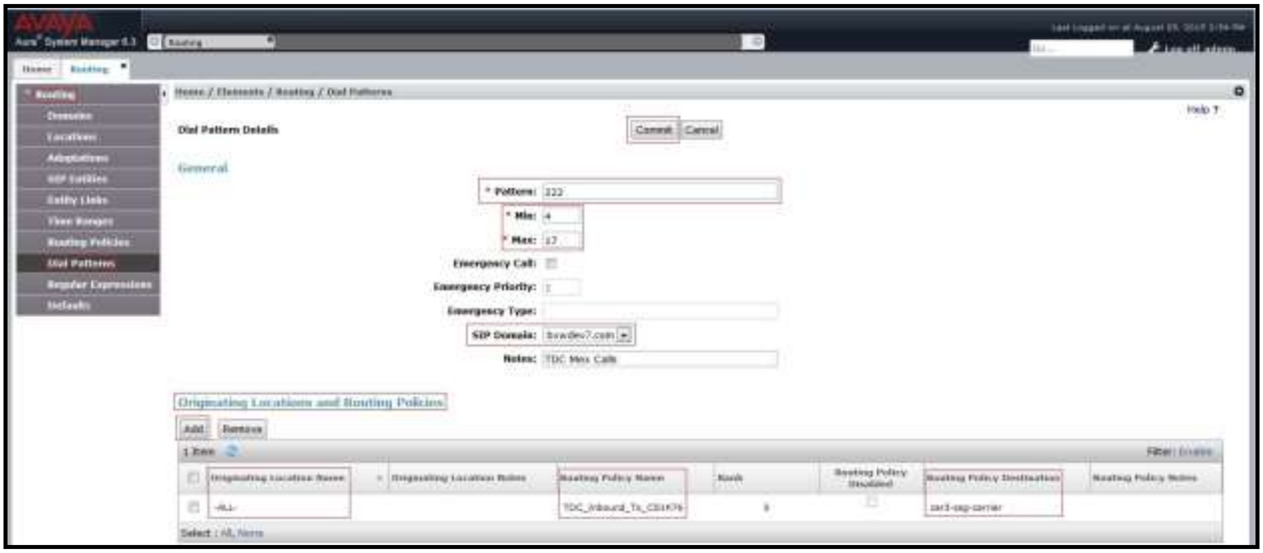


```
within session "ALL"
{

   act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
         {

    // Replace Mex Mobile number of FROM and Contact headers by Mex fixed number

        %HEADERS["From"][1].URI.USER.regex_replace("(\+46760005961)","46100005874");
        %HEADERS["Contact"][1].URI.USER.regex_replace("(\+46760005962)","46100005874");
        %HEADERS["From"][1].URI.USER.regex_replace("(\+46760005921)","46100005872");
        %HEADERS["Contact"][1].URI.USER.regex_replace("(\+46760005821)","46100005972");

   // Remove "+" for incoming calls

          %HEADERS["From"][1].URI.USER.regex_replace("(\+)","");
          %HEADERS["Contact"][1].URI.USER.regex_replace("(\+)","");
          %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\+)","");
          %HEADERS["To"][1].URI.USER.regex_replace("(\+)","");

         }

   act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
     {

   // Remove unwanted Headers
          remove(%HEADERS["History-Info"][3]);
          remove(%HEADERS["History-Info"][2]);
          remove(%HEADERS["History-Info"][1]);

     }

}
```

Figure 98 - Signaling Manipulation for Mex Testing

13.1.2. Configure Session Manager – Dial Pattern

There are four examples of dial patterns defined in this configuration: dial patterns for incoming calls: 222, 2225872, 2225874, and dial pattern for outgoing call: 46394980.



Dial Pattern Details

General

* Pattern: 222

* Min: 4

* Max: 17

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: TDC Max Calls

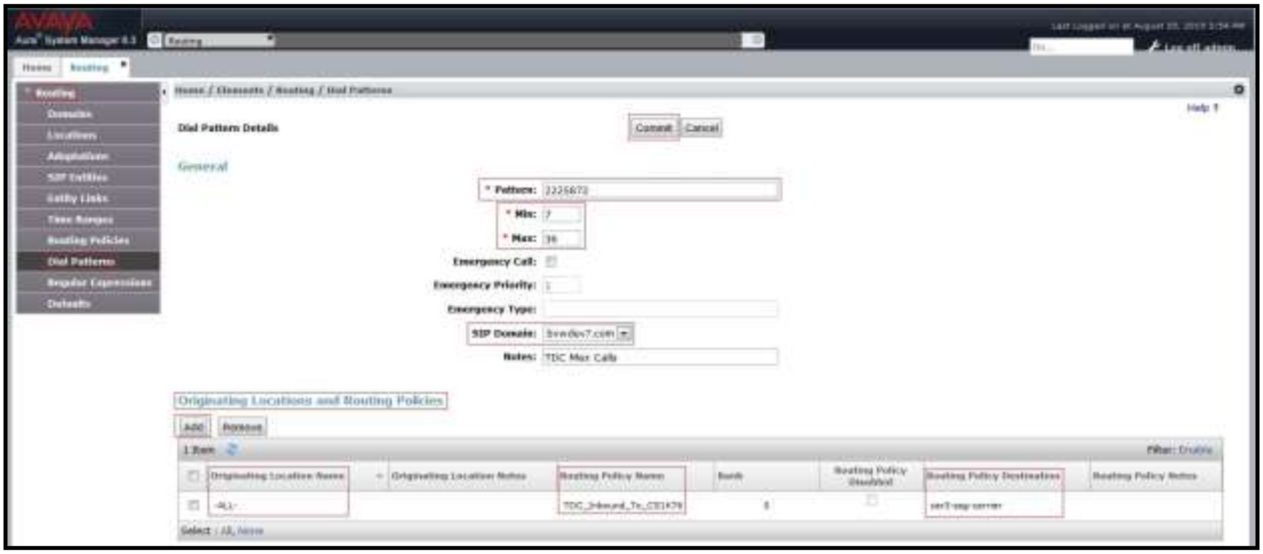
Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Inbound_To_CS1K76	0	□	sar3-sip-carrier	

Select : All, None

Figure 99 - Dial Pattern 222



Dial Pattern Details

General

* Pattern: 2225872

* Min: 7

* Max: 36

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: TDC Max Calls

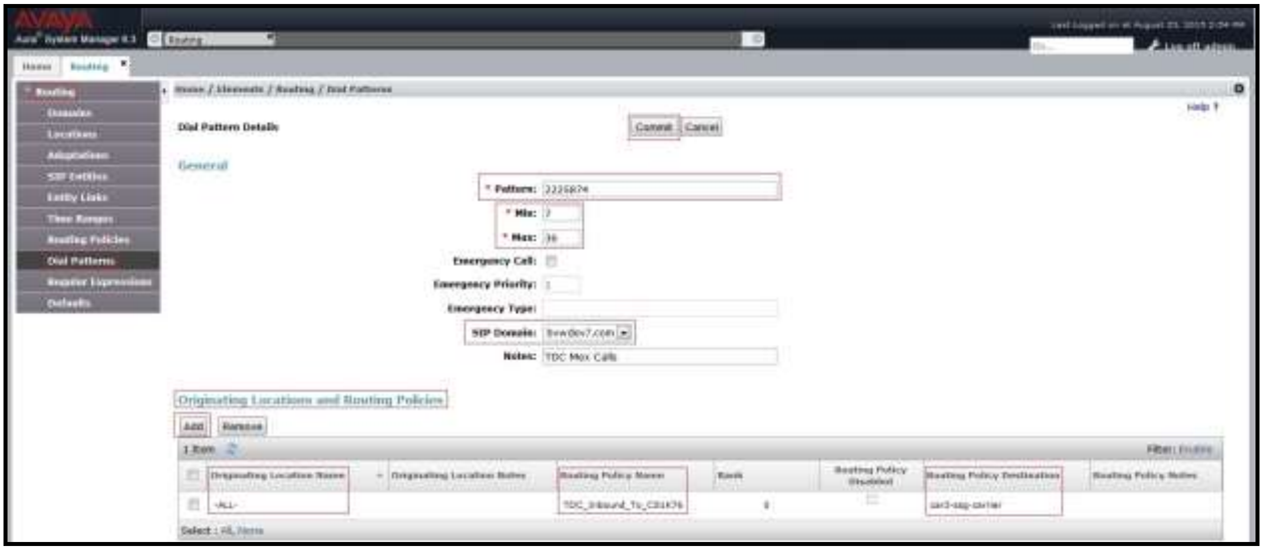
Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Inbound_To_CS1K76	0	□	sar3-sip-carrier	

Select : All, None

Figure 100 - Dial Pattern 2225872



Dial Pattern Details

General

* Pattern: 2225874

* Min: 7

* Max: 36

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

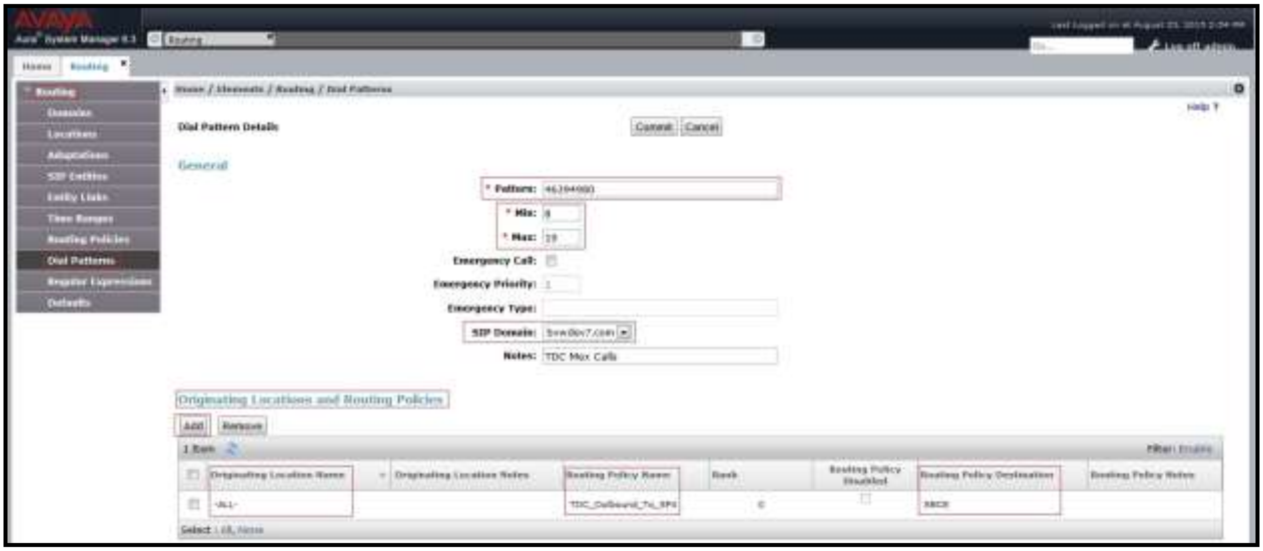
Notes: TDC Mex Calls

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Inbound_To_CS1K76	0	□	cs1k-sip-carrier	

Figure 101 - Dial Pattern 2225874



Dial Pattern Details

General

* Pattern: 46394980

* Min: 8

* Max: 19

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: TDC Mex Calls

Originating Locations and Routing Policies

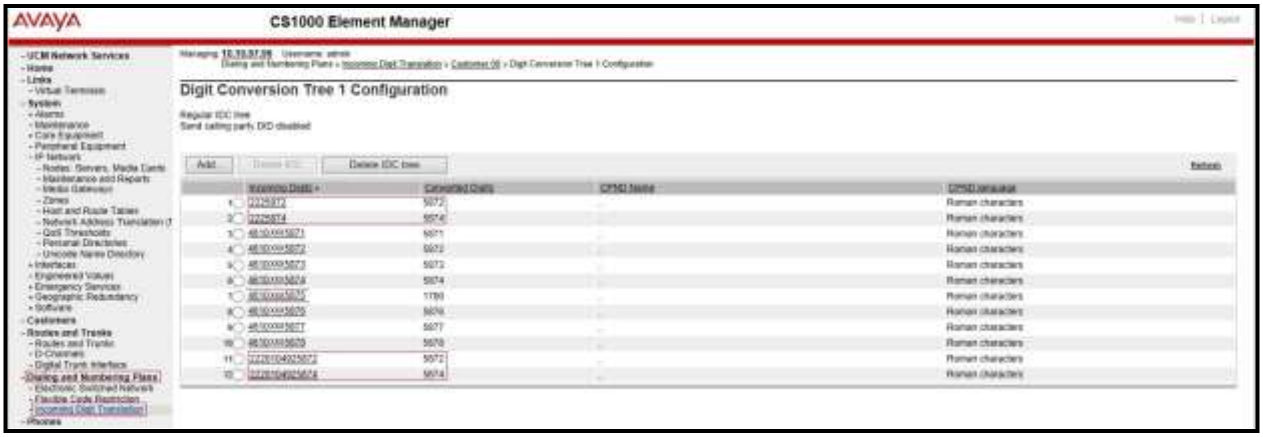
1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Outbound_To_SP6	0	□	SBCE	

Figure 102 - Dial Pattern 46394980

13.1.3. Configure CS1000 – Incoming Digit Conversion

In the following configuration, the incoming calls to **2225872** or **2220104925872** will be translated to the associated DN **5872**. The incoming calls to **2225874** or **2220104925874** will be translated to the associated DN **5874**.



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

	Incoming Digits ▲	Converted Digits	CPND Name	CPND language
1 ○	2225872	5872	...	Roman characters
2 ○	2225874	5874	...	Roman characters
3 ○	4610XXX5871	5871	...	Roman characters
4 ○	4610XXX5872	5872	...	Roman characters
5 ○	4610XXX5873	5873	...	Roman characters
6 ○	4610XXX5874	5874	...	Roman characters
7 ○	4610XXX5875	1780	...	Roman characters
8 ○	4610XXX5876	5876	...	Roman characters
9 ○	4610XXX5877	5877	...	Roman characters
10 ○	4610XXX5878	5878	...	Roman characters
11 ○	2220104925872	5872	...	Roman characters
12 ○	2220104925874	5874	...	Roman characters

Figure 103 - Incoming Digit Conversion for MEX testing

13.1.4. Configure CS1000 – Mobile Extension Users

The CS1000 Mobile Extensions feature enabled MEX mobile connected to a CS1000 system to appear as office extensions (MEX fixed number or MEX extension number). Incoming calls to an office telephone number automatically call out to the MEX mobile associated with the office telephone number.

```
LD 11
REQ: new
TYPE: uext
TN   96 0 0 19
UXTY
DATE
PAGE
DES  MOBX
TN   096 0 00 19  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY MOBX
UXID 46767225962
NUID
NHTN
MRT
ERL  0
ECL  0
FDN
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  CTD FBA WTA LPR MTD FNA HTD TDD HFD CRPD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDD
     CFTD SFD MRD DDV CNID 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 AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY
DNO3 MCBN
    FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD
    MSNV FRA  PKCH CCMD MWTD DVLD CROD ELCD VMSA
CPND_LANG ENG
RCO  0
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 5874 0
      CPND
        CPND_LANG ROMAN
          NAME TDC5874
          XPLN 13
          DISPLAY_FMT FIRST,LAST
    01 HOT P 20 64639498046767225962 ← (6 is an Access Code, 46394980: Prefix,
46767225962: MEX1 enabled mobile)
    02
    03
    04
    05
    06
    07
    08
    09
    10
    11
    12
    13
    14
    15
    16
```

```
   17 TRN
   18 AO6
   19 CFW 16
   20 RGA
   21 PRK
   22 RNP
   23
   24 PRS
   25 CHG
   26 CPN
   27
   28
   29
   30
   31
```

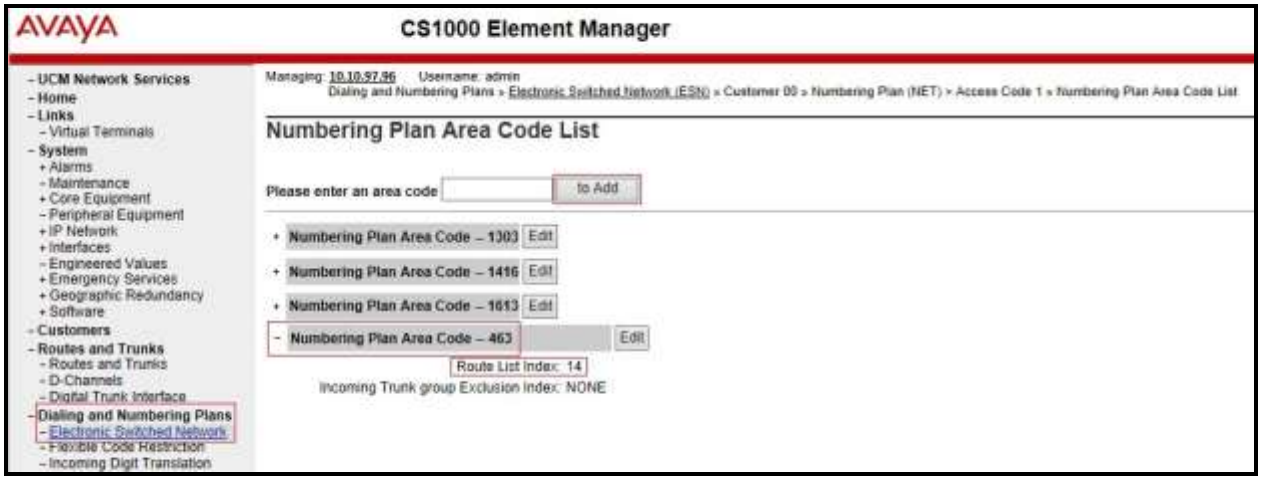
```
LD 11
REQ: new
TYPE: uext
TN   96 0 0 20
UXTY
DATE
PAGE
DES  MOBX
TN   096 0 00 20  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY MOBX
UXID 46767225921
NUID
NHTN
MRT
ERL  0
ECL  0
FDN
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
```

```
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR MTD FND HTD TDD HFD CRPD
    MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LND CNDD
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
    ICDD CDMD LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXD ARHD CLTD ASCD
    CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
    UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY
DNO3 MCBN
    FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD
    MSNV FRA  PKCH CCMD MWTD DVLD CROD ELCD VMSA
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 5872 0     MARP
      CPND
        CPND_LANG ROMAN
          NAME TDC5872
          XPLN 13
          DISPLAY_FMT FIRST,LAST
    01 HOT P 20 64639498046767225921 ← (6 is an Access Code, 46394980: Prefix,
46767225921: MEX2 enabled mobile)

    02
    03
    04
    05
    06
```

```
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```

13.1.5. Configure CS1000 – NPA 463

There is an example of **Numbering Plan Area Code 463** defined in this configuration for outgoing calls. This area code was associated to **Route List Index 14** created in **Section 5.6.4**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List

Numbering Plan Area Code List

Please enter an area code

+ Numbering Plan Area Code – 1303

+ Numbering Plan Area Code – 1416

+ Numbering Plan Area Code – 1613

- Numbering Plan Area Code – 463

Route List Index: 14

Incoming Trunk group Exclusion Index: NONE

Figure 104 – NPA 463

13.2. Outbound Call from MEX Enabled Mobile Number

This section explains MEX enabled mobile calls to PSTN numbers. After receiving the SIP Invite from TDC, the PBX should send a SIP re-Invite against the SIP trunk with the To header user part containing PSTN number in international format and the From header user part replaced by the MEX fixed number.

Example:

Assuming a call from MEX enabled mobile with number +46767225962 to PSTN 0016139675206 and R1 is using +222.

Firstly, TDC sent the SIP Invite to Avaya with To and From headers:

```
To: <sip:+2220016139675206@test11.btrunk.se>
From: <sip:+46767225962@test11.btrunk.se>
```

Then, Avaya PBX sent SIP re-Invite to TDC with the To and From headers:

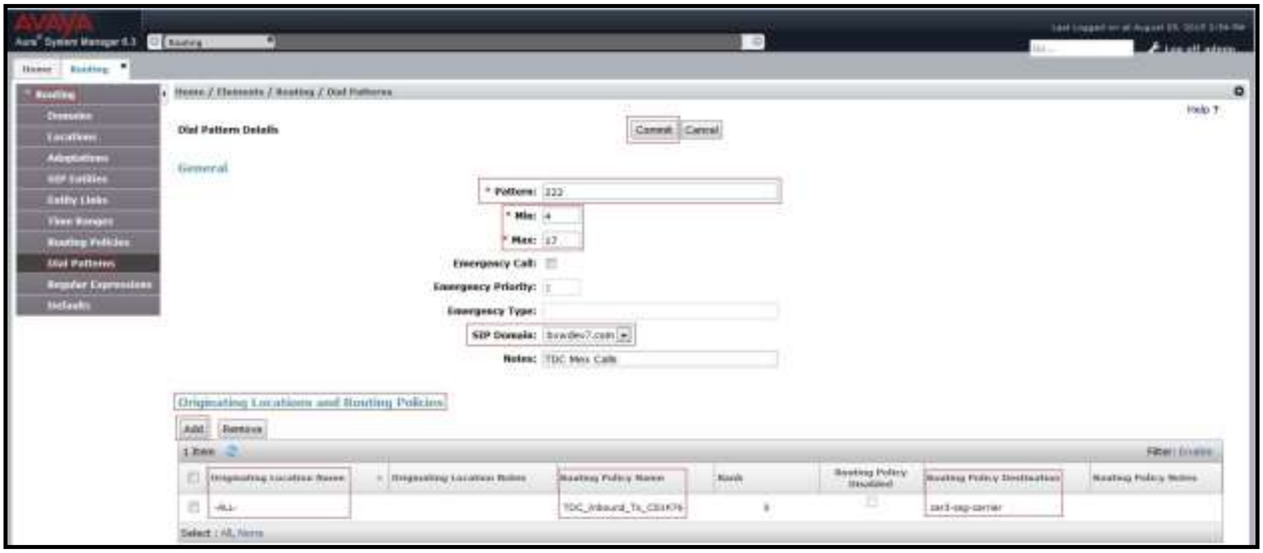
```
To: <sip:+0016139675206@test11.btrunk.se>
From: <sip:+46104925874@test11.btrunk.se>
```

13.2.1. Configure Signaling Manipulation on Avaya SBCE

Use the same SIP manipulation script defined in **Section 13.1.1**. The script was edited to replace MEX enabled mobile number on From and Contact headers with MEX fixed number for incoming calls.

13.2.2. Configure Session Manager – Dial Pattern

There are two examples of dial patterns defined in this configuration: Dial pattern for incoming calls: 222, and dial pattern for outgoing calls: 001. **Note**: The user has to define other dial patterns for outgoing calls to any PSTN numbers that users wish to call.



Dial Pattern Details

General

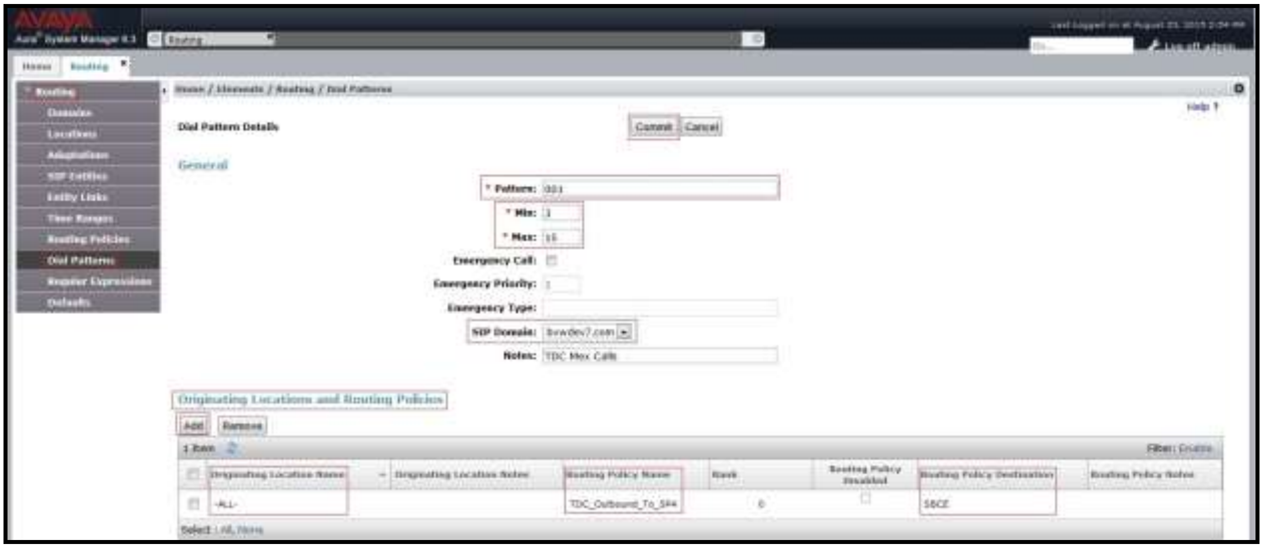
* Pattern:	222
* Min:	4
* Max:	17
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev7.com
Notes:	TDC Mex Calls

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Inbound_To_CS1K76	0	□	sar3-sip-carrier	

Figure 105 - Dial Pattern 222



Dial Pattern Details

General

* Pattern: 001

* Min: 1

* Max: 15

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: TDC Mex Calls

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Outbound_To_SP4	0	□	SBCE	

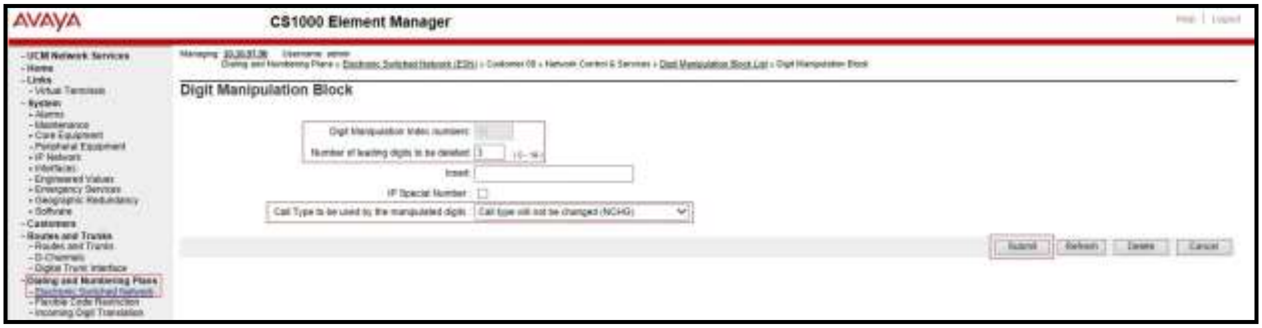
Figure 106 - Dial Pattern 001

13.2.3. Configure CS1000

13.2.3.1 Configure Digit Manipulation Block Index (DMI 15)

Follow steps in **Section 5.6.3** to add DMI. An index was added to the Digit Manipulation Block Index 15.

The DMI 15 was manipulated to delete 3 leading digits, therefore, enter **3** for **Number of leading digits to be deleted** and select **Call type will not be changed (NCHG)** for **Call Type to be used by the manipulated digits**. Click on the **Submit** button.



Digit Manipulation Block

Digit Manipulation Index numbers:

Number of leading digits to be deleted: 3 (0 - 19)

Insert:

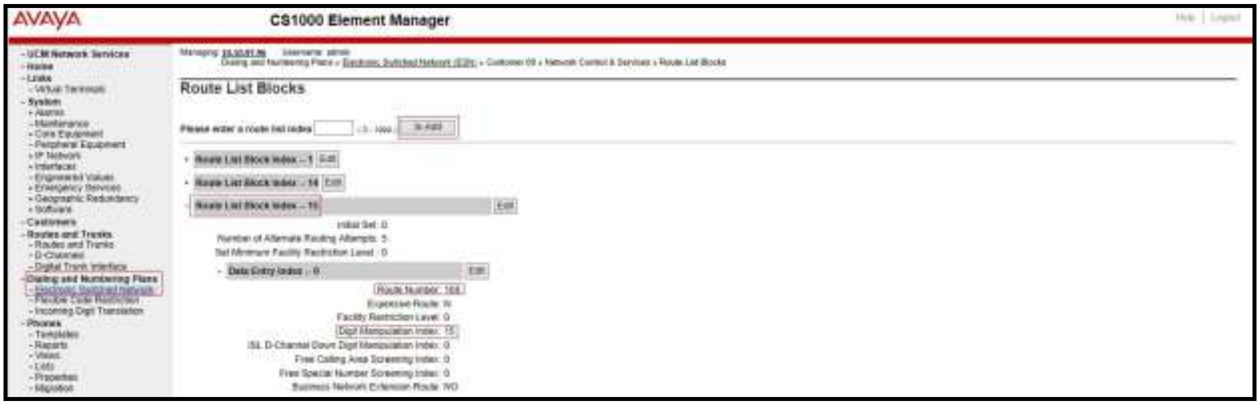
IP Special Number: □

Call Type to be used by the manipulated digits: Call type will not be changed (NCHG)

Figure 107 – DMI 15 Configuration

13.2.3.2 Configure Route List Block Index (RLI)

Follow steps in **Section 5.6.4** to add RLI. The following screen shows the existing **Route List Block Index 15** associated with the **Digit Manipulation Index 15** created in **Section 13.2.3.1** and **Route Number 100** created in **Section 5.5.5**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index (1 - 1000) to Add

- Route List Block Index – 1 Edit
- Route List Block Index – 14 Edit
- Route List Block Index – 15 Edit

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level: 0

- Data Entry Index – 0 Edit

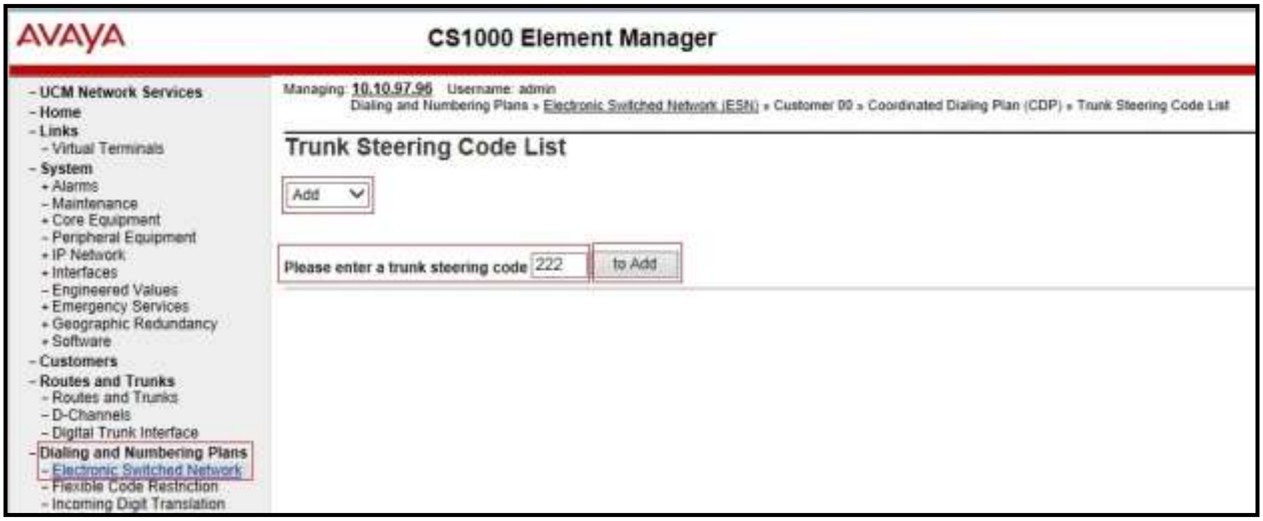
Route Number: 100
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 15
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Figure 108 – RLI 15 Configuration

13.2.3.3 Configure Trunk Steering Code (TSC 222)

There is a Trunk Steering Code 222 configured to be used for this testing.

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 **Trunk Steering Code (TSC)**. Select **Add** from the pull-down options and enter **222** at **Please enter a trunk steering code** and then click on the **to Add** button.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Coordinated Dialing Plan (CDP) » Trunk Steering Code List

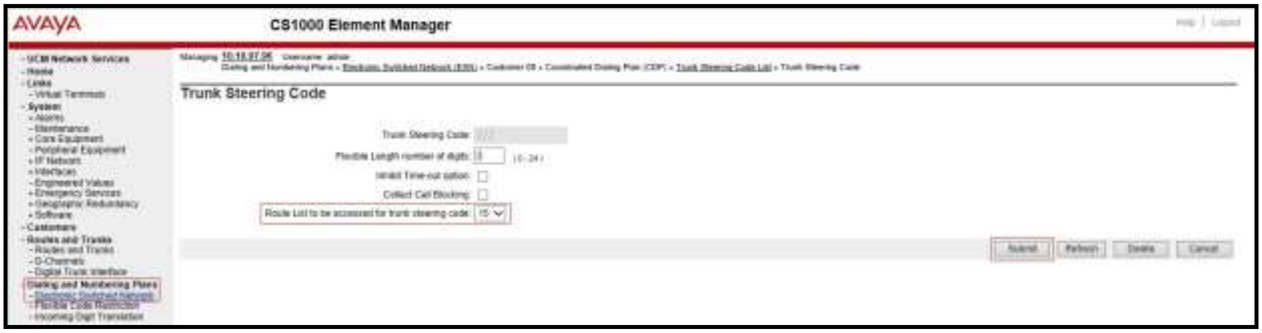
Trunk Steering Code List

Add

Please enter a trunk steering code 222 to Add

Figure 109: Add TSC 222

From the pull-down list of **Route List to be accessed for trunk steering code**, select **15** (**RLI 15** was created in **Section 13.2.3.2**). Click **Submit** to save the changes.



Trunk Steering Code

Trunk Steering Code: 222

Flexible Length number of digits: 0 (0 - 24)

Inhibit Time-out option: □

Collect Call Blocking: □

Route List to be accessed for trunk steering code: 15

Figure 110: TSC 222 associated to RLI 15

14. Appendix C: TDC Special Services Testing

For calls from PBX to Inquire, Emergency, Healthcare, or Police number services, the called service numbers require a prefix/suffix before being sent to the TDC platform. The prefix/suffix needs to be added by the PBX. The prefix is always **463** and is required for the number series starting on 112, 1177, 11414, and 118118. The suffix is always **479** and is required for the number series starting on 112, 1177, 11414.

<u>**Example**</u>:

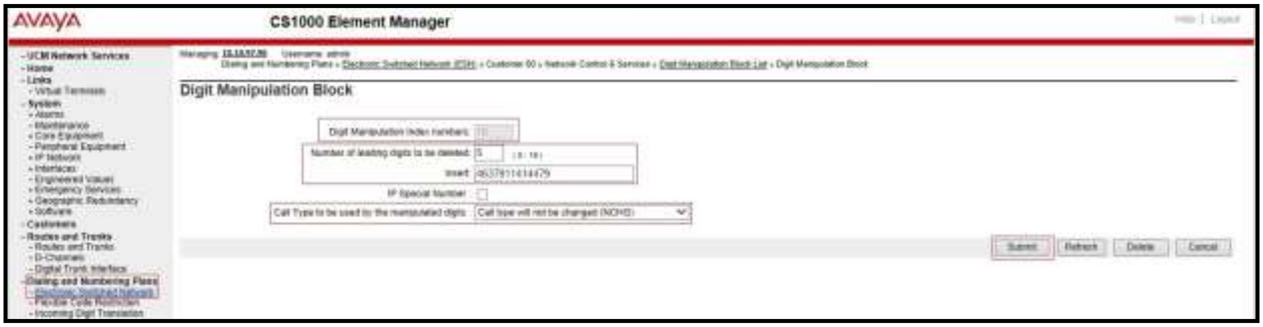
- Calling Police number 11414: The PBX sent + 4637911414479.
- Calling Healthcare number 1177: The PBX sent +463791177479.
- Calling Inquire number 118118: The PBX sent +46379118118.
- Calling Emergency number 112: The PBX sent +46379112479.

14.1. Configure CS1000

14.1.1. Configure Digit Manipulation Block Index (DMI 16)

Follow steps in **Section 5.6.3** to add DMI. An index was added to the Digit Manipulation Block Index 16.

The DMI 16 was manipulated to delete 5 leading digits. Enter **5** for **Number of leading digits to be deleted** and **Insert**: **4637911414479** (this is the special number for calling Police services - 11414). Select **Call type will not be changed (NCHG)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button.



Digit Manipulation Block

Digit Manipulation Index numbers: 16

Number of leading digits to be deleted: 5 (0 - 19)

Insert: 4637911414479

IP Special Number: ☐

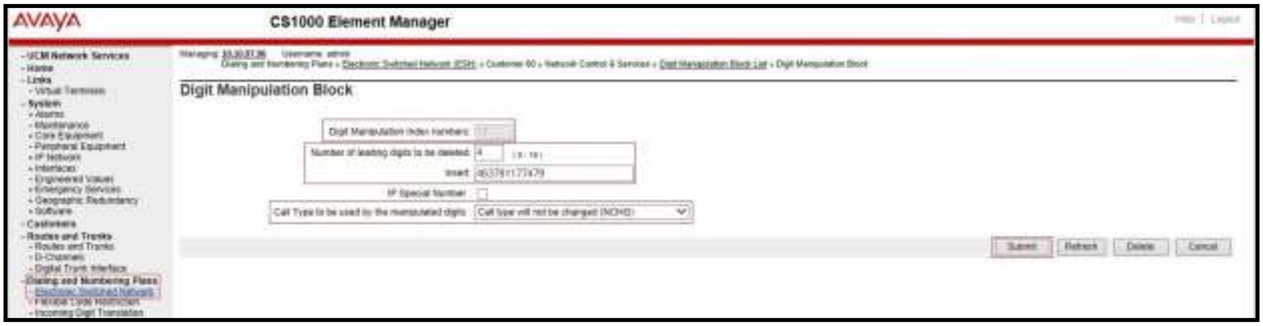
Call Type to be used by the manipulated digits: Call type will not be changed (NCHG)

Figure 111 – DMI 16 Configuration

14.1.2. Configure Digit Manipulation Block Index (DMI 17)

Follow steps in **Section 5.6.3** to add DMI. An index was added to the Digit Manipulation Block Index 17.

The DMI 17 was manipulated to delete 4 leading digits. Enter **4** for **Number of leading digits to be deleted** and **Insert**: **463791177479** (this is the special number for calling Healthcare services - 1177). Select **Call type will not be changed (NCHG)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button.



Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block

Digit Manipulation Block

Digit Manipulation Index numbers:

Number of leading digits to be deleted: 4 (0 - 19)

Insert: 463791177479

IP Special Number: □

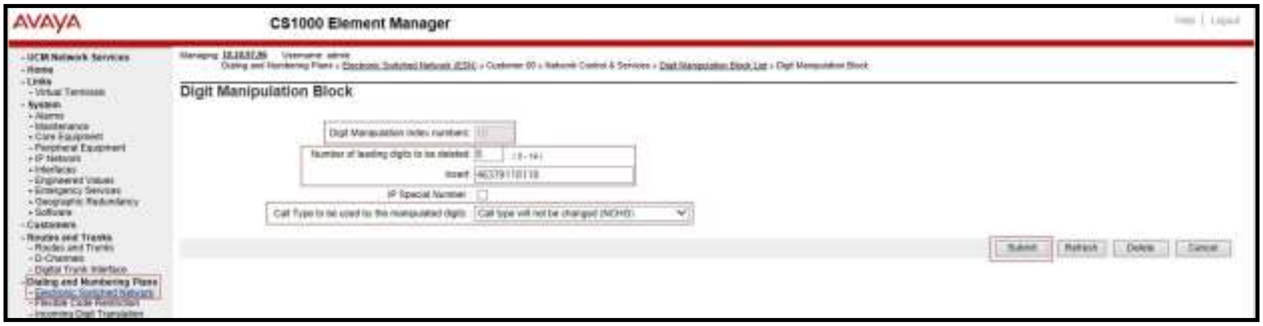
Call Type to be used by the manipulated digits: Call type will not be changed (NCHG)

Figure 112 – DMI 17 Configuration

14.1.3. Configure Digit Manipulation Block Index (DMI 18)

Follow steps in **Section 5.6.3** to add DMI. An index was added to the Digit Manipulation Block Index 18.

The DMI 18 was manipulated to delete 6 leading digits. Enter **6** for **Number of leading digits to be deleted** and **Insert**: **46379118118** (this is the special number for calling Inquire services - 118118). Select **Call type will not be changed (NCHG)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button.



Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block

Digit Manipulation Block

Digit Manipulation Index numbers:

Number of leading digits to be deleted: 6 (0 - 19)

Insert: 46379118118

IP Special Number: □

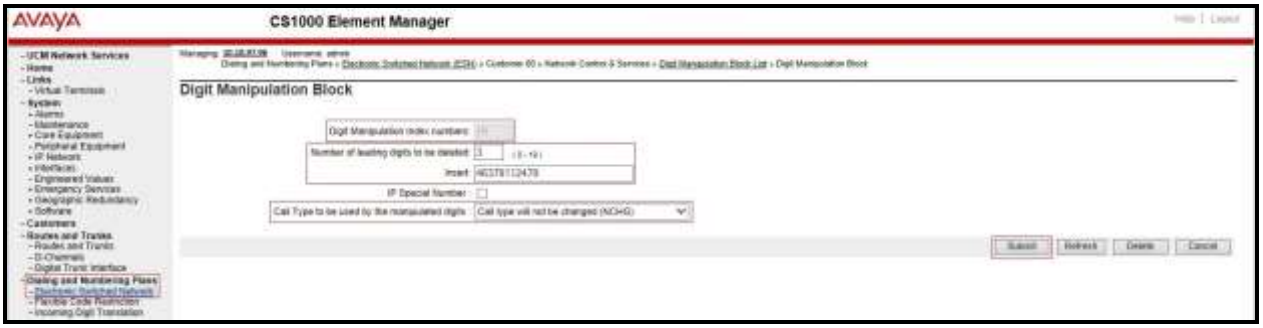
Call Type to be used by the manipulated digits: Call type will not be changed (NCHG)

Figure 113 – DMI 18 Configuration

14.1.4. Configure Digit Manipulation Block Index (DMI 19)

Follow steps in **Section 5.6.3** to add DMI. An index was added to the Digit Manipulation Block Index 19.

The DMI 19 was manipulated to delete 3 leading digits. Enter **3** for **Number of leading digits to be deleted** and **Insert**: **46379112479** (this is the special number for calling Emergency services - 112). Select **Call type will not be changed (NCHG)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button.



Digit Manipulation Block

Digit Manipulation index numbers: 19

Number of leading digits to be deleted: 3 (0 - 19)

Insert: 46379112479

IP Special Number: □

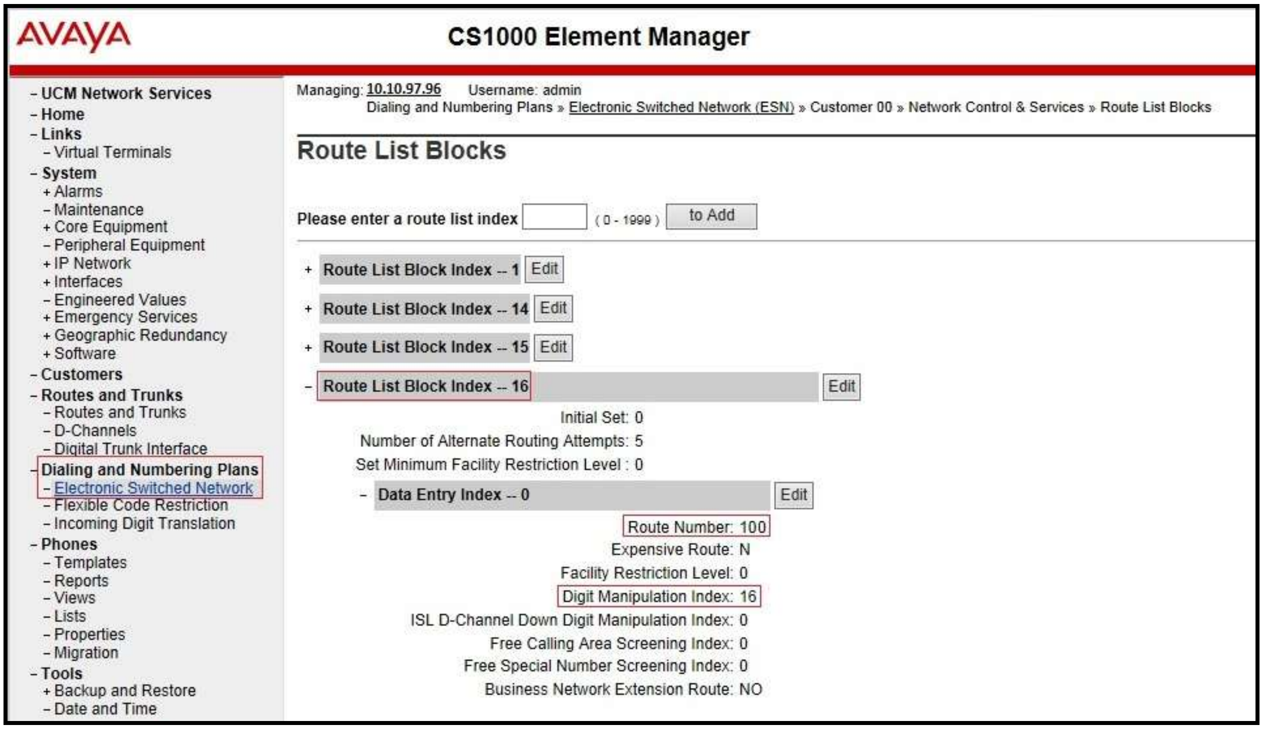
Call Type to be used by the manipulated digits: Call type will not be changed (NCHG)

Figure 114 – DMI 19 Configuration

14.1.5. Configure Route List Block Index

Follow steps in **Section 5.6.4** to add RLI.

The following screen shows the configured **Route List Block Index 16** associated to the **Digit Manipulation Index 16** created in **Section 14.1.1** and **Route Number 100** created in **Section 5.5.5**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Route List Blocks

Route List Blocks

Please enter a route list index (0 - 1999) to Add

+ Route List Block Index -- 1 Edit

+ Route List Block Index -- 14 Edit

+ Route List Block Index -- 15 Edit

- Route List Block Index -- 16 Edit

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 0

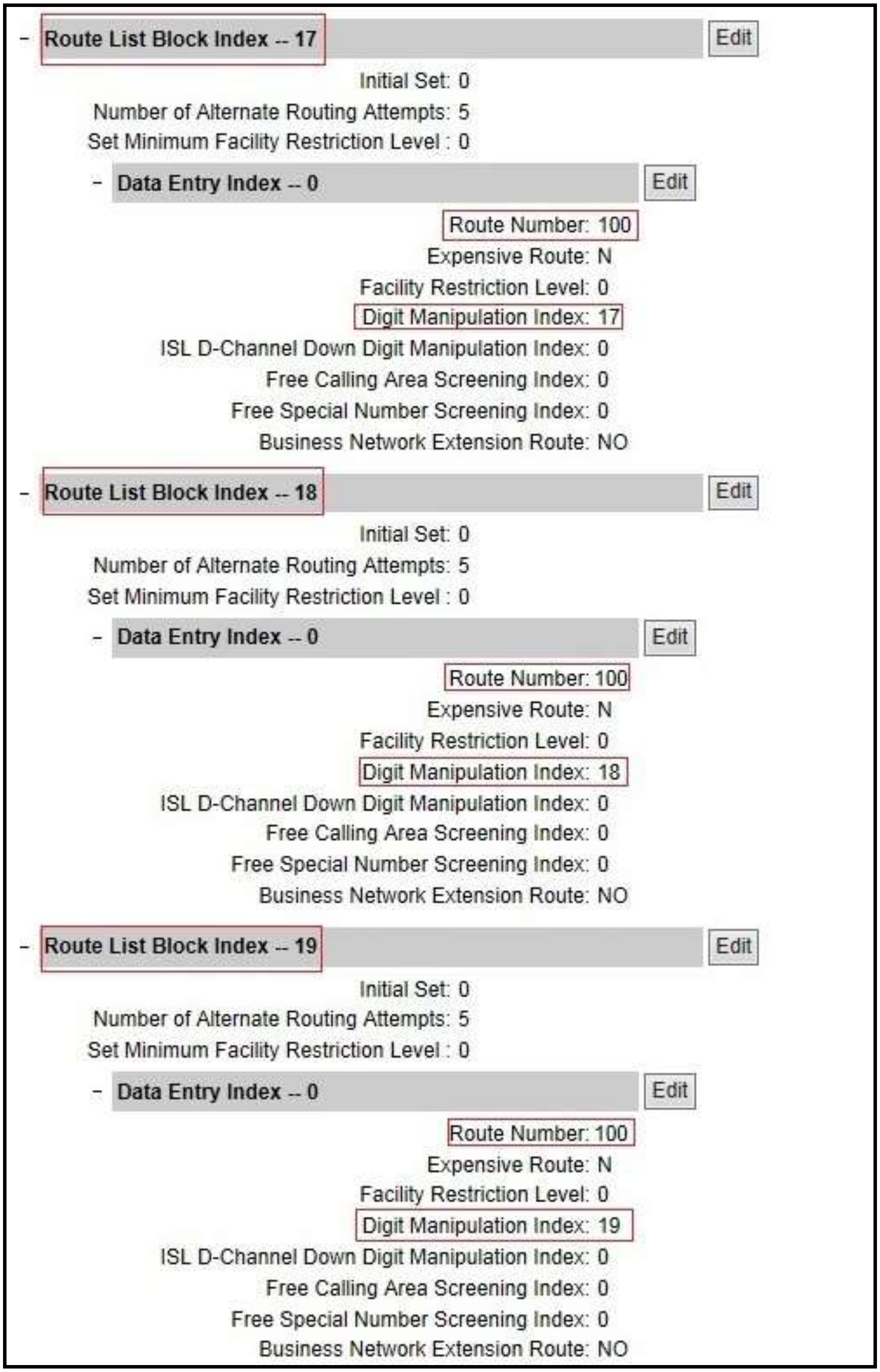
- Data Entry Index -- 0 Edit

Route Number: 100
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 16
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Figure 115 – RLI 16 Configuration

The following screen shows the other configured Route List Block Indexes:

- **Route List Block Index 17** associated to the **Digit Manipulation Index 17** created in **Section 14.1.2** and **Route Number 100** created in **Section 5.5.5**.
- **Route List Block Index 18** associated to the **Digit Manipulation Index 18** created in **Section 14.1.3** and **Route Number 100** created in **Section 5.5.5**.
- **Route List Block Index 19** associated to the **Digit Manipulation Index 19** created in **Section 14.1.4** and **Route Number 100** created in **Section 5.5.5**.



Route List Block Index -- 17

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 0

Data Entry Index -- 0

Route Number: 100
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 17
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Route List Block Index -- 18

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 0

Data Entry Index -- 0

Route Number: 100
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 18
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Route List Block Index -- 19

Initial Set: 0
Number of Alternate Routing Attempts: 5
Set Minimum Facility Restriction Level : 0

Data Entry Index -- 0

Route Number: 100
Expensive Route: N
Facility Restriction Level: 0
Digit Manipulation Index: 19
ISL D-Channel Down Digit Manipulation Index: 0
Free Calling Area Screening Index: 0
Free Special Number Screening Index: 0
Business Network Extension Route: NO

Figure 116 – RLI 17_18_19 Configuration

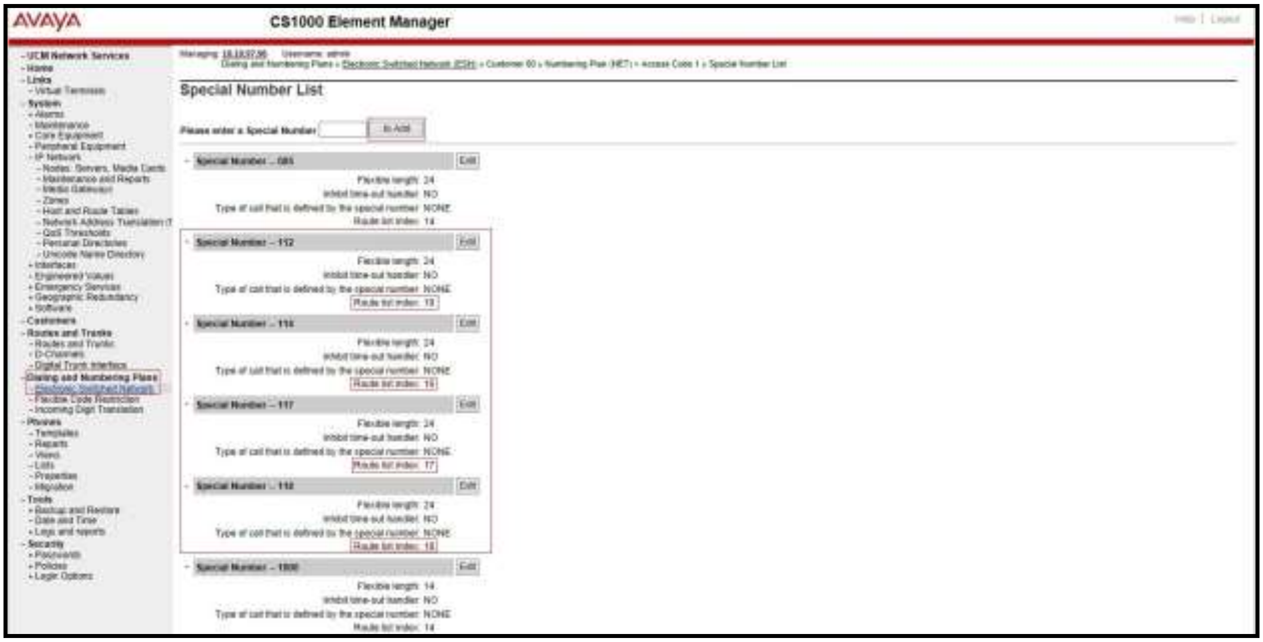
14.1.6. Configure Special Number (SPN)

Some special numbers have been configured to be used for this testing, such as: 112, 114,117, and 118.

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.

The following screen shows the configured special numbers used for this testing.

- **Special Number 112** associated with the **Route list index 19** created in **Section 14.1.5**.
- **Special Number 114** associated with the **Route list index 16** created in **Section 14.1.5**.
- **Special Number 117** associated with the **Route list index 17** created in **Section 14.1.5**.
- **Special Number 118** associated with the **Route list index 18** created in **Section 14.1.5**.



Managing: 10.10.97.96 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Special Number List

Special Number List

Please enter a Special Number: [ ] to Add

Special Number – 085 Edit
Flexible length: 24
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

Special Number – 112 Edit
Flexible length: 24
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 19

Special Number – 114 Edit
Flexible length: 24
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 16

Special Number – 117 Edit
Flexible length: 24
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 17

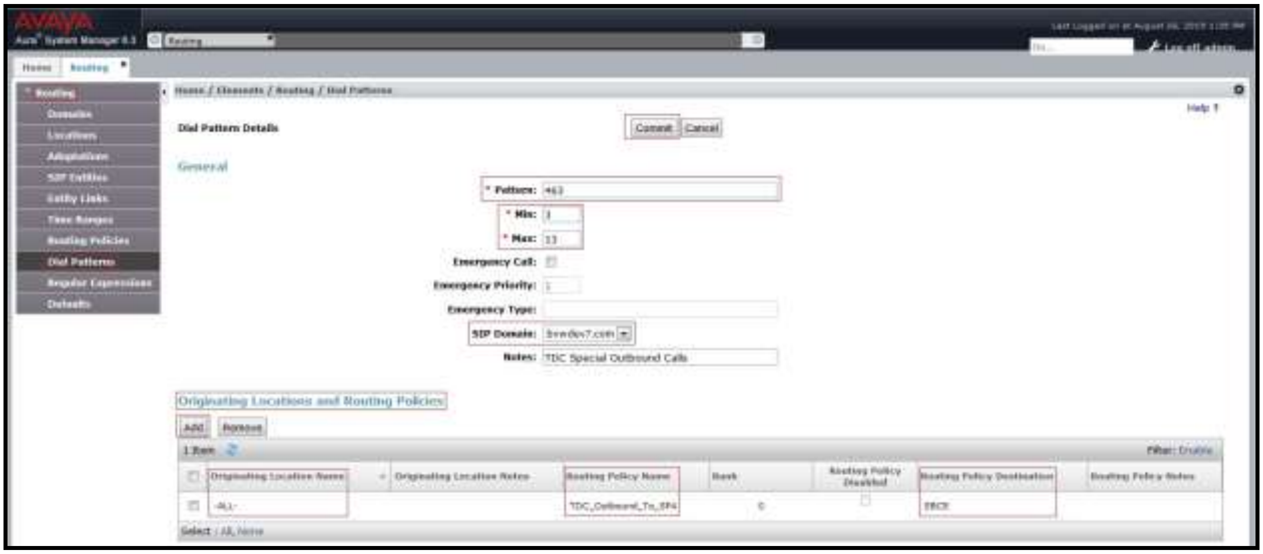
Special Number – 118 Edit
Flexible length: 24
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 18

Special Number – 1800 Edit
Flexible length: 14
Inhibit time-out handler: NO
Type of call that is defined by the special number: NONE
Route list index: 14

Figure 117 – TDC SPN

14.2. Configure Session Manager – Dial Pattern

The example of dial pattern **463** is defined in this configuration for outgoing calls.



Dial Pattern Details

General

* Pattern:	463
* Min:	3
* Max:	13
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	bvwdev7.com
Notes:	TDC Special Outbound Calls

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-		TDC_Outbound_To_SP4	0	□	SBCE	

Figure 118 - Dial Pattern 463

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.